قوانین امنیتی در کشور نیوزیلند

قوانین امنیتی در کشور نیوزیلند

فهرست

فصل اول

فصل دوم

فصل سوم

فصل چهارم

فصل پنجم

فصل ششم

مقدمه

- **مختصری درباره کشور نیوزیلند**

کشوری جزیره‌ای است که در جنوب غربی اقیانوس آرام واقع است حدود ۲۰۰۰ کیلومترمربع وسعت و حدود پنج میلیون نفر جمعیت دارد. در سال ۱۸۴۱ این کشور مستمره انگلستان بوده و در سال ۱۹۰۷ استقلال نسبی خود را بدست آورده و از سال ۱۹۴۷ ملکه انگلیس بعنوان پادشاه این کشور پذیرفته شد و امور داخلی آن زیر نظر فرماندار کل و نخست وزیر انجام می‌گیرد پایتخت آن شهر ولینگتون می‌باشد اکثریت مردم این کشور از نژاد اروپایی می‌باشد و بزرگترین اقلیت آنها بومیان ماثوری می‌باشد (۱۶٪). واحد پول آن دلار نیوزیلند و زبان رسمی آن انگلیسی و دین غالب آنها مسحیت می‌باشد نزدیکترین همسایه آنها کشور استرالیا است.

- **قانون اطلاعات و امنیت نیوزیلند**

در مارس سال ۲۰۱۶ سرمایکل کالن و دام پتی‌ردی اولین بررسی مستقل اطلاعات و امنیت در نیوزیلند را به پارلمان ارائه نمودند این قانون جایگزین کلیه قانون‌های قبلی در این زمینه شد این قانون باهدف اطمینان ازاینکه بصورت گسترده سازمان‌های اطلاعاتی و امنیتی را قادر می‌سازد برای محافظت از منابع کشور نیوزیلند، با محدودیت‌های مناسب در زمینه مقررات توانمندسازی و نظارت قوی و پیشرو در جهان، در همه کشور اعمال شود و زیر امنیت ملی (نخست وزیر) بر این سیستم نظارت دارد **الویت‌های این قانون** در زمینه‌های ذیل می‌باشد

۱) امنیت زیستی و سلامت انسان‌ها
۲) محیط زیست، تغییرات آب و هوایی و منابع طبیعی
۳) نفوذ، دخالت و جاسوسی خارجی
۴) اقتصاد جهانی، تجارت و سرمایه‌گذاری
۵) پیامدهای فناوری نوظهور
۶) حاکمیت بین‌المللی، ژئوپلتیک و امنیت جهانی
۷) فعالیت‌های سایبری مخرب
۸) امنیت منطقه‌ای خاورمیانه
۹) علاقه استراتژیک نیوزیلند به منطقه اقیانوس آسیا
۱۰) ثبات و امنیت و انعطاف‌پذیری در منطقه آرام
۱۱) گسترش سلاح‌های کشتارجمعی و سلاح‌های معمولی
۱۲) امنیت فضا
۱۳) امنیت و حاکمیت سرزمینی
۱۴) تروریسم (خشونت‌های عقیدتی، سیاسی و مذهبی در داخل و خارج)
۱۵) تهدیدهای نیوزیلندیهایی خارج از کشور
۱۶) جرائم سازمان‌یافته فراملی (قاچاق، مهاجرت، جرائم مالی و کلاهبرداری)

فصل ۱
درباره PSI

۱- درباره PSI

۱-۱- بخشنامه امنیت تجارت دولت

در یک منظر تهدید متنوع و پیچیده، مهم است که ادارات دولتی برای کاهش آسیب پذیری های خود سیستم‌هایی در نظر بگیرند .این تهدیدها ممکن است شامل خشونت علیه کارکنان، خسارت کیفری به اموال وزارتخانه، کلاهبرداری قابل توجه، سرقت اطلاعات و مسائل مربوط به امنیت سایبری باشد.

بخشهای مختلف با تهدیدهای مختلف روبرو خواهند شد - بسته به نقش، مقیاس و شرایط آنها .به همین دلیل، الزامات امنیتی محافظتی انعطاف پذیر و مبتنی بر ریسک هستند.

الزامات امنیتی حفاظتی برای کمک به ادارات دولتی در ارزیابی ریسک‌هایی که ممکن است با مردم، اطلاعات و دارایی‌های سازمان آنها روبرو شود، طراحی شده است .این بخش‌ها را قادر می‌سازد تا رویکرد امنیتی را منعکس کنند که ریسک محیط فردی آنها و نیازهای تجاری آنها را نشان می‌دهد .این الزامات با بروز تهدیدهای جدید و همگام شدن با تغییر فناوری تکامل می‌یابند.

در ۸ دسامبر ۲۰۱۴، کابینه به جای امنیت در بخش دولت و کتابچه راهنمای امنیت محافظ، الزامات امنیتی محافظتی را با استفاده از کتابچه راهنمای امنیت اطلاعات نیوزلند تصویب کرد.

کابینه همه ادارات خدمات عمومی و نیروی دفاعی نیوزیلند، پلیس نیوزیلند، سرویس اطلاعات امنیتی نیوزلند و دفتر مشاوره پارلمانی را برای اجرای الزامات امنیتی محافظتی راهنمایی کرده است .این بخشها موظفند اطلاعات اطمینان را در صورت درخواست سازمانهای امنیتی پیشرو (اداره امنیت ارتباطات دولت، سرویس اطلاعاتی و امنیتی نیوزیلند و وزارت نخست وزیر و کابینه) ارائه دهند.

مدیران ارشد مسئول اجرای این الزامات امنیتی محافظتی هستند .یک تیم جدید در انجمن اطلاعاتی نیوزلند از ادارات پشتیبانی می‌کند تا الزامات را از طریق ارتباط، منابع و آموزش پیاده سازی کنند.

الزامات امنیتی محافظتی بهترین روش امنیتی است .بخش دولتی گسترده‌تر و بخش خصوصی با تهدیدات یکسانی روبرو هستند و از آنها برای اجرای الزامات امنیتی محافظتی در حمایت از منافع اجتماعی، اقتصادی و امنیتی نیوزیلند تشویق می‌شوند .

الزامات امنیتی حفاظتی از نزدیک با مدیریت حریم خصوصی در الزامات دولت به رهبری مدیر ارشد حفظ حریم خصوصی دولت هماهنگ خواهد شد

۱-۲- الزامات اجباری

20شرط اجباری که آژانس‌های دولتی موظف به رعایت آنها هستند و سایر سازمان‌ها باید بهترین روش را در نظر بگیرند.

الزامات اجباری حاکمیت

- **حکومتداری صحیح را برقرار و حفظ کنید**

یک ساختار حاکمیتی ایجاد و حفظ کنید که رهبری موفقیت آمیز و نظارت بر خطر امنیت محافظ را تضمین کند .اعضای تیم بزرگسالان را به عنوان:

افسر ارشد امنیت(CSO)، مسئول سیاست امنیتی کلی محافظتی سازمان و نظارت بر اقدامات امنیتی محافظتی.

افسر ارشد امنیت اطلاعات(CISO)، مسئول امنیت اطلاعات سازمان شما.

- **رویکرد مبتنی بر ریسک را در پیش بگیرید**

مطابق با استاندارد نیوزلند ISO 31000: 2018 مدیریت ریسک - رهنمودها، رویکرد مدیریت ریسک را که هر منطقه از امنیت محافظتی را در سراسر سازمان شما پوشش دهد، اتخاذ کنید .سیاست‌ها و برنامه‌های امنیتی متناسب با نیازهای تجاری خاص سازمان خود را تدوین و حفظ کنید .اطمینان حاصل کنید که الزامات امنیتی را در همه زمینه‌ها: حاکمیت، اطلاعات، پرسنل و فیزیکی برطرف می‌کنید.

- **برای تداوم تجارت آماده شوید**

یک برنامه مدیریت تداوم کسب و کار داشته باشید، تا عملکردهای حیاتی سازمان شما در حین ایجاد اختلال تا حد ممکن ادامه یابد .اطمینان حاصل کنید که برای تداوم منابعی که از عملکردهای مهم شما پشتیبانی می‌کنند، برنامه ریزی کرده‌اید.

- **ایجاد آگاهی از امنیت**

اطلاعات منظم، آموزش آگاهی از امنیت و پشتیبانی از همه افراد سازمان خود را ارائه دهید، بنابراین آن‌ها می‌توانند الزامات حفاظتی امنیتی را رعایت کرده و سیاست‌های امنیتی سازمان شما را حفظ کنند.

- **هنگام کار با دیگران خطرات را مدیریت کنید**

قبل از شروع کار با دیگران که ممکن است بخشی از زنجیره تأمین شما شوند، خطرات موجود در افراد، اطلاعات و دارایی‌های خود را شناسایی و مدیریت کنید.

- **مدیریت حوادث امنیتی**

اطمینان حاصل کنید که هر حادثه امنیتی در اسرع وقت شناسایی، گزارش، پاسخ داده شده، مورد تحقیق و بازیابی قرار گرفته است .از انجام اقدامات اصلاحی مناسب اطمینان حاصل کنید.

- **بتوانید به افزایش سطح تهدید پاسخ دهید**

برنامه‌هایی را تدوین کنید و آماده باشید تا در موارد اضطراری یا شرایطی که تهدید بیشتری برای مردم، اطلاعات یا دارایی‌های شما وجود دارد، سطح امنیتی را افزایش دهید.

- **توانایی خود را ارزیابی کنید**

از یک فرآیند ارزیابی مبتنی بر شواهد سالانه برای اطمینان از مناسب بودن توانایی امنیتی سازمان خود استفاده کنید .در صورت درخواست، گزارش اطمینان را از طریق تیم محافظت از امنیت مورد نیاز به دولت ارائه دهید .سیاست‌ها و برنامه‌های خود را هر ۲ سال یا در صورت لزوم تغییر در تهدید یا محیط کار، زودتر مرور کنید.

۱-۱-۱- الزامات اجباری امنیت پرسنل

سازمان‌های دولتی باید از چهار الزام امنیتی اجباری پرسنل پیروی کنند .مشاغل باید اتخاذ این الزامات را به عنوان بخشی از اقدامات خوب در نظر بگیرند.

- **فرد مناسب را استخدام کنید**

اطمینان حاصل کنید که همه افرادی که برای سازمان شما کار می‌کنند (کارمندان، پیمانکاران و کارکنان موقت) که به اطلاعات و دارایی‌های دولت نیوزیلند دسترسی دارند: • هویت آنها مشخص شده است • حق کار در نیوزیلند دارند • برای دسترسی مناسب هستند • موافقت با با سیاست‌ها، استانداردها، پروتکل‌ها و الزامات دولت که از مردم، اطلاعات و دارایی‌ها در برابر آسیب محافظت می‌کند، پیروی کنید.

❖ **اطمینان از مناسب بودن مداوم آنها**

از مناسب بودن مداوم همه افرادی که برای سازمان شما کار می‌کنند اطمینان حاصل کنید .این مسئولیت شامل رسیدگی به هرگونه نگرانی است که ممکن است در شایستگی شخص برای ادامه دسترسی به اطلاعات و دارایی‌های دولت تأثیر بگذارد.

❖ **عزیمت آنها را مدیریت کنید**

عزیمت افراد را مدیریت کنید تا هرگونه خطر برای افراد، اطلاعات و دارایی‌های ناشی از افرادی که از سازمان شما خارج می‌شوند، محدود شود .این مسئولیت شامل اطمینان از بازگشت هرگونه حق دسترسی، مجوزهای امنیتی و دارایی‌ها و درک افراد از تعهدات مداوم خود است.

❖ **مجوزهای امنیتی ملی را مدیریت کنید**

اطمینان حاصل کنید که افراد قبل از اینکه به اطلاعات، دارایی‌ها یا مکان‌های کاربری محرمانه، محرمانه و دسترسی داشته باشند، سطح مجاز ترخیص امنیت ملی را دارند .شایستگی مداوم کلیه دارندگان مجوزهای امنیت ملی برای داشتن مجوز را مدیریت کرده و هرگونه تغییر در مورد ترخیص آنها را به NZSIS اطلاع دهید.

۱-۱-۲- الزامات اجباری امنیت اطلاعات

❖ **آنچه را که برای محافظت از آن نیاز دارید درک کنید**

اطلاعات و سیستم‌های ICT را که سازمان شما مدیریت می‌کند شناسایی کنید .خطرات امنیتی (تهدیدها و آسیب پذیری ها) و تأثیر تجاری هرگونه نقض امنیت را ارزیابی کنید.

❖ **امنیت اطلاعات خود را طراحی کنید**

در اوایل مراحل برنامه ریزی، انتخاب و طراحی، امنیت اطلاعات را در نظر بگیرید .تدابیر امنیتی را طراحی کنید که خطرات سازمان شما را تهدید می‌کند و با اشتهای شما سازگار است .اقدامات امنیتی شما باید مطابق با موارد زیر باشد: • سیستم طبقه بندی امنیتی دولت نیوزیلند • کتابچه راهنمای امنیت اطلاعات نیوزلند • هرگونه تعهدات حریم خصوصی، قانونی و نظارتی که تحت آن فعالیت می‌کنید .یک چارچوب مناسب مدیریت امنیت اطلاعات متناسب با خطرات خود اتخاذ کنید.

❖ **اقدامات امنیتی خود را تأیید کنید**

تأیید کنید که اقدامات امنیتی اطلاعات شما به درستی اجرا شده و برای اهداف مناسب است .فرآیند صدور گواهینامه و اعتبار سنجی را به اتمام برسانید تا از سیستم‌های ICT خود برای تأیید بهره مند شوید.

❖ **امنیت خود را به روز نگه دارید**

اطمینان حاصل کنید که امنیت اطلاعات شما برای هدف مناسب باقی می‌ماند: - نظارت بر رویدادهای امنیتی و پاسخگویی به آنها - به روز نگه داشتن تهدیدات و آسیب پذیری های در حال تکامل - حفظ دسترسی مناسب به اطلاعات شما.

۱-۱-۳- الزامات اجباری امنیت فیزیکی

❖ **آنچه را که برای محافظت از آن نیاز دارید درک کنید**

افراد، اطلاعات و دارایی‌هایی را که سازمان شما باید از آنها محافظت کند و مکان آنها را شناسایی کنید .خطرات امنیتی (تهدیدها و آسیب پذیری ها) و تأثیر تجارت در ضرر و زیان مردم، اطلاعات یا دارایی‌ها را ارزیابی کنید .از درک خود استفاده کنید.:

❖ **امنیت فیزیکی خود را طراحی کنید**

در اوایل مراحل برنامه ریزی، انتخاب، طراحی و اصلاح امکانات امنیتی فیزیکی را در نظر بگیرید .تدابیر امنیتی را طراحی کنید که خطرات سازمان شما را تهدید می‌کند و با اشتهای شما سازگار است .اقدامات امنیتی شما باید مطابق با تعهدات مربوط به بهداشت و ایمنی باشد.

❖ **اقدامات امنیتی خود را تأیید کنید**

تأیید کنید که اقدامات امنیتی جسمی شما به درستی اجرا شده و برای اهداف مناسب است .برای اطمینان از تأیید فعالیت مناطق امنیتی، مراحل صدور گواهینامه و اعتبار سنجی را به اتمام برسانید.

❖ **امنیت خود را به روز نگه دارید**

اطمینان حاصل کنید که از تهدیدات و آسیب پذیری های در حال به روز بودن مطلع هستید و به طور مناسب پاسخ می‌دهید . اطمینان حاصل کنید که اقدامات امنیتی جسمی شما به طور مؤثر حفظ می‌شود تا برای اهداف مناسب باقی بماند.

۳-۱- مروری بر الزامات امنیتی محافظتی

PSRیک چارچوب خط مشی است که مشخص می‌کند سازمان شما برای مدیریت مؤثر امنیت باید چه کاری انجام دهد .این همچنین شامل بهترین راهنمایی برای تمرین است که باید دنبال کنید PSR .برای هر دو سازمان بخش خصوصی و خصوصی مناسب است.

امنیت مؤثر، سازمان‌های نیوزیلند را قادر می‌سازد تا در یک محیط اعتماد و اطمینان با هم کار کنند .محافظت از افراد، اطلاعات و دارایی‌های شما به سازمان شما کمک می‌کند تا اهداف استراتژیک و عملیاتی خود را برآورده کند.

این نمای کلی برای چه کسانی است

این نمای کلی برای:

- روسای سازمان
- کارکنان مدیریت امنیت
- پیمانکاری که مشاوره و خدمات حفاظتی امنیتی را ارائه می‌دهند
- هر کسی که درگیر امنیت کارمندان، اطلاعات و دارایی‌های فیزیکی دولت نیوزیلند باشد.

❖ **آنچه این مروری در بر می‌گیرد**

این مرور کلی سیاست‌های اصلی PSR و الزامات اجباری را پوشش می‌دهد .این اطلاعات در مورد:

- تعریف ساختارهای حاکمیتی و مدیریتی برای امنیت
- شناسایی خطرات و نیازهای امنیتی برای پرسنل، اطلاعات و امنیت فیزیکی

- مطابقت با الزامات اجباری.PSR

۱-۱-۴- سیاست‌های اصلیPSR

سیاست‌های اصلی PSR چهار زمینه اصلی را شامل می‌شود: حاکمیت امنیت، امنیت پرسنل، امنیت اطلاعات و امنیت فیزیکی.

همه سازمان‌ها باید از الزامات مربوط به سیاست‌های اصلی ذکر شده در زیر پیروی کنند.

❖ **حاکمیت امنیتی**

۱) حکومتداری صحیح را برقرار و حفظ کنید
۲) رویکرد مبتنی بر ریسک را در پیش بگیرید
۳) برای تداوم تجارت آماده شوید
۴) ایجاد آگاهی از امنیت
۵) هنگام کار با دیگران خطرات را مدیریت کنید
۶) مدیریت حوادث امنیتی
۷) بتوانید به افزایش سطح تهدید پاسخ دهید
۸) توانایی خود را ارزیابی کنید

❖ **امنیت کارکنان**

۱) فرد مناسب را استخدام کنید
۲) از تناسب مداوم آنها اطمینان حاصل کنید
۳) عزیمت آنها را مدیریت کنید
۴) مجوزهای امنیتی ملی را مدیریت کنید

❖ **امنیت اطلاعات**

۱) آنچه را که برای محافظت از آن نیاز دارید درک کنید
۲) امنیت اطلاعات خود را طراحی کنید
۳) اقدامات امنیتی خود را تأیید کنید
۴) امنیت خود را به روز نگه دارید

❖ **امنیت فیزیکی**

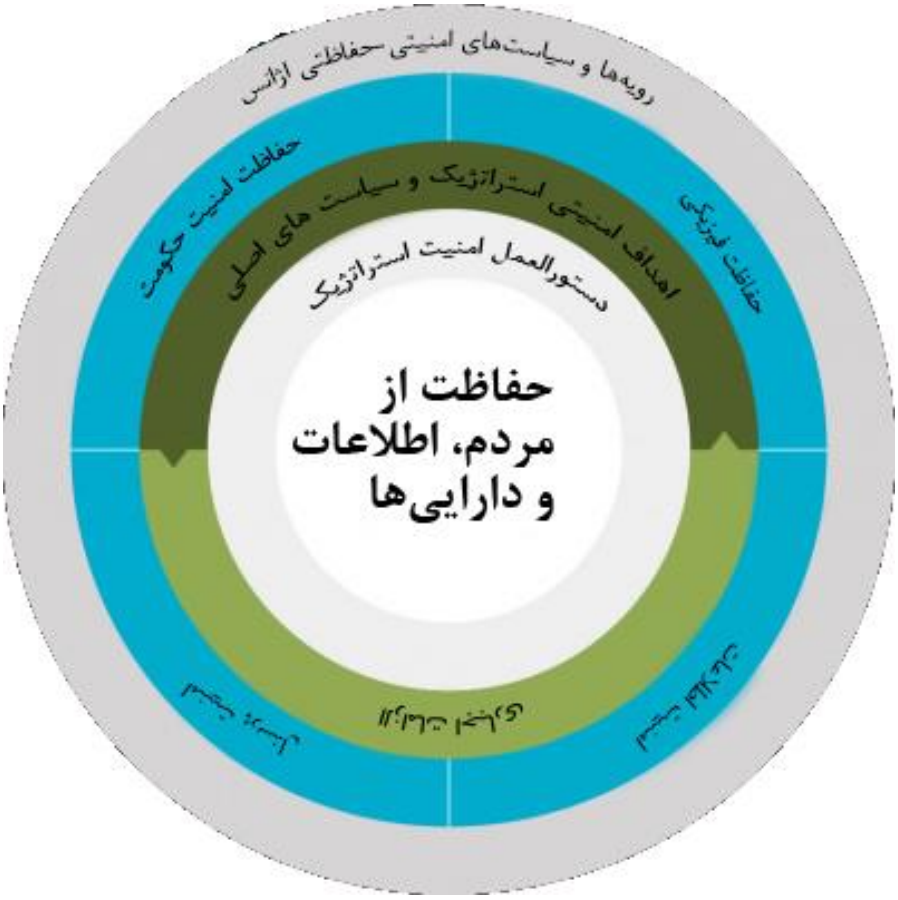
۱) آنچه را که برای محافظت از آن نیاز دارید درک کنید
۲) امنیت فیزیکی خود را طراحی کنید
۳) اقدامات امنیتی خود را تأیید کنید
۴) امنیت خود را به روز نگه دارید

۱-۱-۵- چارچوبی برایPSR

چارچوب سیاست‌های نیوزیلند برای امنیت محافظتی دارای چهار طبقه و یک ساختار سلسله مراتبی است.

این چهار طبقه از سازمانهای دولتی و بخش خصوصی برای اجرای اقدامات امنیتی محافظ حمایت می‌کنند.

❖ **چارچوب امنیت محافظتی**



ردیف ۱ – بخشنامه استراتژیک امنیتی

بخشنامه استراتژیک امنیتی بیانیه کلی سیاست امنیتی دولت نیوزیلند است .این سنگ بنای اصلی PSR است.

این بخشنامه نیاز دولت به امنیت محافظتی را بیان می‌کند :این سازمان را قادر می‌سازد تا در یک محیط اعتماد و اطمینان با هم کار کنند.

ردیف ۲ – سیاست‌های اصلی و الزامات اجباری

ردیف ۲ شامل سیاست‌های اصلی امنیتی و الزامات اجباری است که سازمان‌های دولتی باید برای اطمینان از یک محیط امنیتی سازگار و کنترل شده در بخش عمومی اجرا کنند.

پس از اجرا، این ردیف سازمان‌های دولتی را قادر می‌سازد تا اعتماد بیشتری به شیوه‌های اشتراک اطلاعات و ترتیبات کار مشترک داشته باشند.

الزامات اجباری شامل حاکمیت امنیتی، امنیت پرسنل، امنیت اطلاعات و امنیت فیزیکی است.

ردیف ۳ – پروتکل‌ها و راهنمایی‌های بهترین روش

پروتکل‌ها و راهنمایی‌های دقیق مدیریتی را برای حمایت از سازمان شما برای اجرای الزامات اجباری و ایجاد اقدامات امنیتی بهترین روش ارائه می‌دهد.

اسناد اصلی بهترین روش‌ها عبارتند از:

- پروتکل‌های مدیریتی برای انجام فعالیت‌های امنیتی محافظتی برای تأمین الزامات اجباری
- راهنمایی برای بهبود اقدامات امنیتی شما
- منابع و استانداردهای مربوط به امنیت محافظتی و مدیریت ریسک اضافی.

این اسناد شیوه‌های امنیتی محافظتی را در سراسر دولت استاندارد می‌کند تا:

- اشتراک اطلاعات را فعال کنید
- پشتیبانی از تجارت بین سازمانی
- به انجام تعهدات بین المللی کمک کنید.

دولت نیوزیلند به توسعه و پالایش سیاست امنیتی محافظتی که موثرترین و کارآمدترین روشها را برای تأمین ایمن تجارت دولت ارائه می‌دهد، ادامه خواهد داد.

سیاست‌ها و پروتکل‌ها و الزامات مربوطه چهار حوزه را در بر می‌گیرد: حاکمیت امنیت؛ و پرسنل، اطلاعات و امنیت فیزیکی.

❖ حاکمیت امنیتی

حاکمیت امنیتی خوب مربوط به انطباق و عملکرد است.

"مطابقت" به این معنی است که سازمان شما شرایط اجباری PSR را برآورده می‌کند.

"انجام" به این معنی است که سازمان شما از اقدامات امنیتی استفاده می‌کند تا:

- از طریق تحویل ایمن کالا، خدمات یا برنامه‌ها به عملکرد کلی خود کمک کنید
- از محرمانه بودن، صداقت و در دسترس بودن افراد، اطلاعات و دارایی خود اطمینان حاصل کنید.

❖ اعمال اصول حاکمیت

PSR مبتنی بر اصول حاکمیت بخش عمومی است، از جمله:

- پاسخگویی -پاسخگو بودن در برابر تصمیمات و داشتن مکانیزم های معنی دار برای اطمینان از اینکه سازمان شما از کلیه الزامات امنیتی محافظتی پیروی می‌کند
- شفافیت و گشودگی -داشتن نقش‌ها و مسئولیت‌های روشن برای عملکردهای امنیتی محافظتی، و روشهای روشن برای تصمیم گیری و اعمال اختیار
- کارایی -اطمینان از بهترین استفاده از منابع محدود برای پیشبرد اهداف سازمان، با تعهد به استراتژی‌های مبتنی بر ریسک برای بهبود
- رهبری -دستیابی به یک تعهد در کل سازمان برای عملکرد امنیتی خوب از طریق رهبری از بالا به پایین.

❖ امنیت کارکنان

افرادی که سازمان شما استخدام می‌کند باید برای دسترسی به اطلاعات و دارایی‌های رسمی مناسب باشند .آن‌ها باید از استانداردهای صداقت، صداقت و تحمل برخوردار باشند.

در صورت لزوم، افراد شما باید از سطح امنیتی مناسب برخوردار شوند.

سازمان شما مسئول مدیریت افراد شما در طول چرخه حیات اشتغال برای جلوگیری از نقض امنیت تصادفی یا عمدی است.

❖ **امنیت اطلاعات**

الزامات اجباری برای امنیت اطلاعات بر اساس عناصر زیر است:

- رازداری - اطمینان از در دسترس بودن اطلاعات فقط برای افرادی که مجاز به دسترسی هستند
- یکپارچگی - حفاظت از دقت و کامل بودن اطلاعات و روشهای پردازش
- در دسترس بودن - اطمینان از دسترسی کاربران مجاز به اطلاعات و دارایی‌های مرتبط در صورت لزوم.

سازمان شما همچنین باید از پادمان هایی استفاده کند که:

- اطلاعات در صورت لزوم از نظر محافظتی مشخص و برچسب گذاری می‌شوند
- اطلاعات در سیستم‌های ICT به درستی مدیریت و از طریق تمام مراحل چرخه عمر یک سیستم محافظت می‌شود.

❖ **امنیت فیزیکی**

سازمان شما باید:

- یک محیط کار ایمن برای افراد، پیمانکاران، مشتریان و مردم شما
- یک محیط فیزیکی امن

ردیف ۴ – سیاست‌ها، برنامه‌ها و رویه‌های سازمان شما

سازمان شما باید سیاست‌ها، برنامه‌ها و رویه‌های امنیتی متناسب با نیازهای تجاری شما را تدوین کند.

سیاست‌ها و رویه‌های شما باید:

- سایر اقدامات عملیاتی در سازمان شما را تکمیل و پشتیبانی کنید
- خطراتی را که سازمان شما ایجاد می‌کند و سایر سازمانها را تحت تأثیر قرار می‌دهد شامل کنید
- ریسک‌های منتقل شده از شرکای تجاری را در نظر بگیرید
- در استانداردی برابر یا بالاتر از PSR باشد (نه پایین‌تر).

۱-۱-۶- مطابقت باPSR

PSR زمانی را توضیح می‌دهد که سازمان شما برای انطباق با الزامات اجباری نیاز به تدابیر امنیتی خاص دارد.

❖ **شناسایی اقدامات اجباری**

اقدام امنیتی با رعایت الزامات "باید" یا "نباید" الزامی است .شما باید الزامات اجباری را پیاده یا دنبال کنید مگر اینکه بتوانید نشان دهید که اندازه گیری در متن شما مربوط نیست.

❖ شناسایی اقدامات خوب

اقدام امنیتی با الزام "باید "یا" نباید "عملی خوب و توصیه شده در نظر گرفته می‌شود. دلایل معتبری برای عدم اجرای اقدام امنیتی می‌تواند وجود داشته باشد، از جمله:

- اندازه گیری مربوط نیست زیرا خطر وجود ندارد
- شما یک فرایند یا اندازه گیری قدرت برابر را جایگزین می‌کنید.

❖ با توجه به اینکه کدام اقدامات برای اجرا

استفاده نکردن از تدابیر امنیتی بدون توجه کافی ممکن است خطر باقیمانده را برای سازمان شما افزایش دهد .این خطر باقیمانده باید توسط رئیس سازمان شما موافقت و تأیید شود . سؤالات زیر را قبل از تصمیم به عدم اجرای اندازه گیری مطرح کنید.

۱) آیا سازمان شما حاضر است ریسک اضافی را بپذیرد؟ اگر چنین است، انتخاب شما چه توجیهی دارد؟
۲) آیا تأثیری در امنیت همه دولت در نظر گرفته‌اید؟ اگر چنین است، انتخاب شما چه توجیهی دارد؟

سوابق رسمی قابل کنترل از اینکه چگونه تدابیری را اتخاذ کردید و تصمیم گرفتید به عنوان بخشی از فرایندهای حاکمیت و اطمینان در سازمان شما لازم است.

❖ مطابقت با قانون مربوط به امنیت

الزامات اجباری و اقدامات امنیتی بر اساس قوانینی است که مربوط به امنیت محافظتی است و اهداف دولت را منعکس می‌کند.

هنگامی که قانون شما را ملزم می‌کند امنیت محافظتی را به روشی متفاوت از PSR مدیریت کند، این قانون اولویت دارد.

چند نمونه از قوانینی که ممکن است در مورد برخی از سازمانها اعمال شود عبارتند از:

- قانون جنایات ۱۹۶۱
- قانون افشای جنایی ۲۰۰۸
- قانون گمرک و مالیات غیر مستقیم ۲۰۱۸
- قانون دفاع ۱۹۹۰
- قانون روابط استخدامی ۲۰۰۰
- قانون ایمنی و بهداشت در محل کار ۲۰۱۵
- قانون مالیات بر درآمد ۲۰۰۷
- قانون اطلاعات رسمی ۱۹۸۲
- حریم خصوصی قانون ۲۰۲۰
- قانون دارایی عمومی ۱۹۸۹
- قانون سوابق عمومی ۲۰۰۵
- قانون بخش دولتی ۱۹۸۸
- قانون خلافی خلاصه ۱۹۸۱

۱-۱-۷- حاکمیت امنیتی

PSR شامل هشت مورد حاکمیت است که با هم کار می‌کنند تا نظارت و مدیریت مؤثر بر همه زمینه‌های امنیتی را تضمین کنند.

❖ **ایجاد ساختار حکمرانی خود**

برای اجرای الزامات امنیتی محافظتی، سازمان شما باید به روشنی:

- ساختار حاکمیت امنیتی خود را شناسایی کنید
- مشخص کنید چه کسی مسئول حاکمیت امنیتی است.

❖ **حکومتداری صحیح را برقرار و حفظ کنید**

یک ساختار حاکمیتی ایجاد و حفظ کنید که رهبری موفقیت آمیز و نظارت بر خطر امنیت محافظ را تضمین کند. اعضای تیم بزرگسالان را به عنوان:

- افسر ارشد امنیت(CSO) ، مسئول سیاست امنیتی کلی محافظتی سازمان و نظارت بر اقدامات امنیتی محافظتی.
- افسر ارشد امنیت اطلاعات(CISO) ، مسئول امنیت اطلاعات سازمان شما.

یک ساختار حاکمیتی ایجاد کنید که به شما امکان می‌دهد به طور مؤثر خطرات امنیتی را شناسایی و مدیریت کنید.

رئیس سازمان شما مسئول بررسی و تأیید ساختارهای پیشنهادی مدیریت ریسک امنیتی، سازوکارهای اطمینان و تخصیص منابع است.

❖ **اطلاعات بیشتر :**

- چه چیزی میخواهید بدانید
- چرخه عمر محافظت از امنیت محافظ

❖ **مدیریت خطرات، و ایجاد سیاست‌ها و برنامه‌ها**

رویکرد درست مدیریت ریسک از سازمانی به سازمان دیگر متفاوت است، اما روند کار شما باید شفاف و قابل توجیه باشد .اجتناب از خطر مدیریت ریسک نیست.

❖ **رویکرد مبتنی بر ریسک را در پیش بگیرید**

مطابق با استاندارد نیوزلند ISO 31000: 2018 مدیریت ریسک - رهنمودها، رویکرد مدیریت ریسک را که هر منطقه از امنیت محافظتی را در سراسر سازمان شما پوشش دهد، اتخاذ کنید .سیاست‌ها و برنامه‌های امنیتی متناسب با نیازهای تجاری خاص سازمان خود را تدوین و حفظ کنید .اطمینان حاصل کنید که الزامات امنیتی را در همه زمینه‌ها: حاکمیت، اطلاعات، پرسنل و فیزیکی برطرف می‌کنید.

روند سازمان شما برای مدیریت خطرات امنیتی باید به این ترتیب باشد:

- خطرات خاص افراد، اطلاعات و دارایی‌های خود را شناسایی کنید

- احتمال و تأثیر خطرات رخ داده را ارزیابی کنید
- خطرات در برابر آسیب پذیری ها و کفایت پادمان های موجود را ارزیابی کنید
- سطح تحمل ریسک خود را مشخص کنید
- تعیین کنید که کدام اقدامات محافظتی احتمال کاهش یا از بین بردن خطرات را دارند
- مسئولیت خطرات باقی مانده را شناسایی و قبول کند
- اقدامات امنیتی را برای کاهش خطرات تا سطوح قابل قبول اجرا کنید.

❖ **برای افزایش آگاهی در مورد مدیریت ریسک ارتباط برقرار کنید**

پیام‌های متداول برای مدیریت خوب خطرات امنیتی عبارتند از:

- همه افرادی که برای سازمان شما کار می‌کنند مسئولیت مدیریت خطرات امنیتی را بر عهده دارند (از جمله پیمانکاران)
- مدیریت ریسک، از جمله مدیریت ریسک امنیتی، بخشی از تجارت روزمره است
- روند مدیریت خطرات امنیتی منطقی، سیستماتیک و بخشی از فرایندهای مدیریت استاندارد سازمان شما است
- تغییرات در محیط تهدید سازمان شما باید به طور مداوم کنترل و تنظیم شود در صورت لزوم برای حفظ سطح قابل قبول ریسک و تعادل مناسب بین نیازهای عملیاتی و امنیت.

❖ **تدوین سیاست‌ها و برنامه‌های مؤثر**

سیاست‌ها و برنامه‌های شما برای امنیت محافظتی باید:

- جزئیات اهداف، دامنه و رویکرد مدیریت مسائل امنیتی و خطرات را بیان کنید
- توسط رئیس سازمان شما تأیید شود
- نقش‌ها و مسئولیت‌های امنیتی را شناسایی کنید
- وقتی تغییراتی در تجارت یا تغییر در خطرات امنیتی شما ایجاد می‌شود، مورد بازبینی قرار گیرد
- با یافته‌های ارزیابی خطر امنیتی خود سازگار باشید
- عواقب نقض سیاست‌ها یا دور زدن تدابیر امنیتی را توضیح دهید
- به طور منظم ارتباط برقرار شود

❖ **اطلاعات بیشتر:**

- اجرای رویکرد مبتنی بر ریسک برای امنیت محافظتی
- ISO 31000: 2018مدیریت ریسک - دستورالعمل ها
- HB 167: 2006مدیریت ریسک امنیتی
- HB 327: 2010ارتباط و مشاوره در مورد ریسک

❖ **آماده شدن برای تداوم تجارت**

برای اطمینان از سلامتی، ایمنی، امنیت و رفاه اقتصادی نیوزیلندی‌ها و عملکرد مؤثر دولت، خدمات حیاتی و دارایی‌های مرتبط باید در دسترس باشند.

❖ **برای تداوم تجارت آماده شوید**

یک برنامه مدیریت تداوم کسب و کار داشته باشید، تا عملکردهای حیاتی سازمان شما در حین ایجاد اختلال تا حد ممکن ادامه یابد .اطمینان حاصل کنید که برای تداوم منابعی که از عملکردهای مهم شما پشتیبانی می‌کنند، برنامه ریزی کرده‌اید.

برنامه مدیریت تداوم کسب و کار (BCM) باید بخشی از رویکرد کلی سازمان شما برای مدیریت مؤثر ریسک باشد.

برنامه ریزی BCM فرایندهایی را که باید در صورت اخلال در تجارت دنبال کنید، مشخص می‌کند .یک خطر اساسی برای سازمانها این است که نتوانند در صورت بروز بحران یا اختلال دیگری عملیاتی بمانند.

❖ **یک برنامه قوی تنظیم کنید**

برای اطمینان از مؤثر بودن برنامه BCM فعالیت‌های زیر را انجام دهید.

- در ترتیبات حاکمیت خود، تعیین کنید که چه کسی بر برنامه BCM خود نظارت کرده و مسئولیت آن را بر عهده می‌گیرد و برنامه‌های تداوم تجارت را تأیید و تأیید می‌کند.
- به عنوان بخشی از فرآیند شناسایی دارایی خود، تجزیه و تحلیل تأثیر را برای شناسایی و اولویت بندی خدمات، دارایی‌ها و اطلاعات مهم سازمان خود انجام دهید .هرگونه تبادل اطلاعات با سایر سازمانها و اشخاص خارجی را در بر بگیرید.
- برای اطمینان از ادامه خدمات و دارایی‌های حیاتی خود، برنامه‌ها، اقدامات امنیتی و ترتیبات را تدوین کنید .در صورت تأیید تهدید یا ارزیابی ریسک، هر سرویس یا دارایی دیگری را در آن بگنجانید.
- سطح آمادگی کلی سازمان خود را برای یک رویداد مخرب کنترل کنید.
- اطمینان حاصل کنید که برنامه‌های تداوم کسب و کار خود را به طور مداوم بررسی، آزمایش و حسابرسی می‌کنید.

❖ **اطلاعات بیشتر:**

- ISO 22301: 2019امنیت اجتماعی - سیستم های مدیریت تداوم کسب و کار - الزامات
- موسسه استمرار کسب و کار - رهنمودهای عملکرد خوب (نسخه ۲۰۱۸

❖ **ایجاد آگاهی از امنیت**

برای ارائه موفقیت آمیزPSR ، هرکسی که برای سازمان شما کار می‌کند باید سیاست‌های امنیتی و فرآیندهای شما را بشناسد و آنها را دنبال کند.

❖ **ایجاد آگاهی از امنیت**

اطلاعات منظم، آموزش آگاهی از امنیت و پشتیبانی از همه افراد سازمان خود را ارائه دهید، بنابراین آن‌ها می‌توانند الزامات حفاظتی امنیتی را رعایت کرده و سیاست‌های امنیتی سازمان شما را حفظ کنند.

❖ **در مورد الزامات امنیتی خود به همه بیاموزید**

برای بهبود آگاهی و انطباق با اقدامات امنیتی شما، سازمان شما باید:

- اطمینان حاصل کنید که افرادی که وظایف امنیتی خاص دارند آموزشهای مناسب و به روز را دریافت می‌کنند
- سیاست‌های امنیتی خود را به همه افرادی که برای شما کار می‌کنند، از جمله پیمانکاران، اعلام کنید
- اطمینان حاصل کنید که سیاست‌های امنیتی شما به راحتی قابل درک و دسترسی هستند

- یک برنامه مداوم آگاهی از امنیت را برای یادآوری مرتب مسئولیت‌های امنیتی، مسائل و نگرانی‌ها به مردم اجرا کنید
- مختصر دارندگان تصویب امنیت ملی در مورد شرایط مربوط به سطح ترخیص آنها هنگام گرفتن یا تمدید مجوز، و در صورت نیاز در چرخه تمدید مجوز.

❖ **قانون حمایت از اطلاعات رسمی را رعایت کنید**

راهنمایی در مورد بخشهای مربوط به قانون مربوط به افشای غیر مجاز اطلاعات رسمی، از جمله:

- قانون اطلاعات رسمی ۱۹۸۲ - بخشهای ۶، ۹، ۲۷ و ۳۱
- حریم خصوصی قانون ۲۰۲۰ - اصول حریم خصوصی اطلاعات، بخش ۶
- قانون جرایم ۱۹۶۱ - بندهای ۷۸، A۷۸، 78B، 78Cو ۷۹
- قانون خلافی خلاصه ۱۹۸۱ - بند A.۲۰

اثر ترکیبی قانون جرائم ۱۹۶۱ و قانون جرائم مختصر ۱۹۸۱ این است که افشای غیر مجاز اطلاعاتی که توسط دولت نیوزلند نگهداری می‌شود مشمول مجازات قوانین کیفری است .مردم شما باید از اینکه آیا چنین قوانینی بر نقش آنها اعمال می‌شود آگاه باشند.

❖ **اطلاعات بیشتر**

- ایجاد آگاهی از امنیت محافظ

❖ **مدیریت خطرات هنگام کار با دیگران**

PSRهمانطور که در مورد عملکردهای داخلی شما اعمال می‌شود به همان اندازه که در مورد ارائه دهندگان خدمات و خدمات برون سپاری شده اعمال می‌شود.

❖ **هنگام کار با دیگران خطرات را مدیریت کنید**

قبل از شروع کار با دیگران که ممکن است بخشی از زنجیره تأمین شما شوند، خطرات موجود در افراد، اطلاعات و دارایی‌های خود را شناسایی و مدیریت کنید.

هنگامی که خدمات یا توابع خود را به خارج از کشور واگذار می‌کنید، سازمان شما باید:

- رویه‌های امنیتی پرسنل را در سازمان‌های بخش خصوصی و افرادی که به دارایی‌های دولت نیوزلند دسترسی دارند اعمال کنند
- اطمینان حاصل کنید که دارایی‌های دولت، از جمله سیستم‌هایICT ، از طریق تعیین الزامات امنیتی در شرایط و ضوابط و بازدید از ارائه دهندگان برای ارزیابی انطباق محافظت می‌شود.

❖ **اطلاعات بیشتر**

- امنیت زنجیره تامین

❖ **مدیریت حوادث امنیتی**

هدف از تحقیقات امنیتی مشخص کردن علت و میزان حادثه‌ای است که سازمان شما یا دولت نیوزیلند را به خطر انداخته یا می‌تواند باعث شود.

روند بررسی و گزارش حوادث امنیتی همچنین به شما کمک می‌کند تا آسیب پذیری های خود را درک کرده و خطر حوادث آینده را کاهش دهید.

❖ **مدیریت حوادث امنیتی**

اطمینان حاصل کنید که هر حادثه امنیتی در اسرع وقت شناسایی، گزارش، پاسخ داده شده، مورد تحقیق و بازیابی قرار گرفته است .از انجام اقدامات اصلاحی مناسب اطمینان حاصل کنید.

وقتی تحقیق می‌کنید منصفانه و درست رفتار کنید

تحقیقات امنیتی باید هم از منافع دولت نیوزیلند و هم از حقوق افراد آسیب دیده محافظت کند.

سازمان شما باید اصول عدالت طبیعی و انصاف رویه را در کلیه تحقیقات امنیتی اعمال کند.

رویه‌های شما باید به اطمینان از صحت هرگونه تحقیق فعلی یا آتی توسط سازمان شما یا سازمان دیگر توجه داشته باشند.

موارد جدی امنیتی را به مقامات مناسب گزارش دهید

اگر حادثه‌ای بالقوه جدی است، باید با موارد زیر مشورت کنید:

- پلیس نیوزیلند
- سرویس اطلاعات امنیتی نیوزلند(NZSIS)
- اداره امنیت ارتباطات دولتی (GCSB) یا افسر ارشد دیجیتال دولت (GCDO) یا هر دو .

❖ **اطلاعات بیشتر**

- گزارش حوادث و انجام تحقیقات امنیتی
- پاسخ به افزایش سطح تهدید
- سازمان شما باید آماده پاسخگویی به شرایط اضطراری و افزایش تهدید باشد.

❖ **بتوانید به افزایش سطح تهدید پاسخ دهید**

برنامه‌هایی را تدوین کنید و آماده باشید تا در موارد اضطراری یا شرایطی که تهدید بیشتری برای مردم، اطلاعات یا دارایی‌های شما وجود دارد، سطح امنیتی را افزایش دهید.

برنامه‌های شما برای بالا بردن سطح امنیتی باید با سایر برنامه‌های پیشگیری و واکنش اضطراری تلفیق و هماهنگ شود .به عنوان مثال، برنامه‌هایی برای پاسخگویی در صورت آتش سوزی، تهدید بمب، نشت مواد شیمیایی خطرناک، قطع برق، تخلیه یا اضطراری دفاع مدنی.

❖ **ارزیابی توانایی امنیتی شما**

خودارزیابی سالانه به سازمان شما کمک می‌کند تا بفهمد اقدامات امنیتی شما درست است و در صورت لزوم امنیت را بهبود می‌بخشد.

❖ **توانایی خود را ارزیابی کنید**

از یک فرآیند ارزیابی مبتنی بر شواهد سالانه برای اطمینان از مناسب بودن توانایی امنیتی سازمان خود استفاده کنید .در صورت درخواست، گزارش اطمینان را از طریق تیم محافظت از امنیت مورد نیاز به دولت ارائه دهید .سیاست‌ها و برنامه‌های خود را هر ۲ سال یا در صورت لزوم تغییر در تهدید یا محیط کار، زودتر مرور کنید.

فرایند ارزیابی و گزارش دهی به شما کمک می‌کند تا سازمان شما را بررسی کند که شما اطمینان حاصل کنید که:

- مردم شما ایمن هستند
- منابع اساسی شما رازداری، صداقت و در دسترس بودن خود را حفظ می‌کنند.

این فرایند شامل ارزیابی و گزارش گیری داخلی و در برخی موارد گزارشگری خارجی برای هدایت سازمانهای امنیتی است.

❖ **اطلاعات بیشتر**

- ارزیابی و گزارش گیری از خود

۴-۱- امنیت کارکنان

برای محافظت از منابع دولتی، سازمان شما باید اطمینان حاصل کند که دسترسی به اطلاعات و دارایی فقط به افراد مناسب داده می‌شود.

اقدامات امنیتی پرسنل شما باید از مرحله قبل از استخدام شروع شود و در طول چرخه حیات پرسنل ادامه یابد.

❖ **اتخاذ رویکردی مبتنی بر ریسک**

از یک روش مبتنی بر ریسک برای امنیت پرسنل استفاده کنید تا خطرات از دست رفتن، آسیب دیدن یا به خطر انداختن منابع دولتی را کاهش دهد.

یک رویکرد مبتنی بر ریسک به شما کمک می‌کند تا تصمیمات امنیتی مناسبی اتخاذ کنید، هزینه‌های غیرضروری را کاهش می‌دهد و ایجاد اختلال در افراد و فعالیت‌های شما را به حداقل می‌رساند.

برای کمک به شما از ارزیابی خطر استفاده کنید:

- خطرات مرتبط با هر نقش را شناسایی کنید
- اقدامات امنیتی مناسب را برای هر مرحله از چرخه حیات پرسنل اتخاذ کنید.

اقدامات امنیتی پرسنل خود را با مدیریت مؤثر خط، استفاده صحیح از اصل "نیاز به دانستن"، کنترل دسترسی و اقدامات امنیتی اطلاعات پشتیبانی کنید.

❖ **برای اطلاعات بیشتر به:**

- ISO 31000: 2018مدیریت ریسک - دستورالعمل ها
- HB 167: 2006مدیریت ریسک امنیتی

❖ **استخدام فرد مناسب**

امنیت پرسنل به سازمان شما کمک می‌کند صداقت، امانتداری و وفاداری افرادی را که ممکن است به منابع دولتی دسترسی داشته باشند، ارزیابی کند. همه افرادی که در دولت نیوزیلند استخدام شده‌اند ممکن است تحت بررسی امنیتی قرار بگیرند.

❖ فرد مناسب را استخدام کنید

اطمینان حاصل کنید که همه افرادی که برای سازمان شما کار می‌کنند (کارمندان، پیمانکاران و کارکنان موقت) که به اطلاعات و دارایی‌های دولت نیوزیلند دسترسی دارند: • هویت آنها مشخص شده است • حق کار در نیوزیلند دارند • برای دسترسی مناسب هستند • موافقت با با سیاست‌ها، استانداردها، پروتکل‌ها و الزامات دولت که از مردم، اطلاعات و دارایی‌ها در برابر آسیب محافظت می‌کند، پیروی کنید.

سازمان شما باید:

- بررسی‌های صحیح قبل از استخدام را انجام دهید
- انتظارات درستی را در مورد امنیت در هنگام استقرار تعیین کنید

❖ اطلاعات بیشتر

- پروتکل مدیریت برای امنیت پرسنل
- راهنمای امنیت پرسنل برای سازمان شما
- اطمینان از مناسب بودن مداوم آنها

تغییر در شرایط شخصی، نیاز به نقش یا مشخصات خطر سازمان شما می‌تواند در هر مرحله از چرخه حیات پرسنل اتفاق بیفتد.

❖ اطمینان از مناسب بودن مداوم آنها

از مناسب بودن مداوم همه افرادی که برای سازمان شما کار می‌کنند اطمینان حاصل کنید .این مسئولیت شامل رسیدگی به هرگونه نگرانی است که ممکن است در شایستگی شخص برای ادامه دسترسی به اطلاعات و دارایی‌های دولت تأثیر بگذارد.

فرایندهای زیر را انجام دهید تا اطمینان حاصل کنید افراد شما برای استخدام و دسترسی به اطلاعات و دارایی‌های شما مناسب باقی می‌مانند. گزارش و پاسخگویی به حوادث امنیتی .برای کمک به شما در مدیریت حوادث امنیتی، روش‌های گزارش دهی و پاسخگویی را تعیین کنید .برای مهار اثرات، مدیریت عواقب و بهبود سریع در صورت افزایش خطرات امنیتی، بررسی‌های اضافی را انجام دهید .تغییرات قابل توجه در شرایط شخصی یا فعالیت مشکوک را گزارش دهید .رفتار مشکوک به جرم را به پلیس گزارش دهید.

مجوزهای امنیتی ملی را مدیریت کنید .ارائه آموزش و توجیهات، گزارش تغییرات در شرایط شخصی، مدیریت دسترسی و تغییرات در سطح ترخیص .مجوزها را در صورت لزوم بررسی کنید. مسئولیت امنیت را بر عهده همه بگذارید .آگاهی از اقدامات و فرآیندهای امنیتی خود را افزایش دهید .گزارش رفتار مشکوک را برای افراد خود آسان کنید.

تغییرات نقش را مدیریت کنید .قبل از انتقال افراد به سمت نقشهایی با خطرات بالاتر، بررسی‌های صحیح قبل از استخدام را انجام دهید.

❖ اطلاعات بیشتر

- پروتکل مدیریت برای امنیت پرسنل
- چرخه حیات امنیت پرسنل

❖ مدیریت عزیمت آنها

هنگامی که شخصی سازمان شما را ترک می‌کند، دانش خود را در مورد عملیات تجاری، مالکیت معنوی، اطلاعات رسمی و آسیب پذیری های امنیتی شما حفظ می‌کند .مدیریت خوب عزیمت آنها خطر سو this استفاده از این دانش را کاهش می‌دهد.

❖ عزیمت آنها را مدیریت کنید

عزیمت افراد را مدیریت کنید تا هرگونه خطر برای افراد، اطلاعات و دارایی‌های ناشی از افرادی که از سازمان شما خارج می‌شوند، محدود شود .این مسئولیت شامل اطمینان از بازگشت هرگونه حق دسترسی، مجوزهای امنیتی و دارایی‌ها و درک افراد از تعهدات مداوم خود است.

❖ دسترسی را از بین ببرید و دارایی‌ها را جمع آوری کنید

قبل از رفتن شخص:

- دسترسی آنها به منابع الکترونیکی، منابع فیزیکی و سایتهای فیزیکی را حذف کنید
- تمام کارتهای شناسایی و کارتهای دسترسی را جمع آوری کنید، از جمله هر ابزاری که به آنها امکان دسترسی از راه دور به سیستمهای مدیریت اطلاعات شما را می‌دهد
- اطمینان حاصل کنید که تمام دارایی‌ها پس داده شده‌اند (از دارایی معنوی یا اطلاعات رسمی خود مراقبت کنید).

❖ از سازمان خود و دیگران محافظت کنید

برای یادگیری از روند عزیمت و مدیریت خطرات، همچنین باید:

- مصاحبه‌های خروج انجام دهید
- خطرات شناسایی شده را ارزیابی و مدیریت کنید (به عنوان مثال، وقتی کسی احساس نارضایتی می‌کند)
- در صورت بالا بودن خطر از محرمانه بودن استفاده کنید
- ارجاعات صادقانه و دقیق ارائه دهید.

❖ اطلاعات بیشتر

- پروتکل مدیریت برای امنیت پرسنل
- چرخه حیات امنیت پرسنل
- عزیمت آنها را مدیریت کنید

❖ مدیریت مجوزهای امنیت ملی

روند به دست آوردن مجوز امنیت ملی اطمینان می‌دهد که به افراد شما می‌توان از اطلاعات طبقه بندی شده، دارایی‌ها یا محل کار محافظت کرد .پس از پاکسازی، سازمان شما مسئولیت مدیریت شایستگی مداوم آنها برای تصویب را دارد.

❖ **مجوزهای امنیتی ملی را مدیریت کنید**

اطمینان حاصل کنید که افراد قبل از اینکه به اطلاعات، دارایی‌ها یا مکان‌های کاربری محرمانه، محرمانه و دسترسی داشته باشند، سطح مجاز ترخیص امنیت ملی را دارند .شایستگی مداوم کلیه دارندگان مجوزهای امنیت ملی برای داشتن مجوز را مدیریت کرده و هرگونه تغییر در مورد ترخیص آنها را به NZSIS اطلاع دهید.

❖ **ابتدا از NZSIS پیشنهادی دریافت کنید**

قبل از اینکه سازمان شما مجوز امنیت ملی را دریافت کند، باید یک توصیه بررسی امنیتی از NZSIS دریافت کنید. NZSIS مسئول فرآیند بررسی امنیتی و توصیه‌هایی درباره قابلیت اطمینان امنیتی است. روند بررسی امنیتی سرزده است .با این حال، NZSISباید فرآیند را با دقت و حساسیت و مطابق با سیاست دولت انجام دهد. تمام تصمیمات مربوط به بررسی بر اساس ارزیابی کل فرد است و اصول عدالت طبیعی و انصاف رویه در تمام مراحل دنبال می‌شود. حتی در صورت داشتن مجوزهای قانونی از افراد، فقط در صورت نیاز مشکوک به منابع دارای علامت محافظ اجازه دسترسی می‌دهید - براساس راحتی یا نقش شخصی در سازمان خود اجازه دسترسی ندهید .

❖ **مسئولیت‌های خود در مورد تصویب‌های امنیت ملی را بدانید و آنها را انجام دهید**

مسئولیت‌های زیر در صورت مدیریت دارنده‌های تصفیه امنیت ملی الزامی است .سازمان شما باید:

- موقعیت‌هایی را که نیاز به دسترسی به اطلاعات، دارایی‌ها یا مکان‌های کاربری محرمانه، اسرارآمیز و دارند، شناسایی، ثبت و بررسی کنید
- قبل از اینکه به وی اجازه دسترسی دهید، از سطح صحیح ترخیص اطمینان حاصل کنید
- اطمینان از شایستگی مداوم کلیه دارندگان ترخیص برای ادامه تصدیق امنیت ملی .

سازمان شما همچنین باید موارد زیر را به NZSIS اطلاع دهد:

- تصمیم برای اعطای یا رد مجوز امنیت ملی
- تصمیم منجر به تغییر در مجوز امنیت ملی
- نگرانی‌هایی که ممکن است در شایستگی فرد برای بدست آوردن یا حفظ سطح مناسب ترخیص تأثیر بگذارد
- دارنده ترخیص کالا که سازمان شما را ترک می‌کند یا با شما قرارداد بسته است

❖ **اطلاعات بیشتر**

- راهنمای مدیریت دارندگان مجوزهای امنیت ملی

۵-۱- امنیت اطلاعات

دولت نیوزیلند برای انجام وظایف خود اطلاعات را جمع آوری و دریافت می‌کند و از همه کسانی که این اطلاعات را دارند یا به آنها دسترسی دارند انتظار دارد که از آنها محافظت کنند.

اقدامات امنیتی اطلاعات شما باید بر اساس الزامات شما برای محرمانه بودن، صداقت و در دسترس بودن اطلاعات باشد.

❖ **آنچه شما باید انجام دهید**

سازمان شما باید اقدامات امنیتی را برای حفاظت از اطلاعات در برابر استفاده غیر مجاز، اصلاح تصادفی، از بین رفتن یا انتشار، تدوین، اجرا و بررسی کند .شما این کار را از طریق انجام می‌دهید:

- ایجاد فرهنگ امنیت اطلاعات
- اجرای اقدامات امنیتی متناسب با ارزش، حساسیت و هرگونه علامت گذاری محافظ اطلاعات شما
- رعایت الزامات قانونی.

❖ تعریف دارایی اطلاعات

اصطلاح دارایی‌های اطلاعاتی به هر نوع اطلاعاتی اطلاق می‌شود، از جمله:

- اسناد و مدارک چاپ شده
- داده‌های الکترونیکی
- نرم افزار یا سیستم‌ها و شبکه‌های ICT که اطلاعات در آن ذخیره، پردازش یا ارتباط برقرار می‌شود
- اطلاعات فکری (دانش) کسب شده توسط افراد
- موارد فیزیکی که می‌توان از آنها اطلاعات مربوط به طراحی، اجزا و یا کاربردها را بدست آورد.

❖ درک اینکه برای محافظت از چه اطلاعاتی نیاز دارید

برای اجرای صحیح اقدامات امنیتی اطلاعات، باید بدانید که چه دارید و چگونه سازمان شما تحت تأثیر خسارت یا آسیب قرار می‌گیرد.

❖ آنچه را که برای محافظت از آن نیاز دارید درک کنید

اطلاعات و سیستم‌های ICT را که سازمان شما مدیریت می‌کند شناسایی کنید .خطرات امنیتی (تهدیدها و آسیب پذیری ها) و تأثیر تجاری هرگونه نقض امنیت را ارزیابی کنید.

برای مطابقت با مراحل زیر را انجام دهید.

- از سیستم‌های اطلاعاتی و فناوری اطلاعات و ارتباطات خود، از جمله سیستم‌هایی که از برنامه‌های تداوم تجارت و بازیابی بلایا پشتیبانی می‌کنند، موجودی خود را انجام دهید.
- برای ارزیابی تأثیرات در معرض خطر بودن، از سطوح تأثیر تجاری استفاده کنید .بدانید که سازمان شما در معرض نقض امنیت چیست، با چه تهدیدهایی روبرو هستید و چگونه تحت تأثیر قرار می‌گیرید.
- خطرات ناشی از زنجیره تأمین و اطلاعات جمع شده (مجموعه‌ای از اطلاعات در قالب‌های الکترونیکی یا چاپی) را وارد کنید.
- اقدامات امنیتی موجود خود را تجزیه و تحلیل کنید تا دریابید در چه مواردی ممکن است نیاز به پیشرفت داشته باشید.

اطلاعاتی را که به آنها نیاز دارد، طبقه بندی و اختصاص دهید، بنابراین افراد شما می‌دانند که چگونه اطلاعات را اداره کنند و از آنها محافظت کنند.

❖ اقدامات امنیتی اطلاعات شما را طراحی می‌کند

هنگامی که خطرات موجود در اطلاعات سازمان خود را درک کردید، باید اقدامات امنیتی مناسب را طراحی کنید .این اقدامات باید متناسب با خطرات شما و مطابق با میزان اشتیاق شما باشد.

❖ امنیت اطلاعات خود را طراحی کنید

در اوایل مراحل برنامه ریزی، انتخاب و طراحی، امنیت اطلاعات را در نظر بگیرید .تدابیر امنیتی را طراحی کنید که خطرات سازمان شما را تهدید می‌کند و با اشتهای شما سازگار است .اقدامات امنیتی شما باید مطابق با موارد زیر باشد: • سیستم طبقه بندی امنیتی دولت نیوزیلند • کتابچه راهنمای امنیت اطلاعات نیوزلند • هرگونه تعهدات حریم خصوصی، قانونی و نظارتی که تحت آن فعالیت می‌کنید .یک چارچوب مناسب مدیریت امنیت اطلاعات متناسب با خطرات خود اتخاذ کنید.

❖ اقدامات امنیتی اطلاعات خود را طراحی کنید

اقدامات زیر را برای طراحی اقدامات امنیتی متناسب انجام دهید.

- برای کاهش خطرات موجود در اطلاعات خود از چندین لایه امنیتی - "امنیت در عمق" استفاده کنید.
- نکاتی را بدانید که اطلاعات شما می‌تواند با خطرات اساسی روبرو شود.
- چارچوبی برای امنیت اطلاعات ایجاد کنید که امنیت و هزینه و تأثیر آن را بر عملکرد شما متعادل کند.
- تدابیر امنیتی را که طراحی می‌کنید در برنامه‌های تداوم کسب و کار و بازیابی فاجعه قرار دهید.
- الزامات اجباری اطلاعات، سیستم‌هایICT ، شبکه‌ها (از جمله دسترسی از راه دور)، زیرساخت‌ها و برنامه‌ها را رعایت کنید.
- از مدیر ارشد امنیت اطلاعات (CISO) یا مجری معادل خود ثبت نام کنید

❖ اقدامات امنیتی اطلاعات خود را اجرا کنید

هنگامی که CISO شما موافقت کرد که طرح امنیتی پیشنهادی نیازهای ویژه امنیت اطلاعات سازمان شما را برطرف می‌کند، شما باید:

- اقدامات امنیتی و حفظ حریم خصوصی مورد توافق، از جمله سیاست‌ها، فرایندها و اقدامات امنیتی فنی را اجرا کنید
- با تأمین کنندگان خود کار کنید تا اطمینان حاصل کنید که آنها شرایط امنیتی شما را درک می‌کنند و می‌توانند آن را برآورده کنند
- خطرات اطلاعاتی مربوط به چرخه عمر سیستم ICT را در نظر بگیرید
- سیستم‌های خود را هنگام توسعه و قبل از پذیرش آزمایش کنید.

❖ مطابق با الزامات مربوطه

اقدامات امنیتی شما باید با هرگونه تعهدات حریم خصوصی، قانونی و نظارتی که تحت آن کار می‌کنید و شرایط موجود در:

- سیستم طبقه بندی امنیتی دولت نیوزیلند
- کتابچه راهنمای امنیت اطلاعات نیوزلند
- اعتبار سنجی اقدامات امنیتی اطلاعات شما

شما باید اقدامات انجام شده خود را تأیید کنید تا اطمینان حاصل شود که مطابق انتظار عمل می‌کنند.

❖ اقدامات امنیتی خود را تأیید کنید

تأیید کنید که اقدامات امنیتی اطلاعات شما به درستی اجرا شده و برای اهداف مناسب است .فرآیند صدور گواهینامه و اعتبار سنجی را به اتمام برسانید تا از سیستم‌های ICT خود برای تأیید بهره مند شوید. CISOشما مسئول تصمیم گیری در مورد اینکه آیا اقدامات امنیتی شما خطرات سازمان را تا حد قابل قبولی کاهش می‌دهد، است .سپس تیم اجرایی شما می‌تواند به اقدامات، از جمله نحوه اداره آنها اطمینان داشته باشد. سیستم‌های ICT باید با روند صدور گواهینامه و اعتباربخشی در کتابچه راهنمای امنیت اطلاعات نیوزلند مطابقت داشته باشند.

❖ **امنیت اطلاعات خود را به روز نگه دارید**

با تغییر فناوری، تجارت و اطلاعات، تهدیدها، آسیب پذیری ها و خطرات اطلاعات سازمان شما تغییر خواهد کرد.

❖ **امنیت خود را به روز نگه دارید**

اطمینان حاصل کنید که امنیت اطلاعات شما برای هدف مناسب باقی می‌ماند: - نظارت بر رویدادهای امنیتی و پاسخگویی به آنها - به روز نگه داشتن تهدیدات و آسیب پذیری های در حال تکامل - حفظ دسترسی مناسب به اطلاعات شما برای به روز نگه داشتن امنیت اطلاعات و مطابقت با، فعالیت‌های زیر را انجام دهید.

تهدیدات و آسیب پذیری های در حال تحول را تحلیل کنید .نظارت و مشاهده کنید تا بتوانید آسیب پذیری ها را شناسایی کرده و رویدادهای مربوطه را تشخیص دهید .برای ایمن سازی سیستم‌ها، شبکه‌ها، پیکربندی‌ها و فرایندهای خود اقدام پیشگیرانه انجام دهید. اقدامات امنیتی اطلاعات خود را به روز نگه دارید .سیستم‌های کنترل دسترسی را حفظ کرده و از تجهیزات ICT محافظت کنید .وقتی فرآیندها، سیستم‌ها و قابلیت‌های جدید یا به روز شده را اتخاذ می‌کنید، اطمینان حاصل کنید که برنامه‌های تداوم شغلی و بازیابی خطرات شما آزمایش شده است. به حوادث امنیتی اطلاعات پاسخ دهید .اطمینان حاصل کنید که به سرعت تحقیق کرده و پاسخ می‌دهید، بدون معطلی با طرف‌های آسیب دیده یا مقامات مربوطه ارتباط برقرار می‌کنید و از حوادث برای بهبود امنیت درس می‌گیرید.

❖ **ارزیابی توانایی شما**

بررسی اقدامات شما به شما کمک می‌کند تا در صورت لزوم امنیت اطلاعات خود را بهبود ببخشید، یا تغییر دهید.

❖ **توانایی خود را ارزیابی کنید**

از یک فرآیند ارزیابی مبتنی بر شواهد سالانه برای اطمینان از مناسب بودن توانایی امنیتی سازمان خود استفاده کنید .در صورت درخواست، گزارش اطمینان را از طریق تیم محافظت از امنیت مورد نیاز به دولت ارائه دهید .سیاست‌ها و برنامه‌های خود را هر ۲ سال یا در صورت لزوم تغییر در تهدید یا محیط کار، زودتر مرور کنید.

مخلوطی از بررسی‌های منظم و دوره‌ای همراه با ارزیابی سالانه به شما کمک می‌کند تا بدانید چه زمانی تغییر لازم است، و اقدامات شما به خوبی اجرا و پیگیری می‌شود.

همچنین می دانید چه زمانی اطلاعات باید بایگانی شوند، از بین بروند، دوباره مورد استفاده قرار بگیرند یا به طور ایمن از بین بروند.

❖ **راهنمایی برای کمک به شما در برآوردن نیازها**

- پروتکل مدیریت امنیت اطلاعات

- کتابچه راهنمای امنیت اطلاعات نیوزلند
- سیستم طبقه بندی امنیتی دولت نیوزیلند
- الزامات رسیدگی به اطلاعات و تجهیزات دارای علامت محافظ

۶-۱- امنیت فیزیکی

هر سازمان دولتی نیوزلند برای حفاظت از مردم، اطلاعات و دارایی‌ها باید تدابیر امنیتی فیزیکی در نظر بگیرد. امنیت فیزیکی چند وجهی است و اقدامات امنیتی شما را در زمینه‌های دیگر تکمیل می‌کند. امنیت فیزیکی مناسب از استانداردهای ایمنی و بهداشت پشتیبانی می‌کند و به سازمان شما کمک می‌کند تا کارایی موثرتر و موثرتری داشته باشد. برای دستیابی به سطح صحیح محافظت فیزیکی برای افراد سازمان، اطلاعات و دارایی‌های خود، رویکرد مدیریت ریسک را در پیش بگیرید.

❖ درک آنچه شما برای محافظت نیاز دارید

دانستن اینکه نقاط ضعف شما کجاست، اولین قدم برای رسیدن به امنیت فیزیکی قوی است .شاید لازم باشد از آنها محافظت کنید:

- افراد، اطلاعات و دارایی‌های شما
- مردم و مشتریان
- منابع فرهنگی.

هنگامی که خطرات خود را شناسایی کردید، باید احتمال و تأثیر هر یک از ریسک‌ها را ارزیابی کنید .ارزیابی خطرات به شما کمک می‌کند تا درک کنید که در کجا باید اقدامات بیشتری انجام دهید.

❖ آنچه را که برای محافظت از آن نیاز دارید درک کنید

افراد، اطلاعات و دارایی‌هایی را که سازمان شما باید از آنها محافظت کند و مکان آنها را شناسایی کنید .خطرات امنیتی (تهدیدها و آسیب پذیری ها) و تأثیر تجارت در ضرر و زیان مردم، اطلاعات یا دارایی‌ها را ارزیابی کنید .از درک خود استفاده کنید.:

طبق قانون ایمنی و بهداشت در محل کار ۲۰۱۵ ، سازمان شما باید:

- خطرات افراد خود را شناسایی کرده و برای کاهش آنها اقدام کنید
- از مشتریان و مردم در برابر آسیب محافظت کنید.

برای امکانات خود، باید در نظر بگیرید که چگونه از آنها استفاده می‌شود، چه کسی از آنها استفاده می‌کند و چه چیزی در آنها ذخیره می‌شود.

مناطق دیگری که باید به آنها فکر کنید:

- ترتیبات برای افرادی که دور از دفتر کار می‌کنند
- توافق نامه‌های مکان یابی با طرف‌های دیگر
- برنامه‌هایی برای سایتها یا ساختمانهای جدید، و برنامه‌هایی برای تغییرات
- تجهیزات و اطلاعاتICT
- زنجیره تأمین شما

❖ **اطلاعات بیشتر:**

- ISO 31000: 2018مدیریت ریسک - دستورالعمل ها
- HB 167: 2006مدیریت ریسک امنیتی
- ارزیابی ریسک
- سطوح تأثیر تجاری

❖ **طراحی امنیت فیزیکی زودهنگام**

برای کاهش هزینه‌ها و بهبود اثربخشی، اقدامات امنیتی بدنی خود را در مراحل اولیه در هر مرحله در نظر بگیرید:

- برنامه ریزی سایت‌ها یا ساختمانهای جدید
- انتخاب سایت‌های جدید
- برنامه ریزی تغییرات در ساختمانهای موجود.

شما همچنین باید خطرات مربوط به امنیت فیزیکی را برای افرادی که دور از دفتر کار می‌کنند و سایر امکانات مشترکی که استفاده می‌کنید ارزیابی کنید.

❖ **امنیت فیزیکی خود را طراحی کنید**

در اوایل مراحل برنامه ریزی، انتخاب، طراحی و اصلاح امکانات امنیتی فیزیکی را در نظر بگیرید .تدابیر امنیتی را طراحی کنید که خطرات سازمان شما را تهدید می‌کند و با اشتهای شما سازگار است .اقدامات امنیتی شما باید مطابق با تعهدات مربوط به بهداشت و ایمنی باشد.

❖ **خطرات را ارزیابی کرده و برنامه‌ها را تهیه کنید**

قبل از انتخاب سایت‌ها، باید خطرات امنیتی فیزیکی را ارزیابی کنید .سپس برنامه‌های امنیتی سایت را تهیه کنید که جزئیات اقدامات امنیتی لازم برای کاهش خطرات را بیان می‌کند.

❖ **مطابق با الزامات منطقه امنیتی**

از مناطق امنیتی مناسب و اقدامات مربوط به آنها برای اطلاعات و دارایی‌های دارای علامت محافظ استفاده کنید .مناطق امنیتی ممکن است به محافظت از سایر اطلاعات و منابع ارزشمند نیز کمک کنند .هر منطقه دارای حداقل الزاماتی است که باید اجرا کنید.

❖ **روش خوبی را برای طراحی امنیت فیزیکی اعمال کنید**

تمرین خوب شامل موارد زیر است:

- به دنبال مدل'Deter ، Detect، Delay، Respond، Recover'
- با استفاده از چندین لایه امنیتی - "امنیت در عمق"
- در صورت لزوم از محصولات امنیتی مورد تأیید NZSIS استفاده کنید
- پرداختن به تمام نقاطی که ممکن است امنیت فیزیکی شما نقض شود
- دانستن و مطابقت با کلیه قوانین و استانداردهای مربوط

- استفاده از "پیشگیری از جرم از طریق طراحی محیطی(CPTED) "
- اضافه کردن الزامات امنیتی فیزیکی به برنامه‌های تداوم کسب و کار و بازیابی فاجعه.

❖ **طراحی امنیت فیزیکی خود را قبول کنید**

افسر ارشد امنیتی شما (CSO) باید بپذیرد که طرح امنیتی پیشنهادی برای اهداف مناسب است و نیازهای خاص سازمان شما را برطرف می‌کند.

❖ **اقدامات امنیتی جسمی خود را اجرا کنید**

اجرای اقدامات امنیتی فیزیکی مورد توافق شما شامل اجرای سیاستها و فرآیندهای مربوطه و اقدامات فنی موردنیاز شما می‌باشد.

❖ **امنیت فیزیکی را در معاملات تجاری خود بگنجانید**

امنیت فیزیکی را در قراردادها، روابط تجاری و مشارکت‌های خود ایجاد کنید .اطمینان حاصل کنید که همه از الزامات امنیتی جسمی شما آگاه هستند و از نظر انطباق اطمینان حاصل کنند.

❖ **روند برنامه ریزی و ساخت خود را مدیریت کنید**

اطمینان حاصل کنید که اقدامات امنیتی جسمی شما هنگام ایجاد ساختمان جدید، بازسازی یا دارایی منتقل شده از یک محل کار یا منطقه به مکان دیگر، انجام می‌شود.

❖ **اطلاعات بیشتر :**

- پروتکل مدیریت برای امنیت فیزیکی
- اعتبار سنجی اقدامات امنیتی شما
- افسر ارشد امنیتی شما مسئول تأیید اقدامات شما است .آن‌ها باید تصمیم بگیرند که آیا سازمان شما:
- اقدامات امنیتی فیزیکی به خوبی مدیریت شده است
- خطرات به درستی شناسایی و کاهش یافته است
- اقدامات امنیتی فیزیکی این امکان را فراهم می‌کند که مسئولیت‌های حاکمیت برآورده شود

❖ **اقدامات امنیتی خود را تأیید کنید**

تأیید کنید که اقدامات امنیتی جسمی شما به درستی اجرا شده و برای اهداف مناسب است .برای اطمینان از تأیید فعالیت مناطق امنیتی، مراحل صدور گواهینامه و اعتبار سنجی را به اتمام برسانید.

پیروی از مراحل صدور گواهینامه و اعتبارسنجی برای مناطق امنیتی، اقدامات امنیتی فیزیکی شما را برای محافظت مناسب و صحیح اجرا می‌کند.

❖ **امنیت خود را به روز نگه دارید**

تهدیدها و آسیب پذیری های شما احتمالاً با گذشت زمان تغییر می‌کند .فناوری، فرآیندها، ترتیب‌ها و اهداف جدید می‌تواند به معنای تغییر امنیت فیزیکی شما باشد .شما باید نسبت به تغییرات هوشیار باشید و برای به روز نگه داشتن امنیت خود اقدام کنید.

❖ **امنیت خود را به روز نگه دارید**

اطمینان حاصل کنید که از تهدیدات و آسیب پذیری های در حال به روز بودن مطلع هستید و به طور مناسب پاسخ می‌دهید . اطمینان حاصل کنید که اقدامات امنیتی جسمی شما به طور مؤثر حفظ می‌شود تا برای اهداف مناسب باقی بماند.

افراد شما باید درباره تغییراتی که روی آنها تأثیر می‌گذارد و هرگونه سیاست جدیدی که اعمال می‌کنید بدانند. شما همچنین باید آنها را تشویق کنید که هر گونه خطری که با آن روبرو می‌شوند یا نگران آن هستند را گزارش دهند.

برای ماندن در بالای محیط تهدید خود:

- نظارت بر سیستم‌ها، دارایی‌ها و افراد
- رویدادها و روندها را مشاهده کنید تا بتوانید تهدیدها را تشخیص دهید
- اقدامات خود را مرتباً ارزیابی کنید تا ببینید آیا تغییرات لازم است
- تجزیه و تحلیل و گزارش در مورد خطرات
- اعمال و پیگیری رفع

وقتی حوادث امنیتی اتفاق می افتد، اطمینان حاصل کنید که از آنچه اتفاق افتاده است، از جمله نحوه پاسخگویی و مدیریت سازمان به حوادث، یاد می‌گیرید.

❖ **ارزیابی توانایی شما**

اقدامات امنیتی جسمی خود را ارزیابی کنید تا بفهمید چه مواردی برای حفاظت بهتر از افراد، اطلاعات و دارایی‌های شما باید بهبود یا تغییر یابد.

❖ **توانایی خود را ارزیابی کنید**

از یک فرآیند ارزیابی مبتنی بر شواهد سالانه برای اطمینان از مناسب بودن توانایی امنیتی سازمان خود استفاده کنید .در صورت درخواست، گزارش اطمینان را از طریق تیم محافظت از امنیت مورد نیاز به دولت ارائه دهید .سیاست‌ها و برنامه‌های خود را هر ۲ سال یا در صورت لزوم تغییر در تهدید یا محیط کار، زودتر مرور کنید.

برای کمک به شما در یافتن این موارد از ترکیبی از روش‌ها مانند نظارت و گزارش دهی، بازبینی و حسابرسی استفاده کنید.

- سیاست‌های امنیتی فیزیکی شما دنبال می‌شود (از جمله سیاست‌های بازنشستگی یا از بین بردن ایمن اطلاعات و دارایی‌ها)
- کنترل‌های امنیتی فیزیکی شما طبق برنامه کار می‌کنند
- هر گونه تهدید یا عملکرد تجاری جدید ظاهر شده است.

۷-۱- چه چیزی می‌خواهید بدانید

امنیت محافظتی به عهده کلیه افراد و خدمات شاغل در سازمان از جمله کارمندان، پیمانکاران و کارکنان موقت است .در حالی که مسئولیت‌های خاصی به عهده روسای آژانس‌ها و پزشکان امنیتی است، اما تقویت توانایی کلی امنیتی و فرهنگ آژانس باعث می‌شود که بتواند به طور مؤثر عمل کند و خطرات تجاری را بهتر مدیریت کند.

❖ **مدیران ارشد و مدیران ارشد**

نقش‌ها و مسئولیت‌ها

روسای آژانس مسئول امنیت محافظتی در آژانس خود هستند و پاسخگو هستند.

الزامات امنیتی حفاظتی (PSR) انتظارات دولت از مدیریت امنیت پرسنل، امنیت فیزیکی و اطلاعات را مشخص می‌کند. این به وضوح مشخص می‌کند که آژانس‌ها برای اطمینان از کنترل امنیت محافظتی باید در نظر بگیرند و باید در نظر بگیرند.

با پیاده سازیPSR :

- مدیریت بهتر خطرات تجاری
- اطمینان از تداوم ارائه خدمات
- به دولت و مردم اطمینان دهید که اقدامات مناسب و موثری را برای محافظت از مردم، اطلاعات و دارایی‌های نیوزلند انجام داده‌اید.

PSRموارد زیر را برای شما فراهم می‌کند:

- اسناد اصلی سیاست که الزامات اجباری سطح بالایی را که آژانس‌ها ملزم به اجرای و ارائه گزارش در برابر آنها هستند، توصیف می‌کنند
- پروتکل‌ها و الزامات مدیریتی که جهت بیشتری در مورد نحوه تأمین الزامات اجباری ارائه می‌دهند.

روسای آژانس‌ها و مدیران ارشد باید با درکی که از مسیرهایی برای محافظت موفقیت آمیز از مردم، اطلاعات و دارایی‌ها ایجاد می‌کند، از الزامات امنیتی محافظتی (PSR) استفاده کنند.

به عنوان روسای سازمان و مدیران ارشد، مسئولیت‌های شما عبارتند از:

- ایجاد یک فرهنگ امنیتی قوی و پایدار در آژانس خود
- مرور سیاست‌ها و رویه‌های مدیریت امنیت حفاظتی آژانس به طور منظم به عنوان بخشی از رویکرد آژانس برای مدیریت ریسک و برنامه ریزی تجاری
- اطمینان از برآورده شدن الزامات اجباری PSR و اطمینان از وجود نظارت مربوطه
- انتصاب یک افسر ارشد امنیت (CSO) و کار با آنها هنگام توسعه، حفظ و نظارت بر سیاست‌ها و اقدامات امنیتی محافظتی
- تأیید ساختارهای مدیریت ریسک امنیتی، فعالیت‌های اطمینان و تخصیص منابع
- سیاست‌ها و پروتکل‌های آژانس خود را برای پرسنل، اطلاعات و امنیت فیزیکی تأیید کنید
- اعطای مجوزهای امنیتی به کارمندان و پیمانکاران پس از دریافت توصیه‌ای از سرویس اطلاعات امنیتی نیوزلند (NZSIS).

❖ **پزشکان امنیتی**

نقش‌ها و مسئولیت‌ها

پزشکان امنیتی که در آژانس‌ها استخدام شده و یا با آنها قرارداد دارند با اجرای الزامات اجباری و ایجاد روشهای امنیتی محافظتی متناسب با نیازهای آژانس خود، نقش مهمی در مدیریت پرسنل، امنیت فیزیکی و اطلاعاتی ایفا می‌کنند.

پزشکان امنیتی که در آژانس‌ها استخدام شده و یا با آنها قرارداد دارند نقش مهمی در مدیریت امنیت پرسنل، جسمی و اطلاعات دارند.

با پیاده سازیPSR :

- مدیریت بهتر خطرات تجاری
- اطمینان از تداوم ارائه خدمات

به دولت و مردم اطمینان دهید که اقدامات مناسب و موثری را برای محافظت از مردم، اطلاعات و دارایی‌های نیوزلند انجام داده‌اید.

PSR موارد زیر را برای شما فراهم می‌کند:

- اسناد اصلی سیاست که الزامات اجباری سطح بالایی را که آژانس‌ها ملزم به اجرای و ارائه گزارش در برابر آنها هستند، توصیف می‌کنند.
- پروتکل‌ها و الزامات مدیریتی که جهت بیشتری در مورد نحوه تأمین الزامات اجباری ارائه می‌دهند.

پزشکان امنیتی با درکی که از مسیرهایی برای محافظت موفقیت آمیز از مردم، اطلاعات و دارایی‌ها ایجاد می‌کند، از الزامات امنیتی محافظتی (PSR) استفاده می‌کنند.

به عنوان یک متخصص امنیت، مسئولیت‌های شما شامل موارد زیر است:

- ایجاد یک فرهنگ امنیتی قوی و پایدار در آژانس خود
- ایجاد سیاست و روشهای خاص آژانس که مطابق با الزامات اجباری PSR باشد
- مرور سیاست‌ها و رویه‌های مدیریت امنیت حفاظتی آژانس به طور منظم به عنوان بخشی از رویکرد آژانس برای مدیریت ریسک و برنامه ریزی تجاری
- گزارش دادن به مدیریت ارشد در مورد انطباق با الزامات اجباری و برنامه‌های توافق شده برای کاهش خطر
- تعیین نقش‌ها و مسئولیت‌های خاص برای امنیت در سراسر سازمان شما
- ارائه راهنمایی به رئیس آژانس خود در مورد مسائل امنیتی
- مدیریت و گزارش حوادث امنیتی
- ترویج و اجرای سیاست امنیتی حفاظتی
- نظارت بر امنیت حراست آژانس

❖ کارمندان

نقش‌ها و مسئولیت‌ها

کارمندان نقش مهمی در کمک به آژانس خود در حفظ امنیت پرسنل، جسمی و اطلاعاتی دارند .این مسئولیت فرد است که با سیاست‌ها و روش‌های امنیتی آژانس خود آشنا شود.

کارمندان نقش مهمی در کمک به آژانس خود در حفظ امنیت پرسنل، جسمی و اطلاعاتی دارند .این مسئولیت فرد است که با سیاست‌ها و روش‌های امنیتی آژانس خود آشنا شود.

با رعایت سیاست‌های امنیتی آژانس خود، شما:

- اطمینان از تداوم ارائه خدمات
- به دولت و مردم اطمینان دهید که اقدامات مناسب و موثری را برای محافظت از مردم، اطلاعات و دارایی‌های نیوزلند انجام داده‌اید.

PSR به آژانس‌ها موارد زیر را ارائه می‌دهد:

- اسناد اصلی سیاست که الزامات اجباری سطح بالایی را که آژانسها ملزم به اجرای و گزارش درمورد آن‌ها هستند توصیف می‌کند
- پروتکل‌ها و الزامات مدیریتی که جهت چگونگی تأمین الزامات اجباری را راهنمایی می‌کنند.
- کارمندان دولت باید سیاست‌های امنیتی را با درکی که مسیرهایی برای محافظت موفقیت آمیز از مردم، اطلاعات و دارایی‌ها فراهم می‌کند، رعایت کنند.
- به عنوان یک کارمند دولت، مسئولیت‌های شما شامل موارد زیر است:
- با سیاست‌ها و رویه‌های نمایندگی و نقش خود آشنا شوید و آنها را دنبال کنید
- دانستن اینکه چه کسی مسئول امنیت محافظت در آژانس شما است
- دانستن اولین نقطه تماس خود برای هر گونه سؤال در مورد امنیت محافظتی
- گزارش هرگونه حادثه امنیتی، رخ داده یا ممکن است رخ داده، به رئیس ارشد امنیتی (CSO) شما.
- بسته به نقش شما، ممکن است لازم باشد مجوز امنیت ملی را بدست آورید و آن را حفظ کنید و تعهدات و مسئولیت‌های امنیتی خود را به عنوان یک دارنده مجوز کاملاً روشن کنید.

❖ ارائه دهندگان خدمات

نقش‌ها و مسئولیت‌ها

ارائه دهندگان خدمات که در سازمان‌های دولتی استخدام می‌شوند نقش مهمی در کمک به سازمان‌های دولتی در حفظ امنیت پرسنلی، جسمی و اطلاعات دارند .این مسئولیت ارائه دهندگان خدمات است که با PSR آشنا باشند تا اطمینان حاصل کنند خدمات آنها منعکس کننده الزامات است.

با پیاده سازیPSR :

- به مدیریت ریسک‌های تجاری کمک کنید
- اطمینان از تداوم ارائه خدمات

اطمینان از دولت و مردم اقدامات مناسب و موثری برای محافظت از مردم، اطلاعات و دارایی‌های نیوزلند در نظر گرفته شده است.

PSR موارد زیر را برای شما فراهم می‌کند:

- اسناد اصلی سیاست که الزامات اجباری سطح بالایی را که آژانسها ملزم به اجرای و گزارش درمورد آن‌ها هستند توصیف می‌کند
- پروتکل‌ها و الزامات مدیریتی که جهت چگونگی تأمین الزامات اجباری را راهنمایی می‌کنند.
- به عنوان یک ارائه دهنده خدمات، مسئولیت‌های شما شامل موارد زیر است:

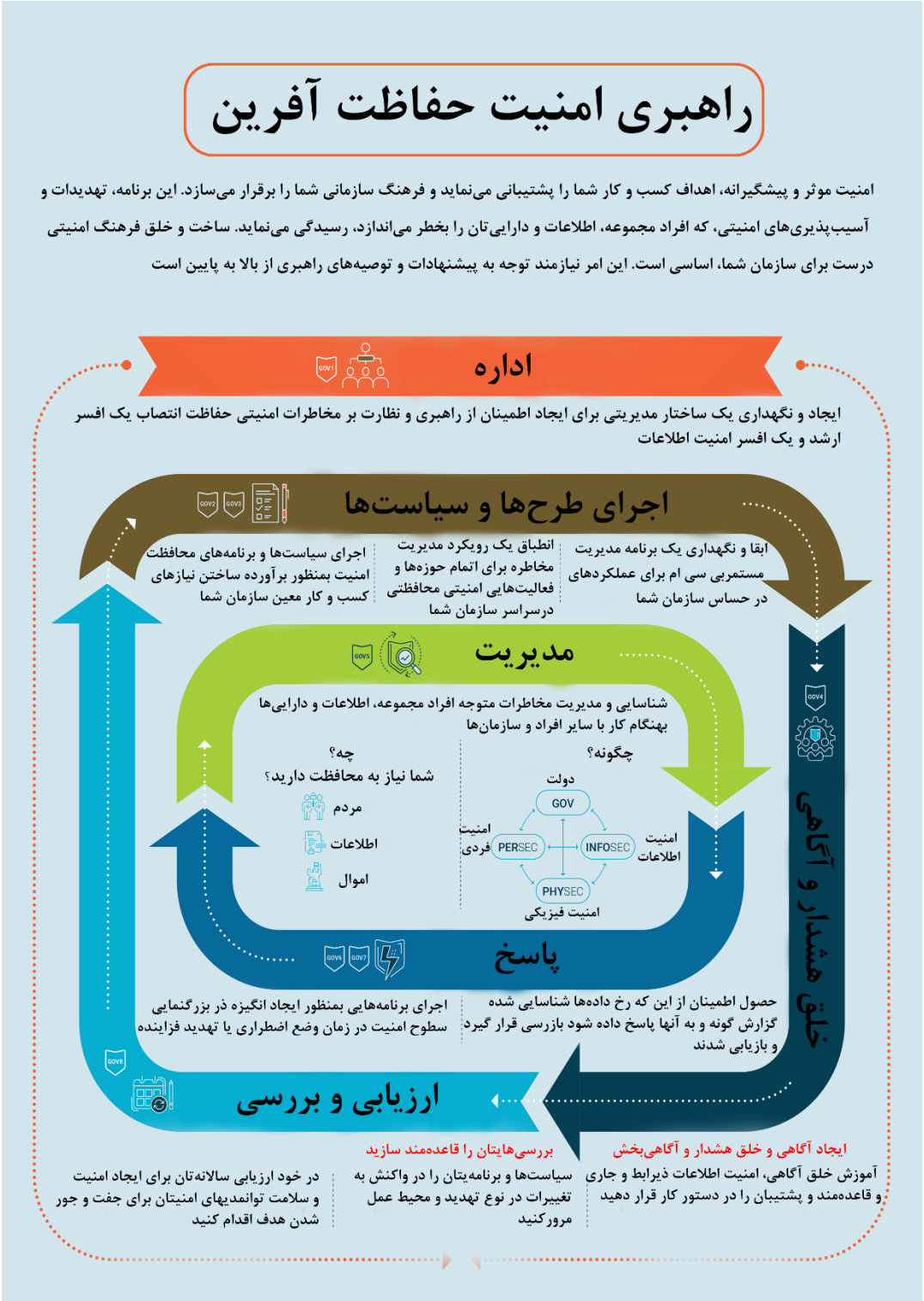
- آگاهی از PSR و سیاست‌ها و رویه‌های امنیتی اعمال شده برای آژانس کارفرمایی شما (به ویژه تعهدات شما که در شرایط و ضوابط قراردادی تعیین شده است)
- درک تأثیر سیاست‌ها و رویه‌های امنیتی آژانس کارفرمایی بر خدمات ارائه شده (خدماتی مانند مدیریت اطلاعات، فناوری اطلاعات و ارتباطات، طراحی و مدیریت امکانات، استخدام پرسنل، خدمات امنیتی عمومی)
- ایجاد یک رابطه کار مثبت با آژانس کارفرمایی خود برای ارتقا ارتباطات آزاد و افزودن ارزش به محیط امنیتی از طریق شناسایی سریع و حل و فصل مسائل.
- بسته به نقش، ممکن است لازم باشد شما یک مجوز امنیت ملی (با حمایت مالی آژانس کارفرمای خود) بدست آورید و آن را حفظ کنید و تعهدات و مسئولیت‌های امنیتی خود را به عنوان یک دارنده ترخیص به روشنی درک کنید.

فصل ۲

حکومت

۲- چرا حاکمیت مهم است

مدیریت خطرات امنیتی به طور متناسب و سازمان‌ها را قادر می‌سازد تا از مردم، اطلاعات و دارایی‌ها محافظت کنند. برای مدیریت موفقیت آمیز خطرات امنیتی، سازمان‌ها باید اطمینان حاصل کنند که امنیت بخشی از فرهنگ سازمانی، رویه‌ها و برنامه‌های عملیاتی آنها است.



۲-۱- الزامات اجباری

الزامات اصلی حکمرانی که آژانس‌های دولتی مأمور باید از آن پیروی کنند و سایر سازمان‌ها باید بهترین روش را در نظر بگیرند.

❖ **حکومتداری صحیح را برقرار و حفظ کنید**

یک ساختار حاکمیتی ایجاد و حفظ کنید که رهبری موفقیت آمیز و نظارت بر خطر امنیت محافظ را تضمین کند.

اعضای تیم بزرگسالان را به عنوان:

- افسر ارشد امنیت(CSO) ، مسئول سیاست امنیتی کلی محافظتی سازمان و نظارت بر اقدامات امنیتی محافظتی.
- افسر ارشد امنیت اطلاعات(CISO)، مسئول امنیت اطلاعات سازمان شما.

❖ **رویکرد مبتنی بر ریسک را در پیش بگیرید**

مطابق با استاندارد نیوزلند ایزو ۳۱۰۰۰: ۲۰۱۸ مدیریت ریسک - رهنمودها، رویکرد مدیریت ریسک را که همه حوزه‌های امنیتی محافظتی را در سازمان شما پوشش می‌دهد، اتخاذ کنید. سیاست‌ها و برنامه‌های امنیتی متناسب با نیازهای تجاری خاص سازمان خود را تدوین و حفظ کنید .اطمینان حاصل کنید که الزامات امنیتی را در همه زمینه‌ها: حاکمیت، اطلاعات، پرسنل و فیزیکی برطرف می‌کنید.

❖ **برای تداوم تجارت آماده شوید**

یک برنامه مدیریت تداوم کسب و کار داشته باشید، تا عملکردهای حیاتی سازمان شما در حین ایجاد اختلال تا حد ممکن ادامه یابد .اطمینان حاصل کنید که برای تداوم منابعی که از عملکردهای حیاتی شما پشتیبانی می‌کنند، برنامه ریزی کرده‌اید.

❖ **ایجاد آگاهی از امنیت**

اطلاعات منظم، آموزش آگاهی از امنیت و پشتیبانی از همه افراد سازمان خود را ارائه دهید، بنابراین آن‌ها می‌توانند الزامات حفاظتی امنیتی را رعایت کرده و سیاست‌های امنیتی سازمان شما را حفظ کنند.

❖ **هنگام کار با دیگران خطرات را مدیریت کنید**

قبل از شروع کار با دیگران که ممکن است بخشی از زنجیره تأمین شما شوند، خطرات موجود در افراد، اطلاعات و دارایی‌های خود را شناسایی و مدیریت کنید.

❖ **مدیریت حوادث امنیتی**

اطمینان حاصل کنید که هر حادثه امنیتی در اسرع وقت شناسایی، گزارش، پاسخ داده شده، مورد تحقیق و بازیابی قرار گرفته است. از انجام اقدامات اصلاحی مناسب اطمینان حاصل کنید.

بتوانید به افزایش سطح تهدید پاسخ دهید

برنامه‌هایی را تدوین کنید و آماده باشید تا در موارد اضطراری یا شرایطی که تهدید بیشتری برای مردم، اطلاعات یا دارایی‌های شما وجود دارد، سطح امنیتی را افزایش دهید.

توانایی خود را ارزیابی کنید

از یک فرآیند ارزیابی مبتنی بر شواهد سالانه برای اطمینان از مناسب بودن توانایی امنیتی سازمان خود استفاده کنید. در صورت درخواست، گزارش اطمینان را از طریق تیم محافظت از امنیت مورد نیاز به دولت ارائه دهید. سیاست‌ها و برنامه‌های خود را هر ۲ سال یا در صورت لزوم تغییر در تهدید یا محیط کار، زودتر مرور کنید.

۲-۲- اجرای رویکرد مبتنی بر ریسک برای امنیت محافظتی

چگونگی تدوین سیاست‌ها، برنامه‌ها و فرآیندهای امنیت حفاظتی را با استفاده از یک رویکرد سازگار و سازگار درک کنید.

❖ **رویکرد مبتنی بر ریسک را در پیش بگیرید**

مطابق با استاندارد نیوزلند ISO 31000: 2018 مدیریت ریسک - رهنمودها، رویکرد مدیریت ریسک را که هر منطقه از امنیت محافظتی را در سازمان شما پوشش دهد، اتخاذ کنید .سیاست‌ها و برنامه‌های امنیتی متناسب با نیازهای تجاری خاص سازمان خود را تدوین و حفظ کنید .اطمینان حاصل کنید که الزامات امنیتی را در همه زمینه‌ها: حاکمیت، اطلاعات، پرسنل و فیزیکی برطرف می‌کنید.

این دستورالعمل‌ها به سازمان شما کمک می‌کند تا:

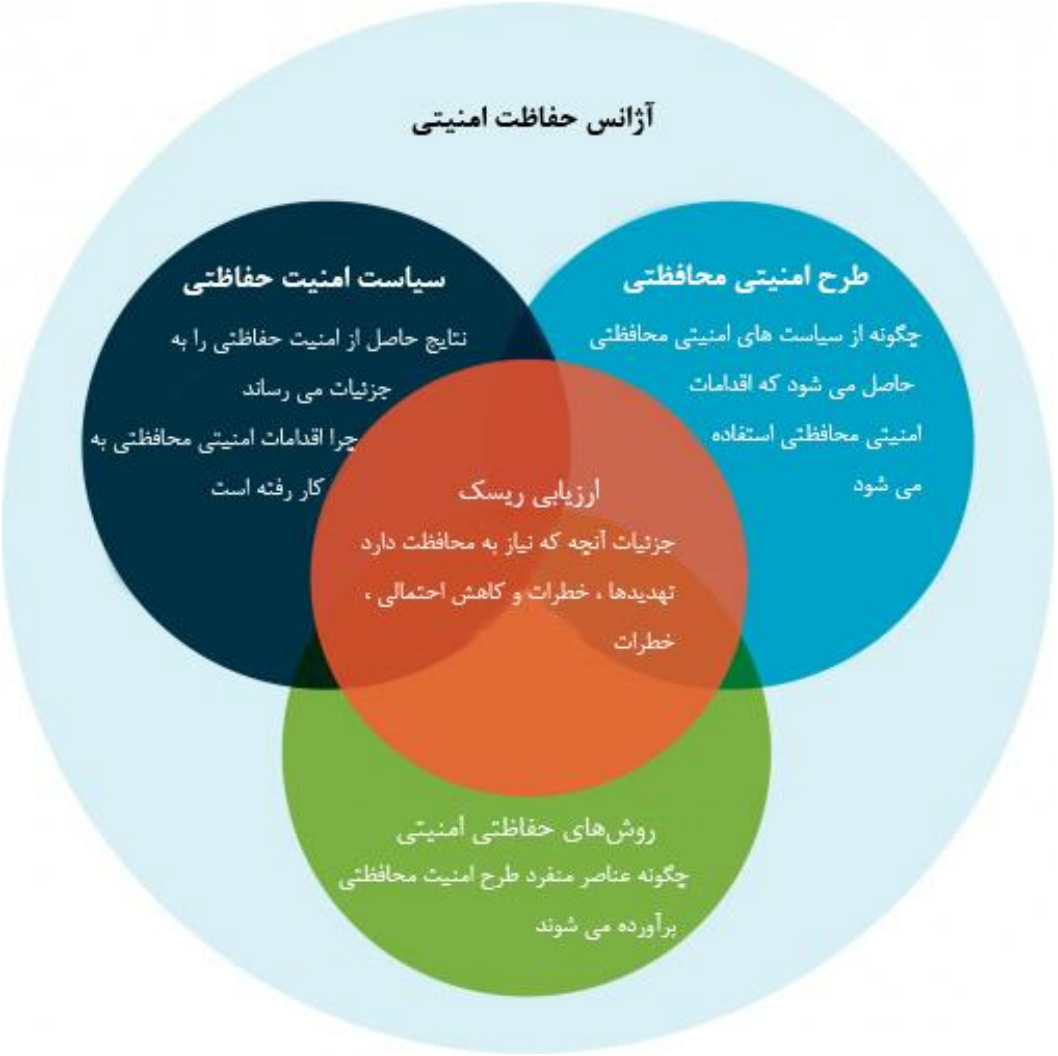
- خطرات امنیتی را مدیریت کنید
- تهدیدهای امنیتی را برآورده کنید
- از مردم، اطلاعات و دارایی محافظت کنید
- به سازمانهای دیگری که با آنها کار می‌کنید اطمینان دهید.

❖ **نحوه تدوین سیاست‌ها، برنامه‌ها و فرایندها - یک نمای کلی**

ابتدا چارچوبی را براساس نیازهای عملیاتی سازمان خود تنظیم کنید. سپس مشخص کنید که از کدام دارایی برای محافظت نیاز دارید - دارایی‌های مورد نیاز برای فعالیت‌های مداوم سازمان یا منافع ملی شامل پرسنل، اطلاعات، دارایی‌های فیزیکی و خدمات باشد. بعد، ارزیابی ریسک را انجام دهید .استفاده از سطوح تاثیر کسب و کار (BILs) برای کمک به شما خطر را ارزیابی کنند BIL .ها ارزیابی سازگار تأثیر را در صورت به خطر افتادن یا از بین رفتن دارایی‌ها امکان پذیر می‌کنند. برای آگاهی از خط مشی‌ها، برنامه‌ها و فرآیندهای خود از ارزیابی ریسک استفاده کنید - تا به شما بگویید کدام اقدامات امنیتی را باید اجرا کنید، چگونه و چه زمانی.

به یاد داشته باشید که سایر سیاست‌ها و نتایج عملیاتی را که می‌تواند تحت تأثیر سیاست‌ها، برنامه‌ها و روندهای شما قرار گیرد، در نظر بگیرید. سیاست‌ها، برنامه‌ها و روندهای خود را در یک سند یا اسناد جداگانه ثبت کنید .اگر می‌خواهید از اسناد جداگانه استفاده کنید، مطمئن شوید که توسعه آنها را هماهنگ می‌کنید. اطمینان حاصل کنید که کل سازمان شما از سیاست امنیتی، برنامه‌ها و فرایندهای شما مطلع است .انتشار آنها در اینترانت و تبلیغ آنها را در نظر بگیرید. آموزش آگاهی از امنیت اطلاعات بیشتری دارد. آن‌ها را مرتباً مرور کنید تا شکاف‌ها را شناسایی کنید و با تغییرات عوامل خطر همراه باشید - حداقل هر ۲ سال.

نمودار ۱ نشان می‌دهد که چگونه سیاست‌ها، برنامه‌ها و فرایندهای شما بهم پیوسته و از طریق ارزیابی ریسک شما مطلع می‌شوند.



❖ **سیاست امنیتی ایجاد کنید که حاکمیت، پرسنل، اطلاعات و دارایی‌ها را پوشش دهد**

سیاست امنیتی محافظ شما دستورالعمل برنامه و پروسه‌های امنیتی محافظتی سازمان را به شما می‌دهد .باید شرایط اجباری PSR را داشته باشد.

رئیس اجرایی / رئیس آژانس یا نماینده آنها باید سیاست امنیتی محافظ شما را تأیید و از اجرای آن حمایت کند .مدیر ارشد امنیتی (CSO) شما باید به طور فعال سیاست را کنترل کند.

سیاست‌های امنیتی محافظتی باید چهار حوزه کلیدی شامل دولت، پرسنل، اطلاعات و امور فیزیکی را شامل شود.

هر خط مشی باید بیان کند که چرا سیاست لازم است و چه کسی آن را مجاز دانسته است .

۲-۱-۱- ترتیبات حکمرانی

ترتیبات حاکمیت نحوه ارتباط امنیت محافظتی با سایرمولفه‌های حاکمیت عملیاتی را شامل می‌شود، از جمله:

- ایمنی عمومی کارمند
- الزامات امنیتی در قراردادها
- تعیین نقش مدیریت امنیت
- سطوح تأثیر تجاری(BILs)

- گزارش حسابرسی و انطباق
- مدیریت ریسک کلاهبرداری
- تهیه و مدیریت اطلاعات دولت خارجی
- فرایندهایی برای استثنائات سیاست
- فرآیندهای بررسی و اصلاح.

۲-۱-۲- سیاست امنیتی پرسنل

اطمینان حاصل کنید که سیاست‌های امنیتی پرسنل شما شامل موارد زیر است:

- بررسی‌های امنیتی برای کارمندان و پیمانکاران
- الزامات ترخیص امنیتی، از جمله مدیریت مجوزهای امنیتی
- دسترسی اضطراری به مواد دارای علامت محافظ
- چگونه حوادث امنیتی را بررسی و مدیریت خواهید کرد.

۲-۱-۳- سیاست امنیت اطلاعات

سیاست امنیت اطلاعات شما باید شامل موارد زیر باشد:

- مارک محافظ اسناد
- دسترسی به ICT و ذخیره سازی
- استفاده از ایمیل و اینترنت
- محاسبه کار از راه دور و تلفن همراه
- حذف اطلاعات از محل سازمان شما
- کنترل اطلاعات سازمان شما در اختیار نهادهای تجاری

کنترل اطلاعات شخصی و تجاری که به نمایندگی از طرف‌های دیگر توسط سازمان‌ها نگهداری می‌شود ایجاد خط مشی برای علامت گذاری محافظ اسناد ، راهنمایی دقیق در مورد این جنبه از سیاست امنیت اطلاعات شما را به شما می‌دهد.

هنگام تدوین سیاست امنیت اطلاعات، باید از منابع زیر به عنوان راهنمای اصلی خود استفاده کنید:

- پروتکل مدیریت امنیت اطلاعات
- کتابچه راهنمای امنیت اطلاعات نیوزلند
- سیستم طبقه بندی امنیتی دولت نیوزیلند
- الزامات رسیدگی به اطلاعات و تجهیزات دارای مارک محافظ

AS / NZS ISO / IEC 27002: 2013 فناوری اطلاعات - تکنیک‌های امنیتی - آیین نامه مدیریت امنیت اطلاعات، بخش ۵.

۲-۳- سیاست امنیت فیزیکی

خط مشی امنیت فیزیکی شما باید آدرس زیر باشد:

- دسترسی افراد، بازدید کنندگان و کودکان به امکانات شما - اگر امکانات مختلف نقش یا خطرات مختلفی داشته باشند، ممکن است به سیاست‌های خاص سایت نیاز داشته باشید

- امنیت و امنیت مردم شما - اطمینان حاصل کنید که سیاست امنیتی شما با سایر سیاست‌های ایمنی شما متناسب است
- دور از دفتر کار کردن
- امنیت فیزیکی اطلاعات شما

❖ برنامه و فرایندهای امنیتی خود را توسعه دهید

برنامه و فرآیندهای امنیتی محافظتی سازمان شما باید خطرات امنیتی را کاهش دهد در حالی که به اشتراک گذاری ایمن اطلاعات امکان پذیر است. فرآیندهای امنیتی محافظتی ممکن است بخشی از برنامه امنیتی شما باشد، یا توصیه مستقل به کارمندان باشد.

برنامه شما باید جامع و دقیق باشد .این را بدست آورید:

- با افراد از هر بخش سازمان خود مشورت کنید
- درگیر کردن کارکنانی که مستقیماً کارهای امنیتی یا مربوطه را مدیریت می‌کنند (به عنوان مثال مدیر ارشد امنیت، رئیس امنیت اطلاعات، مدیر بهداشت و ایمنی، مدیر امنیت فناوری اطلاعات، مدیر حریم خصوصی، مدیران املاک و مدیر امنیتی / مشاوران) هنگام تهیه و بررسی طرح.

همچنین برای اطمینان از موفقیت برنامه، مدیریت ارشد را درگیر کرده و از آنها حمایت کنید.

اهداف یک برنامه امنیتی باید به شرح زیر باشد:

- از ارزیابی ریسک برای شناسایی زمینه‌های خطر امنیتی استفاده کنید
- مراحل عملی را برای به حداقل رساندن خطرات ترسیم کنید.

برای هر یک از سایتهای جداگانه برنامه‌های امنیتی سایت را تهیه کنید.

نحوه طبقه بندی و محافظت از برنامه امنیتی و تأثیر تجاری در صورت به خطر افتادن محرمانه بودن برنامه را به دقت در نظر بگیرید .عناصر جداگانه طرح را در صورت مناسب طبقه بندی کنید.

برنامه امنیتی شما باید چهار حوزه اصلی را شامل شود: امنیت حاکمیت، پرسنل، اطلاعات و دارایی‌های فیزیکی.

❖ ترتیبات حکمرانی

- ترتیبات حکمرانی باید شامل موارد زیر باشد:
- نقش‌ها و مسئولیت‌های امنیتی
- ارائه دهندگان خدمات قرارداد و امنیت شخص ثالث
- برنامه‌های تداوم تجارت و بازیابی بلایا
- اقدامات برای افزایش امنیت در صورت افزایش تهدیدات سازمان شما
- گزارش حوادث و انجام تحقیقات امنیتی
- گزارش حسابرسی و انطباق
- مدیریت ریسک کلاهبرداری
- بررسی و اصلاح.

اگر ترتیبات حاکمیتی برنامه‌های مستقلی است که توسط بخش‌های دیگر سازمان شما مدیریت می‌شود، هنگام تهیه برنامه‌های فردی، با پرسنل مدیریت امنیت خود مشورت کنید.

❖ **ترتیبات امنیتی پرسنل**

ترتیبات امنیتی پرسنل باید شامل موارد زیر باشد:

- مقررات امنیتی پرسنل در فرآیند استخدام، کار با تیم مدیریت منابع انسانی شما
- لیست‌های بررسی و ترخیص امنیت ملی
- گزارش تماس
- مدیریت ترخیص امنیتی
- آموزش مداوم آگاهی از امنیت

❖ **ترتیبات امنیت اطلاعات**

ترتیبات امنیت اطلاعات باید شامل موارد زیر باشد:

- مدیریت اطلاعات در داخل سازمان، در حال حمل و نقل و خارج از دفتر
- بایگانی اطلاعات محافظت شده، با مدیریت سوابق شما کار می‌کند
- دسترسی و ذخیره سازیICT
- امنیت شبکهICT
- محاسبه کار از راه دور و تلفن همراه
- ذخیره اطلاعات و چاپ اطلاعات.

❖ **ترتیبات امنیت فیزیکی**

ترتیبات امنیتی بدنی باید شامل موارد زیر باشد:

- برنامه‌های امنیتی سایت
- امنیت فیزیکی مردم، بازدید کنندگان و مردم، همراه با برنامه‌های ایمنی
- امنیت فیزیکی اطلاعات
- حفاظت از دارایی‌های فیزیکی
- سیستم‌های کنترل دسترسی
- سیستم‌های هشدار امنیتی
- امنیت بازیابی فاجعه یا سایت‌های جایگزین، همراه با برنامه‌های تداوم تجارت
- امنیت فیزیکی برای کار از راه دور و دور از دفتر کار

۴-۲- قالب پیشنهادی برای یک طرح امنیتی

در اینجا عنوان‌ها و بخش‌های پیشنهادی برای برنامه امنیتی سازمان شما آورده شده است.

❖ **پیش گفتار رئیس اجرایی / رئیس سازمان**

اهمیت برنامه ریزی امنیتی را بیان کنید، این طرح را تأیید کنید و نیاز به مدیریت مؤثر ریسک امنیتی را ترسیم کنید.

❖ **بیان هدف و اهداف**

برنامه امنیتی را به خط مشی امنیتی پیوند دهید .نقش و مسئولیت سازمان و اقدامات امنیتی مورد نیاز برای به حداقل رساندن اختلال در عملکرد و منابع آن را مشخص کنید.

❖ **ارزیابی اقدامات امنیتی موجود**

ارزیابی اقدامات امنیتی محافظتی فعلی سازمان و توصیف قرار گرفتن در معرض فعلی و تهدیدهای احتمالی .این ممکن است یک ارزیابی تهدید رسمی باشد.

❖ **بخش**

اصلی بخش اصلی را حداقل به چهار قسمت تقسیم کنید .این قسمت‌ها می‌توانند اسناد جداگانه یا یک پرونده واحد باشند.

اقدامات و استراتژی‌ها :نحوه دستیابی به اهداف و درمان خطرات امنیتی مشخص شده در ارزیابی تهدیدها را بیان کنید.

منابع و مسئولیت‌ها :منابع مورد نیاز و مسئولیت اجرای استراتژی‌ها را شرح دهید.

نتایج دلخواه و شاخص‌های عملکرد :نتایج خود را بیان کنید و اینکه چگونه اهداف تحقق یافته را اندازه گیری می‌کنید .نمونه‌هایی از یک شاخص عملکرد می‌تواند:

- کاهش سطح خطر به مکان‌های فیزیکی
- کاهش تقلب، سرقت، یا تلفات به منابع یا دارایی‌ها.

فرآیندهای مرتبط :شامل فرایندهایی هستند که از طرح پشتیبانی می‌کنند .این فرایندها ممکن است پیوست یا اسنادی مستقل برای افراد شما باشد.

پیوست‌های دیگر ممکن است شامل موارد زیر باشد:

- ارزیابی خطر امنیتی شما
- برنامه‌های سایت
- اسناد سیاست
- صفحه گسترده ردیابی یا نگاشت انطباق
- پیوند به برنامه‌های عملیاتی و انطباق سایر آژانس‌ها.

۵-۲- ایجاد خط مشی برای علامت گذاری محافظ اسناد

با یک سیاست جامع برای علامت گذاری محافظ اسناد، اطلاعات ارزشمند خود را ایمن نگه دارید.

❖ **اهداف سیاست خود را تعیین کنید**

در سیاست خود هدف قرار دهید:

ارزش اطلاعات خود را شناسایی کنید

- تعیین سطح مارک محافظتی مورد نیاز، بر اساس تأثیر در صورت به خطر افتادن محرمانه بودن اطلاعات.

- ضمن اینکه اشتراک اطلاعات را امکان پذیر می‌کند، خطرات موجود در امنیت اطلاعات خود را کاهش دهید
- تعادل نیاز به در دسترس قرار دادن اطلاعات تا حد امکان با محافظت از منافع ملی و امنیت ملی.
- سیاست خود را بر اساس سیستم طبقه بندی امنیتی دولت نیوزیلند قرار دهید.

❖ **به طور گسترده مشورت کنید**

برای اطمینان از اینکه مارک محافظتی شما تا حد ممکن جامع است، با نمایندگان هر بخش از سازمان خود مشورت کنید.

اگر سازمان شما چندین کارکرد داشته باشد، ممکن است برای هر عملکرد به بیش از یک خط مشی یا بخشی از خط مشی خود نیاز داشته باشید.

همچنین ممکن است به سیاست‌هایی برای کمک به شرکای تجاری خود برای علامت گذاری اطلاعات طبقه بندی شده‌ای که از طرف سازمان شما ایجاد می‌کنند، نیاز داشته باشید.

به یاد داشته باشید که آیا بیمه نامه شما به مارک محافظتی احتیاج دارد (کل سیاست یا هر قسمت جداگانه).

❖ **اطلاعات را براساس نوع و آسیب احتمالی گروه بندی کنید**

در خط مشی خود، گروه بندی اطلاعات را بر اساس نوع و آسیب احتمالی در نظر بگیرید تا انتخاب سطح مناسب علامت گذاری محافظ را برای مردم آسان‌تر کند .

نمونه‌هایی از گروه بندی برای انواع اطلاعات عبارتند از:

- اطلاعات مشتری
- اطلاعات مالی
- اطلاعات پرسنل
- اطلاعات پروژه - شما ممکن است پروژه‌هایی را با اهداف یا فرایندهای مشابه گروه بندی کنید.

نمونه‌هایی از گروه بندی برای میزان آسیب احتمالی عبارتند از:

- اشخاص حقیقی
- سازمان‌های
- سازمان شما
- دولت
- منافع ملی یا امنیت ملی.

❖ **یک راهنمای مارک محافظ تهیه کنید**

برای توسعه راهنمایی مناسب، موارد زیر را در نظر بگیرید:

- قابلیت‌های سیستم‌های ICT برای برچسب گذاری، ذخیره و انتقال اطلاعات
- فرایندهای بایگانی شما
- فرآیندهای دفع شما، به دنبال قانون سوابق عمومی ۲۰۰۵
- چگونه از یکپارچگی اطلاعات محافظت خواهید کرد
- که مسئول و مسئول مواد محافظت شده خواهد بود.

الزامات رسیدگی به اطلاعات و تجهیزات دارای مارک محافظ دارای اطلاعات بیشتری است.

❖ **بگویید کدام اطلاعات نیاز به علامت گذاری دارد**

- در راهنمای خود، خلاصه‌ای از انواع اطلاعاتی را که نیاز به علائم محافظ دارند، بر اساس:
- تأثیر در صورت محرمانه بودن رازداری
- نگرانی‌های حساسیت خاص که نیاز به تأیید و یا علامت گذاری‌های محفظه‌ای دارند
- هرگونه مقررات مربوط به رازداری قانونگذاری.
- به یاد داشته باشید که فرایندی را برای اطلاعات تولید شده از اطلاعات دارای علامت محافظتی که از منابع دیگر به دست آمده است، قرار دهید .در مورد:
- علامت گذاری اطلاعات در همان سطح یا بالاتر از آنچه دریافت شده است
- درخواست اجازه استفاده از اطلاعات در سطح پایین‌تر.

شما همچنین به یک فرآیند برای اطلاعات دولت‌های خارجی نیاز دارید. رسیدگی باید به موجب توافق با دولت خارجی صورت گیرد.

❖ **نحوه اعمال علائم محافظ را بیان کنید**

دستورالعمل‌هایی را برای نحوه استفاده از علائم محافظ به موارد زیر ارائه دهید:

- اسناد از طریق الگوها یا به صورت دستی
- پرونده‌ها در سیستم مدیریت سوابق شما
- ابرداده سند در سیستم‌های مدیریت سوابق الکترونیکی شما
- ایمیل‌ها (شامل انواع اطلاعاتی که می‌توان از طریق ایمیل ارسال کرد و برای چه کسی)

نحوه استفاده از چارچوب‌های زمانی را برای اطلاعات خاص رویداد در نظر بگیرید.

❖ **فرآیند بازبینی و محرمانه سازی را وارد کنید**

فرایندهایی برای بررسی و طبقه بندی اطلاعات دارای علامت محافظ داشته باشید.

بایگانی کردن اطلاعات دارای علامت محافظ می‌تواند هزینه‌های بالای اداری و مالی ایجاد کند .همانطور که تأثیر بیشتر اطلاعات با گذشت زمان تغییر می‌کند، شما باید فرایندهایی برای بررسی علائم محافظ داشته باشید.

❖ **در صورت لزوم دستورالعمل‌های دیگری اضافه کنید**

اگر در جاهای دیگر فرآیندهای امنیت اطلاعات شما گنجانده نشده است، موارد زیر را پوشش دهید:

- مشاوره ذخیره سازی، از جمله ذخیره سازی در سازمان شما و ارائه دهندگان خارجی
- نحوه انتقال اطلاعات به آژانس‌های دیگر
- فرآیندهای تخریب شما (مطابق با قانون سوابق عمومی ۲۰۰۵)، از جمله مکان‌های خرد کن و سطل آشغال و نحوه استفاده صحیح از آنها

۶-۲- نقش‌ها و مسئولیت‌های امنیتی محافظتی

رهنمودهایی برای برنامه ریزی و تعیین مسئولیت‌ها برای امنیت محافظتی.

❖ **هدف**

هنگام برنامه ریزی و تعیین مسئولیت‌هایی برای امنیت محافظ، از این راهنما استفاده کنید .

این شامل اطلاعات مربوط به نقش در سازمان شما و در سراسر دولت و همچنین سیاست‌های امنیتی است.

❖ **این اطلاعات برای چه کسانی است**

این اطلاعات در درجه اول برای مدیران ارشد، افسران ارشد امنیتی و پزشکان امنیتی است .این همچنین یک مرجع مفید برای پیمانکارانی است که توصیه‌های امنیتی محافظتی را ارائه می‌دهند.

❖ **الزامات قانونی**

در مواردی که الزامات قانونی بالاتر از کنترل‌های مشخص شده در الزامات امنیتی محافظتی باشد، الزامات قانونی مقدم است و باید اعمال شود.

- سیاست امنیتی در سازمان شما
- چرا سیاست امنیتی مهم است

استفاده مناسب از اقدامات امنیتی محافظتی توسط نهادهای دولتی، فضای عملیاتی لازم برای انجام مطمئن و مطمئن تجارت دولتی را تضمین می‌کند.

مدیریت خطرات امنیتی به طور متناسب سازمان‌های دولتی را قادر می‌سازد تا از مردم، اطلاعات و دارایی محافظت کنند.

۲-۱-۴- مسئولیت کلی امنیت محافظتی

دولت مسئول امنیت حفاظتی نیوزیلند است .روسای آژانس‌ها مسئول تأمین امنیت نمایندگی‌های خود هستند.

روسای آژانس مسئول حفاظت از عملکرد آژانس، منابع رسمی، کارمندان (از جمله پیمانکاران) و بازدید کنندگان هستند.

یک رئیس آژانس می‌تواند کتباً هر یک از اختیارات یا کارکردهای تعیین شده در PSR را به شخص دیگری واگذار کند اما مسئولیت کلی آن را برای امنیت آژانس حفظ کند.

۲-۱-۵- اصول امنیتی محافظ

هر رئیس آژانس مسئول ایجاد و حفظ محیط مناسب برای:

- از مردم و مشتریان در برابر خطرات قابل پیش بینی محافظت کنید
- تسهیل به اشتراک گذاری مناسب اطلاعات رسمی برای دولت برای انجام کار مؤثر
- محدود کردن پتانسیل برای به خطر انداختن رازداری، صداقت و در دسترس بودن اطلاعات و دارایی‌های رسمی آن، شناسایی خطرات مانند خطرات مرتبط با تجمیع اطلاعات
- دارایی‌های رسمی را از دست دادن یا سو استفاده محافظت کنید
- بدون در نظر گرفتن اختلالات ناشی از انواع خطرات، از ادامه تحویل مشاغل اساسی آژانس حمایت کنید.

روسای آژانس‌ها باید خطرات امنیتی را درک، اولویت بندی و مدیریت کنند تا از آسیب رساندن به منابع رسمی و ایجاد اختلال در اهداف تجاری جلوگیری کنند .امنیت محافظتی و مدیریت تداوم کسب و کار زیربنای انعطاف پذیری سازمانی است.

آژانس‌ها باید اطمینان حاصل کنند که امنیت بخشی از فرهنگ سازمانی، رویه‌ها و برنامه‌های عملیاتی آنها است.

روسای آژانس‌ها مسئول اجرای و مدیریت سیاست امنیتی در آژانس‌های خود هستند.

آن‌ها باید محیط‌های امنیتی مناسبی را ایجاد کنند و از آنها محافظت کافی از پرسنل، اطلاعات رسمی، تجهیزات دارای علامت محافظ و سایر دارایی‌ها را محافظت کنند. سطح حفاظت باید با سطح ارزیابی شده خطر مطابقت داشته باشد.

امنیت محافظتی معمولاً شامل اقدامات زیر است:

- امنیت پرسنل
- امنیت فیزیکی
- امنیت اطلاعات، از جمله امنیت فناوری اطلاعات و ارتباطات.(ICT)

PSR کنترل‌های اجباری، الزامات انطباق و مشاوره در مورد بهترین روش را ارائه می‌دهد. یک محیط امنیتی مناسب نیاز به یک رویکرد سیستماتیک و هماهنگ دارد. آژانس‌های دولتی مسئول ارائه مشاوره امنیتی ممکن است اسناد خاص خود را (راهنمای ردیف چهار) برای تکمیل PSR تهیه کنند.

یک آژانس ابتدا باید محیط خطر خود را شناسایی و ارزیابی کند، سپس یک طرح امنیتی تهیه کند .برای اثربخشی، برنامه ریزی برای مدیریت خطرات امنیتی باید به بخشی جدایی ناپذیر از فرهنگ آژانس تبدیل شود. امنیت باید در فلسفه، اقدامات و برنامه‌های آژانس ادغام شود .باید به جای یک فعالیت جداگانه، به عنوان یک فعال کننده تجارت رفتار شود .همه مدیران باید تشویق شوند که مدیریت ریسک را بشناسند و اقدامات صحیح امنیتی بخشی اساسی از مدیریت است.

در حالی که برنامه امنیتی هر آژانس ارتباط مستقیمی با فرهنگ، محیط، موقعیت جغرافیایی، عملکردها و ساختار شرکتی آن دارد، اما همه آژانس‌های دولتی باید تعهد خود را نسبت به سیاست امنیتی دولت، اصول و حداقل استانداردها نشان دهند.

۲-۱-۶- سند سیاست امنیتی

رئیس آژانس باید یک سیاست امنیتی را تصویب، منتشر و اجرا کند که رویکرد و تعهد مدیریت در مورد امنیت را مشخص کند.

چارچوب امنیتی سیاست باید:

- مبتنی بر تجزیه و تحلیل خطر قوی است
- پشتیبانی عملیات آژانس و تداوم تجارت
- در عین تأمین امنیت کافی عملی و قابل استفاده باشد
- مقرون به صرفه باشد

سیاست امنیتی آژانس باید شامل موارد زیر باشد:

- راهنمایی درباره نقشها و مسئولیتهای امنیتی
- تعاریف روشنی از فرآیندهای امنیتی
- در صورت لزوم، راهنمایی دقیق‌تر برای سایت‌ها، سیستم‌ها یا خدمات منفرد
- تعاریف روشنی از مسئولیت استفاده از مواد محافظت شده علامت گذاری شده، چه به صورت الکترونیکی و چه به صورت نسخه چاپی
- برنامه مداوم آگاهی و آموزش کاربر.

۲-۱-۷- بررسی و ارزیابی

فرآیند بررسی خط مشی باید توسط هرگونه تغییر تأثیرگذار بر اساس ارزیابی اصلی خطر امنیتی ایجاد شود.

به عنوان مثال، پس از:

- حوادث امنیتی قابل توجه
- معرفی آسیب پذیری های جدید
- تغییر در عملکردهای آژانس، ساختار یا زیرساخت‌های فنی.

برنامه ریزی بررسی‌های دوره‌ای از:

- اثربخشی سیاست، اندازه گیری شده توسط ماهیت، تعداد و تأثیر حوادث امنیتی ثبت شده
- هزینه و تأثیر کنترل‌های امنیتی
- اثرات آن بر سیاست تغییرات فناوری
- سطح انطباق کاربر

۲-۷- نقش‌ها و مسئولیت‌ها در سازمان شما

❖ **مسئولیت‌های شما**

هر آژانس باید یک رویکرد امنیتی روشن با تخصیص واضح مسئولیت برای همه جنبه‌های امنیتی داشته باشد.

روسای آژانس در مورد کلیه جنبه‌ها و عناصر امنیتی در آژانس خود مسئول و پاسخگو هستند.

دولت از روسای سازمان‌ها می‌خواهد برنامه‌های امنیتی محافظتی داشته باشند که تضمین می‌کند:

- ظرفیت آژانس آنها برای عملکرد
- مردم می‌توانند به دولت اعتماد داشته باشند
- منابع رسمی و اطلاعاتی که دولت به مردم اعتماد و اعتماد دارد، و افرادی که سایر کشورها با اطمینان ارائه می‌دهند، محافظت می‌شوند
- ایمنی افراد شاغل برای انجام وظایف دولت و کسانی که مشتری دولت هستند.

هر آژانس باید یک ساختار امنیتی با تخصیص واضح مسئولیت در مورد همه جنبه‌های امنیتی داشته باشد .

۲-۱-۸- افسر ارشد امنیت

مسئولیت کلی امنیت باید به یک شخص ارشد منصوب شود به عنوان CSO که مسئول امور مربوط به امنیت باشد و به آن دسترسی آزاد داشته باشد.

برای اکثر آژانس‌ها، نقش نهادهای مدنی سازمان به جای یک موقعیت تمام وقت، علاوه بر پاره وقت، به نقش ارشد موجود نیز اضافه می‌شود.

مسئولیت‌های CSO شامل موارد زیر است:

- نظارت بر امنیت محافظ آژانس
- گردش و اجرای سیاست امنیتی محافظتی
- ارائه راهنمایی به رئیس آژانس در امور امنیتی
- مدیریت و گزارش حوادث امنیتی
- اجرای یک برنامه آگاهی از امنیت

- ارتباط با آژانس‌های امنیتی در رابطه با الزامات امنیتی محافظتی

در مواردی که اندازه آژانس اجازه می‌دهد، سازمان امنیت اجتماعی نباید مسئولیت عملیاتی خدمات شرکتی مانندICT ، منابع انسانی یا امور مالی را بر عهده داشته باشد، اطمینان حاصل کند که این سازمان می‌تواند مشاوره و اطمینان مستقلی را در آژانس ارائه دهد.

بسته به اندازه آژانس، مشخصات ریسک و مقدار مواد محافظتی نگهداری شده و تجهیزات مورد استفاده توسط آژانس، ممکن است لازم باشد یک واحد امنیتی محافظتی تخصصی ایجاد شود و / یا کارکنان امنیتی متخصصی که از CSO گزارش می‌دهند و یا از آن حمایت می‌کنند منصوب شوند.

پرسنل امنیتی و / یا واحد امنیتی محافظ باید در همکاری نزدیک با سایر واحدهای تجاری همکاری کنند تا اطمینان حاصل شود که الزامات امنیتی به طور مناسب مدیریت می‌شود. در صورت لزوم، برای مثال، مدیر امنیت فناوری اطلاعات باید پرسنل امنیتی غیر از سازمان امنیت داخلی به عنوان مدیر امنیتی یا افسر با توصیف نقش متخصص تعیین شوند. در همه موارد، وظایف مربوط به امنیت باید به طور واضح انجام شود.

۲-۱-۹- کمیته‌های امنیتی

در آژانس‌های بزرگ‌تر ممکن است لازم باشد که یک گروه متشکل از نمایندگان مدیریت برای هماهنگی کنترلهای امنیتی تشکیل شود .این گروه باید به عنوان گروه مرجع امنیت (SRG) تعیین شود .متناوباً نقش SRG ممکن است توسط کمیته خطر و ممیزی موجود یا معادل آن تأمین شود.

CSOو / یا SRG باید:

- در مورد نقش‌ها و مسئولیت‌های خاص برای امنیت در سراسر سازمان توافق کنید
- اطمینان حاصل کنید که امنیت محافظتی در فرایندهای مدیریت ریسک، حسابرسی و اطمینان آژانس ادغام شده است
- در مورد روش‌ها و فرآیندهای خاص برای امنیت، مانند روش‌های ارزیابی ریسک
- سیستم‌هایی برای علامت گذاری محافظ اطلاعات و دارایی‌ها
- ارزیابی و هماهنگی اجرای کنترلهای امنیتی خاص برای سیستمها یا خدمات جدید
- حوادث امنیتی را بررسی کرده و بهبودهای مناسب را پیشنهاد دهید
- از ابتکارات امنیتی در کل سازمان مانند برنامه‌های آگاهی حمایت کنید
- اطمینان حاصل کنید که در دسترس بودن پشتیبانی داخلی به خوبی تبلیغ شده است.

۲-۸- نقش‌ها و مسئولیت‌ها در سراسر دولت

❖ مسئولیت‌های شما

هر آژانس دولتی مسئول تدوین و اجرای ترتیبات امنیتی حفاظتی خود مطابق با PSR است.

موفقیت این سیستم به موارد زیر بستگی دارد:

- ترتیبات امنیتی در داخل هر آژانس
- توافق نامه‌های بین آژانس در مورد سیاست‌های امنیتی و حداقل استانداردهای مشترک
- دسترسی آژانس‌ها به سوابق اطلاعات امنیتی و مشاوره تخصصی در مورد مسائل خاص امنیتی.

برای کمک به آژانس‌ها در انجام این مسئولیت، تعدادی از آژانس‌ها و کمیته‌های امنیتی در مورد سیاست‌های امنیتی تصمیم گیری می‌کنند، مشاوره می‌دهند و راهنمایی می‌کنند .

۲-۱-۱۰- کمیته‌های مسئول امنیت حفاظتی

کمیته‌های زیر مسئولیت‌های امنیتی محافظتی دارند:

- هیئت امنیت و اطلاعات(SIB)
- کمیته امنیت ارتباطات دولتی .(GCSC)

برای اطلاعات بیشتر، به - DPMC سیستم امنیت ملی نیوزیلند مراجعه کنید

۲-۱-۱۱- هیئت امنیت و اطلاعات(SIB)

هدف شورای امنیت و اطلاعات (SIB) ایجاد یک بخش امنیتی و اطلاعاتی با عملکرد بالا، منسجم و مؤثر از طریق حاکمیت مناسب، همسویی و اولویت بندی سرمایه گذاری، سیاست و فعالیت است .این موضوع بر تهدیدات خارجی و مسائل اطلاعاتی متمرکز است.

SIBتوسط معاون رئیس اجرایی امنیت و اطلاعات وزارت نخست وزیر و کابینه اداره می‌شود .عضویت در SIB شامل مدیران ارشد وزارت نخست وزیر و کابینه، دفتر امنیت ارتباطات دولت، وزارت امور خارجه و تجارت، وزارت دفاع، گمرک نیوزلند، نیروی دفاعی نیوزلند، پلیس نیوزلند، و سرویس اطلاعات امنیتی نیوزلند .در صورت لزوم، رئیس می‌تواند از سایر رئیسان اجرایی یا مقامات دعوت شود تا در جلسات SIB شرکت کنند. شرایط مرجع SIBدر منابع مرجع SIBبه تفصیل آورده شده است .

۲-۱-۱۲- کمیته امنیت ارتباطات دولتی(GCSC)

GCSCمسئول تدوین و بررسی دکترین و استانداردهای امنیت ارتباطات نیوزلند است. عضویت کمیته اصلی GCSC ازGCSB ، MFAT، NZDFو NZSIS حاصل می‌شود .نمایندگان اضافی ممکن است در صورت لزوم از سایر ادارات دولتی انتخاب شوند. شرایط مرجع GCSC در شرایط مرجع GCSC شرح داده شده است.

۲-۱-۱۳- آژانس‌های ارائه دهنده اطلاعات، استانداردهای فنی و مشاوره امنیتی محافظ

آژانس‌های زیر مشاوره تخصصی در مورد اطلاعات، استانداردهای فنی و / یا امنیت محافظتی ارائه می‌دهند.

❖ **سرویس اطلاعات امنیتی نیوزلند**

– www.nzsis.govt.nz

NZSISاستانداردهای امنیت فیزیکی و پرسنلی را طبق مجوز قانون اطلاعات و امنیت سال ۲۰۱۷ تعیین می کند . NZSIS در مورد موضوعات مربوط به جاسوسی، مداخله خارجی، خشونت با انگیزه سیاسی، خشونت جمعی، خرابکاری، حمله به سیستم دفاعی نیوزلند و تهدیدهای جدی برای یکپارچگی مرز نیوزلند اقدام به جمع آوری، تحلیل و مشاوره می‌کند. NZSISدولت را در مورد موارد نگران کننده در اثر عملیات جمع آوری اطلاعات مطلع می‌کند.

بنا به درخواست آژانس‌های دولتی، NZSISبرای دسترسی به مواد دارای علامت محافظ، پرسنلی را که نیاز به مجوزهای امنیتی ملی دارند، کنترل می‌کند.

❖ **اداره امنیت ارتباطات دولتی(GCSB)**

– www.gcsb.govt.nz

GCSB مرجع ملی امنیت سیستم‌های اطلاعاتی است .در چارچوب دولت، این حفاظت از اطلاعات رسمی در برابر افشای غیرمجاز، دستکاری، تخریب یا تغییر است .این ارتباطات، امنیت فنی و رایانه را در بر می‌گیرد. GCSB به طور مستمر محیط تهدید را رصد می‌کند و تحقیقاتی را در مورد تأثیر امنیتی روندهای نوظهور انجام می‌دهد.

مسئولیت‌های GCSB شامل موارد زیر است:

- سیاست امنیت ملی اطلاعات و استانداردهای دولت را به گردش در می‌آورد
- مشاوره دادن به آژانسهای دولتی در مورد اعمال سیاستها و استانداردهای ملی امنیت اطلاعات
- ارائه خدمات بازرسی امنیت اطلاعات برای دولت
- ارائه برنامه آموزش و آموزش امنیت اطلاعات برای پرسنل دولت

❖ **وزارت امور خارجه و تجارت(MFAT)**

– www.mfat.govt.nz

- MFAT مسئول حفاظت و ارتقا منافع نیوزیلند در خارج از کشور است.
- MFAT منبع اصلی مشاوره دولت در زمینه سیاست خارجی و تجاری و مسائل دیپلماتیک و کنسولی است.

در سطح بین المللی، MFATتلاش می‌کند تا امنیت و منافع اقتصادی نیوزیلند پیشرفته و محافظت شود و از حقوق و ایمنی نیوزیلندی‌های خارج از کشور محافظت شود.

❖ **پلیس نیوزیلند**

– www.police.govt.nz

پلیس نیوزیلند وظایفی در برقراری صلح، حفظ امنیت عمومی، اجرای قانون، پیشگیری از جرم، حمایت و اطمینان جامعه، امنیت ملی، مدیریت اضطراری و مشارکت در فعالیت‌های پلیس خارج از نیوزیلند دارد.

❖ **دفتر کمیسر حفظ حریم خصوصی**

– www.privacy.org.nz

دفتر کمیسر حفظ حریم خصوصی برای توسعه و ترویج فرهنگی که در آن اطلاعات شخصی محافظت و احترام می‌گذارد، تلاش می‌کند. کمیسر رازداری در مورد چگونگی جمع آوری، استفاده، ذخیره و افشای اطلاعات شخصی و آزادی اطلاعات نظارت و مشاوره می‌دهد.

❖ **دفتر حسابرس کل(OAG)**

– www.oag.govt.nz

حسابرس کل مسئول کار حسابرسی و اطمینان بخشی برای بهبود عملکرد و اعتماد عمومی به بخش دولتی است.

❖ **وزارت دادگستری**

– www.justice.govt.nz

وزارت دادگستری برای ایجاد نیوزلند منصفانه و مطمئن‌تر، اجرای قوانین و کمک به سیستم عدالت معتبر و مؤثر وجود دارد.

❖ **افسر ارشد دیجیتال دولت(GCDO)**

– www.digital.govt.nz

GCDOکه قبلاً مدیر ارشد اطلاعات دولت GCIO نامیده می‌شد (به عنوان رهبر عملکردی ICT دولت، مسئول تحولات ICT در ارگان‌های دولتی برای ارائه خدمات بهتر به شهروندان است.

❖ **انجمن امنیت نیوزیلند(NZSA)**

- www.security.org.nz

NZSAسازمانی مستقل است که برای ارتقا a صنعت امنیت حرفه‌ای تأسیس شده است. NZSA حداقل استانداردها را برای اعضای خود که در کدهای عملی آن منتشر شده است تعیین می‌کند (همچنین برای افراد غیر عضو نیز در دسترس است) برنامه‌های آموزش و آموزش امنیت را توسعه می‌دهد تماس با آژانس‌های بین المللی مشابه را تقویت می‌کند.

❖ **انجمن امنیت صنعتی آمریکا (NZ) شرکت(ASIS)**

- www.asis.org.nz

ASIS با توسعه برنامه‌ها و مطالب آموزشی که علایق گسترده امنیتی و همچنین موضوعات خاص امنیتی را برطرف می‌کند، به افزایش کارایی و بهره وری متخصصان امنیتی اختصاص دارد. ASIS همچنین از نقش و ارزش حرفه مدیریت امنیت برای تجارت، رسانه‌ها، نهادهای دولتی و مردم حمایت می‌کند.

۹-۲- نقش‌ها و مسئولیت‌های امنیت اطلاعات

روسای آژانس‌ها، افسران ارشد امنیت اطلاعات(CISO) ، مدیران امنیت فناوری اطلاعات(ITSM) ، دارندگان سیستم و کاربران سیستم همه در اطمینان از قوی بودن امنیت اطلاعات نقش دارند .این بخش مسئولیت‌های افراد در این نقش‌ها را به طور خلاصه شرح داده و توصیف می‌کند.

وقتی کلمه "باید" را می‌بینید، به این معنی است که وظیفه یا فعالیت بهترین روش است .وقتی کلمه "باید" را می‌بینید، به معنی اجباری بودن کار یا فعالیت است .امنیت اطلاعات زمانی قوی‌تر است که شما بهترین عملکردها و وظایف و فعالیت‌های اجباری را با هم ترکیب کنید.

۲-۱-۱۴- مسئولیت کلی با رئیس سازمان است

اگر رئیس آژانس هستید، در مورد امنیت اطلاعات آژانس خود پاسخگو هستید .شما همچنین مرجع اعتباربخشی سازمان خود هستید. **توجه:** ممکن است مسئول یک سازمان عنوان دیگری داشته باشد .به عنوان مثال، مدیر ارشد اجرایی (مدیر عامل)، مدیر کل، مدیر یا موارد مشابه.

❖ **مرجع اعتباربخشی را با دقت تفویض کنید**

هنگامی که تصمیم می‌گیرید مرجع اعتباربخشی خود را تفویض کنید، باید تمام ریسک‌های مرتبط را با دقت در نظر بگیرید، زیرا مسئولیت تصمیماتی که نماینده شما می‌گیرد، باقی می‌ماند. نماینده شما باید یک مدیر ارشد باشد و دارای دانش تخصصی در زمینه امنیت اطلاعات و مدیریت ریسک امنیتی، ترجیحاً مدیر ارشد امنیت اطلاعات (CISO) شما باشد.

اگر نماینده شما CISO نباشد، حداقل باید عضو تیم اجرایی ارشد یا در یک سمت مدیریتی معادل باشد. اگر اختیارات خود را به یک هیئت، کمیته یا هیئت واگذار کنید، الزامات این بخش در مورد رئیس یا رئیس آن نهاد اعمال می‌شود.

❖ **وقتی سازمان شما کوچک است و وظایف نمی‌توانند کاملاً تفکیک شوند**

اگر به دلیل بزرگی سازمان خود نمی‌توانید تمام تفکیک وظایف را برآورده کنید، باید اطمینان حاصل کنید که تعارض منافع بالقوه به وضوح شناسایی، اعلام و به طور فعال مدیریت می‌شود.

❖ **از امنیت اطلاعات در سراسر سازمان خود پشتیبانی کنید**

بدون حمایت کامل شما، افراد شما ممکن است به منابع و اختیار کافی برای اجرای موفقیت آمیز امنیت اطلاعات در سازمان شما دسترسی نداشته باشند. اگر حادثه‌ای، نقض یا افشای اطلاعات رسمی یا طبقه بندی شده در شرایط قابل پیشگیری رخ دهد، در نهایت پاسخگو خواهید بود.

۲-۱-۱۵- امنیت اطلاعات را هدایت و نظارت می‌کند

نقش CISO بر اساس اقدامات خوب در صنعت امنیت و حاکمیت است .این نقش اطمینان از مدیریت امنیت اطلاعات در سطح مدیریت ارشد را تضمین می‌کند .بدونCISO بعید است که سازمان شما بتواند به طور مؤثر امنیت اطلاعات را مدیریت کند.

❖ **مسئولیت‌های سطح بالایCISO**

CISO شما، اگر یکی از آنها را دارید، دارای مسئولیت‌های سطح بالا زیر است .

❖ **اطمینان از جریان ارتباطات از اهداف امنیتی پشتیبانی می‌کند**

CISO شما ارتباط بین امنیت، ICT و پرسنل تجاری را تضمین می‌کند تا از امنیت اهداف سازمان شما همسو باشد.

این مسئولیت ارتباطی شامل موارد زیر است:

- تفسیر مفاهیم و اطلاعات امنیت اطلاعات به مفاهیم و زبان تجاری
- اطمینان از اینکه تیم‌های تجاری با تیم‌های امنیت اطلاعات برای تعیین اقدامات امنیتی مناسب هنگام برنامه ریزی پروژه‌های جدید تجاری مشورت می‌کنند.

❖ **ارائه راهنمایی استراتژیک**

CISOشما راهنمایی استراتژیک در مورد امنیت اطلاعات را ارائه می‌دهد. آن‌ها مسئول این موارد هستند:

- برنامه امنیت اطلاعات سازمان خود را در سطح استراتژیک توسعه دهید
- مدیریت کلی امنیت اطلاعات در سازمان شما.

❖ **اطمینان از مطابقت سازمان شما با الزامات**

CISOشما مطابقت سازمان شما را با موارد زیر تضمین می‌کند:

- سیاست ملی، استانداردها، مقررات و قوانین امنیتی امنیت اطلاعات
- سیاست‌ها و استانداردهای داخلی برای امنیت اطلاعات.

❖ **اطمینان حاصل کنید که آموزش اجرا شده است**

CISOشما اطمینان حاصل می‌کند که یک برنامه آموزش و آگاهی از امنیت اطلاعات تهیه و حفظ می‌شود.

❖ **پرسنل امنیت اطلاعات را رهبری کنید**

- نظارت بر مدیریت پرسنل امنیت اطلاعات در سازمان شما.

❖ **مشاوره و هماهنگی**

CISOشما در بهترین حالت قرار دارد:

- به رهبران پروژه ICT در جهت استراتژیک امنیت اطلاعات در سازمان خود مشاوره دهید

- توصیه‌ای را به مرجع اعتباربخشی در مورد پذیرش خطرات باقیمانده مرتبط با عملکرد سیستم‌های سازمان خود ارائه دهید
- استفاده از منابع امنیت اطلاعات خارجی را برای اطمینان از اینکه رویکرد سازگار در سازمان شما اعمال می‌شود، هماهنگ کنید.

❖ **مسئولیت‌های سازمان شما با نقش CISO**

بودجه امنیت اطلاعات خود را کنترل کنید تا اطمینان حاصل کنید که CISO بودجه کافی برای حمایت از پروژه‌ها و ابتکارات امنیت اطلاعات را دارد. انتظار نداشته باشید CISO شما لزوماً یک متخصص فنی در زمینه امنیت اطلاعات باشد .بلکه انتظار داشته باشید که آنها از دانش خود در مورد استانداردهای ملی و بین المللی و اقدامات خوب برای برقراری ارتباط با کارشناسان فنی سازمان شما استفاده کنند.

❖ **تعیین CISO**

سازمان شما باید CISO را تعیین کند یا این نقش را به شخصی که از قبل در سازمان شما کار می‌کند اختصاص دهد.

شخصی که شما برای CISO منصوب می‌کنید باید:

- عضو تیم اجرایی ارشد خود یا یک سمت مدیریت معادل باشید (نیازی به ایجاد موقعیت اختصاصی جدید ندارید)
- از مهارت و تجربه کافی برخوردار باشد تا بتواند مسئولیت پذیری و اعتبار را به مدیریت امنیت اطلاعات برساند
- گزارش مستقیماً به رئیس آژانس در مورد مسائل امنیت اطلاعات در داخل سازمان.

قبل از اینکه CISO نقش خود را شروع کند، سازمان شما باید:

- آن‌ها را برای دسترسی به تمام اطلاعات طبقه بندی شده پردازش شده در سیستم‌های سازمان خود پاک کنید
- بتوانید آنها را در مورد هرگونه اطلاعات مختصر در سیستم‌های سازمان خود مختصر کنید.

❖ **مدیریت تعارض منافع**

اگر CISO شما نقش دیگری داشته باشد، مانند اینکه شما مدیر ارشد اطلاعات (CIO) یا مدیر یک واحد تجاری باشید، ممکن است در صورت مغایرت الزامات عملیاتی با الزامات امنیتی، تضاد منافع ایجاد شود .تمرین خوب این نقش‌ها را از هم جدا می‌کند.

هنگامی که CISO شما دارای چندین نقش است، شما باید:

- تعارضات بالقوه منافع را به وضوح شناسایی کنید
- اجرای مکانیزمی برای تصمیم گیری مستقل در مناطقی که ممکن است درگیری رخ دهد.

اگر سازمان شما عملکرد CISO را برون سپاری می‌کند ، باید تعارض منافع، در دسترس بودن و زمان پاسخگویی را شناسایی و با دقت مدیریت کنید تا سازمان شما در معرض آسیب نباشد .هنگام معامله CISO با سایر فروشندگان، در مورد تعارض منافع احتمالی هوشیار باشید.

❖ **مسئولیت‌های شما به عنوان CISO**

اگر CISO هستید، باید مسئولیت کارهای زیر را بر عهده بگیرید.

❖ **برنامه امنیت اطلاعات سازمان خود را تهیه و حفظ کنید**

- تهیه و نگهداری یک برنامه جامع و استراتژیک امنیت اطلاعات و برنامه مدیریت ریسک امنیتی با هدف محافظت از اطلاعات رسمی و طبقه بندی شده سازمان شما.
- تدوین برنامه ارتباطی برای امنیت اطلاعات را رهبری کنید.
- روند مدیریت ریسک امنیت اطلاعات سازمان خود را ایجاد و تسهیل کنید.

❖ **اطمینان از انطباق با سیاست‌ها و استانداردها**

- اطمینان حاصل کنید که سازمان شما با سیاست‌ها و استانداردهای امنیت اطلاعات خود مطابقت دارد.
- با تسهیل برنامه مداوم صدور گواهینامه و اعتبار سنجی بر اساس مدیریت ریسک امنیتی، اطمینان حاصل کنید که سازمان شما با راهنمای امنیت اطلاعات نیوزلند (NZISM) مطابقت دارد.
- از اجرای معیارهای امنیت اطلاعات و شاخص‌های کلیدی عملکرد اطمینان حاصل کنید.

❖ **هماهنگی و هماهنگی امنیت با اهداف تجاری**

- تسهیل امنیت اطلاعات و ترازبندی مشاغل و ارتباطات در مورد این امور از طریق کمیته راهبری یا هیئت مشورتی که بطور رسمی و منظم تشکیل جلسه می‌دهد و متشکل از مدیران کل بازرگانی و ICT است.
- تیم‌های امنیت تجاری و اطلاعاتی را که در پروژه‌های مدیریت ریسک امنیت و امنیت اطلاعات کار می‌کنند، هماهنگ کنید.
- با تیم‌های تجاری کار کنید تا فرایندهای تجزیه و تحلیل و مدیریت ریسک امنیتی را تسهیل کنید.
- اطمینان حاصل کنید که روشهای شناسایی سطح قابل قبول ریسک در سازمان شما سازگار است.

❖ **با مدیران و مدیران پروژه ICT کار کنید**

- در مورد پروژه‌ها و عملیات ICT آژانس خود راهنمایی استراتژیک ارائه دهید.
- برای اطمینان از هماهنگی ساختارهای امنیتی و سازمانی، با تیم‌های معماری در ارتباط باشید.

❖ **با فروشندگان کار کنید**

- استفاده سازمان خود را از منابع امنیت اطلاعات خارجی، از جمله قرارداد و مدیریت منابع، هماهنگ کنید.

❖ **بودجه بندی را کنترل کنید**

- بودجه امنیت اطلاعات را کنترل کنید.

❖ **بازیابی فاجعه را هماهنگ کنید**

- توسعه سیاست‌ها و استانداردهای بازیابی حوادث را هماهنگ کنید تا از عملکردهای حیاتی سازمان شما پشتیبانی شود و در صورت بروز یک فاجعه امنیت اطلاعات حفظ شود.

❖ **نظارت بر آموزش**

- بر توسعه و بهره برداری از برنامه‌های آموزشی آگاهی و امنیت اطلاعات سازمان خود نظارت کنید.

❖ **مشاوره امنیتی ارائه دهید**

- مشاوره معتبر امنیتی ارائه دهید و با استانداردهای ملی و بین المللی و اقدامات صحیح آشنا باشید

۱۰-۲- ITSMاقدامات امنیتی را اجرا کرده و تخصص آنها را فراهم می‌کند

ITSM مدیران درون سازمانی هستند .آن‌ها مجاری بین جهت‌های استراتژیک ارائه شده توسط CISO و تلاش‌های فنی مدیران سیستم‌ها هستند .در حالی که CISO جهت استراتژیک امنیت اطلاعات را تعیین می‌کند، ITSM اجرای اقدامات امنیت اطلاعات را مدیریت می‌کند. ITSM معمولاً به عنوان متخصصان امنیت اطلاعات در سازمان خود در نظر گرفته می‌شوند.

❖ **جنبه‌های اصلی نقشITSM**

ITSMمسئول کنترل اداری و فرآیند مربوط به امنیت اطلاعات هستند .جنبه‌های اصلی کار آنها شامل موارد زیر است:

- بهبود امنیت اطلاعات سیستم‌ها
- ارائه ورودی به پروژه‌هایICT
- کمک به سایر پرسنل امنیتی در داخل سازمان خود
- کمک به آموزش امنیت اطلاعات
- پاسخ به حوادث امنیتی اطلاعات

ITSMهمچنین می‌تواند برای کمیته‌ها، مانند کمیته‌های راهبری امنیت اطلاعات، کمیته‌های مدیریت تغییر یا کمیته‌های بین آژانس، مشاوره ارائه دهد. از آنجا که ITSM از کلیه جنبه‌های امنیت اطلاعات آگاهی دارند، بهترین کار را برای کار با تیم‌های پروژه ICT برای شناسایی و ترکیب اقدامات امنیتی مناسب دارند. برای اطمینان از اینکه CISO شما از تمام مسائل مربوط به امنیت اطلاعات آگاه است و می‌تواند در صورت لزوم رئیس نمایندگی خود را مختصر معرفی کند، ITSMنیاز به ارائه گزارش‌های منظم در مورد:

- تحولات سیاست
- تغییرات و پیشرفتهای سیستم پیشنهادی
- حوادث امنیتی اطلاعات
- هر زمینه‌ای که نگران کننده باشد.

در حالی که CISO شما بر توسعه و بهره برداری از برنامه‌های آموزشی آگاهی و امنیت اطلاعات نظارت دارد، ITSMهای شما ترتیب آن آموزش را می‌دهند.

❖ **مسئولیت‌های سازمان شما با نقشITSM**

سازمان شما باید حداقل یک ITSM تعیین کند .اگر سازمان شما در چندین سایت در مکان‌های مختلف پخش شده است، باید ITSMرا در هر سایت اصلی تعیین کنید.

❖ **تعیین و پاکسازی ITSM ها**

هر ITSM ای که تعیین می‌کنید باید:

از تجربه، اقتدار و آموزش کافی برای ایفای نقش در سازمانی به اندازه خود یا حوزه مسئولیت آنها در سازمان خود برخوردار باشید از هر شرکتی که خدمات ICT ارائه می‌دهد مستقل باشد (برای جلوگیری از تضاد منافع).

ITSM باید باشد:

- برای دسترسی به تمام اطلاعات طبقه بندی شده پردازش شده در سیستم‌های سازمان شما پاک شده است
- دارای یک مجوز امنیت ملی است که به آنها امکان می‌دهد در مورد هرگونه اطلاعات محفوظ در سیستم‌های سازمان شما مختصر باشند.

ITSM نباید مسئولیت‌های اضافی فراتر از وظایف مورد نیاز برای ایفای نقش خود داشته باشند.

❖ **مسئولیت‌های شما به عنوانITSM**

به عنوانITSM ، شما باید:

به دارندگان سیستم کمک کنید تا اعتبار را بدست آورند و حفظ کنند اطمینان حاصل کنید که برنامه‌های مدیریت ریسک امنیت(SRMP) ، برنامه‌های امنیتی سیستم (SecPlan) و هرگونه روش عملیاتی استاندارد (SOP) برای سیستم‌های سازمان شما توسعه، نگهداری، به روز شده و اجرا می‌شوند.

❖ **کار باCISO**

شما باید با CISO خود کار کنید تا:

- یک برنامه امنیت اطلاعات ایجاد کنید
- پیش بینی بودجه امنیت اطلاعات و تخصیص منابع را بر اساس اهداف کوتاه مدت و بلند مدت توسعه دهید
- پروژه‌ها را بر عهده بگیرند و مدیریت کنند تا خطرات امنیتی را شناسایی کنند

❖ **کار با پروژه‌ها و سیستم‌هایICT**

شما باید با رهبران پروژه ICT و اعضای تیم کار کنید تا:

- سیستم‌هایی را که به اقدامات امنیتی اطلاعاتی نیاز دارند را شناسایی کرده و در انتخاب اقدامات مناسب به آنها کمک کنید
- اطمینان حاصل کنید که هنگام ارزیابی، انتخاب، نصب، پیکربندی و بهره برداری از تجهیزات و نرم افزارIT ، امنیت اطلاعات لحاظ شده است.

❖ **شما باید با تیم‌های معماری سازمانی کار کنید تا:**

- اطمینان حاصل کنید که ارزیابی ریسک امنیتی در معماری سیستم گنجانده شده است
- راه حل‌های امنیت اطلاعات را شناسایی کنید، ارزیابی کنید و انتخاب کنید که اهداف امنیتی سازمان شما را برآورده کند.

شما همچنین باید با دارندگان سیستمICT ، گواهینامه‌ها و اعتباربخشی‌ها کار کنید:

- بررسی کنید که کدام سیاست‌های امنیت اطلاعات از سیستم‌ها به بهترین وجه محافظت می‌کند
- مطابقت با الزامات امنیتی محافظتی، به ویژه مrelevant لفه های مربوط بهNZISM

به عنوان یکITSM ، شما باید:

- برای اطمینان از شناسایی صحیح خطرات، در فرایندهای مدیریت تغییر و کنترل سازمان خود گنجانده شوید
- هرگونه تغییر قابل توجهی را که ممکن است بر اعتبار آن سیستم تأثیر بگذارد، به مرجع اعتباربخشی اطلاع دهید.

❖ **کار با فروشندگان**

شما باید با فروشندگان و افراد خریدار و حقوقی در سازمان خود ارتباط برقرار کنید تا قراردادهای امنیتی اطلاعات و توافق نامه‌های سطح خدمات را که قابل قبول هستند، تنظیم کنید.

❖ **اجرای امنیت**

برای اجرای اقدامات امنیتی، باید:

ارزیابی ریسک امنیتی را بر روی هرگونه برنامه اجرایی تجهیزات یا نرم افزار جدید یا به روز شده فناوری اطلاعات انجام دهید و در صورت لزوم استراتژی‌های کاهش خطر را تدوین کنید

- اطمینان حاصل کنید که سیاست‌های امنیت اطلاعات با انتخاب و هماهنگی اجرای کنترل‌هایی که آنها را پشتیبانی و اجرا می‌کنند، قوی هستند
- ادغام استراتژی‌های امنیت اطلاعات و معماری را با استراتژی‌ها و معماری تجارت و ICT هدایت و هدایت کنید
- تخصص فنی و مدیریتی را برای مدیریت ابزارهای مدیریت امنیت اطلاعات فراهم کنید.

❖ **گزارشگری و حسابرسی**

تو باید:

- هماهنگی، اندازه گیری و گزارش در مورد جنبه‌های فنی مدیریت امنیت اطلاعات
- نظارت و گزارش در مورد انطباق سازمان خود با سیاست‌های امنیتی اطلاعات و اجرای آن
- به طور منظم در مورد حوادث امنیتی اطلاعات و سایر زمینه‌های مورد توجه CISO گزارش دهید
- تهدیدها، آسیب پذیری ها و خطرات امنیتی باقی مانده را ارزیابی و گزارش دهید
- اقدامات اصلاحی را برای کاهش خطرات توصیه کنید
- به صاحبان سیستم و پرسنل امنیتی کمک کنید تا شکستهای حسابرسی گزارش شده توسط حسابرسان را درک و پاسخ دهند.

❖ **کمک به بازیابی فاجعه**

شما باید به تیم مسئول برنامه ریزی برای بازیابی حوادث کمک کنید:

- انتخاب استراتژی‌های بازیابی
- در حال توسعه، آزمایش و حفظ برنامه‌های بهبودی در برابر بلایا.

❖ **آموزش**

تو باید:

- آگاهی و آموزش امنیت اطلاعات را برای همه افراد سازمان خود فراهم یا ترتیب دهید
- تهیه مطالب اطلاعات فنی و کارگاه‌های آموزشی در مورد روند امنیت اطلاعات، تهدیدها، اقدامات خوب و سازوکارهای کنترل به صورت مناسب.

❖ **ارائه دانش امنیتی به روز**

به عنوان یکITSM ، شما باید:

- نگهداری یک پایگاه دانش امنیتی به روز شامل کتابخانه مرجع فنی، مشاوره و هشدارهای امنیتی، اطلاعات مربوط به روندها و اقدامات امنیتی، قوانین و مقررات مربوطه و استانداردها و دستورالعمل‌ها
- راهنمایی‌های تخصصی در مورد مسائل امنیتی پروژه‌های ICT را ارائه دهید
- در صورت لزوم برای کمیته راهبری امنیت اطلاعات، کمیته مدیریت تغییر و سایر کمیته‌ها مشاوره فنی ارائه دهید
- درک به روز و دقیق از محیط تهدید مربوط به سیستم‌ها و انتقال این اطلاعات به دارندگان سیستم، بنابراین در هنگام فعالیت‌های اعتباربخشی در نظر گرفته می‌شود
- CISO و دارندگان سیستم را با اطلاعات به روز در مورد تهدیدات فعلی مطلع کنید.

۲-۱-۱۶- دارندگان سیستم سیستم‌ها را نگهداری و اداره می‌کنند

همه سیستم‌ها باید صاحب باشند. همه دارندگان سیستم باید اطمینان حاصل کنند که فرایندهای حاکمیت فناوری اطلاعات رعایت شده و الزامات تجاری برآورده می‌شوند. دارندگان سیستم برای سیستم‌های بزرگ یا حیاتی باید بخشی از تیم اجرایی ارشد سازمان شما باشند یا یک موقعیت مدیریتی معادل داشته باشند.

❖ **مسئولیت‌های شما به عنوان یک مالک سیستم**

شما به عنوان یک مالک سیستم، مسئولیت عملکرد و نگهداری کلی سیستم، از جمله خدمات پشتیبانی مرتبط یا خدمات برون سپاری شده مانند سرویس ابری را بر عهده دارید. شما می‌توانید مدیریت و عملکرد روزمره سیستم را به یک مدیر سیستم یا مدیران محول کنید.

❖ **عملکرد سیستم و حفظ اعتبار**

شما باید اطمینان حاصل کنید که سیستمی که متعلق به شماست برای تأمین نیازهای عملیاتی سازمان شما معتبر است .شما مسئول دریافت و حفظ اعتبارنامه هستید.

- اگر سیستم اصلاح شود، باید اطمینان حاصل کنید:
- تغییرات به درستی و مستند انجام شده است

که هرگونه فعالیت مجدد اعتبار مجدد لازم به پایان رسیده است.

❖ **تهیه، نگهداری و اجرای اسناد**

به عنوان یک مالک سیستم، باید اطمینان حاصل کنید که اسناد امنیت اطلاعات سیستم، توسعه، نگهداری و پیاده سازی شده است. مستندات مربوط به سیستم شامل SRMP ، SecPlansو SOP است. شما باید پرسنل امنیتی را در مراحل مستند سازی مشارکت دهید تا اطمینان حاصل شود که یک نگرش جامع به امنیت اطلاعات می‌تواند با درک شما از خطرات امنیتی برای سیستم خاص شما ترسیم شود. شما باید اطمینان حاصل کنید که اسناد کامل، دقیق و به روز هستند .همچنین باید اقداماتی را که برای توسعه، نگهداری و اجرای اسناد انجام می‌دهید مستند کنید. هنگام تهیه یا به روزرسانی اسناد امنیتی اطلاعات، باید ITSMخود را درگیر کنید.

۲-۱-۱۷- کاربران سیستم با پیروی از خط مشی‌ها و رویه‌ها از سیستم‌ها محافظت می‌کنند

توسعه و حفظ فرهنگ امنیتی به کاربران کمک می‌کند تا از خط مشی‌ها و رویه‌های امنیتی پیروی کنند .کاربران سیستم باید از خطرات هر سیستمی که استفاده می‌کنند آگاه باشند و نقشی را که در کاهش این خطرات دارند، درک کنند.

❖ **مسئولیت‌های شما به عنوان کاربر سیستم**

به عنوان یک کاربر سیستم، سطح دسترسی شما هر چه باشد، باید:

- با سیاست‌ها و رویه‌های امنیتی سیستم مطابقت داشته باشید
- اطمینان حاصل کنید که احراز هویت حساب شما از قدرت کافی برای محافظت از سیستم برخوردار است (به عنوان مثال رمزهای عبور و سایر جزئیات ورود به سیستم)
- احراز هویت حساب‌ها را بدون تأیید به اشتراک نگذارید
- مسئولیت کلیه اقدامات تحت حساب خود را بر عهده بگیرید

- فقط از دسترسی خود برای انجام کارها و عملکردهای مجاز استفاده کنید.

❖ **وقتی می‌خواهید خط مشی یا روال را دور بزنید**

سیاست‌ها و رویه‌های امنیتی با هدف پوشش دادن همه موقعیت‌هایی است که ممکن است در یک سازمان ایجاد شود .با این حال، گاهی اوقات شما ممکن است دلیل موجهی داشته باشید که بخواهید یک خط مشی یا روال را دور بزنید .در این صورت، قبل از اقدام باید از CISO یا ITSM خود تأیید رسمی بگیرید

۱۱-۲- استفاده از سطوح تأثیر تجاری

به عنوان بخشی از روند ارزیابی ریسک، سطح تأثیرات تجاری (BIL) را به خطرات امنیتی سازمان خود اختصاص دهید BIL برای ارزیابی مداوم تأثیرات احتمالی نقض امنیت استفاده می‌شود.

- اختصاص BILs به شما کمک می‌کند اقدامات امنیتی متناسب با خطرات شما را طراحی و اجرا کنید.
- مقیاس BIL از ۱ (کم) تا ۶ (فاجعه بار) است .هرچه این تأثیر بیشتر باشد، اقدامات امنیتی شما باید قوی‌تر باشد.

BILها رویکردی سازگار و ساختار یافته برای دسته بندی خطرات و تأثیرات امنیتی در سراسر دولت ارائه می‌دهند. این سازگاری امنیت اطلاعات به اشتراک گذاری بین سازمانها را بیشتر می‌کند و درک مشترکی از پیامدهای نقض امنیت فراهم می‌کند.

❖ **برای هر خطری که آژانس شما با آن روبرو است از BIL استفاده کنید**

هنگامی که BIL را در معرض خطر قرار می‌دهید، تأثیر احتمالی نقض امنیت را ارزیابی می‌کنید - سطح آسیب، خسارت یا سازش که می‌تواند منجر شود .شما باید BIL ها را برای افراد، اطلاعات و دارایی خود بسازید. اطمینان حاصل کنید که BIL هایی که تعیین می‌کنید تأثیرات واقعی خطرات امنیتی شما را نشان می‌دهد، بنابراین می‌توان آنها را به خوبی مدیریت کرد.

شما باید بتوانید تأثیر ناشی از به خطر افتادن رازداری، از بین رفتن صداقت یا در دسترس نبودن دارایی‌هایی را که در دست دارید یا تولید می‌کنید، بیان کنید. سطح تأثیرات تجاری محافظتی دولت نیوزیلند (BILS) خطرات چارچوبی برای ارزیابی BIL ها برای اطلاعات، سیستم‌های ICT و دارایی‌ها به شما می‌دهد. به یاد داشته باشید که اگر امنیت اطلاعات جمع شده شما (مجموعه اطلاعات) نقض شود، چه تاثیری خواهد داشت. همچنین باید زمان تغییر سطح تأثیر را در نظر بگیرید و توجه داشته باشید که در BIL ها .به عنوان مثال، ممکن است با پایان یافتن یک پروژه، اهمیت یک دارایی تغییر کند.

❖ **همکاری با سازمانها یا شرکای دیگر در موردBILs**

BILها می‌توانند بر اساس کارکرد و اندازه آنها بین آژانس‌ها بسیار متفاوت باشند .دارایی‌های مشابه می‌توانند در یک آژانس در مقایسه با نمایندگی دیگر تأثیرات بسیار متفاوتی داشته باشند .اطمینان حاصل کنید که هرگونه تفاوت در BIL ها را بین سازمانی که با آن همکاری می‌کنید یا در آنجا مستقر هستید، درک می‌کنید، بنابراین می‌توانید درباره اقدامات امنیتی که برای کاهش خطرات برای همه طرفها لازم است، مذاکره کنید.

❖ **رابطه بین BIL ها و سطح طبقه بندی**

در بعضی مواقع، ممکن است بین طبقه بندی امنیتی اطلاعات رسمی و BIL ها رابطه وجود داشته باشد .هنگام بررسی محرمانه بودن اسناد یا پرونده‌های فردی، طبقه بندی‌های امنیتی مستقیماً با BIL ها مطابقت دارند .با این حال، این لزوماً در مورد مجموعه دارایی‌ها صدق نمی‌کند .به عنوان مثال، در مجموعه دارایی‌ها با سطح تأثیر تجارتی کل ۴ - بسیار زیاد، ممکن است هر مورد منفرد به عنوان محرمانه علامت گذاری نشود.

با این وجود، مارک محافظتی یا محرمانه بودن دارایی تنها عاملی نیست که باید هنگام تهیه BIL در نظر بگیرید .قبل از اعمال BIL باید تمام عوامل مؤثر بر امنیت دارایی را در نظر بگیرید BIL .ها همچنین باید یکپارچگی و در دسترس بودن را در نظر بگیرند.

رابطه احتمالی بین علائم محافظ وBIL

BIL	علامت گذاری سند
۱- کم	**طبقه بندی نشده (ممکن است علامت گذاری نشده باشد)**
۲- متوسط	**با اطمینان**
۳- بالا	**حساس یا محدود شده است**
۴- بسیار بالا	**محرمانه**
۵- افراطی	**راز**
۶- فاجعه بار	**فوق سری**

سطوح تاثیر کسب و کار دولتی زلاندنو در باب مخاطرات امنیت حفاظت(BIL)

۱) پایین	۲) متوسط	۳) بالا	۴) خیلی بالا	۵) فوق‌العاده	۶) فاجعه‌بار
قابل انتظار در ایجاد تاثیر بر عملکردهای موسسات دولتی، نهادهای بازرگانی یا اعضای نهادهای عمومی به واسطه	قابل انتظار در ایجاد سد و مانع در سر راه عملیات‌های موسسه دولتی، نهادهای بازرگانی یا اعضای نهاد عمومی می‌گردد به واسطه	قابل انتظار در ایجاد تاثیر بر امنیت ملی، عملکرد موسسات دولتی، نهادهای بازرگانی و یا اعضای نهادهای همگانی به واسطه	قابل انتظار در بروز صدمه به امنیت ملی، عملکردهای موسسات دولتی نهادهای بازرگانی یا اعضای نهادهای عمومی به واسطه	قابل انتظار در بروز یک تاثیر عمومی امنیت ملی، عملکردی موسسات دولتی، نهادهای تجاری و اعضای نهادهای عمومی به واسطه	توقع تاثیر جدی روی امنیت ملی، عملیات‌های موسسات دولتی، نهادهای تجاری و عمومی به واسطه
- تنزل یافتن توانمندی سازمان در یک گستره و فاصله زمانی، که به واسطه آن، موسسه دولتی در همین اثنا توانایی انجام عملکردهای ابتدایی خود را دارد، کارآمدی عملکردیاش قابل ملاحظه است، هرچند که به طور موقت کاهش داشته باشد.	-تخریب اموال دولتی -تعدیل(تا میزان یک میلیون دلار) منابع مالی موسسه -پوشش رسانه‌ای نامطلوب شکل جزئی و بومی شده -به‌واسطه یک بازرسی داخلی یا یک تحقیق تفحص داخلی	-تنزل درجه در سطح واسطه‌ها یا اتلاف، توانمندی‌های سازمانی در یک گستره‌ای که به واسطه آن موسسه از انجام یکی یا بیشتر از عملکردهای خود برای یک بازه زمانی وسیع باز بماند. -تخریب عمده در اموال موسسه	-تنزل شدید و قوی در تلف، توانمندی سازمان در یک گستره‌ای که در آن چندین شرکت از انجام برخی عملکردهای ابتدایی و جاری خود عاجز می‌مانند -توقف قابل ملاحظه در کار زیر ساختارهای ملی	-ایجاد هدر رفت در توانایی سازمان در یک گستره‌ای از زمان و حجم که موجب عاجز ماندن موسسه از انجام عملکردهای خودش گردد -صدمات جدی به کارکنان یا عموم مردم از قبیل از دست دادن جان -تهدید مستقیم ثبات سیاست داخلی زلاندنو یا کشورهای دوست	-پیشروی مستقیم امور به سوی اتلاف گسترده حیات انسانی -تخریب جدی و دیرپای در زیرساخت‌های مهم ملی -پیشرفت تاثیرات ملی دیرپا اقتصاد ملی -ایجاد تخریب جدی و عمده و مداوم کارایی و تاثیر

-به طور بالقوه، تاثیر وارونه ناشی از حریم خصوصی فرد -منتج از یک تخریب جزئی در دارائی موسسه -منتج در اتلاف مالی جزئی در موسسه، که شامل اعتبارات موجود باشد -یا از طریق یک انباشتی از تهاجمات از نوع مشابهی که علاقه خود را برای آن افزایش می‌دهد، باعث می‌شود سطح حفاظت امنیتی افزایش یابد.	-به واسطه بروز برونگرانی‌های سطح پایین در وزارتخانه -ایجاد مانع در امر تحقیق و بازرسی یا عمل به جرم خرد -به واسطه برخی موضوعات اعتباری مالی با سهامداران و طرفهان ذینفع داخلی و بین بخشی -به واسطه ضرر و صدمه و صدمه جزئی به کارمندان در یا اعضای نهادهای عمومی -تهلیل رفتن پایداری مالی زلاندنو یا سازمان‌های جدید تحت مالکیت زلاندنو	-تخریب عمده در منابع مالی(تا میزان ۲۵ میلیون دلار) -محروم شدن تصدی از شرکت‌های زلاندنو از حقوق خود -اختلال در توانایی بازرسی جرم -پدیدارشدن انتقاد و اعتراض همگانی یا مستقیم به یک یا چند وزیر -ایجاد پوشش نامطلوب رسانه‌ای ملی -تاثیر شگرف در روابط بین طرفین ذینفع دولتی -ضررو صدمه بالقوه به حیات انسان -که می‌تواند موجب از مرگ شود -ارجاع به یک مدافع حقوق بشر با کمسیونر حفظ حریم خصوصی با یافته‌های نامطلوب گزارش شده	-تاثیر قابل ملاحظه در اعتبار بین‌المللی زلاندنو -تخریب مادی روابط دیپلماتیک به عنوان مثال انجام اعتراضات رسمی یا سایر تحریم‌ها -ایجاد مانع سر راه زلاندنو در باب مذاکرات بین اللملی، به عنوان مثال، قرارگرفتن در معرض خطر پیشرفته در مسیر راهبرد مذاکراتی زلاندنو، یا در سر راه عواید قابل قبول در مفاد ملازمات تجاری دو جانبه -تخریب عمده روی اموال و امنیت ملی -تخریب توانمندیهای اطلاعاتی زلاندنو یا گروه موتلف آن -نارسایی پایدار در پوشش رسانه‌ای بین‌المللی -تحقیق تفحیص رسمی خارجی -ایجاد یک ثاثر غیر مصالحه پذیر منفی روی روابط وزارتخانه‌ای -تعدیل در پیامدهای اجتماعی یا محیط زیست	-ایجاد تنش بین‌المللی یا تخریب جدشار روابط با دولتهای دوست -محرومیت شدید زلاندنو در مذاکرات بین‌المللی، به عنوان مثال، قرار گرفتن کشور در معرض خطر پیشرفته در راهبرد مذاکراتی یا عواید قابل قبول در منازعات تجاری دو جانبه -تخریب جدی کارآمدی عملیاتی یا امنیت زلاندنو یا نیروهای موتلف -تخریب شدید توانمندی اطلاعاتی زلاندنو یا کشورهای موتلف نقصان عمده و طولانی مدت در توانایی تحقیق و تخصیص حدی روی جنایات سازمان یافته -تخریب جدی و طولانی در تجارت جهانی بروز هزینه‌های عمده اجتماعی و زیست محیطی	بخش عملیاتی فوق‌العاده با ارزش بالای اطلاعات -تاثیرات فوق‌العاده و جبران‌ناپذیر در هزینه زیست محیطی -قرارگرفتن منافع ملی در معرض خطر در یک گستره شدید

۱۲-۲- در حال توسعه سطح هشدار امنیتی

از این راهنما برای کمک به شما در جهت ارتقا levels سطح هشدار سازمان خود برای حرکت به سمت افزایش امنیت در موارد اضطراری یا افزایش تهدید استفاده کنید.

مشاوره در این راهنما شامل موارد زیر است:

- افرادی که در مدیریت امنیت کار می‌کنند
- پیمانکاری که مشاوره و خدمات امنیتی را به سازمانهای دولتی ارائه می‌دهند
- هر کسی که مسئول امنیت مردم نیوزلند، اطلاعات یا دارایی‌ها باشد.

❖ **چگونگی متناسب بودن این راهنما با نیازهای دولت**

این راهنما از اجرای الزامات امنیتی محافظتی (PSR) پشتیبانی می‌کند .براساسPSR ، آژانس‌های دولتی باید برنامه‌هایی را تدوین کرده و آماده باشند تا در صورت لزوم به سطح بالاتری از امنیت بروند .

❖ **- GOV7بتوانید به افزایش سطح تهدید پاسخ دهید**

برنامه‌هایی را تدوین کنید و آماده باشید تا در موارد اضطراری یا شرایطی که تهدید بیشتری برای مردم، اطلاعات یا دارایی‌های شما وجود دارد، سطح امنیتی را افزایش دهید.

شرایط زیر مربوط به سطح هشدار امنیتی است:

- اجرای رویکرد مبتنی بر ریسک برای امنیت محافظتی
- پروتکل مدیریت برای امنیت فیزیکی
- پروتکل مدیریت امنیت اطلاعات
- سطح تاثیر کسب و کار

تصمیمات خود را در مورد سطح هشدار امنیتی بر اساس هر کدام از بالاترین نیازها تعیین کنید - توصیه‌های این راهنما، الزامات مربوطه ذکر شده در بالا یا هر قانونی که اعمال می‌شود.

❖ **چرا باید سطح هشدار امنیتی را توسعه دهید**

سطح هشدار امنیتی اطلاعات مربوط به اقدامات امنیتی را که برای کاهش خطرات در شرایط اضطراری و سایر مواقع افزایش خطر استفاده می‌کنید، به شما اعلام می‌کند. سطح هشدار همچنین به شما امکان می‌دهد اقدامات امنیتی را که استفاده می‌کنید مقیاس بندی کنید، بنابراین با نوع حادثه متناسب هستند و با افزایش یا کاهش خطرات، به راحتی تغییر می‌کنند. ایجاد سطوح هشدار به سازمان شما کمک می‌کند اقدامات امنیتی را قبل یا حین حادثه سریع انجام دهد .پاسخ سریع می‌تواند توانایی شما را در محافظت از افراد، اطلاعات و دارایی‌های شما بسیار افزایش دهد.

❖ **چگونه می‌توان سطح هشدار امنیتی را توسعه داد**

برای توسعه سطح هشدار، رویکرد "همه خطرات" را در پیش بگیرید .این بدان معنی است که انواع تهدیدها را از همه منابع در بر می‌گیرید، بنابراین می‌توانید یک پاسخ متعادل ایجاد کنید .تهدیدهای فیزیکی و محیطی ممکن است تأثیر مشابه یا بیشتر بر توانایی سازمان شما به عنوان تهدیدهای امنیتی سنتی داشته باشد.

هرگونه اقدامات امنیتی محافظتی که با سطح هشدار خود اجرا می‌کنید، باید خطرات افراد، اطلاعات و دارایی‌های شما را کاهش دهد .آن‌ها همچنین باید هرگونه ترتیب اطلاعات و توزیع دارایی را که دارای امنیت بیشتری هستید، انجام دهند.

❖ **منابع خطرات جسمی خود را بررسی کنید**

سطح هشدار خود را بر اساس منابع احتمالی خطر برای امنیت خود قرار دهید - خطراتی که در ارزیابی ریسک امنیتی سازمان خود شناسایی کرده‌اید.

منابع خطرات امنیتی جسمی به سه دسته اصلی تقسیم می‌شوند:

- **رویداد**- یک اتفاق یا حادثه مهمی است که بر توانایی عملکرد سازمان شما تأثیر می‌گذارد .به عنوان مثال می‌توان به رویداد آب و هوایی مانند طوفان یا حوادث اضطراری مانند زمین لرزه اشاره کرد.
- **تهدید**- قصد و توانایی اعلام شده برای صدمه زدن به مردم، اطلاعات یا دارایی شما.
- **فعالیت**- عملی توسط یک یا چند نفر که ممکن است تأثیر منفی بر امنیت فیزیکی بگذارد .به عنوان مثال، فعالیت معترض، اشغال یا اقدام به اشغال، یا فیلمبرداری در نزدیکی محل زندگی خود.

اگر اقدامات امنیتی محافظتی شما در اثر یک رویداد یا فعالیت آسیب دیده یا نقض شده باشد، یا شواهد موثقی برای تأیید احتمال تهدید داشته باشید، ممکن است لازم باشد سطح هشدار را افزایش دهید.

❖ **خطرات منحصر به فرد هر مرکز یا محل کار را ارزیابی کنید**

هر مرکز یا محل کار در داخل یک مرکز ممکن است خطرات امنیتی منحصر به فردی داشته باشد .برای شناسایی و ارزیابی خطرات امنیتی فیزیکی که ممکن است در هنگام وقایع، تهدیدها یا فعالیت‌ها روی هر سایت تأثیر بگذارد، افراد مدیریت امنیت شما باید با این موارد کار کنند:

- مدیران محلی مسئول هر تسهیلات
- افرادی که با تداوم تجارت، بهبودی بلایا و مدیریت ریسک درگیر هستند.

❖ **از منابع اطلاعاتی داخلی و خارجی استفاده کنید**

اطلاعات مربوط به خطرات را از منابع داخلی و خارجی جستجو کنید.

❖ **منابع داخلی**

ارزیابی کلی خطر سازمان شما منبع بسیار خوبی از اطلاعات است .ارزیابی را بررسی کنید و برای کسب اطلاعات بیشتر با حوزه‌های تجاری خود مشورت کنید.

حوزه‌های تجاری شما باید بتوانند در مورد موارد زیر به شما بگویند:

- تأثیر تجاری اختلالات در عملکرد آنها، آسیب رساندن به مردم آنها، یا سازش یا از دست دادن اطلاعات یا دارایی‌ها
- هنگامی که ممکن است به دلیل تغییر در اهمیت دارایی (به عنوان مثال در پایان یک پروژه) سطح تأثیر تجاری (BIL)تغییر کند.

سایر منابع مهم داخلی اطلاعات در مورد خطرات عبارتند از:

- بررسی‌های امنیتی محافظتی
- گزارش‌های امنیتی و حادثه‌ای
- ثبت امنیت و ریسک عملیاتی.

❖ **منابع خارجی**

منابع خارجی شامل هر سازمانی است که در آن کار می‌کنید، با آن شریک هستید یا در آنجا مستقر هستید .شما باید BIL های هر کار مشترک و یا توافق نامه مشترک را در نظر بگیرید .آیا نمایندگی‌های دیگر فاکتورهای خطر منحصر به فردی دارند و چگونه ممکن است بر برنامه‌های ترکیبی تداوم تجارت شما تأثیر بگذارند؟

مثال‌های دیگری از منابع اطلاعاتی خارجی که می‌توانید از آنها استفاده کنید:

- سطح تهدید تروریسم ملی
- سطح هشدار ملی
- مشاوره ارزیابی تهدید ملی
- مشاوران پلیس، MetService و دفاع مدنی
- مرکز امنیت سایبری ملی (NZSC) وCERT NZ
- گزارش‌های رسانه‌ای

❖ **مراقب باشید از محافظت کم یا زیاد محافظت نکنید**

هنگام طراحی یا انتخاب سطح هشدار، رویکردی متعادل را هدف قرار دهید زیرا محافظت بیش از حد یا کم از افراد، اطلاعات و دارایی‌های شما می‌تواند مشکلاتی را ایجاد کند.

❖ **محافظت بیش از حد**

محافظت بیش از حد، هزینه بر، ناکارآمد است و می‌تواند مانعی برای فعالیت‌های شما باشد .محافظت بیش از حد اغلب به دلیل موارد زیر ایجاد می‌شود:

- تفسیر شخصی از میزان آسیب احتمالی از یک منبع خطر
- نداشتن سطح هشدار کافی برای افزایش مرحله‌ای اقدامات متناسب با افزایش خطر

❖ **تحت حفاظت**

کمبود محافظت می‌تواند بر ایمنی شخصی و امنیت اطلاعات و دارایی شما تأثیر بگذارد. برای جلوگیری از کمبود محافظت، راهنمایی ارائه کنید که تشخیص اینکه کدام منابع خطر به افزایش سطح هشدار نیاز دارند، برای افراد شما آسان است .و اجرای آن را آسان کنید.

❖ **تصمیم بگیرید که به چند سطح هشدار نیاز دارید**

تعداد سطح هشدار برای استفاده به محیط کار شما و تغییرات پیش بینی شده در منابع خطر بستگی دارد .عوامل اساسی برای در نظر گرفتن ماهیت سازمان شما، انواع تسهیلات مورد استفاده شما، نقش عملیاتی شما و میزان خطر شناخته شده شماست.

❖ **نمونه‌هایی از سطح هشدار**

چهار مثال زیر از سطح هشدار نشان می‌دهد که چگونه می‌توانید:

- سطح هشدار را تعریف کنید
- شرایطی را که هر سطح پوشش می‌دهد توصیف کنید
- معیارهایی را که برای هر سطح اعمال می‌شود خلاصه کنید

❖ **کم**

این سطح هشدار امنیتی هنگامی اعمال می‌شود که احتمال وقوع آسیب برای رویدادی کم باشد .تدابیر امنیتی موجود الزامات عملیاتی داخلی عادی را برآورده می‌کند.

سطح هشدار پایین:

هنگامی اعمال می‌گردد که یک رخ داد، تهدید عمومی و یا فعالیت فیزیکی در ایجاد اسباب ضرر و آسیب در حال وقوع دخیل باشد. هیچ تهدید مشخص هدایت شده در سازمان و یا هر یک از تاسیسات آن وجود ندارد.
اقدامات را می توان به طور نامحدود حفظ کرد.

مثال: رویداد، تهدید، فعالیت		**اقدامات**
	**رخ داد** هنگامی اعمال می شود که فقط نگرانی های عمومی وجود داشته باشد یا هیچ رویدادی شناخته نشده باشد. تهدید عمومی ، فعالیت بدنی که ممکن است به سازمان یا هر یک از امکانات آن آسیب برساند	– کارکنان در مورد مسائل امنیتی و هشدار یادآوری می شوند – برنامه عملیاتی و امنیت عملیاتی و اورژانس بررسی می شود (حداقل یک بار در سال) – فعالیت های آموزش آگاهی آغاز می شود
	**تهدید** حمله تروریستی بعید ارزیابی شده است	
	**فعالیت** نگرانی های عمومی در مورد فعالیت های جنایی از جمله تخریب و سرقت وجود دارد اما هیچ تأثیر قابل توجهی در مشاغل و کارکنان انتظار نمی رود	

❖ **متوسط**

این سطح هشدار امنیتی هنگامی اعمال می‌شود که یک رویداد، تهدید عمومی یا فعالیت بدنی ممکن است باعث آسیب شود .با این حال، تهدید خاصی متوجه سازمان یا امکانات شما نیست .اقدامات امنیتی را که اعمال می‌کنید می‌توانید به طور نامحدود حفظ کنید، با کمترین تأثیر بر عملکرد سازمان شما.

سطح هشدار متوسط:

هنگامی اعمال می‌گردد که یک رخ داد، تهدید عمومی و یا فعالیت فیزیکی در ایجاد اسباب ضرر و آسیب در حال وقوع دخیل باشد. هیچ تهدید مشخص هدایت شده در سازمان و یا هر یک از تاسیسات آن وجود ندارد.

مثال: رویداد، تهدید، فعالیت		اقدامات
	**رخ داد** یک طوفان کلی یا سونامی واقع شده و هشدار لازم توسط سرویس هواشناسی برای حوزه ای مهم صادر گردیده است.	— کارکنان هشدارلازم دریافت می‌کنند تا فعالیت‌های غیرمعمول را دریابند و چگونگی گزارش آنها را بفهمند. — برنامه‌های عملیاتی عادی و رویه‌های معمول به‌روز نگاهداشته می‌شود. — آگاهی بخش‌های اضطراری و امنیتی قاعده‌مند صادر می‌گردد. — کارکنان و نیروهای کنترل اضطراری آموزش می‌ببینند و برای مقابله با رخ دادن اضطراری بومی هشدار دریافت می‌کنند. — برنامه‌های بازیابی بلایای طبیعی تهدید و امنیتی هر سال مورد بررسی قرار می‌گیرند.
	**تهدید** یک حمله تروریستی به مثابه امکان وقوع، ارزیابی گردیده که در آینده واقع خواهد گردید. لیکن هیچ تهدید مشخصی درک نمی شود	
	**فعالیت** یک فعالیت اعتراض آمیز غیراعلام شد از قبل(از سوی گروه‌ها یا افراد مستقل) در نزدیکی یا مقابل محیط پیرامون سازمان درحال وقوع است	

❖ **بالا**

این سطح هشدار امنیتی هنگامی اعمال می‌شود که پیش بینی می‌شود یک رویداد، تهدید یا فعالیت بدنی برای سازمان یا هر یک از تأسیسات شما ایجاد شود. هرگونه تدابیر امنیتی که اعمال می‌کنید می‌تواند برای مدت طولانی بدون ایجاد سختی بیش از حد برای مردم خود، تأثیر بر توانایی عملیاتی یا تشدید روابط با جامعه محلی حفظ شود.

سطح هشدار بالا:

هنگامی اعمال می شود که تهدیدی یا فعالیت بدنی احتمالاً برای سازمان یا امکانات آن رخ دهد اقدامات را می توان برای مدت طولانی بدون ایجاد سختی بیش از حد ، تأثیر بر توانایی عملیاتی یا تشدید روابط با جامعه محلی حفظ کرد

مثال: رویداد، تهدید، فعالیت		اقدامات
	**رخ داد** — یک هشدار شدید هوا یا وقوع سونامی توسط سرویس دهنده خدمات برای منطقه صادر می شود — هشدار آتش به دلیلی نامعلوم فعال شده است	— تدابیر امنیتی پایین تا متوسط اعمال شده است — چراغ های هشدار دهنده ممکن است برای مدت محدودی کار کنند

	**تهدید** – ارزیابی وجود دارد که حمله تروریستی عملی است و می تواند به خوبی برای سازمان اتفاق بیفتد – یک نامه الکترونیکی مشکوک از طریق پست دریافت می شود	– پرسنل کنترل ظهور هشدار داده می شوند و در صورت لزوم اقدامات اضطراری مستقر می شوند – کارکنان از تغییر سطح هشدار مطلع می شوند – روشهای اضافی غربالگری و / یا محدودیت بازدید کننده ممکن است شامل هیچ بازدید کننده مجاز و وسایل نقلیه تحت بازرسی یا دسترسی محدود باشد – استراتژی های جایگزین عملیات تجاری زمانی ارزیابی می شوند که ارزیابی شود وضعیت باید حفظ شود
	**فعالیت** یک فعالیت اعتراضی شناخته شده (توسط گروهها یا یک فرد) قرار است در نزدیکی یا علیه سازمان واقع شود اما هیچگونه خشونت پیش بینی نشده است	

❖ **مفرط**

این سطح هشدار امنیتی هنگامی اعمال می‌شود که تهدیدی یا فعالیت بدنی که ممکن است صدمه قابل توجهی وارد کند، در شرف وقوع است یا برای سازمان یا هر یک از امکانات شما رخ داده است.

شما قادر نخواهید بود اقدامات امنیتی لازم را برای دوره‌های طولانی حفظ کنید و ممکن است مردم شما را با سختی مواجه سازد، بر توانایی عملیاتی تأثیر بگذارد یا روابط با جامعه محلی را بدتر کند.

سطح هشدار شدید:

وقتی حادثه، تهدید یا فعالیت بدنی که ممکن است صدمه قابل توجهی ایجاد کند قریب الوقوع است یا برای آژانس یا تأسیسات آن رخ داده اعمال می‌شود

اقدامات سختی ایجاد می‌کند، بر فعالیت ها و پرسنل محل تأثیر می‌گذارد، در طولانی مدت پایدار نیستند و بسته به نوع حادثه ممکن است برای سایر اماکن نیز تأثیراتی داشته باشد

مثال: رویداد، تهدید، فعالیت		**اقدامات**
	**رخ داد** – یک رویداد شدید هوا یا سونامی رخ داده است که به طور مستقیم بر سازمان و کارکنان تأثیر می گذارد – یک زلزله مهم اتفاق افتاده است که به طور مستقیم بر سازمان و کارکنان تأثیر می گذارد – هشدار آتش برای یک حادثه آتش سوزی یا اضطراری فعال شده است و شامل تخلیه کارکنان است	– اقدامات امنیتی کم ، متوسط و بالا در حال انجام است – مناطق حقوقی و مناطق اطراف به پایین نگاه می شوند – هیچ بازدید کننده ای مجاز نیست و وسایل نقلیه تحت بازرسی و دسترسی محدود هستند – ارسال و سایر تحویل ها به حالت تعلیق در می آید

	**تهدید** – ارزیابی وجود دارد که حمله تروریستی قریب الوقوع است و می تواند به خوبی برای سازمان رخ دهد یا رخ داده است – سازمان تهدید به بمب دریافت می کند	– کارکنان مهم، امنیتی و کنترل اضطراری در حالت آماده باش یا مستقر هستند – ارتباط مکرر با کارکنان – برنامه ها تحت بررسی مداوم هستند تا زمانی که هشدار مجدداً به حد بالایی برگردانده شود
	**فعالیت** یفعالیتهای اعتراضی (توسط گروهها یا یک فرد) در نزدیکی سازمان یا علیه سازمان اتفاق می افتد و اقدامات خشونت آمیز پیش بینی یا در جریان استک فعالیت اعتراض آمیز غیراعلام شد از قبل(از سوی گروهها یا افراد مستقل) در نزدیکی یا مقابل محیط پیرامون سازمان درحال وقوع است	

❖ اقدامات امنیتی خود را انجام داده و تأیید کنید

برای ارزیابی اینکه چه تدابیر امنیتی برای هر سطح هشدار نیاز دارید، از ارزیابی خود از منابع خطر و نیازهای عملیاتی هر مرکز استفاده کنید. چندین اقدام عمومی ممکن است در هر سطح هشدار مناسب باشد .برای مثال، به " اقدامات امنیتی عملیاتی برای سطح هشدار " مراجعه کنید. افراد مدیریت امنیت شما باید با مدیران محلی کار کنند و با مدیران ریسک شما مشورت کنند تا روشهای مربوط به هر مرکز و منبع خطر را تهیه کنند.

❖ محیط خطر خود را کنترل کرده و در صورت لزوم تغییر دهید

شما باید فعالانه محیط ریسک سازمان خود را کنترل کرده و سطح هشدار را تغییر دهید (افزایش یا کاهش دهید) تا با هر گونه تغییر در خطرات مطابقت داشته باشد.

❖ راهنمایی برای میزان هشدار امنیتی خود تهیه کنید

تهیه راهنما به شما کمک می‌کند تا سطح هشدار و اقدامات امنیتی مرتبط را اصلاح کنید .مهم است که با حوزه‌های مختلف تجاری در سازمان خود مشورت کنید .سعی کنید بفهمید که راهنمای شما مeffective ثر است یا تأثیراتی برای سایر فرایندهای امنیتی سازمان شما دارد .هنگامی که راهنمای شما تهیه شود، منبع حیاتی اطلاعاتی در مورد سطح هشدار امنیتی شما خواهد بود.

برای شناسایی موارد زیر با هر منطقه تجاری مشورت کنید:

- خطرات فعلی خطر برای افراد ، اطلاعات یا دارایی های شما
- هر منبع شناخته شده ای از خطر که ممکن است به دلیل تغییر در عملیات افزایش یابد
- سطح تأثیر تجارت در هر گونه عدم توانایی در ارائه خدمات
- هرگونه الزامات قانونی برای محافظت از مردم ، اطلاعات یا دارایی ها

سطح هشدار را ایجاد کنید که گزینه های کنترل امنیتی را فراهم می کند

- کاهش هرگونه تغییر مورد انتظار (افزایش یا کاهش) در سطح آسیب
- شرایط قانونی خود را برآورده کنید
- اجازه می دهد تا برای تغییر در سطح هشدار ملی

برای دریافت بازخورد آنها درباره اقدامات پیشنهادی خود ، با مناطق تجاری مشورت

راهنمای خود را تولید کنید

سطح هشدار امنیتی خود را پیاده سازی کنید

❖ **برنامه ارتباطی را تدوین کنید**

برقراری ارتباط با تغییر در سطح هشدار برای دریافت پاسخ‌های صحیح ضروری است .مردم شما باید بدانند که چه عواملی تغییر کرده و چه کاری باید انجام دهند.

برنامه ارتباطی شما به شما کمک می‌کند تا یک استراتژی موفق ایجاد کنید .شما باید مخاطبان، پیام‌ها، روش‌ها و مسئولیت‌ها را در نظر بگیرید.

مخاطبان :چه کسی باید در مورد هشدار بداند و چه چیزی باید بداند؟ ممکن است ارتباطات متفاوتی برای مخاطبان مختلف (مدیریت ارشد، کارکنان، کارکنان امنیتی) مورد نیاز باشد.

پیام‌ها :برای برقراری ارتباط با هر مخاطب کدام پیام‌ها را نیاز دارید؟ هدف ایجاد جملات موجز و بدون ابهام است که موضوعات و اقدامات لازم را به روشنی مشخص کند.

روش‌ها :چگونه پیام‌ها را برقرار می‌کنید؟ بهترین رسانه یا ترکیبی از رسانه‌ها را انتخاب کنید تا پیام‌های خود را در اسرع وقت و مؤثر به مخاطبان خود برسانید.

مسئولیت‌ها :استراتژی شما باید به وضوح شناسایی کند:

چه کسی مسئول تعیین سطح هشدار است (این ممکن است برای هر سطح و امکانات متفاوت باشد)

هر نقش یا مسئولیت خاصی برای مشاغل دیگر و همچنین کلیه کارکنان.

هنگام تهیه برنامه ارتباطی، از تیم ارتباطی خود برای مشاوره تخصصی بخواهید.

❖ **راهنمایی مرتبط**

HB167: 2006مدیریت ریسک امنیتی

این کتاب راهنما پیشنهاد می‌کند از ابزار IRACI (مداخله، مسئولیت، پاسخگویی، مشاوره و اطلاع رسانی) برای بررسی اینکه چه کسی باید در تدوین استراتژی نقش داشته باشد استفاده کنید .فرایندهای خود را مرور و به روز کنید

شما باید فرایندهای سطح هشدار خود را مرور کنید:

- وقتی پروژه‌های جدید را به عهده می‌گیرید
- با تغییر محیط خطر
- پس از یک حادثه قابل توجه که توانایی شما را برای کار کردن تحت تأثیر قرار می‌دهد
- حداقل هر ۲ سال

مراحل فعال سازی برای سطح هشدار و همچنین اقدامات امنیتی برای هر سطح را تمرین و مرور کنید .از مواردی که یاد می‌گیرید برای شناسایی شکاف‌ها و به روزرسانی راهنمای خود استفاده کنید.

❖ **پس از رفتن به سطح هشدار زیاد یا شدید، مرطوب شوید**

شرح مختصر می‌تواند برای بهبود پاسخ شما مفید باشد .بعد از هر تغییر سطح هشدار به "زیاد" یا "شدید"، رفع اشکال کنید .یک شرح مختصر باید در نظر بگیرد:

- چرا تغییر سطح هشدار آغاز شده است
- چگونه تغییر سطح هشدار آغاز شد
- چه فعالیت‌ها و اقداماتی برای تغییر سطح هشدار انجام شده است
- در صورت وجود، در چه مواردی و در کجا می‌توان پیشرفت‌هایی برای رویه‌ها و ارتباطات سطح هشدار ایجاد کرد.

تاثیرکسب و کار	نگهبانان	پلیس	کارکنان	پست‌ومر سولات	پیمانکاران	بازدیدکنندگ ان	درب‌ها	مثال:محرک، رخ داد، تهدید، یا فعالیت	سطح تهدید
عادی	عملیات عادی	درخواستی نیست	آگاهی بخش عادی	به ازاء هر سیاست	به ازاء هریک از سیاست‌های پیمانکاران	به ازاء هر یک سیاست‌های بازدید	عملیات معمول		عادی
هیچ تاثیری روی عملیات‌های عادی نیست	احتمال درخواست برای درب اصلی	درخواستی نیست	تیم امنیت یا مدیر امنیت، به پرسنل از باب مخاطرات ناشی از پست الکترونیک و خود فرد، مشاوره می‌دهند	غربالگری اضافی برای تمامی مرسولات و پستی	به ازاء هریک از سیاست‌های پیمانکاران	به ازاء هر یک سیاست‌های بازدید	عملیات معمول	تجمع اعتراضی، دریافت تهدید	پایین
-هیچ بازدیدکننده‌ای نیست و هیچ تاثیری روی فعالیت‌های خرد نیست - صرفا عملیات‌های کسب و کار اساسی صورت گیرد	حضور نگهبان در درب اصلی -پایش‌گری مستمر دوربین مداربسته CC TV -جستوجوی تمام کیف‌های همراه کارمندان -ممانعت از ورود غیر مجاز	- اطلاع‌رسانی و اخذ مشاوره پلیس، بسته به نوع رخ داد واقیع - ضرورت حضور پلیس	-ارائه مشاوره بهنگام ورود و خروج و هشدارهای لازم و آمادگی برای تغییر برنامه ها با اعلام مختصر، در صورت ضرورت -صرفا کارمندان امور اساسی به کارمندان امور غیر اساسی سازمان مشورت و دستور داده می‌شود تا در سرکار حاضر نشوند -آغاز آمادگی در انتقال عملیاتی حساس سازمان به سیاست‌های جایگزین در کوتاه‌مدت	-غربالگری اضافی روی تمامی مرسولات پستی - هیچ مرسوله یا پست غیر مورد انتظار پذیرش نخواهد گردید -تمام مرسولات و اقلام واصله چک و بررسی در وضعیت‌های مختلف و متناوب	-هیچ‌کار پیمانکاری نامعین انجام نگردد صرفا پیمانکاران ذیربط امنیت شاغل در امر عملیات امنیت مجاز به تردد هستند -هیچ پیمانکاری حاضر نخواهد بود	-هیچ بازدید غیراساسی و لازم(ترجیحا هیچ بازدید) صورت نگیرد لیکن در شرایط خاص یک بازدید کننده معلوم یا تجمع در همایش تمکن است فعال گردد -هیچ بازدید کننده‌ای نداریم	-درب‌ها به حالت وضعیت شب درآیند و تمام درب‌ها نیاز به کارت دسترسی داشته باشند -کارت‌های کنترل دسترسی روی درب‌های بیرونی غیرفعال شوند -نگهبانان درب‌های بیرونی را کنترل نمایند	-تجمع اعتراض آمیز محتمل است یا به جریان افتاده اعتراضات خشونت بار در منطقه -تهدید بمب‌گذاری نامعین -خطرفزاینده از ناحیه آب و هوا -تهدید صدمه رساندن به کارکنان - تهدید فعلی در جریان است(تجمع خشونت بار اعتراضی) -بلایای طبیعی، رویداد شدید آب و هوایی -رخ داد داخلی عمومی مانند حریق یا سیل	متوسط
عملیات اساسی در خیابان‌ها و گذرهای جایگزین ادامه یابد	حضور نگهبانان در تمام درب‌ها	ضرورت حضور پلیس	تاسیسلت بسته شوند و عملیات اساسی در محل جایگزین فعال کردد. به کارکنان اعلام گرد در محل کار حاضر نشوند -هیچ فردی از ساختمان وارد و خارج نگردد	هیچ پیمانکاری	هیچ پیمانکاری	هیچ بازدیدکننده ای	درب‌ها به طور مکانیکی ایمن‌سازی شدند و با کلید قفل شوند	تجمع اعتراضی خارج از حد کنترل یا آشوب یا رویداد تروریستی محتمل یا مورد انتظار -احتمال بالقوه در صدمات فیزیکی -فاجعه عمومی طبیعی	فوق‌العاده

۱۳-۲- آگاهی امنیتی ایجاد کنید

آگاهی از امنیت را با هرکسی در سازمان خود ایجاد کنید، بنابراین آنها از خطرات امنیتی شما آگاه هستند و فرایندهای امنیتی شما را دنبال می‌کنند

ارائه آموزش آگاهی از امنیت بخشی از تأمین نیازهای امنیتی محافظتی (PSR) است .این به سازمان شما کمک می‌کند تا یک فرهنگ امنیتی قوی ایجاد کند که از افراد، اطلاعات و دارایی‌های شما محافظت کند.

❖ **نیازهای آموزشی سازمان خود را حل کنید**

اگر مسئولیت آموزش یا مشاوره امنیتی را بر عهده دارید، از یک رویکرد سازگار و سازگار برای برآوردن نیازهای آموزشی سازمان خود استفاده کنید.

❖ **آموزش آگاهی از امنیت خود را طراحی کنید تا:**

- خطرات سازمان خود را در هنگام بررسی ریسک شناسایی کنید
- اطمینان حاصل کنید که سیاست‌ها و فرایندهای امنیتی سازمان شما دنبال می‌شود
- مسئولیت شخصی را برای امنیت توسط کلیه کارکنان و پیمانکاران، بدون در نظر گرفتن نقش و سطح دسترسی، ارتقا دهید.

❖ **دامنه را درست بگیرید**

امکانات و مکانهایی برای گنجاندن

آموزش شما باید اقدامات امنیتی را در موارد زیر پوشش دهد:

- امکانات شما
- سایر امکانات که اطلاعات و دارایی‌های شما را کنترل می‌کنند
- مکان‌هایی که کارمندان یا پیمانکاران شما در آنجا کار می‌کنند.

❖ **اقدامات امنیتی برای پوشش دادن**

آموزش شما باید شامل سیاست‌ها و فرایندهای زیر باشد:

- حفظ ایمنی شخصی
- محافظت از دارایی‌ها
- محافظت از اطلاعات رسمی
- گزارش دهی (حوادث امنیتی، تغییر شرایط شخصی و هرگونه الزامات گزارش اجباری یا قانونی)
- شرکت در جلسات امنیتی (در صورت لزوم).

❖ **مردم درگیر شوند**

به افراد زیر آموزش یا توجیهی درباره آگاهی از امنیت ارائه دهید:

- کلیه کارمندان، افراد اعطا شده و پیمانکاران مستقر در امکانات شما
- همه کارمندان، افراد دوم، پیمانکاران و سایر افرادی که به اطلاعات رسمی شما دسترسی دارند
- همه دارندگان تصفیه امنیتی دولت نیوزیلند.

❖ **اهداف آموزشی را تعیین کنید**

هر کس در سازمان شما باید قوانین امنیتی شما، و هر مسئولیت خاصی را که در مورد نقش یا زمینه‌های کاری آنها اعمال می‌شود، درک کند. هدف این است که به دانش خود دانش لازم برای انجامم. ثر وظایف امنیتی خود را بدهید .آن‌ها باید تهدیداتی را که اقدامات امنیتی شما برای مقابله با آنها طراحی کرده‌اند درک کنند، بنابراین می‌توانند به حفظ امنیت کمک کنند.

❖ **از ارائه آموزش با کیفیت اطمینان حاصل کنید**

در برنامه‌های آموزشی شما باید ترکیبی از روشهای زایمان استفاده شود و از اصول آموزش بزرگسالان پیروی کند.

در صورت لزوم، از یک ارائه دهنده آموزش امنیتی تأیید شده توسط سازمان صلاحیت نیوزلند (NZQA) استفاده کنید.

❖ **آموزش آگاهی از امنیت خود را پیاده سازی کنید**

آموزش آگاهی از امنیت باید بخشی مداوم و منظم از عملیات سازمان شما باشد.

❖ **آموزش امنیت را بخشی از القا کنید**

آموزش آگاهی از امنیت را به محض پیوستن افراد جدید به سازمان خود شروع کنید - آن را بخشی از برنامه القایی سازمان خود قرار دهید.

❖ **به طور مرتب آموزش تازه سازی ارائه دهید**

جلسات تازه سازی را به طور منظم برگزار کنید تا اقدامات امنیتی را به افراد یادآوری کرده و از اقدامات جدید به آنها اطلاع دهید.

❖ **در صورت تغییر محیط تهدید، آموزش هدفمند ارائه دهید**

هنگامی که محیط تهدید سازمان شما تغییر می‌کند یا خطر نقض امنیت افزایش می‌یابد، آموزش آگاهی از امنیت هدفمند را ارائه دهید.

❖ **برای افراد در نقش‌های اضطراری، ایمنی یا امنیتی آموزش‌هایی را ارائه دهید**

شما باید افراد و بازدید کنندگان خود را تا حد ممکن ایمن نگه دارید .برای افرادی که نقش اضطراری، ایمنی یا امنیتی دارند آموزش‌های اضافی طراحی کنید، بنابراین می‌توانند به ایمنی همه در مواقع خطر یا تهدید کمک کنند .تمریناتی را برای کمک به آنها در تمرین مهارت‌ها و تأیید صلاحیت مداوم خود انجام دهید.

برای اطلاعات بیشتر به:

- قانون ایمنی و بهداشت در محل کار ۲۰۱۵
- مقررات مربوطه
- کدها و استانداردها، مانند - AS / NZS 4804: 2001 سیستم مدیریت ایمنی و بهداشت شغلی.

❖ **برای ارتقا فرهنگ امنیتی خود به طور مثر ارتباط برقرار کنید**

برای حمایت از آموزش و فرهنگ آگاهی از امنیت خود، باید در مورد اقدامات امنیتی خود ارتباط برقرار کنید .برخی از راه‌های بالا بردن سطح آگاهی از امنیت عبارتند از:

- استفاده از کمپین‌های امنیتی برای رفع نیازهای امنیتی مداوم یا نیازهای خاص مربوط به مناطق حساس، فعالیت‌ها یا دوره‌های زمانی خاص
- ترویج فرایندها و نکات امنیتی از طریق نشریات، بولتن‌های الکترونیکی و نمایش‌های تصویری مانند پوسترها
- انجام تمرین‌ها و تمرین‌های امنیتی
- از جمله امنیتی در مصاحبه‌های شغلی
- از جمله نگرش‌ها و عملکردهای امنیتی در برنامه مدیریت عملکرد شما.

❖ **یک کتابچه راهنمای ایمنی کارمندان تهیه کنید**

یک کتابچه راهنمای ایمنی کارمندان ایجاد کنید و آن را به راحتی در دسترس همه سازمان خود قرار دهید.

کتاب راهنمای شما باید شامل موارد زیر باشد:

- دستورالعمل‌ها و تماس‌های واکنش اضطراری
- الزامات و رویه‌های ایمنی
- اقدامات ایمنی برای مناطق با خطر بیشتر، مانند مکانهای عمومی.

استانداردهای مربوط به این الزامات ایمنی - AS / NZS 4804: 2001 سیستم مدیریت ایمنی و بهداشت شغلی است.

❖ **در مورد نحوه محافظت از دارایی مشاوره دهید**

اطمینان حاصل کنید که همه می‌دانند چگونه دارایی‌های سازمان شما را ایمن نگه دارند .قبل از اینکه اجازه دسترسی به دارایی‌ها را بدهید، در مورد موارد زیر آموزش دهید:

- استفاده از سیستم‌های کنترل دسترسی و اقدامات دیگر برای محافظت از دارایی‌ها
- رعایت الزامات قانونی برای محافظت از دارایی‌ها
- گزارش دارایی‌های از دست رفته، آسیب دیده یا مسروقه
- الزامات حسابرسی و سهامداری دارایی‌ها.

❖ **آموزش محافظت از اطلاعات رسمی را ارائه دهید**

همه افراد در سازمان شما باید بدانند که اگر اطلاعات رسمی شما از بین برود، آسیب ببینند یا به خطر بیفتد، چه آسیبی می‌تواند ایجاد کند .آن‌ها همچنین باید از چگونگی آسیب پذیری منابع ارزشمند شما در برابر سازش یا سو mis استفاده آگاه باشند.

درباره مارک‌های محافظ و نیازهای دست زدن به آموزش، مانند:

- علائم محافظ فناوری اطلاعات و ارتباطات(ICT)
- تمهیدات ویژه برای تولید اسنادی که بالاتر از قابلیت سیستمهای ICT مشخص شده‌اند
- الزامات حسابرسی و پاسخگویی برای مواد مشخص شده به عنوان نیاز به حفاظت بالا.

❖ **به افراد خود آموزش دهید تا نگرانی‌های امنیتی را گزارش دهند**

یک فرایند داخلی برای گزارش نگرانی‌های امنیتی ایجاد کنید و سپس همه را آموزش دهید تا هر گونه خطرات امنیتی را که با آن روبرو می‌شوند گزارش دهند .به عنوان مثال، افراد خود را به گزارش تشویق کنید:

- رفتار مشکوک
- رفتار تهدیدآمیز از طریق نامه‌ها، تهدیدهای بمبی و تماس‌های تلفنی برقرار می‌شود
- ICTو تجهیزات امنیتی گمشده، به سرقت رفته یا خراب شده است
- نقض امنیت و نقض
- سطل‌های زباله کاملاً ایمن
- کارت‌های هویتی یا اعتباری گمشده
- مواد محافظتی یا مارک رسمی را از دست داده باشید
- تخلف جدی (در سازمان شما یا سازمان دیگر).

الزامات گزارشگری شما همچنین باید شامل هرگونه مقررات افشای محافظت شده ("افشاگری") باشد .همچنین شما باید از قانون محافظت از افشای محافظت شده ۲۰۰۰ تبعیت کنید.

❖ **گزارش منابع**

سازمان شما باید الگوهایی برای گزارش نگرانی‌های امنیتی داشته باشد.

- گزارش تغییرات شرایط
- با گزارش تماس بگیرید

❖ **در صورت لزوم، جلسات امنیتی اضافی ارائه دهید**

در برخی شرایط، باید توجیهات امنیتی ارائه دهید که فراتر از فعالیت‌های منظم آموزش و آگاهی شما باشد .مثال‌ها شامل جلسات توجیهی (و شرح مختصر) برای:

- سفرهای خارج از کشور و نیوزیلند (برای اهداف رسمی تجاری یا شخصی)
- دسترسی به مطالبTOP SECRET
- دسترسی به اطلاعات دارای علامت محافظ یا منابعی که دارای تأیید هستند، به صورت محفظه‌ای یا دارای محافظت از رمزعبور هستند
- مقاصد پرخطر
- دسته‌های خاصی از اشتغال، به عنوان مثال، مسائل امنیتی منحصر به فرد برای کارکنان فناوری اطلاعات، دانشمندان و دیگران
- پیمانکاران، کارمندان موقت، بازدید کنندگان و خانواده‌ها
- نیازهای امنیتی فرد، به عنوان بخشی از یک برنامه مدیریت مداوم.

۱۴-۲- گزارش حوادث و انجام تحقیقات امنیتی

نحوه گزارش، مدیریت و تحقیق درباره حوادث امنیتی را با استفاده از یک رویکرد سازگار و سازگار درک کنید.

این دستورالعمل‌ها نحوه مدیریت حوادث امنیتی را به عنوان بخشی از الزامات امنیتی محافظتی دولت نیوزلند پوشش می‌دهند .آن‌ها بهترین روش برای اجرای تحقیقات امنیتی را توصیف می‌کنند.

❖ گزارش حوادث امنیتی - یک نمای کلی

یک حادثه امنیتی عبارت است از:

- نقض، نقض یا نقض سیاست امنیتی یا روش محافظتی
- رویکردی از کسی که به دنبال دسترسی غیر مجاز به منابع رسمی است
- تلاشی برای دستیابی غیر مجاز به منابع رسمی
- هر رویداد دیگری که به امنیت دولت نیوزیلند، مؤسسات یا برنامه‌های آن آسیب برساند یا ممکن است آسیب برساند.

همه حوادث امنیتی به اندازه کافی قابل توجه نیستند که نیاز به بررسی داشته باشند .از آژانسهای پشتیبانی - پلیس، NZSIS، GCSB، نیروی دفاعی نیوزیلند یا سایر سازمانهای مربوطه راهنمایی بگیرید.

اگر مقامات خارجی به دنبال دسترسی غیرمجاز به منابع رسمی هستند، توصیه‌های جداگانه‌ای دارد.

❖ نقش سازمان شما

سازمان شما باید آسیب‌های ناشی از هر حادثه امنیتی را ارزیابی کند .تأثیر ضرر، سازش یا افشای واقعی، بالقوه یا مشکوک بر دولت نیوزیلند را تعیین کنید.

شما باید:

- تشخیص اینکه این حادثه جزئی است (تخلف یا نقض قانون) یا عمده (تخلفی که باید گزارش دهید)
- گزارش این حادثه را به سایر نهادهای مربوطه مانند سرویس اطلاعات امنیتی نیوزیلند(NZSIS) ، دفتر امنیت ارتباطات دولتی(GCSB) ، CERT، کمیسر حریم خصوصی یا افسر ارشد دیجیتال دولت (GCDO) گزارش دهید.

❖ همیشه این نوع حوادث امنیتی را گزارش دهید

افراد و پیمانکاران شما باید گزارش دهند:

- جرایمی مانند سرقت یا اقدام به سرقت، سرقت، خسارت به عنوان مثال تخریب، کلاهبرداری یا تعرض
- وقایع طبیعی مانند آتش سوزی یا طوفان که ممکن است امنیت را به خطر بیندازد
- مدیریت نادرست اطلاعاتی که از نظر محافظتی مشخص شده است.

❖ افراد و وظایف دخیل در گزارش حوادث امنیتی

سازمان شما باید خط مشی گزارش دهی حوادث امنیتی را داشته باشد .این باید نقش‌ها و مسئولیت‌های افرادی را که به حوادث امنیتی رسیدگی می‌کنند و تحقیقات امنیتی را انجام می‌دهند، پوشش دهد.

❖ **رئیس اجرایی یا روسای آژانس**

رئیس اجرایی یا رئیس آژانس شما باید از موارد زیر اطمینان حاصل کند:

- فرآیندهای کارمندان، پیمانکاران و کارمندان پیمانکار برای گزارش حوادث امنیتی
- سوابق عملکرد امنیتی و نیازهای سازمان.

❖ **مدیران ارشد**

مدیران ارشد مسئول اقدامات مربوط به گزارش و ضبط حوادث امنیتی - در مناطق خود و به طور کلی سازمان هستند .افسر ارشد امنیت (CSO) یا نماینده آنها باید به آنها کمک کند.

در تحقیقات امنیتی، یک مدیر ارشد، مستقل از حادثه، باید شرایط مرجع و اهداف را تأیید کند .آن‌ها همچنین باید گزارش‌های منظمی درباره پیشرفت تحقیقات دریافت کنند.

❖ **مدیران**

مدیران شما باید اطمینان حاصل کنند که حوادث امنیتی به سازمان امنیت ملی گزارش شده است و در مورد هرگونه نگرانی امنیتی با آنها همکاری نزدیک داشته باشند.

اگر حادثه‌ای شامل سیستم ICT شما باشد، ممکن است لازم باشد که خود را به رئیس ارشد امنیت اطلاعات (CISO) گزارش دهید.

مدیران نقش مهمی دارند .از آنجا که آنها از نزدیک با کارکنان همکاری می‌کنند، آن‌ها می‌توانند اولین کسی باشند که یک حادثه امنیتی را تشخیص می‌دهند یا رفتار مشکوکی را مشاهده می‌کنند.

❖ **CSO**

سازمان امنیت داخلی یا نماینده شما اطلاعات مربوط به حوادث امنیتی را دریافت و عمل می‌کند.

آن‌ها باید حوادث امنیتی و نتیجه تحقیقات را ثبت کنند و از عملکرد امنیتی به طور مرتب به مدیران ارشد گزارش دهند.

❖ **CISO مدیر امنیت فناوری اطلاعات(ITSM)**

CISOیا ITSM شما اطلاعات مربوط به حوادث مربوط به سیستم‌های ICT را دریافت و عمل می‌کند .این موارد شامل حملات انکار سرویس، حملات ایمیل مخرب هدفمند و از بین رفتن دارایی‌ها یا اطلاعات ICT است. آن‌ها باید وقایع مهم امنیتی ICT را به مرکز ملی امنیت سایبری (NCSC) گزارش دهند. آن‌ها باید در مورد هرگونه حادثه امنیتی ICT و تأثیرات احتمالی به سازمان امنیت ملی شما اطلاع دهند CISO .ممکن است در بررسی حوادث امنیتی ICT نقشی داشته باشد.

❖ **کارمندان**

هرکسی که برای سازمان شما کار می‌کند باید از روند شما برای گزارش حوادث امنیتی مطلع باشد و آن را دنبال کند.

سازمان شما باید آموزش آگاهی از امنیت را برای کارمندان، پیمانکاران و کارمندان پیمانکاران ارائه دهد.

۱۵-۲- فرایندهای گزارش حوادث امنیتی

سازمان شما باید فرآیندهای رسمی برای پاسخگویی و گزارش حوادث امنیتی محافظ داشته باشد .شما باید همه را از مسئولیت‌های خود و فرایندهای گزارش آگاه کنید.

آن‌ها باید از ضرورت گزارش هرکسی که به دنبال دسترسی به اطلاعاتی است که اجازه دسترسی به آنها را ندارند، آگاه باشند.

برای گزارش تخلف از امنیت سایبری، در راهنمای امنیت اطلاعات نیوزلند - حوادث امنیت سایبری مشاوره پیدا کنید .

❖ **ضعف‌های امنیتی را گزارش دهید**

افراد شما باید نقاط ضعف امنیتی را که می‌بینند یا به آنها مشکوک هستند، و تهدیدهای مربوط به روندها، سیاست‌ها، سیستم‌ها یا خدمات را گزارش دهند .آن‌ها باید در اسرع وقت نقاط ضعف را گزارش دهند.

مردم شما هرگز نباید سعی کنند ضعف مشکوک را ثابت کنند .این برای محافظت از خودشان است .آزمایش یک ضعف ممکن است به عنوان سو mis استفاده از سیستم تلقی شود.

❖ **از حوادث بیاموزید**

سازمان شما باید فرایندهایی برای نظارت و اندازه گیری انواع، حجم و هزینه‌های حوادث و سو mal عملکردها داشته باشد .از اطلاعات استفاده کنید تا:

- مشکلات تکرار شونده یا تأثیر زیاد را شناسایی کنید
- بررسی کنید که آیا برای محدود کردن مشکلات به اقدامات بیشتری نیاز دارید یا بهتر
- سیاست امنیتی را مرور کنید.

❖ **یک روند رسمی داشته باشید**

سازمان شما باید برای کارکنانی که خط مشی‌ها و روندهای امنیتی شما را نقض می‌کنند، فرایند رسمی داشته باشد .این ممکن است بخشی از روند شما برای رسیدگی به سو رفتار باشد.

این تضمین می‌کند که با هرکسی که به نقض امنیت مشکوک است رفتار منصفانه‌ای انجام می‌شود.

این فرایند را به عنوان بخشی از انگیزه‌های کارکنان و در آموزش آگاهی از امنیت خود پوشش دهید.

❖ **اطمینان حاصل کنید که کارکنان حوادث امنیتی را گزارش کرده‌اند**

سیاست و فرآیندهای امنیتی سازمان شما باید:

- ایجاب می‌کند که کارکنان و پیمانکاران شما موارد امنیتی را گزارش دهند
- شامل روشها و سازوکارهای رسمی برای آسان کردن گزارش دهی است
- به CSO نیاز دارد تا پرونده وقایع را ثبت کند.

آموزش آگاهی از امنیت سازمان شما باید شامل چگونگی گزارش حوادث باشد و بیان کند که کارکنان باید حوادث را گزارش دهند.

❖ **ثبت وقایع امنیتی**

روش‌هایی را برای ثبت حوادث متناسب با محیط امنیتی و عملکرد سازمان خود ایجاد کنید.

در پرونده خود از حوادث امنیتی، موارد زیر را وارد کنید:

- زمان، تاریخ و مکان
- نوع منابع رسمی درگیر
- شرح شرایط حادثه
- خواه این حادثه عمدی بوده باشد یا تصادفی
- ارزیابی میزان سازش یا آسیب
- خلاصه‌ای از اقدامات فوری و طولانی مدت شما.

ثبت حوادث امنیتی بینش ارزشمندی در مورد محیط امنیتی و عملکرد یک سازمان فراهم می‌کند .به عنوان مثال، اگر بسیاری از حوادث امنیتی جزئی داشته باشید، این می‌تواند نشان دهد که آگاهی کارکنان ضعیف است و شما نیاز به آموزش بیشتر آگاهی از امنیت دارید. سازمان‌های اجتماعی باید مرتباً جزئیات حوادث امنیتی و هرگونه روند را به رئیس سازمان شما گزارش دهند.

❖ **فرآیندهای شخصی خود را برای حوادث جزئی امنیتی ایجاد کنید**

سازمان شما منحصر به فرد است، بنابراین شما باید فرآیندهای مربوط به خود را برای بررسی حوادث امنیتی جزئی توسعه دهید.

در مورد حوادث امنیتی مربوط به دارندگان مجوزهای امنیتی به NZSIS بگویید باید در مورد این موارد به سرویس اطلاعاتی امنیتی نیوزلند (NZSIS) بگویید:

- تکرار حوادث امنیتی جزئی
- حوادث مهم امنیتی که مربوط به شایستگی شخص در داشتن یک مجوز امنیتی است
- نتیجه هرگونه تحقیقات امنیتی که مربوط به شایستگی شخص در داشتن یک مجوز امنیتی است .

❖ **گزارش تماس با مقامات خارجی**

هر کارمندی که دارای مجوز امنیتی است باید تماس غیرمعمول یا مشکوک با مقامات خارجی یا درخواست مقامات خارجی برای دسترسی به دارایی‌های شما یا اطلاعات دارای محافظ را گزارش کند اطلاعات بیشتر در Contact Reporting وجود دارد.

❖ **رویه‌های رسمی را برای یک حادثه مهم امنیتی ایجاد کنید**

سیاست‌ها و فرایندهای شما برای مقابله با حوادث مهم امنیتی باید رسمیت بیشتری داشته باشد.

❖ **وقتی سازمان دیگری درگیر آن باشد**

اگر یک حادثه امنیتی مهم مشکوک به منابعی از سازمان دیگری است، قبل از شروع تحقیقات از آن سازمان مشاوره بگیرید .این سازمان ممکن است الزامات امنیتی عملیاتی داشته باشد .برای سازمان منشأ origin یا مسئول انجام تحقیقات ممکن است مناسب‌تر باشد .اصل "نیاز به دانستن" را اعمال کنید.

وقایع مهم امنیتی را به آژانس‌های امنیتی گزارش دهید

- در صورت بروز هرگونه مورد مشکوک، باید به آژانس امنیتی مناسب گزارش دهید:
- جاسوسی(NZSIS)
- خرابکاری(NZSIS) ، NZ Policeیا هر دو
- اقدامات دخالت خارجی(NZSIS)
- حملات به سیستم دفاعی نیوزیلند (نیروی دفاعی نیوزیلند)
- خشونت با انگیزه سیاسیNZSIS ،(پلیس NZ یا هر دو)
- تحریک به خشونت جمعیNZSIS ، (پلیس NZ یا هر دو)
- تهدیدهای جدی برای مرز نیوزیلند (گمرک و مهاجرت، وزارت صنایع اولیه یا هر دو).

یک ارزیابی اولیه انجام دهید، سپس در اسرع وقت با آژانس یا آژانس‌های مربوطه تماس بگیرید .اطلاعات را فقط بر اساس نیاز بدانید تا زمانی که خلاف این به شما گفته شود .در صورت عدم اطمینان با مدیر تعامل PSR خود تماس بگیرید.

❖ **گزارش حوادث امنیت سایبری به مرکز امنیت سایبری ملی**

هر گونه مورد مشکوک به امنیت سایبری را به مرکز ملی امنیت سایبری گزارش دهید از جمله:

- ایمیل‌های مشکوک یا ظاهراً هدفمند با پیوست یا پیوند
- هرگونه مصالحه یا فساد اطلاعات
- هک کردن
- ویروس‌ها
- اختلال یا آسیب رساندن به خدمات یا تجهیزات
- نشت داده‌ها

برای جلوگیری از به خطر افتادن تصادفی در تحقیقات امنیت سایبری، سیاست‌ها و برنامه‌های امنیتی ICT سازمان شما نیاز به تماس زودهنگام با NCSC دارد.

❖ **گزارش وقایع امنیتی مربوط به مواد کابینه به دفتر کابینه**

گزارش وقایع مظنون امنیتی مربوط به کابینه به کابینه در دفتر نخست وزیر و کابینه.

کتابچه راهنمای کابینه امنیت و نحوه رسیدگی به اسناد کابینه را پوشش می‌دهد .کتابچه راهنمای کابینت آنلاین.

❖ **حوادث جنایی را به نهادهای انتظامی گزارش دهید**

در مواردی که این حادثه ممکن است یک جرم جنایی باشد، ممکن است لازم باشد که به نهاد اجرای قانون مربوطه گزارش دهید .از پلیس NZ مشاوره بخواهید. برای حوادث مهم مربوط به امنیت عمومی از کمک اضطراری استفاده کنید در مواردی که زندگی یا امنیت عمومی در معرض خطر است، با خدمات اضطراری تماس بگیرید - شماره ۱۱۱ را بگیرید.

حوادث مهمی که ممکن است بر ایمنی عمومی تأثیر بگذارد شامل انواع زیر است:

❖ **حملات شخصی:**

- حمله کردن
- استفاده از سلاح از جمله سلاح گرم

- تهدیدات صدمه به خود یا دیگران
- تظاهرات خشن با اخلال جدی در نظم عمومی
- حمله شیمیایی، بیولوژیکی یا رادیولوژیکی (CBR) یا حمله CBR مشکوک
- حوادث پودر سفید، از جمله حوادث واقعی و قابل توجه حقه.

❖ **گروگان گیری، واقعی یا مشکوک:**

- وضعیت گروگان گیری
- هواپیماربایی
- آدم ربایی
- حملات به دارایی یا اطلاعات:
- آتش سوزی یا مشکوک به آتش سوزی
- بمب گذاری
- بمب پست الکترونیکی یا بمب پست الکترونیکی مشکوک
- حمله به زیرساخت اطلاعات ملی یا زیرساختهای حیاتی که از آن استفاده می‌کند.

❖ **موارد مهم بهداشت و ایمنی شغلی را گزارش دهید**

شما باید وقایع بهداشتی و ایمنی را که منجر به جراحات یا مرگ جدی شده است به WorkSafeنیوزیلند گزارش دهید.

❖ **هنگام گزارش موارد مهم امنیتی، این جزئیات را وارد کنید**

هنگام گزارش موارد مشکوک امنیتی مهم، این جزئیات را پوشش دهید:

- تاریخ و زمان حادثه یا زمان گزارش یا کشف آن
- محل
- جزئیات مختصر
- آنچه ممکن است به خطر بیفتد (و نوع و سطح مارک محافظ، در صورت وجود)
- اگر می دانید نام افراد درگیر این حادثه است
- نام و اطلاعات تماس آژانس برای پیگیری
- ارزیابی اولیه از آسیب یا خسارت
- شما چه اقدامی انجام داده‌اید

اگر یک حادثه مهم را گزارش کرده‌اید، اطمینان حاصل کنید که هر گونه به روزرسانی و تغییر وضعیت را نیز گزارش می‌کنید.

شما مسئول گردش اطلاعات در مورد حوادث درون سازمان خود هستید.

۱۶-۲- بررسی حوادث امنیتی

تحقیقات امنیتی مشخص می‌کند که چه چیزی باعث بروز این حادثه شده و تا چه حد امنیت مردم، اطلاعات یا دارایی‌ها را به خطر انداخته یا تهدید کرده است .

❖ **اصول انصاف را اعمال کنید**

اصول انصاف رویه در همه تحقیقات اعمال می‌شود .به افرادی که حقوق، منافع یا انتظارات آنها تحت تأثیر قرار گرفته است باید به آنها رسیدگی شود و به آنها فرصت داده شود تا توسط یک تصمیم گیرنده بی طرف شنیده شوند.

اقدامات ناشی از تحقیقات باید منصفانه باشد .اطلاعات بیشتر در مورد الزامات عدالت رویه ای است.

❖ نتایج احتمالی تحقیقات را درک کنید

نتایج یک تحقیق می‌تواند شامل موارد زیر باشد:

- انصراف از اتهامات انضباطی
- آموزش / آموزش
- تغییر در سیاست‌ها، رویه‌ها یا روش‌های اداری یا امنیتی
- نتیجه امنیت، از جمله از دست دادن احتمالی امنیت امنیتی
- ارجاع به آژانس خارجی برای تحقیقات بیشتر یا پیگرد قانونی
- اقدام انضباطی.

❖ اقدامات موقت در حالی که تحقیقات در جریان است

در برخی شرایط، لازم است اقدامات امنیتی موقت انجام شود، در حالی که تحقیقات در حال انجام است .آنچه مناسب است در هر مورد متفاوت خواهد بود .شما باید نیاز به محافظت از افراد، اطلاعات یا دارایی‌های خود را با تعهدات شغلی خود از عدالت طبیعی متعادل کنید.

اقدامات موقت شما ممکن است در نظر بگیرید:

- انجام حسابرسی از اطلاعات مربوطه
- نظارت بر استفاده از رایانه
- نظارت بر دسترسی ساختمان
- دسترسی کامپیوتر را محدود می‌کند
- از بین بردن دسترسی به رایانه
- محدود کردن دسترسی پس از ساعت به محل کار
- از بین بردن دسترسی به محل کار (به دنبال تصمیم به تعلیق پیگیری مراحل قانونی).

هر گونه پاسخ باید توجیه پذیر و متناسب با نگرانی موجود باشد و به طور مناسب جهت محافظت از افراد، اطلاعات یا دارایی‌های بالقوه در معرض خطر باشد .این باید یک گام موقت برای محافظت از افراد، اطلاعات یا دارایی شما باشد در حالی که تحقیقات امنیتی در حال انجام است.

در بیشتر شرایط مناسب است که به کارمند بگوییم چه اقدامات موقت انجام می‌شود، به ویژه در جایی که کارمند در محل کار باقی می‌ماند .به عنوان مثال، محدود کردن دسترسی به ساختمان یا سیستم باید به وضوح توضیح داده شود .به کارمند باید گفته شود که اقدامات امنیتی در حال انجام است، ضمن ادامه تحقیقات امنیتی، اقدامات موقت است و از پیش تعیین شده‌ای را نشان نمی‌دهد .اقدامات باید با توجه به نگرانی‌های موجود انجام شود و خودسرانه اعمال نشود.

با این حال، مواردی وجود خواهد داشت که اطلاع رسانی به کارمند در مورد اقدامات موقت مناسب نیست .به عنوان مثال، هنگامی که نظارت بر استفاده از رایانه ضروری تلقی می‌شود، اطلاع دادن به کارمند ممکن است هدف از نظارت را به خطر

بیندازد. تعامل زودهنگام با منابع انسانی برای اطمینان از اقدامات امنیتی مناسب و متعادل سازی تعهدات شغلی عدالت طبیعی ضروری است.

❖ **چه کسی باید درگیر شود؟**

اگر یک تحقیق امنیتی را آغاز کردید، هنگامی که تخلف ممکن است شامل امنیت ملی یا رفتار جنایی باشد، از پلیس یا NZSIS مشاوره بگیرید.

اگر حادثه‌ای به بیش از یک نوع تحقیق نیاز دارد، برای تعیین اولویت‌ها و رویکرد تحقیق با آژانس (های) دیگر همکاری کنید.

❖ **نقش تحقیقات جنایی**

تحقیقات جنایی شواهدی را جمع آوری می‌کند که ممکن است منجر به معرفی مجرمین در دادگاه شود.

ممکن است لازم باشد در مواردی مانند کلاهبرداری، سرقت و افشای غیرمجاز اطلاعات رسمی تحقیقات جنایی را انجام دهید.

اطلاعات جمع آوری شده در تحقیقات امنیتی ممکن است در تحقیقات جنایی رضایت بخش نباشد.

❖ **نقش تحقیقات امنیتی**

هدف از تحقیقات امنیتی مشخص کردن آنچه اتفاق افتاده و چگونه است تعیین اینکه آیا جرمی کیفری مرتکب شده است، کمک به تعقیب قضایی یا حل و فصل اختلافات مربوط به شغل یا نحوه رفتار نیست.

تحقیقات امنیتی بر ایجاد موارد زیر متمرکز است:

- ماهیت حادثه
- چگونه حادثه رخ داده است
- چه شرایطی منجر به حادثه شد
- که درگیر بود
- میزان آسیب به منافع امنیت ملی
- روش‌های مورد نیاز برای جلوگیری از یک رویداد مشابه یا کاهش احتمال آن.

اگر تحقیقات امنیتی جای خود را به تحقیقات جنایی داد، از آن به بعد شما باید از مراحل تحقیق جنایی و جمع آوری مدارکی که در دادگاه قابل قبول است استفاده کنید.

❖ **رویه‌هایی را برای بررسی حوادث امنیتی تنظیم کنید**

سازمان شما باید خط مشی و رویه‌هایی را برای بررسی حوادث امنیتی تعیین کند .این الزامات را پوشش دهید.

مسئولیت‌ها و اقدامات:

- مسئولیت‌های بازپرس و مدیریت ارشد
- وقتی شکایتی یا ادعایی دریافت کردید، از جمله ادعاهای ناشناس و گزارش‌های افشاگران، چه کاری باید انجام دهید
- شرایط مرجع تحقیق
- چه زمانی تحقیقات امنیتی را بهNZSIS ، پلیس یا سایر آژانس‌های خارجی ارجاع دهید.

روش‌ها:

- استانداردهای رفتار اخلاقی توسط بازرسان، ثبت فعالیت‌ها و نحوه مدیریت موارد تحقیق
- روش‌های عملیاتی مانند برگزاری مصاحبه.

الزامات گزارش

- حفظ یادداشت‌های پرونده دقیق
- مدیریت ارشد را از پیشرفت آگاه سازید
- گزارش نهایی که شامل اطلاعات پیشینه است
- خلاصه‌ای از یافته‌ها و توصیه‌های عمده

❖ یک محقق را انتخاب کنید

یک بازرس منصوب کنید که به طور مناسب آموزش دیده و واجد شرایط باشد .آن‌ها باید بی طرف باشند .آن‌ها نباید در تحقیقات تضاد منافع، واقعی یا آشکار داشته باشند.

اگر بازپرسی که منصوب کرده‌اید قدرت و اختیاری برای جمع آوری هیچ مدرکی ندارد، یا در صورت بروز تعارض منافع، تحقیقات را با هیئت‌های لازم به شخص یا سازمانی ارجاع دهید.

اطلاعات بیشتر در مورد الزامات عدالت رویه ای است.

❖ نقش یک محقق را درک کنید

وظایف اصلی یک محقق باید شامل موارد زیر باشد:

- درک واقعه و شرایط مرجع
- شناسایی قانون، سیاست یا رویه‌های مربوطه
- جمع آوری تمام حقایق مرتبط
- تأیید اینکه آیا این حادثه جرم است
- گزارش یافته‌ها، و دلایل یافته‌ها
- پیشنهاد دادن

❖ ماهیت تحقیق را تعیین کنید

در ابتدا، ارزیابی کنید:

- اینکه تحقیقات احتمالاً تحقیق جنایی است، امنیتی یا نوع دیگری است
- منابع مورد نیاز
- مرزهای قانونی برای تحقیق
- مجوز لازم است
- ماهیت نتیجه احتمالی

❖ **شرایط مرجع را برای تحقیقات تعیین کنید**

شرایط مرجع باید روشن، جامع و شامل هر محدودیتی باشد .آن‌ها می‌توانند شامل موارد زیر باشند:

- پس زمینه
- منابع تخصیص یافته (به عنوان مثال، مردم، مالی)
- چارچوب زمان
- انواع سالاتی که باید انجام شود
- اختیارات افسر تحقیق برای جمع آوری شواهد
- قالب گزارش
- هرگونه الزامات خاص یا عوامل خاص تحقیق

همچنین نحوه جمع آوری شواهد از سوی محقق توسط موارد زیر را پوشش دهید:

- از سیاست‌ها، فرایندها و روش‌ها
- از سوابق و مطالب مربوطه
- از طریق مصاحبه
- با جستجو و نظارت

در آغاز تحقیقات، یک کارمند ارشد را برای تأیید شرایط مرجع و برنامه تحقیق منصوب کنید.

❖ **فرآیندهایی را برای انجام تحقیقات تعیین کنید**

فرایندهای تحقیق سازمان شما باید شامل موارد زیر باشد:

- قانونگذاری و اختیارات خاص و خاص سازمان
- روابط بین آژانس‌ها
- هنگام دریافت ادعایی چه کاری باید انجام شود (از جمله روند "افشاگران" تحت قانون افشای محافظت شده)
- روش‌های مدیریت و پشتیبانی تحقیقات
- شیوه‌های تحقیق
- گزارش تحقیق یا مختصر شواهد
- اصول حفظ حریم خصوصی اطلاعات(IPP)
- نتیجه تحقیق و بررسی
- اقدامات بهبودی

❖ **حادثه را ارزیابی کنید**

محقق باید ارزیابی کند:

- قوانین مربوط

- ماهیت حادثه
- جدی بودن حادثه و میزان احتمالی آسیب رساندن به سازمان یا دولت
- اینکه آیا این حادثه نشان می‌دهد که یک مشکل سیستمی وجود دارد
- خواه بخشی از یک الگو باشد
- آیا ممکن است قانون نیوزیلند را نقض کند

❖ برنامه تحقیق را تدوین کنید

از ارزیابی حادثه برای تهیه برنامه تحقیق استفاده کنید که مشخص کند:

- موضوعات کلیدی مورد بررسی
- هر قانون مربوطه، مفاد یک آیین نامه رفتار، سیاست و رویه‌های سازمان، استانداردها و الزامات
- شواهد مورد نیاز
- روش‌های جمع آوری شواهد
- الزامات قانونی و رویه‌هایی که باید در جمع آوری شواهد دنبال شود
- تخصیص وظایف، منابع
- زمان سنجی.

اگر در طول تحقیقات شرایط مرجع و طرح تحقیق تغییر کند، محقق باید با شخصی که تحقیق را مجاز کرده است مشورت کند.

❖ جمع آوری اطلاعات

یک محقق اطلاعاتی را اثبات یا رد می‌کند که واقعیت‌های مربوط به حادثه را شناسایی، جمع آوری و ارائه می‌کند .انواع اطلاعات عبارتند از:

- فیزیکی
- مستند
- دهانی
- مشاوره تخصصی

❖ تمام شواهد را ثبت و ذخیره کنید

محققان باید برای هر تحقیق پرونده جداگانه‌ای داشته باشند .آن و هرگونه مدرک فیزیکی را به صورت ایمن ذخیره کنید.

پرونده باید یک پرونده کامل از تحقیقات باشد .هر مرحله، شامل تاریخ و زمان، تمام بحث‌ها، تماس‌های تلفنی، مصاحبه‌ها، تصمیمات و نتیجه گیری را مستند کنید .نحوه رسیدگی به شواهد فیزیکی را درج کنید.

اگر در حین تحقیقات اطلاعاتی با علامت محافظ جمع آوری یا ایجاد شده باشد، محققان باید از استانداردهای ذخیره سازی برخوردار باشند .اطلاعات بیشتر در مورد رسیدگی به الزامات اطلاعات و تجهیزات دارای علامت محافظ است.

❖ **گزارش تحقیق را تهیه کنید**

محقق باید یافته‌ها را به نهاد سفارش دهنده یا تصمیم گیرنده گزارش دهد .آن‌ها باید دلایل یافته‌ها را با توجه به شرایط مرجع شناسایی کنند، از مطالب پشتیبانی کننده استفاده کنند و توصیه‌هایی ارائه دهند.

❖ **تحقیق را ببندید و بررسی کنید**

وقتی تمام گزارش‌ها به اتمام رسید و شواهد مستند و ثبت شد، تحقیقات مختومه می‌شود.

یک فرد مستقل، در حالت ایده آل با تجربه تر از بازپرس، باید تحقیقات مختومه را بررسی کند .آن‌ها باید تحقیقات را بی طرفانه ارزیابی کنند و این می‌تواند نحوه بهبود الزامات تحقیقات آینده را شناسایی کند.

۱۷-۲- مدیریت تداوم کسب و کار

با برنامه مدیریت تداوم تجارت، انعطاف پذیری سازمان خود را تقویت کرده و اقدامات امنیتی خود را تقویت کنید .

❖ **برای تداوم تجارت آماده شوید**

یک برنامه مدیریت تداوم کسب و کار داشته باشید، تا عملکردهای حیاتی سازمان شما در حین ایجاد اختلال تا حد ممکن ادامه یابد .اطمینان حاصل کنید که برای تداوم منابعی که از عملکردهای حیاتی شما پشتیبانی می‌کنند، برنامه ریزی کرده‌اید.

تداوم تجارت توانایی سازمان برای ادامه تحویل محصولات یا خدمات در سطوح قابل قبول از پیش تعریف شده پس از یک حادثه مخرب است.(ISO 22301: 2012)

ایجاد اختلال هر چیزی است که به طور معمول فعالیت شما را قطع کند .به هر دلیلی اختلالات ممکن است در هر زمان رخ دهد و تأثیر آنها متفاوت باشد. از جمله دلایل بروز این اختلالات می‌توان به وقایع طبیعی مانند زمین لرزه یا شرایط جوی شدید، از بین رفتن منبع اصلی مانند قطع برق یا اختلال در زنجیره تأمین و تهدیدات امنیتی مانند حملات سایبری اشاره کرد.

❖ **چرا مدیریت تداوم تجارت مهم است**

برنامه‌ای برای مدیریت تداوم کسب و کار به شما کمک می‌کند تا بدون در نظر گرفتن علت، تأثیرات اختلالات را مدیریت کنید .یک برنامه موفق شامل موارد زیر است:

- برنامه ریزی و بهبود مستمر
- انجام فعالیتهایی برای اطمینان از آمادگی در برابر حوادث مخرب
- تعمیم تجارت در فرهنگ و عملکرد سازمان شما.
- مدیریت تداوم کسب و کار از یک چرخه مداوم پیروی می‌کند:
- دامنه و رویکرد برنامه خود را تأیید کنید
- توابع حیاتی را شناسایی و اولویت بندی کنید
- منابع و نیازهای مورد نیاز برای حفظ عملکردهای مهم را در نظر بگیرید
- راه حل‌ها را شناسایی و به کار گیرید تا اطمینان حاصل کنید که می‌توانید الزاماتی را که شناسایی کرده‌اید برآورده کنید

- برنامه‌های سند برای تداوم تجارت و فرآیندهای پاسخگویی به حوادث
- تأیید کنید که برنامه‌ها و فرآیندهای شما از طریق تمرین و بررسی منظم کار می‌کنند.

❖ **چگونه برنامه ریزی برای تداوم تجارت امنیت شما را تقویت می‌کند**

اطلاعاتی که برای برنامه تداوم فعالیت سازمان خود جمع می‌کنید، با شناسایی آنچه برای محافظت از آن نیاز دارید، برنامه‌های امنیتی جسمی و اطلاعاتی شما را تقویت می‌کند.

هنگامی که افراد از سایر رشته‌های محافظتی سازمان شما درگیر شناسایی تهدیدات احتمالی و اقدامات پیشگیرانه باشند، می‌توانید با همکاری یکدیگر مقاومت سازمان خود را بهبود بخشید.

- دامنه برنامه تداوم کسب و کار خود را تنظیم کنید
- توابع حیاتی و نیازهای آنها را شناسایی کنید
- برای حفظ عملکردهای حیاتی خود برنامه ریزی کنید
- در صورت ایجاد اختلال، تیم‌هایی را برای مدیریت تداوم تجارت تنظیم کنید
- برنامه تداوم تجارت خود را حفظ کنید
- الزامات قانونی، استانداردهای ISO و بهترین روش برای مدیریت تداوم تجارت

۲-۱-۱۸- دامنه برنامه تداوم کسب و کار خود را تنظیم کنید

اولین مرحله در اجرای برنامه تداوم تجارت تأیید دامنه با مدیریت ارشد است.

❖ **دامنه برنامه خود را مشخص کنید**

دامنه، زمینه‌های اولویتی را که برنامه شما در بر خواهد گرفت، در سطح بالایی تعریف می‌کند - نه همه کارهایی که سازمان شما به عنوان "تجارت معمول" انجام می‌دهد، می‌تواند یا باید در هنگام اختلال حفظ شود .دامنه برنامه شما باید سازمان شما را در نظر بگیرد:

- مسئولیت‌های قانونی
- استراتژی کلی
- اهداف
- ساختار

وقتی دامنه را تنظیم می‌کنید، اطمینان حاصل کنید که مناطق اولویت شما به آن بستگی دارد، مانند عملکردها و منابع پشتیبانی.

هنگامی که برنامه تداوم کسب و کار را ایجاد کردید، دامنه آن را مرتباً مرور کنید تا همچنان منعکس کننده مسئولیت‌ها، اهداف و عملکردهای سازمان شما باشد.

❖ **سیاستی برای مدیریت تداوم تجارت ایجاد کنید**

سیاستی تدوین کنید که اهداف و پوشش برنامه تداوم تجارت شما را مشخص کند .مدیریت ارشد باید این خط مشی را تأیید کند.

خط مشی مدیریت تداوم تجارت باید شامل موارد زیر باشد:

- تعریفی از مدیریت تداوم تجارت
- به هر استاندارد و راهنمایی که دنبال می‌کنید مراجعه کنید
- آنچه برنامه شما پوشش می‌دهد
- چگونه برنامه شما ساختار یافته و اجرا می‌شود
- ارتباط با سایر سیاست‌ها، فرایندها و رشته‌های درون سازمانی شما (به عنوان مثال، مدیریت ریسک).

❖ **افراد توانمند را شناسایی کنید و مسئولیت تعیین کنید**

شما برای انجام مدیریت تداوم شغل به افرادی از همه سطوح سازمان نیاز دارید .افراد توانمند را برای مجوز، مدیریت و اجرای برنامه خود شناسایی کنید .نقش‌هایی که باید پوشش دهید عبارتند از:

- یک تیم حکمرانی
- یک مدیر ارشد برای حمایت از برنامه
- تیمی برای اجرای برنامه
- رهبران بخش‌ها، صاحبان برنامه‌ها و کارشناسان موضوع
- تیم‌های پاسخگویی به حوادث.

❖ **پاسخ خود را در بین رشته‌ها هماهنگ کنید**

برنامه تداوم کسب و کار شما باید چارچوبی را برای مدیریت یکپارچه حوادث برای سازمان شما فراهم کند .در مواردی که سایر عملکردها - مانند امنیت، حریم خصوصی و فناوری اطلاعات - رویه‌های مدیریت حوادث را دارند، اطمینان حاصل کنید که هر تیم از ساختارهای پاسخ دیگران، عوامل تحریک کننده و مسیرهای تشدید آگاهی دارد.

برای اطمینان از یک واکنش جامع و کل سازمان در برابر همه حوادث، روش‌های مختلف مدیریت حوادث و برنامه‌های مرتبط باید بتوانند به طور مستقل یا مشترک

۲-۱-۱۹- برای حفظ عملکردهای حیاتی خود برنامه ریزی کنید

روندی را دنبال کنید تا برنامه ریزی کنید که چگونه عملکردهای حیاتی خود را حفظ خواهید کرد .سپس برنامه‌های خود را مستند و تأیید کنید.

❖ **راه حل‌ها را طراحی و اجرا کنید**

پس از شناسایی الزامات مورد نیاز برای هر عملکرد حیاتی، می‌توانید نحوه نگهداری یا از سرگیری این عملکردها را در صورت مختل شدن برنامه ریزی کنید.

طیف وسیعی از راه حل‌ها را که می‌توانید برای هر منبع مورد نیاز به کار ببرید، در نظر بگیرید، استراتژی مورد نظر را پیاده سازی کنید و خلأهای خود را برطرف کنید.

راه حل‌ها عبارتند از:

- متنوع سازی (به عنوان مثال، داشتن مکان‌های جداگانه که در آن فعالیت مشابه به طور موازی اتفاق می افتد)

- تکرار (به عنوان مثال، داشتن افرادی در مکان دیگری که آموزش دیده و قادر به انجام یک فرآیند مهم هستند، اما این کار را به عنوان "تجارت معمول" انجام نمی‌دهند)
- استفاده از گزینه‌های آماده به کار (به عنوان مثال، حفظ امکانات جایگزین که می‌تواند در بازه زمانی بهبودی عملیاتی شود)
- به دست آوردن یک منبع یا خدمات پس از یک حادثه
- برون سپاری عملکرد به شخص ثالث
- داشتن بیمه
- با استفاده از راه حل‌های دستی
- هیچ کاری نکردن

برای اجرای راه حل‌ها، ممکن است به پشتیبانی تخصص یا منابع، مانند فناوری اطلاعات، نیاز داشته باشید .متن سازمان خود را در نظر بگیرید .ممکن است لازم باشد تجزیه و تحلیل هزینه و سود را انجام دهید تا به شما کمک کند تصمیم بگیرید کدام راه حل را دنبال کنید.

به یاد داشته باشید که راه حلهای انتخاب شده خود را در کلیه منابعی که از تداوم تجارت پشتیبانی می‌کنند - افراد، امکانات، تجهیزات و تجهیزات، اطلاعات، فناوری و تأمین کنندگان - استفاده کنید.

❖ **برنامه‌ها و روندهای خود را ثبت کنید**

یک طرح تداوم کسب و کار ایجاد کنید تا رویه‌های سازمان خود را برای پاسخگویی به اختلالات از هر نوع ثبت کند.

- ساختار برنامه‌های تداوم کسب و کار شما به سازمان شما بستگی دارد.
- سازمان‌های کوچک ممکن است تمام اطلاعات را در یک برنامه داشته باشند.

سازمان‌های بزرگتر ممکن است برنامههای جداگانه‌ای داشته باشند که نیازها یا عملکردهای مختلف تجاری را پوشش دهند .به عنوان مثال، یک سازمان بزرگ ممکن است یک برنامه کلی داشته باشد که دامنه تداوم کسب و کار و رویه‌های پاسخگویی را شرح دهد، و برنامه‌های جداگانه‌ای را برای واحدهای تجاری، مکان‌های خدمات یا عملکردهای خاص داشته باشد.

برنامه‌های سازمان شما باید شامل موارد زیر باشد:

- فرآیندهای اطلاع رسانی، فعال سازی و تشدید
- نقش‌ها، مسئولیت‌ها و اختیارات برای استناد به طرح و پاسخگویی به اختلالات
- تداوم رهبری
- ساختارها و فرایندها برای پاسخگویی به اختلالات
- جزئیات توابع مهم:
- الزامات و بازه‌های زمانی
- فرآیندهای حفظ عملکرد، از جمله جایی که روشهای عملیاتی یا برنامه‌های دقیق می‌توان یافت
- روش‌های ارتباطی (داخلی، خارجی)
- هرگونه پیوند به برنامه‌ها و فرآیندهای دیگر در سازمان.

برنامه‌ها باید ساده، مناسب برای اهداف و استفاده از آنها تحت فشار موقعیت پاسخ دهی آسان باشند .برای آسان ساختن برنامه‌ها از الگوها و چک لیست‌ها استفاده کنید.

❖ **تمریناتی را برای آزمایش برنامه‌های خود و آماده شدن برای ایجاد اختلال انجام دهید**

به طور سیستماتیک برای کنترل اختلالات با اجرای تمرینات آموزش دهید .برنامه‌های سازمان خود را برای اطمینان از تداوم تجارت آزمایش، ارزیابی، تمرین و بهبود دهید.

تمرینات به شما امکان می‌دهد مفروضاتی را که در طی روند برنامه ریزی مطرح کرده‌اید، مورد تأیید قرار دهید و موارد یا شکاف‌های موجود در برنامه ریزی را شناسایی کنید .تمرینات همچنین توانایی تیمهای پاسخگویی شما را ایجاد می‌کند.

تمرینات منظم را به عنوان بخشی از یک روند بهبود مستمر انجام دهید، به طوری که با گذشت زمان به تدریج می‌توانید ظرفیت و توانایی ایجاد کنید.

نوع تمریناتی که برای استفاده انتخاب می‌کنید به اهداف ورزش شما بستگی دارد .هر نوع تمرین برای آماده سازی و تسهیل به زمان متفاوتی نیاز دارد و سطح متفاوتی از خطر و هزینه را به همراه دارد.

ورزش	شرح
تمرین بحث	بحثی که در آن شرکت کنندگان برنامه‌ها را مرور می‌کنند، یا در یک منطقه خاص برای پیشرفت تمرکز می‌کنند.
ورزش سناریو	یک تمرین بحث با یک سناریو و بازه زمانی .شرکت کنندگان با پیشبرد اوضاع، برنامه‌های پاسخ خود را نشان می‌دهند.
تمرین شبیه سازی	تمرینی با سناریوی دقیق‌تر، با اطلاعاتی که همزمان با اوضاع ارائه می‌شود، شبیه سازی یک حادثه واقعی .شرکت کنندگان نقش‌های خود را تمرین می‌کنند.
ورزش زنده	تمرین در زمان واقعی بخشی یا کل پاسخ.
تست	آزمایش فناوری، تجهیزات یا رویه‌ها، منجر به عبور یا عدم موفقیت می‌شود.

۲-۱-۲۰- برنامه تداوم تجارت خود را حفظ کنید

برنامه تداوم تجارت خود را فعالانه حفظ کنید .مطمئن شوید که فعلی باقی مانده و همچنان منعکس کننده مسئولیتها، اهداف و عملکردهای سازمان شماست .

تغییر در برنامه شما ممکن است به دلیل موارد زیر لازم باشد:

- تغییرات در سازمان شما، مانند تغییر در ساختار سازمان
- توابع جدید، یا تغییر در عملکردهای موجود، مانند تغییر در نحوه تحویل عملکرد
- تغییراتی در الزاماتی که عملکردهای شما را پشتیبانی می‌کند، مانند سیستم جدید فناوری اطلاعات معرفی شده
- درس‌هایی که از یک تمرین یا حادثه آموخته‌اید
- یافته‌های یک ارزیابی یا بررسی.

❖ **برنامه مدیریت تداوم تجارت خود را مرور کنید**

بازبینی‌ها به شما کمک می‌کنند سیاست‌ها، برنامه‌ها و فرآیندهای خود را ارزیابی کنید تا از مناسب و مؤثر ماندن آنها مطمئن شوید و زمینه‌های پیشرفت را مشخص کنید .انواع بازبینی شامل:

- حسابرسی
- خودارزیابی
- فعالیت‌های تضمین کیفیت
- بررسی عملکرد تأمین کننده
- بررسی مدیریت
- ارزیابی عملکرد در برابر نقشها و مسئولیتهای تداوم تجارت.
- توصیه‌های شما از روند بررسی باید بر بهبود انعطاف پذیری باشد.

❖ **برنامه‌های تداوم کسب و کار خود را ادغام کنید**

تداوم تجارت فقط داشتن یک برنامه نیست .این فرایندی با مراحل عملی برای انعطاف پذیری بیشتر و به حداقل رساندن تأثیر هرگونه اختلال بدون توجه به علت است.

برای موفقیت، مدیریت تداوم تجارت نمی‌تواند جداگانه رخ دهد .شما باید برنامه خود را با فرایندهای پاسخگویی تیم‌های دیگری که از عملکرد سازمان شما محافظت می‌کنند - مانند امنیت، بهداشت و ایمنی، مدیریت اضطراری، مدیریت اطلاعات و مدیریت ریسک - ادغام کنید .اگر این توابع را یکپارچه کنید، انعطاف پذیری سازمان خود را افزایش می‌دهید.

به عنوان مثال، برنامه تداوم کسب و کار شما می‌تواند تهدیدات احتمالی و اقدامات پیشگیرانه برای امنیت را شناسایی کند .و اتخاذ اصول مدیریت ریسک از شما برای ارزیابی خطرات ایجاد اختلال در عملکردهای مهم پشتیبانی می‌کند.

❖ **مردم خود را تربیت کنید**

آموزش، آموزش و آگاهی مهم است .اطمینان حاصل کنید که فرآیند تداوم کسب و کار شما به خوبی شناخته شده است .آن‌ها را بخشی از عمل کاری و فرهنگ سازمان خود قرار دهید.

افرادی را برای تیم‌های پاسخگویی خود انتخاب کنید که از مهارت‌ها و شایستگی‌های مناسبی برخوردار باشند و آنها را به طور مناسب آموزش دهید .افراد پشتیبان را برای این نقشهای مهم انتخاب و آموزش دهید .در صورت امکان، اطمینان حاصل کنید که افراد دارای نقش حیاتی مسئولیت‌های رقابتی ندارند.

۲-۱-۲۱- توابع حیاتی و نیازهای آنها را شناسایی کنید

عملکردهای حیاتی سازمانهای خود و مواردی را که برای ادامه کار یا بازیابی سریع آنها لازم است، شناسایی کنید.

عملکردهای حیاتی سازمان شما همان وظایفی است که برای ایجاد اختلال در آنها بیشتر نیاز دارید .هنگامی که وظایف حیاتی خود را شناسایی می‌کنید، دامنه برنامه تداوم کسب و کار خود را در نظر بگیرید و تأثیر ایجاد اختلال در این عملکردها را به مرور ارزیابی کنید.

❖ **منابع و نیازهای خود را در نظر بگیرید**

کدام منابع و الزامات برای حفظ عملکردهای حیاتی شما ضروری است؟ به این فکر کنید:

- مردم و توانایی‌های آنها

- امکانات
- لوازم و تجهیزات
- اطلاعات
- فناوری (سیستم‌ها، برنامه‌ها)
- تأمین کنندگان کالا و خدمات.

❖ **تجزیه و تحلیل تأثیر تجارت را انجام دهید**

متخصصان تداوم کسب و کار از تکنیکی به نام تجزیه و تحلیل تأثیر تجارت برای شناسایی نیازهای تداوم تجارت استفاده می‌کنند.

تجزیه و تحلیل تأثیر تجاری می‌تواند سطوح مختلفی از جزئیات را به دست آورد .نیازهای سازمان خود و مرحله‌ای را که در اجرای برنامه خود دارید در نظر بگیرید.

در تجزیه و تحلیل تأثیرات تجاری شما:

- الزامات لازم برای ارائه عملکرد را شناسایی کنید
- تأثیر اختلال در عملکرد و جدول زمانی مربوطه را ارزیابی کنید
- در چه مرحله‌ای تأثیر غیر قابل قبول است (حداکثر دوره تحمل قابل تحمل)؟
- چه زمانی شما قصد دارید این عملکرد را توسط (هدف زمان بهبودی خود) بازیابی کنید؟
- در چه مرحله‌ای به نیازهای مشخص شده نیاز دارید، بنابراین می‌توانید به هدف زمان بهبودی برسید؟
- افراد، خدمات یا تأمین کنندگان داخلی یا خارجی دیگری را که عملکرد به آنها بستگی دارد شناسایی کنید
- تعیین کنید که عملکرد در طول زمان چقدر حیاتی است .

❖ **ارزیابی ریسک را انجام دهید**

تجزیه و تحلیل تأثیر تجاری باید شامل ارزیابی ریسک برای شناسایی و کمی سازی خطر ایجاد اختلال در عملکرد، از جمله خطرات مربوط به الزامات مورد نیاز عملکرد باشد .برای انجام ارزیابی سنجش با افراد سازمان خود که مسئول مدیریت ریسک هستند همکاری کنید .به یاد داشته باشید که خطراتی را که سازمان شما قبلاً شناسایی کرده است، و هرگونه تدابیری را برای کاهش آنها که از قبل اعمال شده‌اند، در نظر بگیرید.

❖ **نگاه گسترده‌ای داشته باشید**

با در نظر گرفتن دیدگاه سازمان، اطلاعات حاصل از تجزیه و تحلیل تأثیرات تجاری خود را جمع آوری و مرور کنید .سپس می‌توانید موارد زیر را در نظر بگیرید:

- وابستگی متقابل بین توابع
- نیازهای مشترک در سازمان شما.

۲-۱-۲۲- در صورت ایجاد اختلال، تیم‌هایی را برای مدیریت تداوم تجارت تنظیم کنید

یک ساختار در کل سازمان برای مدیریت و پاسخگویی به طیف وسیعی از حوادث و اختلالات ایجاد کنید .نقش‌ها و مسئولیت‌های اصلی را تعیین کنید و اطمینان حاصل کنید که فرایندهای درست وجود دارد.

ساختار شما برای تداوم تجارت باید:

- ادغام با سایر ساختارهای پاسخ در سازمان شما (به عنوان مثال امنیت یا فناوری اطلاعات)
- انعطاف پذیر و مقیاس پذیر باشد، بنابراین می‌تواند حوادث با مقیاس و تأثیر متفاوت را کنترل کند
- در یک طرح کل سازمان مستند شود.

اگر طبق قانون مدیریت اضطراری دفاع مدنی ۲۰۰۲ مسئولیتی دارید، اطمینان حاصل کنید که تنظیمات شما با سیستم مدیریت حوادث هماهنگ (CIMS) نیوزیلند همسو است.

❖ فرایندها را در جای خود قرار دهید

اطمینان حاصل کنید که فرایندهای پاسخ شما شامل موارد زیر است:

- چه کسی نقشهای اصلی را در یک پاسخ (نظارت استراتژیک، تاکتیکی و عملیاتی) ایفا خواهد کرد
- اولویت‌های پاسخ
- چه کسی مجاز به فعال کردن و مدیریت پاسخ است و این مسئولیت ممکن است به چه کسی واگذار شود
- اطلاع رسانی، فعال سازی و تشدید

❖ تیم‌هایی برای مدیریت استراتژی، تاکتیک‌ها و عملیات ایجاد کنید

سازمان شما باید ساختار پاسخ شما را در سطح استراتژیک، تاکتیکی و عملیاتی در نظر بگیرد. برای برخی از سازمان‌ها، یک تیم پاسخ ممکن است همه سطوح را مدیریت کند .در سازمانهای بزرگ ممکن است لازم باشد تیمهای جداگانه‌ای برای مدیریت این مسئولیت‌ها ایجاد کنید. برای اطمینان از اینکه مردم می‌دانند چه کاری باید انجام دهند، تمرینات منظمی را انجام دهید، ترتیبات مناسب برای هدف مناسب است و شما هر گونه خلأ را تشخیص می‌دهید.

❖ تیم پاسخ استراتژیک - تیم مدیریت بحران شما

تیم پاسخ استراتژیک شما از منظر سازمان بر موضوعات تمرکز می‌کند .این تیم معمولاً با مدیریت عالی اداره می‌شود و اغلب تیم مدیریت بحران نامیده می‌شود .این نوع تیمها باید انعطاف پذیر باشند و مدیران باتجربه را در اختیار داشته باشند تا منابع کامل سازمان را برای پاسخگویی استفاده کنند.

❖ تیم پاسخ تاکتیکی - هماهنگ کننده‌ها

تیم پاسخ تاکتیکی فرایندهای مورد نیاز برای ارائه عملکردهای حیاتی شما و اطمینان از تخصیص مناسب منابع را مدیریت و هماهنگ می‌کند.

❖ تیم پاسخ عملیاتی - امکان تداوم یا بازیابی

تیم پاسخ عملیاتی شما عملکردهای حیاتی را ادامه می‌دهد یا کار برای بازیابی آنها را انجام می‌دهد.

❖ برای اطمینان از اثربخشی برنامه‌ها را مرتباً مرور کنید

هر زمان که برنامه‌های پاسخگویی را فعال می‌کنید (یا در یک تمرین یا در حوادث زندگی واقعی)، اثربخشی آنها را بررسی کنید تا از نظر هدف مناسب باشند.

۲-۱-۲۳- الزامات قانونی، استانداردهای ISO و بهترین روش برای مدیریت تداوم تجارت

طبق قانون، سازمان‌های دولتی موظفند از عملیات خود در برابر اختلال محافظت کنند .سازمان استاندارد بین المللی (ISO) استانداردهای تداوم تجارت را تعیین می‌کند.

مدیر اجرایی شما مسئولیت کلی این را دارد که سازمان شما برای مدیریت تداوم تجارت ترتیبات لازم را فراهم کند.

❖ **الزامات قانونی برای تداوم تجارت**

طبق قانون مدیریت اضطراری دفاع مدنی 2002 (CDEM) ، سازمان شما باید مقدمات لازم را برای رسیدگی به اخلال در تجارت شما فراهم کند

شما باید:

- فعالیت‌هایی را انجام دهید تا اطمینان حاصل کنید که می‌توانید در حین و بعد از اضطراری به حداکثر عملکرد خود عمل کنید (حتی اگر این در سطح کمتری باشد)
- فعالیت برنامه ریزی تداوم تجارت را انجام دهید تا:
- اطمینان حاصل کنید که طبق قانون CDEM می‌توانید نقش‌های پاسخ و بهبودی خود را انجام دهید
- کاهش خطرات اخلال در تجارت
- برنامه‌ها و استراتژی‌هایی را برای ادامه فرآیندهای حیاتی کسب و کار در نظر بگیرید.

دو منبع دیگر مورد نیاز برای ادامه کار و فرآیندهای بازیابی فاجعه که باید دنبال کنید:

- کتابچه راهنمای امنیت اطلاعات نیوزلند - (NZISM) تداوم تجارت و بازیابی بلایا
- راهنمای دفاع مدنی برای برنامه ملی ۲۰۱۵ ، بخش ۱۹ ، برنامه ریزی(PDF)

❖ **استانداردهای ISO برای مدیریت تداوم تجارت**

استاندارد مربوط به الزامات ذکر شده در این صفحات وب ISO 22301: 2012 امنیت اجتماعی - سیستم های مدیریت تداوم تجارت - الزامات

استانداردهای پشتیبانی، مولفه های خاص برنامه مدیریت تداوم تجارت را در بر می‌گیرد:

- ISO22300: 2018امنیت و انعطاف پذیری - واژگان
- ISO 22313: 2012 BCMSراهنما
- ISO 22316: 2017تاب آوری سازمانی - اصول و ویژگی‌ها
- ISO 22317: 2015 BCMSرهنمودهایی برای تجزیه و تحلیل تأثیر تجارت
- ISO 22318: 2015 BCMSرهنمودهایی برای تداوم زنجیره تأمین
- ISO 22330: BCMS 2018رهنمودهایی برای جنبه‌های تداوم تجارت در مردم
- ISO 22331در دست توسعه - BCMS (رهنمودهایی برای استراتژی تداوم تجارت)
- ISO 22398: 2013رهنمودهایی برای تمرینات.

❖ **دستورالعمل‌های خوب**

موسسه تداوم تجارت، دستورالعمل‌هایی را منتشر می‌کند که در دسترس اعضا است.

- رهنمودهای تمرین خوب (نسخه ۲۰۱۸)
- نسخه ساده "راهنماها" به صورت رایگان در دسترس است.
- Good Practice Guidelines 2018 Lite Edition

۱۸-۲- چرا امنیت زنجیره تأمین مهم است

اکثر سازمان‌ها برای ارائه محصولات، سیستم‌ها و خدمات به تأمین کنندگان اعتماد می‌کنند .این تأمین کنندگان به توسعه کسب و کار شما تبدیل می‌شوند و خطراتی را که در معرض آن هستید گسترش می‌دهند.

یک "زنجیره تأمین" را می‌توان به عنوان "شبکه‌ای از سازمان‌ها که با مجموعه‌ای از روابط شامل تأمین کالا یا خدمات متصل شده‌اند، توصیف کرد.

زنجیره‌های تأمین می‌توانند بزرگ و پیچیده باشند، بسیاری از تأمین کنندگان درگیر کارهای مختلف هستند .به عنوان مثال، برخی از سازمان‌ها ممکن است:

- به یک ارائه دهنده حقوق و دستمزد که سیستم‌های آن در فضای ابری میزبانی شده و توسط ارائه دهنده نرم افزار دیگری نگهداری می‌شوند، برون سپاری کنید
- برای ارائه خدمات خط مقدم با یک سازمان دیگر) به عنوان مثال، یک (NGO شریک شوید، و شریک زندگی به نوبه خود از چندین ارائه دهنده خدمات برای حمایت از تجارت خود استفاده می‌کند.

بسیاری از سازمان‌ها از همه تأمین کنندگان زنجیره تأمین خود آگاهی ندارند. تأمین امنیت زنجیره تأمین شما می‌تواند چالش برانگیز باشد زیرا شناسایی آسیب پذیری ها یا شناخت محل ورود و بهره برداری از آنها دشوار است.

۲-۱-۲۴- تهدیدات و خطرات ناشی از زنجیره تأمین خود را درک کنید

تهدیدات ناشی از زنجیره تأمین شما اشکال مختلفی دارد .به عنوان مثال، یک تأمین کننده ممکن است:

- قادر به ایمن سازی کافی سیستم‌های خود نیستند
- یک شخص مخرب برای آنها کار می‌کند
- اقدامات منفی را برای منافع خود انجام دهند.

یا ممکن است شما نتوانید به وضوح الزامات امنیتی خود را اعلام کنید، بنابراین یک تأمین کننده کارهای اشتباه را انجام می‌دهد.

ممکن است در معرض ترکیبی از خطرات زیر قرار بگیرید:

- آسیب رساندن به مردم یا مشتریان شما
- از دست دادن داده‌ها
- نقض حریم خصوصی
- از دست دادن مالکیت معنوی
- خدمات را مختل کرد
- خطرات مالی
- خطرات شهرت

❖ **طیف وسیعی از سناریوهای تهدید را در نظر بگیرید**

مثال‌های زیر روابط و خطرات احتمالی زنجیره تأمین را نشان می‌دهد.

❖ **یک پیمانکار از دسترسی آنها به محل کار شما سو استفاده می‌کند**

یک پیمانکار تعمیر و نگهداری با دسترسی بعد از ساعت، رایانه‌های شما را می دزد و برای پرداخت بدهی‌ها می‌فروشد .رایانه‌ها حاوی مالکیت معنوی متعلق به چندین شرکت هستند که با آنها کار می‌کنید.

❖ **تأمین کننده یکی از تأمین کنندگان مستقیم شما هک می‌شود**

تأمین کنندگان طرف اصلی که با آنها قرارداد بسته‌اید سیستم‌های ICT خود را هک کرده‌اند) .در سال ۲۰۱۷، این برای یک پیمانکار دفاعی استرالیایی اتفاق افتاد. هکر اطلاعات بسیار حساس تجاری در مورد ساخت و طراحی هواپیماهای جنگنده جدید، شناورهای نیروی دریایی و هواپیماهای نظارتی را به سرقت برد. پیمانکار - یک تأمین کننده سطح ۴ - در اجرا و نگهداری شکست خورده بود اقدامات امنیتی متناسب با ماهیت کار(.

❖ **یک تأمین کننده مستقیم نتواند جزئیات تأمین کنندگان شخص ثالث خود را فاش کند**

شما فقط از طریق تأمین کننده مستقیم خود به دنبال پشتیبانی سیستم هستید تا دریابید که این پشتیبانی از طریق اشخاص ثالث مستقر در خارج از کشور ارائه می‌شود .دسترسی به اطلاعات حساس و یا مالکیت معنوی شما از خارج از کشور، آن را مستعد ابتلا به سرقت یا مصالحه می‌کند.

❖ **یک تأمین کننده مستقیم نتواند در زنجیره تأمین خود دقت لازم را انجام دهد**

تأمین کننده مستقیم شما مایل نیست مسئولیت آسیب پذیری ضعف رمز عبور را که در سیستم شما شناسایی شده است، به عهده بگیرد .این آسیب پذیری توسط یکی از تأمین کنندگان یا پیمانکاران شخص ثالث ایجاد شده است .سیستم شما در وضعیت آسیب پذیر باقی می‌ماند در حالی که شما از تأمین کننده مستقیم رضایت می‌گیرید و ممکن است آسیب پذیری را کندتر و گران‌تر کنید.

❖ **ارائه دهنده فناوری اطلاعات شما درگیر یک کمپین جهانی نفوذ در فضای مجازی شده است**

یک کمپین گسترده ارائه دهندگان خدماتی را که مدیریت IT و ارائه دهندگان cloud را دارند که اطلاعات را ذخیره می‌کنند، هدف قرار می‌دهد .شما یکی از چندین سازمان دولتی و شرکت خصوصی هستید که اطلاعات حساس و ارزش معنوی ارزشمند آنها به خطر افتاده و به اشخاص دیگر فروخته می‌شود.

❖ **پیمانکاری که برای یک تأمین کننده کار می‌کند اطلاعات را می‌دزدد**

یک نگهبان امنیتی که با یک تأمین کننده قرارداد بسته است، اسنادی را که حاوی اطلاعات امنیت ملی است، می‌دزدد .آن‌ها سعی می‌کنند اسناد را به یک سرویس اطلاعاتی خارجی بفروشند.

❖ **مشخص شده است که تجهیزات جدید IT آسیب پذیر هستند**

وقفه در زنجیره تأمین شما به این معنی است که یک تأمین کننده تجهیزات جایگزین فناوری اطلاعات به سرعت مورد نیاز است .تجهیزات تهیه شده جدید شامل آسیب پذیری عمدی است که در کارخانه معرفی شده است .این آسیب پذیری بعداً توسط یک بازیگر دولتی مورد سو استفاده قرار می‌گیرد.

❖ **افراد شما IT را بدون مجوز تهیه می‌کنند**

یک تیم بدون گذراندن مراحل خرید یا تعامل با افراد امنیتی IT شما، از یک سرویس مبتنی بر ابر جدید برای طراحی مشترک یک محصول جدید شروع می‌کند .مالکیت معنوی شما از طریق این "خرید سایه فناوری اطلاعات" در معرض دید قرار می‌گیرد.

❖ **شخص ثالث از دسترسی خود به اطلاعات شما سو استفاده می‌کند**

شما با چیدمان نرم افزار به عنوان سرویس (SaaS) یک راه حل فناوری اطلاعات خریداری می‌کنید .شما نمی‌دانید که توسط شخص ثالث در خارج از کشور میزبانی می‌شود .کارکنان ارائه دهنده خدمات دریایی از دسترسی مجاز خود به سیستم‌های ذخیره و پردازش اطلاعات شما برای سرقت مالکیت معنوی شما و اطلاعات شخصی مشتریان شما استفاده می‌کنند.

شما نمی‌توانید به اندازه کافی یک تأمین کننده را در مورد نیازهای امنیتی خود مطلع کنید

شما برای کمک به راه اندازی محصول جدید با یک تأمین کننده خارجی درگیر می‌شوید .با این حال، شما نیازهای امنیتی خود را به اندازه کافی، به ویژه حساسیت اطلاعاتی که به آنها دسترسی دارند، برقرار نمی‌کنید .تأمین کننده اطلاعات شما را به طور گسترده‌تری از آنچه شما می‌خواهید به اشتراک می‌گذارد و تأثیر راه اندازی محصول شما را کاهش می‌دهد.

❖ **اطلاعات بیشتر**

- مجموعه امنیت زنجیره تأمین - CPNI) مرکز حمایت از زیرساخت های ملی انگلستان(
- راهنمای امنیت اطلاعات نیوزلند - (NZISM) زنجیره تأمین
- دفتر حسابرس کل - راهنمای خرید برای اشخاص عمومی

۲-۱-۲۵- اصول امنیت زنجیره تأمین

برای بدست آوردن و حفظ کنترل زنجیره تأمین خود از این اصول پیروی کنید .دوازده اصل به چهار مرحله تقسیم شده است، که فرآیند ایمن سازی زنجیره تأمین شما را پوشش می‌دهد .

❖ **هنگام کار با دیگران خطرات را مدیریت کنید**

قبل از شروع کار با دیگران که ممکن است بخشی از زنجیره تأمین شما شوند، خطرات موجود در افراد، اطلاعات و دارایی‌های خود را شناسایی و مدیریت کنید.

خطرات را درک کنید

۱) درک کنید که چه چیزی باید محافظت شود و چرا
۲) بدانید که تأمین کنندگان شما چه کسانی هستند و درکی از اقدامات امنیتی آنها ایجاد کنید
۳) خطرات امنیتی ناشی از زنجیره تأمین خود را درک کنید.

❖ **کنترل ایجاد کنید**

۴) دیدگاه خود در مورد نیازهای امنیتی را به تأمین کنندگان خود منتقل کنید
۵) حداقل الزامات امنیتی برای تأمین کنندگان خود را تنظیم و ابلاغ کنید
۶) ملاحظات امنیتی را در روند قرارداد خود در نظر بگیرید و از تأمین کنندگان خود بخواهید که همان کار را انجام دهند
۷) مسئولیت‌های امنیتی خود را به عنوان یک تأمین کننده و مصرف کننده انجام دهید
۸) آگاهی از امنیت را در زنجیره تأمین خود افزایش دهید
۹) پشتیبانی از حوادث امنیتی.

❖ **ترتیبات خود را بررسی کنید**

۱۰) فعالیت‌های اطمینان را در مدیریت زنجیره تأمین خود ایجاد کنید.

❖ **به دنبال بهبود مستمر باشید**

۱۱) بهبود مستمر امنیت در زنجیره تأمین خود را تشویق کنید

۱۲) ایجاد اعتماد با تأمین کنندگان.

۲-۱-۲۶- بفهمید چه چیزی باید محافظت شود و چرا

باید بدانی که:

- حساسیت قراردادهایی که اجازه می‌دهید
- ارزش اطلاعات یا دارایی‌هایی که تأمین کنندگان به عنوان بخشی از قرارداد خود با شما در اختیار دارند، به آنها دسترسی دارند یا از آنها استفاده می‌کنند
- تأثیر در سازمان شما از دست دادن یا آسیب رساندن به اطلاعات یا دارایی‌هایی که تأمین کنندگان نگهداری، دسترسی یا مدیریت می‌کنند.

به سطح حفاظتی که تأمین کنندگان شما باید از دارایی‌ها و اطلاعات شما به عنوان بخشی از قرارداد و همچنین محصولات یا خدماتی که ارائه می‌دهند، ارائه دهند، فکر کنید.

به یاد داشته باشید که طبق قانون سوابق عمومی ۲۰۰۵، سازمان شما مسئولیت مدیریت و محافظت از سوابق رسمی را در زمانی که خارج از سایت نگه داشته می‌شوند، حفظ می‌کند.

هنگامی که یک عملیات را به برون سپاری می‌کنید، باید شرایط محافظت از اطلاعات ذکر شده در:

- پروتکل مدیریت امنیت اطلاعات
- کتابچه راهنمای امنیت اطلاعات نیوزلند

۲-۱-۲۷- بدانید تأمین کنندگان شما چه کسانی هستند و درکی از اقدامات امنیتی آنها ایجاد کنید

شما باید بدانید که تأمین کنندگان شما چه کسانی هستند و چه کسی آنها را تأمین یا پشتیبانی می‌کند .به این فکر کنید که چقدر باید از زنجیره تأمین خود پایین بیایید تا بفهمید تأمین کنندگان شما چه کسی هستند و به آنها اعتماد کنید.

ممکن است مجبور باشید برای کسب اطلاعات در مورد پیمانکاران فرعی به تأمین کنندگان فوری خود اعتماد کنید و کشف کامل دامنه زنجیره تأمین خود به زمان نیاز دارد.

سعی کنید پاسخ به پرسش‌های زیر را تعیین کنید.

- ترتیبات امنیتی فعلی تأمین کنندگان شما چقدر مؤثر است؟ ترتیب آنها چقدر بوده است؟
- از تهیه کنندگان فوری خود خواسته‌اید کدام اقدامات امنیتی را انجام دهند؟ آن‌ها به نوبه خود از پیمانکاران فرعی خود خواسته‌اند که چه اقداماتی را ارائه دهند؟
- آیا تأمین کنندگان و پیمانکاران فرعی آنها الزامات امنیتی مورد نظر شما را ارائه داده‌اند؟
- تأمین کنندگان شما چه دسترسی (فیزیکی و فناوری) به سیستم‌ها، اماکن و اطلاعات شما خواهند داشت؟ چگونه این دسترسی را کنترل خواهید کرد؟
- وقتی تأمین کنندگان در محل کار شما کار می‌کنند، چه اطلاعات دیگری (فراتر از اطلاعاتی که صریحاً به آنها دسترسی داده‌اید) ممکن است بتوانند دسترسی پیدا کنند یا مشاهده کنند؟

- چگونه تأمین کنندگان فوری شما دسترسی و استفاده از اطلاعات و دارایی‌های پیمانکاران فرعی خود را کنترل می‌کنند؟ (به یاد داشته باشید که سیستم‌ها و محل‌های خود را درج کنید)

بر قسمت‌هایی از تجارت یا سیستم‌های تأمین کننده خود تمرکز کنید که اطلاعات قرارداد شما را کنترل می‌کنند یا محصول یا خدمات طرف قرارداد را تحویل می‌دهند

۲-۱-۲۸- خطرات امنیتی ناشی از زنجیره تأمین خود را درک کنید

خطرات موجود در قراردادتان را برای اطلاعات یا دارایی‌هایتان، محصولات یا خدمات تحویل داده شده و زنجیره تأمین گسترده‌تر ارزیابی کنید.

خطرات موجود در زنجیره تأمین به اشکال مختلف صورت می‌گیرد .به عنوان مثال، یک تأمین کننده ممکن است:

- قادر به ایمن سازی کافی سیستم‌های خود نیستند
- یک شخص مخرب برای آنها کار می‌کند
- قرارداد کار با شخصی را که قادر به مدیریت صحیح اطلاعات شما نیست
- سیستم‌های خود را از طریق اقدامات مخرب تضعیف کنید (اگر این سیستم شامل امنیت ملی باشد، اقدامات مخرب ممکن است توسط یک کشور متخاصم پشتیبانی شود)

یا ممکن است ارتباط شما در مورد نیازهای امنیتی ضعیف باشد، بنابراین تأمین کننده کارهای اشتباهی انجام می‌دهد. برای درک این خطرات امنیتی از بهترین اطلاعاتی که می‌توانید استفاده کنید.

۲-۱-۲۹- دیدگاه خود در مورد نیازهای امنیتی را به تأمین کنندگان خود منتقل کنید

اطمینان حاصل کنید که تأمین کنندگان شما مسئولیت خود در قبال محافظت از اطلاعات شما، و محصولات و خدماتشان را درک می‌کنند .اطمینان حاصل کنید که آنها پیامدهای شکست را درک می‌کنند. تصمیم بگیرید که آیا مایلید اجازه دهید قرارداد زیر قرارداد تأمین کنندگان شما کار کند .اگر به آنها اجازه می‌دهید زیر قرارداد ببندند، اختیارات خود را به طور مناسب به آنها واگذار کنید تا به آنها اجازه انجام این کار را دهند .در مورد معیارهای این تصمیمات، به تأمین کنندگان خود راهنمایی روشنی دهید .به آنها بگویید بدون مراجعه به شما با کدام نوع قرارداد می‌توانند قرارداد منعقد کنند و کدام یک از آنها به تأیید و ثبت نام شما نیاز دارند.

از تأمین کنندگان خود اطمینان حاصل کنید:

- مسئولیت‌های امنیتی خود را انجام دهند
- الزامات امنیتی خود را در هرگونه قرارداد قراردادی فرعی قرار دهید

۲-۱-۳۰- حداقل الزامات امنیتی برای تأمین کنندگان خود را تنظیم و ابلاغ کنید

شما باید حداقل شرایط امنیتی را برای تأمین کنندگان موجه، متناسب و قابل دستیابی تعیین کنید .حداقل شرایط خود را در نظر بگیرید:

- حاکمیت امنیتی
- امنیت پرسنل
- امنیت اطلاعات
- امنیت فیزیکی

اطمینان حاصل کنید که این الزامات ارزیابی شما از خطرات امنیتی را منعکس می‌کند .اما همچنین به درستی تنظیمات امنیتی تأمین کنندگان خود توجه کنید .توانایی آنها را در تأمین نیازهای مورد نظر خود در نظر بگیرید.

خاص باشید اگر شما فقط یک شرط کلی را در قرارداد ذکر کرده‌اید که ارائه دهنده خدمات باید از PSR پیروی کند، بعید به نظر می‌رسد که مناسب یا قابل اجرا باشد. شرایطی را که ممکن است غیرمتعارف باشد، مشخص کنید که انتظار داریم تأمین کنندگان حداقل شرایط امنیتی شما را برآورده کنند .به عنوان مثال، تأمین کنندگانی که فقط به دسترسی موقت یا گاه به گاه به داده‌های محدود و خاص یا به محل‌های شما احتیاج دارند .این ملاحظات را مستند کنید. در مورد اقداماتی که قصد دارید برای مدیریت نیازهای امنیتی خود انجام دهید، به پیمانکار راهنمایی کنید .این راهنما می‌تواند حجم کار شما را کاهش دهد و از انجام کارهای اضافی و غیرضروری برای پیمانکاران جلوگیری کند.

❖ تأیید مناسب بودن افراد با چک‌های قبل از استخدام

حداقل چک‌های قبل از استخدام را که انتظار دارید تأمین کنندگان شما برای کارمندان خود انجام دهند، مشخص کنید .حداقل چک‌های خود را با بررسی‌های پایه قبل از استخدام که توسط سازمان‌های دولتی انجام شده مطابقت دهید:

- هویت آنها را تأیید کنید
- ملیت آنها را تأیید کنید
- حق کار در نیوزیلند را تأیید کنید
- منابع را با کارفرمای سابق خود بررسی کنید
- بررسی سوابق کیفری

هنگامی که یک خطر امنیتی افزایش یافته مربوط به یک نقش خاص یا ماهیت دسترسی تأمین کننده خود را شناسایی می‌کنید، بررسی‌های اضافی می‌تواند لازم باشد .به عنوان مثال، یک مدیر فناوری اطلاعات برای یک ارائه دهنده خدمات مدیریت شده ممکن است دسترسی گسترده‌ای به اطلاعات سازمان شما داشته باشد .برای اطمینان از قابل اعتماد بودن آنها و شناسایی عواملی در زندگی که ممکن است خطر تهدید داخلی را افزایش دهد، ممکن است نیاز به بررسی‌های بیشتر داشته باشید.

❖ برای هر پیمانکاری که اطلاعات دارای علامت محافظ را کنترل می‌کنند، مجوز امنیتی دریافت کنید

سازمان شما مسئول حامی مالی، تنظیم و مدیریت مجوزهای امنیتی در طول زندگی یک قرارداد است.

اگر کارمندان یک پیمانکار نیاز به دسترسی به اطلاعات دارای طبقه بندی محرمانه یا بالاتر داشته باشند، باید اطمینان حاصل کنید که هر شخص از سطح امنیتی در سطح مناسب برخوردار است .با سرویس اطلاعات امنیتی نیوزلند (NZSIS) مشورت کنید تا بفهمید آیا هر یک از کارمندان قبلاً دارای گواهی امنیتی معتبر هستند یا خیر .

هر کسی که از نظر امنیتی صحیح نباشد، نباید دسترسی بدون کمک به هر کجا که اطلاعات دارای علامت محافظ کار می‌کند یا ذخیره می‌شود، داشته باشد.

❖ نیازهای امنیتی را مورد به مورد تنظیم کنید

تنظیم الزامات امنیتی مختلف برای انواع مختلف قراردادها، بر اساس خطرات مربوط به آنها .در صورت عدم تناسب و توجیه، از اجبار همه تأمین کنندگان خود برای ارائه مجموعه‌ای از الزامات امنیتی خودداری کنید.

هنگامی که الزامات امنیتی را تعیین می‌کنید، منطق آنها را برای تأمین کنندگان خود توضیح دهید .و از تأمین کنندگان خود بخواهید که این الزامات را به هر پیمانکار فرعی منتقل کنند.

حداقل الزامات امنیتی خود را در اسناد خرید و قراردادهایی که با تأمین کنندگان بسته‌اید وارد کنید.

اگر سازمان شما بررسی شخصیت برای افراد خود را انجام می‌دهد، بررسی کنید که آیا برای کارمندان ارائه دهنده خدمات همان بررسی‌ها را انجام دهید یا خیر. اگر پیمانکاری به اطلاعات رسمی نیاز دارد، باید توافق نامه عدم افشای قرارداد را امضا کند.

۲-۱-۳۱- ملاحظات امنیتی را در روند قرارداد خود در نظر بگیرید و تأمین کنندگان خود را ملزم به انجام همان کار کنید

ملاحظات امنیتی را در فرآیندهای عادی قرارداد خود وارد کنید .این روش به شما کمک می‌کند تا امنیت را در طول قرارداد، از جمله خاتمه و انتقال خدمات به یک تأمین کننده دیگر، مدیریت کنید.

❖ **قبل از عقد قرارداد**

اگر مدیر قرارداد هستید، با مدیر ارشد امنیتی خود (CSO) یا نماینده آنها کار کنید تا هنگام تهیه اسناد مناقصه و همچنین طول مدت قرارداد، شرایط امنیتی اساسی را شناسایی کنید .این مرحله همچنین برای هر کسی که پیشنهادات یا مناقصه‌ها را ارزیابی می‌کند اعمال می‌شود.

هدف اطمینان از الزامات امنیتی:

- با خطرات ارزیابی شده مطابقت داشته باشید
- با مراحل فرایند قرارداد هماهنگ شوید.

تأمین کنندگان احتمالی را بخواهید تا شواهدی از رویکرد خود به امنیت و توانایی آنها در برآورده کردن حداقل الزامات امنیتی تعیین شده را ارائه دهند .اگر تأمین کننده قادر به رعایت حداقل استانداردهای امنیتی شما نیست، نباید آنها را انتخاب کنید.

اگر قراردادی را منوط به شرایط تأمین کننده تأمین می‌کنید، قبل از شروع قرارداد، اطمینان حاصل کنید که آنها شرایط را رعایت می‌کنند. درصورتی که تأمین کننده شما از شرایط امنیتی شما پیروی نکرد، حق فسخ قرارداد را در نظر بگیرید .عدم رعایت این الزام باید شامل تأمین کننده یا عدم توانایی تأمین کننده نقض امنیت باشد. اطمینان حاصل کنید که تأمین کننده شما کدام اطلاعات و دارایی را از جانب شما دراختیار دارد، توافق نامه‌ای را در مورد نحوه مدیریت و دفع اطلاعات و دارایی‌های خود به دست بیاورید و آن را مستند کنید .شرایطی را وارد کنید که از اطلاعات در برابر خطر محافظت می‌کند. هنگام تهیه قراردادها بهتر است از مشاوره حقوقی استفاده کنید.

❖ **شرایط برای اطلاعات محرمانه یا بالاتر با اطلاعات مشخص شده:**

صریحاً بالاترین سطح اطلاعات دارای علامت محافظتی را که تأمین کننده در طول قرارداد به آنها دسترسی خواهد داشت، مشخص کنید. ارائه دهنده خدمات را ملزم به جلوگیری از دسترسی کامل به مطالب دارای علامت محافظ توسط کارکنانی که مجوزهای امنیتی آنها از بین رفته است، کاهش یافته یا لغو کرده یا دیگر نیازی به آن ندارند. در صورت لزوم، شرایطی را که ارائه دهنده خدمات ملزم به گزارش دادن به شما می‌کند، درصورتی که هر یک از کارکنان آنها که دارای مجوز امنیتی نیستند، هرگونه تماس تصادفی یا تصادفی با مواد دارای علامت محافظ داشته باشند، شامل آن‌ها می‌شود .این شرایط به ویژه در قراردادهای نگهبانان امنیتی، نظافت و خدمات ICT بسیار مهم است.

❖ **شرایط اطلاعات رسمی:**

تأثیر هرگونه از دست دادن یا به خطر انداختن اطلاعات رسمی در اختیار یک ارائه دهنده خدمات، به ویژه اطلاعات جمع شده (مجموعه اطلاعات) را در نظر بگیرید .برای کاهش خطرات ارزیابی شده، شرایط قرارداد را درج کنید.

اگر یک قرارداد برای دسترسی به اطلاعات رسمی به یک ارائه دهنده خدمات نیاز دارد، این قرارداد باید شامل شرایط و ضوابط زیر باشد.

❖ **مجوز قرارداد پیمانکاری فرعی**

ارائه دهنده خدمات بدون تأیید کتبی سازمان شما نمی‌تواند سرویس یا عملکردی را که ممکن است نیاز به دسترسی به اطلاعات رسمی داشته باشد، از قرارداد خارج کند .وقتی توافق نامه پیمانکاری فرعی برقرار شد، ارائه دهنده خدمات نمی‌تواند پیمانکار فرعی را بدون تأیید کتبی شما تغییر دهد.

❖ **تضاد علاقه**

ارائه دهنده خدمات باید هرگونه تعارض منافع احتمالی را که بر امنیت تأثیر می‌گذارد، هنگامی که از طرف دولت نیوزلند کار می‌کنند، اعلام کند.

❖ **دسترسی به اطلاعات محافظت شده**

ارائه دهنده خدمات قبل از اینکه به اطلاعات مشخص شده با محافظت دسترسی داشته باشد، باید اطمینان حاصل کند که کارکنان آنها در سطح مناسب پاکسازی شده‌اند.

❖ **ذخیره و مدیریت اطلاعات محافظت شده**

اماکن و امکانات ارائه دهنده خدمات باید حداقل استانداردهای ذخیره سازی و مدیریت اطلاعات رسمی را تا سطح طبقه بندی امنیتی تعیین شده داشته باشند.

❖ **امنیت اطلاعات**

ارائه دهنده خدمات باید دارای سیستم‌هایی باشد که از استانداردهای تعیین شده امنیت اطلاعات برای پردازش، ذخیره، انتقال و دفع اطلاعات رسمی که در قالب‌های الکترونیکی است، برخوردار باشد .برای اطلاعات بیشتر به کتابچه راهنمای امنیت اطلاعات نیوزیلند مراجعه کنید.

❖ **محرمانه بودن**

ارائه دهنده خدمات برای محرمانه نگه داشتن اطلاعات رسمی باید از دستورالعمل‌های مندرج در قرارداد پیروی کند .تعهدات رازداری ممکن است بیش از پایان قرارداد باشد.

❖ **شرایط اطلاعات سازمان شما:**

ریسک قانونی و قضایی را در نظر بگیرید - مانند مواردی که دارندگان ارائه دهنده خدمات در خارج از کشور یا سایر ذینفعان - ممکن است حقوق قانونی داشته باشند که به آنها امکان دسترسی به اطلاعات شما را می‌دهد. اگر این یک خطر است، قرارداد باید شامل شرایط و ضوابطی برای محافظت در برابر دسترسی شخص ثالث باشد .با این حال، در سایر موارد، این شرایط قراردادی ممکن است محافظت کافی نداشته باشد.

❖ **در طول قرارداد**

راهنما، ابزارها و فرایندهای پشتیبانی را ارائه یا توسعه دهید، بنابراین شما و تأمین کنندگان می‌توانید به طور مؤثر امنیت را در تمام سطوح در سراسر زنجیره تأمین خود مدیریت کنید .همه طرفین را در استفاده از آنها آموزش دهید.

لازم است قراردادها در فواصل زمانی مناسب تمدید شوند و همزمان خطرات را دوباره ارزیابی کنید. اطمینان حاصل کنید که تأمین کنندگان شما رویکرد شما در زمینه امنیت را درک کرده و از آن پشتیبانی می‌کنند .فقط از آنها بخواهید در صورت نیاز به مدیریت خطرات امنیتی زنجیره تأمین، اقدام یا ارائه اطلاعات کنند.

۲-۱-۳۲- مسئولیت‌های امنیتی خود را به عنوان یک تأمین کننده و مصرف کننده انجام دهید

- اطمینان حاصل کنید که شما به عنوان یک تأمین کننده، هرگونه الزامات خود را اعمال و برآورده می‌کنید.
- به تیم مدیریت ارشد خود گزارش دهید تا آنها از نحوه مدیریت امنیت مطلع شوند.
- شرایط امنیتی را به پیمانکاران فرعی منتقل کنید.
- از حسابرسی‌های مشتری خود استقبال کنید، درمورد هر مسئله‌ای که با آن روبرو شدید به او بگویید و برای بهبود امنیت با او به طور فعالانه کار کنید.
- اگر مشتریان خود در مورد نیازهای امنیتی خود راهنمایی نمی‌کنند، آن‌ها را به چالش بکشید .اطمینان حاصل کنید که آنها از اقدامات شما خوشحال هستند.

۲-۱-۳۳- آگاهی از امنیت را در زنجیره تأمین خود افزایش دهید

روابط تأمین کننده می‌تواند با بسیاری از نقاط تماس سازمان شما ارتباط برقرار کند .بنابراین مهم است که به افراد خود در مورد چگونگی عملکرد قراردادها و توافق نامه‌های امنیتی مرتبط آموزش دهید. خطرات امنیتی را برای تهیه کنندگان خود با استفاده از زبانی که آن‌ها می‌توانند درک کنند توضیح دهید .تأمین کنندگان خود را تشویق کنید که خطرات افرادشان را توضیح دهند (به خصوص اگر در زمینه‌های خرید، امنیت و بازاریابی کار می‌کنند)، بنابراین آنها مسئولیت‌های خود را برای کمک به مدیریت آن‌ها می‌دانند.

افراد تأمین کننده شما ممکن است به مرور زمان به دلیل جابجایی کارکنان یا تغییر نقش تغییر کنند .با تأمین کنندگان خود کار کنید تا اطمینان حاصل کنید:

- افرادی که به اطلاعات رسمی یا محافظتی دسترسی پیدا کرده‌اند، نیاز مستمر به حفظ رازداری را یادآوری می‌کنند
- افراد جدید الزامات امنیتی شما را درک می‌کنند.

اگر تأمین کننده شما افرادی دارد که به مجوزهای امنیت ملی نیاز دارند، مطمئن شوید که آنها با تعهدات تعیین شده در حفظ مجوز امنیت ملی شما آشنا هستند. اطلاعات امنیتی را در سراسر زنجیره تأمین خود به اشتراک بگذارید تا آنها را در جریان حملات امنیتی ظهور قرار دهید.

۲-۱-۳۴- از حوادث امنیتی پشتیبانی کنید

منطقی است که از تأمین کنندگان خود انتظار داشته باشیم خطرات امنیتی را طبق قرارداد خود مدیریت کنند .اما آماده باشید تا در صورت لزوم پشتیبانی و مساعدت کنید .به عنوان مثال، هنگامی که حوادث امنیتی می‌تواند به طور بالقوه بر تجارت شما یا زنجیره تأمین گسترده شما تأثیر بگذارد.

❖ الزامات را در قراردادهای تأمین کننده روشن کنید

در قراردادهای خود با تأمین کنندگان، الزامات مربوط به مدیریت و گزارش حوادث یا نقض امنیت را به روشنی مشخص کنید.

مسئولیت‌های آنها را برای مشاوره در مورد حوادث روشن کنید .به عنوان مثال، روشن کنید که پس از یک حادثه چه زودتر آنها باید به شما گزارش دهند، گزارش باید به چه کسی مراجعه کند و غیره .بسیار مهم است که اطمینان حاصل کنید ارائه دهندگان خدمات شما حوادث یا حوادث مشکوکی را تحت تأثیر قرار می‌دهند:

- توانایی آنها در ارائه خدمات قراردادی خود
- اطلاعات سازمان شما (هنگامی که آن‌ها آن‌ها را در دست دارند یا حمل می‌کنند).

همچنین باید به وضوح بیان کنید که به دنبال یک حادثه تأمین کنندگان شما از شما انتظار دارند چه حمایتی داشته باشند .بعنوان مثال، با پاکسازی و رسیدگی به ضررها پشتیبانی کنید. روشن کنید که چگونه تأمین کننده شما حوادث یا نقض امنیت را مدیریت می‌کند. شرایط قرارداد را در نظر بگیرید که ارائه دهندگان خدمات مجبور می‌کنند در مورد نقض امنیت ICT که شامل اطلاعات مشتریان دیگر است، به شما گزارش دهند.

❖ **دروس آموخته شده را به اشتراک بگذارید**

وقتی از حوادث امنیتی عبرت گرفتید، آن‌ها را با تمام تأمین کنندگان خود در میان بگذارید .کمک کنید تا از قربانی شدن حملات "شناخته شده و قابل کنترل" جلوگیری شود .

۲-۱-۳۵- فعالیت‌های اطمینان را در مدیریت زنجیره تأمین خود ایجاد کنید

وقتی تأمین کنندگان کلید امنیت زنجیره تأمین شما هستند، شرط قرارداد آنها باشید:

- در مورد عملکرد امنیتی به تیم مدیریت ارشد خود گزارش دهید
- هرگونه سیاست و فرآیند مدیریت ریسک را که تعیین می‌کنید دنبال کنید.

"حق ممیزی" را در کلیه قراردادها ایجاد کرده و از آن استفاده کنید .از تأمین کنندگان خود بخواهید که برای قراردادهایی که اجاره می‌دهند، همین کار را انجام دهند .حسابرسی‌ها ممکن است دسترسی به محل، سوابق و تجهیزات ارائه دهنده خدمات باشد. با این حال، این ممکن است همیشه امکان پذیر یا مطلوب نباشد، به ویژه هنگامی که یک سرویس مبتنی بر ابر است.

وقتی تأمین کنندگانی را که به بیش از یک سازمان دولتی خدمات ارائه می‌دهند ارزیابی می‌کنید، برای جلوگیری از تکرار، ارزیابی را به اشتراک بگذارید. در صورت توجیه، الزامات اطمینان را در الزامات امنیتی خود وارد کنید .به عنوان مثال، گزارش اطمینان، تست‌های نفوذ، ممیزی‌های خارجی و گواهینامه‌های رسمی امنیتی.

- شاخص‌های کلیدی عملکرد را برای اندازه گیری عملکرد مدیریت امنیت زنجیره تأمین خود تعیین کنید.
- هر یافته و آموخته‌ای را مرور کرده و به آنها عمل کنید.
- تأمین کنندگان را تشویق کنید تا رفتارهای امنیتی خوب را ارتقا دهند.

۲-۱-۳۶- بهبود مستمر امنیت در زنجیره تأمین خود را تشویق کنید

تأمین کنندگان خود را تشویق کنید تا به طور مستمر ترتیبات امنیتی خود را بهبود بخشند .هنگام کار در زمینه بهبود، از مشاوران و مشاوران آنها پشتیبانی کنید.

تأکید کنید که چگونه بهبود امنیت به آنها کمک می‌کند تا در آینده برای رسیدن به توافق نامه و برنده شدن در قرارداد شما با یکدیگر رقابت کنند .استفاده از این روش به شما کمک می‌کند تا زنجیره تأمین خود را رشد داده و مجموعه تأمین کنندگان بالقوه خود را که نیازهای امنیتی شما را برآورده می‌کنند، افزایش دهید.

از ایجاد موانع غیرضروری برای پیشرفت خودداری کنید .آماده باشید تا اقدامات امنیتی یا گواهینامه‌های موجود را که نشان می‌دهد چگونه آنها حداقل شرایط امنیتی شما را برآورده می‌کنند، تشخیص دهید. برای تأمین امنیت وقت برای تأمین کنندگان خود در نظر بگیرید، اما از آنها بخواهید که برنامه‌ها و برنامه‌هایی را به شما نشان دهند که نشان می‌دهد چگونه آنها قصد دارند این پیشرفت‌ها را انجام دهند. هرگونه نگرانی را که تأمین کنندگان برجسته می‌کنند، گوش داده و عمل کنید - نگرانی‌هایی که نشان می‌دهد رویکردهای فعلی مثر نیستند .تأمین کنندگان ممکن است هنگام نظارت بر عملکرد، از طریق گزارش یا پس از پاسخ به حوادث امنیتی، مواردی را مطرح کنند.

۲-۱-۳۷- با تأمین کنندگان اعتماد ایجاد کنید

مدیریت زنجیره تأمین یک مسئله مشترک است، بنابراین با تأمین کنندگان اصلی خود مشارکت راهبردی کنید .هنگامی که نیازهای شما و همچنین نیازهای شما را در نظر بگیرد، احتمالاً آنها از رویکرد شما برای امنیت زنجیره تأمین پیروی می‌کنند .ورودی آنها را تشویق و ارزش گذاری کنید و مسائل امنیتی را با آنها به اشتراک بگذارید .ارتباط منظم و داشته باشید.

اشکالی ندارد که به تأمین کنندگان اجازه دهید پیمانکاران فرعی را برای شما مدیریت کنند اما از آنها بخواهید عملکرد امنیتی را گزارش دهند.

۲-۱-۳۸- ارزیابی امنیت زنجیره تأمین خود

برای شروع روند درک وضعیت خود، به جدول زیر برای مثالهایی از امنیت زنجیره تأمین خوب و بد مراجعه کنید.

رویکرد ضعیف	رویکرد خوب
مخاطرات ارزیابی	
شما از ناحیه مخاطراتی که تامین‌کنندگان برای شما و زنجیره گسترده‌تر تامین شما پدید آورند، با درک ضعیفی دارید. شما مخاطراتی را که همراه خدمات و کالاهای آنها نزد شما می‌آید را نمی‌شناسید	شما مخاطراتی را که تامین‌کنندگان برای سازمان شما و زنجیره گسترده‌تر تامین شما پدید می‌آورند را می‌شناسید. شما با مخاطرات مرتبط با کالاها و خدمات ارائه داده شده، آشنا و در جریان هستید.
شما حساسیت اطلاعاتی که نزد تامین‌کنندگان شما قراردارد، را نمی‌دانید، و شما ارزش پروژه‌هایی را که آنها پشتیبانی می‌کنند، نمی‌دانید	شما حساسیت اطلاعات در اختیار تامین‌کنندگان خودتان را می‌دانید و از ارزش پروژه‌های مورد پشتیبانی آنها آگاه هستید.
داشتن اشراف و آگاهی به عمق زنجیره تامین شما	
شما فقط تامین‌کنندگان بلافاصله‌تان را می‌شناسید و از اطلاعات و خود پیمانکاران فرعی یا اطلاع ندارید و یا دارای محدودیت هستید	شما از گستره و پهنه کامل زنجیره تامین خود، شامل پیمانکاران فرعی اطلاع دارید
برخورداری از داشتن امنیت زنجیره تامین خودتان	
شما واقعا و در حقیقت امر از وضع امنیتی زنجیره تامین خود مطلع نیستند، لیکن گمان می‌برند که وضع خوب است و همه چیز مطابق نظر شماست. شما از بررسی و مرور این وضعیت غفلت می‌کنید.	شما از ترتیبات امنیتی تامین‌کنندگان خود آگاهی دارید، و به طور منظم و براساس قاعده به این اطمینان رسیده‌اید که آنها مخاطرات مرتبط با قرارداد شما را به نحوی کارآمد یا مدیریت می‌نمایند.

شما روی زنجیره تامین خودتان تجربه کنترل ضعیف دارید، ورودی پیمانکاران فرعی نظارت ناقص دارید و از بررسی و ممیزی صحیح آنها عاجز می‌مانید.	شما تجربه کنترل برروی زنجیره تامین خودتان را دارید و از حق ممیزی و بررسی آنها برخوردار هستید.
در اغلب موارد، نخستین تماس گروه امنیتی شما با تامین کننده، یک شکل بررسی ممیزی خواهد بود که یک رخ داد را پیگیری می‌کند	درخواست ممیزی یا بررسی نخستین تعامل شما با تامین کننده
شما از تامین‌کنندگان خود درخواست ارائه گزارش در خصوص عملکرد برنامه امنیتی‌تان ننموده‌اید. گروه مدیریت ارشد شما تجربی نمی‌داند که وضعیت امنیتی خوب پیش می‌رود یا نه	شما هم‌چنین از تامین‌کنندگان خود درخواست دارید تا در خصوص عملکرد امنیتی ارائه گزارش نمایند، از ایزو، تیم مدیریت ارشد شما نمی‌تواند از این موضوع اطمینان یابد که تمام کار به جزئی در حال انجام است
تنظیم و برقراری الزامات امنیت حداقلی	
-شما از تعیین و برقراری حداقل الزامات امنیت عاجزمانده‌اید، و آن را معطل نگاه داشته اید تا تامین‌کنندگان کار را خودشان انجام دهند.(شاید آنها دانش و آگاهی لازم امنیتی بمنظور شناخت اقدامات مورد نیاز را در اختیار نداشته باشد، یا این که نمی‌دانند چگونه آنها را به نحوی موثر و کارآمد اجرا نمایند) یا این که شما حداقل الزامات امنیتی را برقرار نموده‌اید، اما از تطبیق و سازگارکردن آنها با ارزیابی شما مخاطرات پیش‌رو که به طور بالقوه امنیت را برای بسیاری از تامین‌کنندگان شما دست نایافتنی می‌نماید، عاجز مانده‌اید. - شما بدون در نظر گرفتن قرار داد و مخاطرات ارزیابی شده، رویکردی نامتناسب ((یک اندازه متناسب برای همه)) برای همه تامین‌کنندگان تنظیم کرده‌اید -شما از حصول اطمینان روی این کنترل، عاجزمانده‌اید که آیا راستی آزمایی شده‌اند یا قابل دست یابی‌اند و این که به بالقوه تامین کنندگان برای عقد قرارداد با شما از گردونه رقابت خارج شده‌اند.	-به استناد ارزیابی شما از مخاطرات و میزان اقدامات امنیتی لازم برای کاستن آنها، شما حداقل الزامات امنیتی را برای تامین‌کنندگان برقرار ساخته‌اند. شما انتظارات امنیتی خودتان را در قرارداد لحاظ می‌نمایید. -شما به سطوح مختلف حفاظت مورد نیاز برای مخاطرات ارزیابی شما و قراردادمعین، مطابقت دارید. شما از این حفاظت‌ها اطمینان یافته‌اید که راستی آرزمایی ، متناسب سازی اش و قابل دست یابی اند. -شما توقع دارید الزامات امنیتی شما در سراسر زنجیره تامین خود، برآورده نمایید. شما برای حصول اطمینان از این که تامین کنندگان شما از آن پیروی می‌کند، را بررسی می‌کنید.
مواجهه با مسئولیت‌های شما به مثابه یک تامین کننده	
-شما نسبت به مسئولیت‌های خود به عنوان یک تامین کننده یا بی توجهی می نمایید تا آنها را نادیده می‌گیرید و به هیچ یک از موارد غیبت در راهنمای مشتری اعتنا ندارید.	-شما نسبت به مسئولیت‌های خود در کسوت یک تامین کننده توجه دارید و با مشتریان خود برای آشنایی با آنچه که کمبود دارید، به چالش می‌پردازید.

-شما از عبور کردن نیازمندی‌هایتان عاجز هستید و از گزارش کردن آن به مدیریت ارشد خود در باب عملکرد امنیتی بازمانده اید.	-شما قادر به عبور و حل نیازهای مشتریان خود هستید و آن را به مدیریت ارشد عملکرد امنیتی گزارش می نمایید.
ترتیبات حمایت از وقوع یک رخ داد	
- شما هیچ گزارش رخ دادی را به تامین کنندگان خودتان ارائه نمی نمایید - شما از ناحیه اقدام یا نظارت در جایی که امکان دارد موضوعات شناخته شده و معلوم برای دیگران حاضر در زنجیره تامین شما تاثیر بگذارند، عاجز مانده‌اید و از اقدام به مطلع ساختن سایرین در خصوص این موضوعات غافل هستند. این فقدان در عمل به طور بالقوه منجر به از هم گسیختگی و وقفه، با وارد آوردن صدماتی از باب موضوعات معلوم به بسیاری از تامین کنندگان می گردد. - به روز نگاهداشتن تامین کنندگان در باب تغییرات مخاطرات سایبری: شما از تامین کنندگان انتظار دارید تا آنها مخاطرات ناشی از حمله سایبری را پیش بینی کرده و در این خصوص یا ارائه پیشنهادی نمی‌کنید تا به حداقل اکتفا نمایند آنهم بدون در نظر گرفتن آگاهی بخشی امنیتی و توانمندیهای آنها	- شما تعددی دستورالعمل در راهنما و امر پشتیبان برای تامین کنندگان در واکنش به رخ داد امنیتی ارائه می دهید - شما دروس آموخته شده را به دیگران ارائه می دهید تا در برابر حوادث امنیتی به تامین کنندگان پاسخ دهند. - شما در خصوص مخاطرات پدیدار شده از باب حملات سایبری به تامین‌کنندگان کوشزد می‌نمایید تا آنها سطح بیداری و آگاهی خود را بالا برند و بهینه سازند. شما به نحوی فعال، بهترین تجارت خود را برای بالابردن استانداردسازی عملی به اشتراک می‌گذارید
با اطمینان، ساختن	
شما از گنجاندن اقدامات اطمینان بخش در الزامات و نیازهای امنیتی خودتان عاجزهستید. شما بر این باور هستید که تامین کنندگان شما، کارهای را به خوبی انجام خواهند داد، بدون در نظر گرفتن اینکه آیا آنها دانش کافی یا تجربه لازم در داشتن آنچه که از آنها توقع دارید، دارند یا نه	شما اقدامات اطمینان بخش لازم را روی حداقل الزامات امنیتی تان بنا می سازید تا از این رهگذر یک دیدگاه مستقل از کارآمدیهای امنیت تامین کنندگان خود ارائه نمایید(اقداماتی مانند ممیزی، بررسی و آزمایش نفوذ و تداخل)
پایش‌گری کارآمدی و اثربخشی امنیت	
-شما از پایش کارآمدی اقدامات امنیتی عاجز هستید -شما از شنیدن بازخوردها غافل هستید.شما اراده ای برای ساخت تغییرات، حتی هنگام آن که شواهد انجام رخ داد بیش از لق لقه زبانی است و حتمی رخ می دهد	-شما کارآمدی در اثر بخشی‌های اقدامات امنیتی را که در حال رخ دادن است پایش می کنید -شما کنترل خود را که به استناد دروس آموخته شده از رخ داده‌ها، بازخوردهای گرفته شده از فعالیت‌های اطمینان بخش، و بازخوردهای گرفته شده از تامین کنندگان درباره موضوعات یا تجدید نظر می نمایید تا از آن ها حرف نظر می کنید.

۱۹-۲- دور از دفتر کار کردن

سازمان‌های بیشتری در حال اتخاذ ترتیبات کاری انعطاف پذیر برای افراد خود (کارمندان و پیمانکاران) و افراد خود را برای کار در هر مکان و در هر زمان تجهیز می‌کنند .در نتیجه، کار در خارج از دفاتر سنتی به امری عادی تبدیل شده است .افراد شما ممکن است برای انجام کارهای خود از دستگاه‌های همراه مانند لپ تاپ، کامپیوترهای نوت بوک، تبلت ها و تلفن‌های هوشمند استفاده کنند .آن‌ها همچنین ممکن است اسناد کپی را به همراه داشته باشند، هرچند این موارد نادر است.

افراد شما ممکن است در خانه، هتل‌ها یا مکان‌های کنفرانس کار کنند .آن‌ها ممکن است هنگام مراجعه به دفاتر مشتری، در حمل و نقل عمومی یا در حین کار میدانی کار کنند .این روش‌های کاری خطراتی را به همراه دارد .برای کمک به شما در شناسایی و کاهش خطرات افراد، اطلاعات و دارایی‌های خود از راهنمایی‌های این بخش استفاده کنید .به یاد داشته باشید که الزامات قانونی ممکن است بر این راهنمایی اولویت داشته باشد.

برنامه ریزی برای کار مردم در خارج از کشور؟ منابع زیر را برای راهنمایی بررسی کنید:

- مشاوره امنیتی برای مقامات دولت نیوزلند که به خارج از کشور سفر می کنند
- www.safetravel.govt.nz
- راهنمای امنیت اطلاعات نیوزلند - خارج از سایت کار می کند
- مسافرت به خارج از کشور با دستگاه های الکترونیکی

برای راهنمایی در مورد کار دور از دفتر به بخشهای زیر مراجعه کنید.

۳۹-۱-۲- قبل از کار دور از دفتر

روش‌های مختلف کار در خارج از دفتر، خطرات سازمان شما را در معرض خطر قرار دهد و نحوه برخورد با برنامه ریزی برای کاهش این خطرات را درک کنید.

❖ راه‌های کار دور از دفتر

دو راه اصلی که افراد دور از دفتر کار می‌کنند، استفاده از طریق تلفن همراه یا کار از راه دور است.

- کار با موبایل عمدتاً توسط افرادی انجام می‌شود که زیاد مسافرت می‌کنند و معمولاً در یک محیط عمومی با کنترل‌های امنیتی محدود کار می‌کنند .به عنوان مثال، هنگام مراجعه به مشتری یا مشتری، انجام کارهای صحرایی، رفت و آمد یا کار در یک کافه یا سالن فرودگاه.
- کار از راه دور زمانی است که افراد از محیط‌های کنترل شده و ثابت کار می‌کنند که در آن خطرات امنیتی ارزیابی شده و اقدامات امنیتی در آن اعمال شده است .به عنوان مثال، افرادی که به طور منظم در خانه کار می‌کنند، یا از مکانی جایگزین دفتر سازمان خود کار می‌کنند.

این تنظیمات انعطاف پذیر ممکن است موقتی یا دائمی باشد و معمولاً به فناوری متکی هستند تا افراد بتوانند کارهای خود را به طور مؤثر انجام دهند.

❖ دور از اداره کار خطراتی دارد

افراد شما وقتی دور از دفتر کار می‌کنند می‌توانند با خطرات مختلفی روبرو شوند .و این خطرات ممکن است گاهی اوقات به خانواده، دوستان و همکاران نیز سرایت کند.

دور از اداره کار همچنین خطرات اطلاعات و دارایی‌های سازمان شما را افزایش می‌دهد - می‌تواند از بین برود، سو استفاده شود، به سرقت برود، آسیب ببیند یا از بین برود.

خطرات بسته به میزان کنترلی که سازمان شما بر محیط کار افراد شما دارد بسیار متفاوت است.

❖ **برای کاهش خطرات خود از قبل برنامه ریزی کنید**

ممکن است سازمان شما اجرای برخی از عناصر امنیتی محافظتی در سناریوهای کار با تلفن همراه و از راه دور را دشوار بداند .با این حال، شما باید تمام اقدامات عملی منطقی را برای اطمینان از ایمنی افراد، اطلاعات و دارایی خود انجام دهید.

برای کمک به شما در انجام این کار، چرخه زندگی امنیت اطلاعات و چرخه زندگی امنیت فیزیکی را در نظر بگیرید .به طور خلاصه، شما باید این پنج مرحله را اجرا کنید.

- خطرات موجود درمورد افراد، اطلاعات و دارایی‌ها (آسیب پذیری های خود) را بشناسید.
- خطرات تهدیدات و تأثیرات احتمالی آنها را بر روی افراد و سازمان خود ارزیابی کنید.
- تدابیر امنیتی لازم برای محافظت از افراد، اطلاعات و دارایی‌های خود را طراحی و اجرا کنید.
- عملیات ایمن را حفظ کرده و پشتیبانی مورد نیاز خود را به مردم ارائه دهید.
- حوادث امنیتی را مرور کرده و از آنها بیاموزید .اقدامات امنیتی خود را بهبود ببخشید، بنابراین برای اهداف مناسب باقی می‌مانند.

۲-۱-۴۰- درک و ارزیابی خطر

قبل از اینکه بتوانید از افراد، اطلاعات و دارایی خود در کار دور از سناریو دفتر محافظت کنید، باید خطرات احتمالی و تأثیرات آن را درک کنید.

سازمان شما بر اساس قانون ایمنی و بهداشت در محل کار ۲۰۱۵ (و هرگونه مقررات و آیین نامه‌های مربوطه که اعمال می‌شود) مسئولیت دارد که تمام اقدامات عملی منطقی را انجام دهد:

- خطرات مردم خود را برطرف کنید
- از صدمه به افراد در و یا در نزدیکی امکانات خود (از جمله مردم) جلوگیری کنید.
- امنیت و امنیت افراد شما باید بر امنیت اطلاعات و دارایی‌های شما ارجحیت داشته باشد .افراد شما برای محافظت از اطلاعات یا دارایی‌ها نباید بی دلیل خود را در معرض آسیب یا صدمه قرار دهند.

شما باید:

- شناسایی خطرات، تهدیدها و خطرات احتمالی (از جمله خطرات شخصی هنگام حمل یا محافظت از اطلاعات و دارایی‌های ارزشمند)
- احتمال بروز خطرات یا خطرات را ارزیابی کنید.

۲-۱-۴۱- ارزیابی خطرات کار با موبایل

خطرات ناشی از کار با موبایل را برای افراد، اطلاعات و دارایی‌های خود در نظر بگیرید.

افراد شما ممکن است با استفاده از دستگاه‌های قابل حمل مانند لپ تاپ، کامپیوترهای نوت بوک، رایانه لوحی و تلفن‌های هوشمند، کار تلفن همراه را انجام دهند .آن‌ها ممکن است از اسناد کپی استفاده کنند، زیرا این امر نادر است.

برخی از سناریوهای نمونه برای کار با تلفن همراه عبارتند از:

- کار میدانی
- کار گاه به گاه از خانه بدون توافق نامه کار از راه دور
- کار موقت از امکانات مشتری
- کار مداوم از محل مشتری که سازمان شما نمی‌تواند ترتیبات امنیتی را اطمینان دهد
- کار انجام شده در حالی که در حال حمل و نقل است.

به محیطی که انتظار می‌رود افراد شما در آن فعالیت کنند بسیار توجه کنید زیرا ممکن است تأثیر مهمی در الزامات امنیتی داشته باشد. محیط‌های کاری سیار می‌توانند از سالن‌های فرودگاه، دفتر یک سازمان دیگر، تا یک مکان از راه دور باشند.

❖ **اگر شرایط منطقه امنیتی اعمال می‌شود، کار کنید**

الزامات منطقه امنیتی ممکن است در بعضی از مکان‌ها اعمال شود .این الزامات به محافظت از اطلاعات و منابع رسمی یا ارزشمند کمک می‌کند .اکثر مکانهای کاری موبایل "منطقه ۱: مناطق دسترسی عمومی" با امنیت محدود در محل هستند.

اگر در یک فضای اداری امن کار می‌کنید، به احتمال زیاد "منطقه ۲: منطقه کاری" در نظر گرفته می‌شود.

با این حال، اگر به سطوح حفاظتی "منطقه ۳: منطقه کار محدود"، "منطقه ۴: منطقه امنیتی" یا "منطقه ۵: منطقه با امنیت بالا" نیاز دارید، اطمینان از اینکه اقدامات امنیتی فیزیکی مطابق با الزامات امنیتی شما است، ممکن است دشوار باشد .در عوض، برای محافظت از اطلاعات و دارایی‌های خود به کنترل‌های امنیتی اداری و ICT اعتماد کنید.

❖ **خطرات خاص مربوط به کار با موبایل را در نظر بگیرید**

خطرات و تأثیرات زیر را برای کار با موبایل در نظر بگیرید و برای کمک به شما در ارزیابی خطرات، از چک لیست زیر استفاده کنید.

چک لیست برای کار با تلفن همراه و از راه دور

❖ **ارعاب و رفتار خشونت آمیز مشتریان یا غریبه‌ها**

هنگام کار دور از دفتر، به ویژه هنگامی که تنها هستید، افراد شما در معرض خطر بیشتری از افرادی هستند که با آنها ارتباط برقرار می‌کنند .به عنوان مثال، افراد شما می‌توانند هدف سو abuse استفاده کلامی یا حملات فیزیکی مشتریان یا غریبه‌ها قرار گیرند.

❖ **ردیابی از طریق GPS یا فرستنده‌های دستگاه**

گیرنده‌ها و فرستنده‌های داخلی داخلی در دستگاه‌ها امکان ردیابی موقعیت‌های دقیق افراد را فراهم می‌کند و آنها و اطلاعات شما را در معرض خطر قرار می‌دهد.

❖ **از دست دادن یا سرقت اطلاعات حساس**

از دست دادن یا سرقت نسخه‌های چاپی کاغذها و دستگاه‌های قابل حمل آسان است .در هر صورت، اطلاعات حساس سازمان شما در معرض دید قرار می‌گیرد .اعتبار یا عملیات شما ممکن است به شدت تحت تأثیر قرار گیرد، یا حریم خصوصی شخصی نقض شود .

❖ **نقض امنیت یا حریم خصوصی باعث مخفی شدن رازداری می‌شود**

اگر افراد شما مقالات را بخوانند و از وسایل در فضاهای عمومی استفاده کنند، ممکن است اطلاعات حساس شنیده یا نظارت شود، که منجر به محرمانه بودن اطلاعات، از بین رفتن مالکیت معنوی یا نقض حریم شخصی می‌شود.

❖ **رهگیری الکترونیکی که منجر به اقدامات مخرب یا مخفیانه می‌شود**

دستگاه‌های مورد استفاده در شبکه‌های بی سیم و عمومی در برابر رهگیری الکترونیکی آسیب پذیر هستند .نرم افزار مخرب می‌تواند ویژگی‌های امنیتی را غیرفعال کرده و میکروفون‌ها و دوربین‌های داخلی را برای ضبط مناظر و صداها فعال کند و به مهاجمان امکان دسترسی به محتوای خصوصی و ممتاز و مکالمات را می‌دهد.

دستگاه‌هایUSB ، دستگاه‌های ذخیره سازی قابل حمل، CDو DVD اهداف آسانی برای فعالیت‌های مخرب مانند توزیع بدافزار و انجام عملیات اکسفیلتراسیون داده‌ها (سرقت داده‌ها) هستند.

❖ **نرم افزار مخرب شبکه‌ها یا تجهیزات را خراب می‌کند**

درست مثل هر رایانه خانگی یا اداری، دستگاه‌های قابل حمل نیز در معرض بدافزار هستند که می‌توانند به شبکه‌های متصل و سایر تجهیزات محاسباتی منتقل شوند .خدمات و عملکردهای شما به طور قابل توجهی مختل می‌شود.

❖ **خطرات قضایی**

اگر در خارج از نیوزیلند کار می‌کنید، برخی از حوزه‌های قضایی قانونی دارند که ممکن است به مقامات محلی اجازه دسترسی به اطلاعات و سیستم‌های شما را بدهد .شما باید در نظر بگیرید که آیا با توجه به ماهیت اطلاعاتی که ذخیره یا انتقال می‌دهید، این یک خطر قابل قبول است.

۲-۱-۴۲- ارزیابی خطرات کار از راه دور

خطرات ناشی از کار از راه دور برای افراد، اطلاعات و دارایی‌های خود را در نظر بگیرید.

وقتی افراد از راه دور کار می‌کنند، ممکن است از نسخه‌های چاپی اطلاعات یا فناوری مانند دستگاه‌های تلفن همراه، رایانه‌های شخصی و شبکه‌های بی سیم استفاده کنند .

ترتیب کار برای کار منظم در خانه ممکن است به شرح زیر باشد:

- بخشی از یک ترتیب کاری عادی، تمام وقت یا نیمه وقت
- ساعت‌ها خارج از ساعت کار عادی (معروف به "افزایش دهنده‌های روز")
- بخشی از یک ترتیب منظم کار از راه دور منظم (به عنوان مثال، برای یک مراقب اولیه).

ترتیبات در حال انجام برای کار مردم از یک مکان دیگر ممکن است در موارد زیر باشد:

- محل مشتری، جایی که سازمان شما توانایی تأمین امنیت محافظتی را دارد
- مکان دیگری (به عنوان مثال، سایت‌های تداوم کسب و کار یا سایت‌های منطقه‌ای)
- امکانات سازمان دیگری.

برای جلوگیری از مشکلات همگام سازی و کاهش هزینه‌ها، تأمین کننده‌های روز و کارگران از راه دور نیمه وقت را با دستگاه‌های قابل حمل اختصاصی در نظر بگیرید.

توسعه دهندگان روز ممکن است در هر زمان، شبانه روز انتظار پشتیبانی ICT را داشته باشند.

کار از یک فضای اداری جایگزین می‌تواند در یک سایت تداوم کسب و کار یا یک سایت منطقه‌ای، در یک سازمان دیگر یا در محل کار مشتری باشد که سازمان شما توانایی تأمین امنیت محافظتی را دارد.

❖ خطرات خاصی را باید در نظر گرفت

خطرات امنیتی اضافی ممکن است با کار از راه دور مرتبط باشد .مکانهای کار از راه دور اغلب ثابت هستند و مکانهای آن‌ها برای بسیاری شناخته شده است، از جمله:

- افرادی که از راه دور کار می‌کنند و همکارانشان
- سایر اعضای سازمان شما و همکاران آنها.

سازمان شما باید الزامات امنیتی همه مکانهای بالقوه برای کار از راه دور را ارزیابی کند، از جمله:

- مدیریت ترخیص امنیتی
- امنیت و امنیت شخصی
- اطلاعات و امنیتICT
- امنیت فیزیکی

برای کمک به شما در ارزیابی خطرات، از چک لیست زیر استفاده کنید.

- چک لیست برای کار با تلفن همراه و از راه دور

به یاد داشته باشید افرادی که بدون پشتیبانی ICT دور از دفتر شما کار می‌کنند ممکن است همچنان به نسخه‌های چاپی، اطلاعات در قالب‌های الکترونیکی و تجهیزات مورد نیاز برای محافظت دسترسی داشته باشند .

❖ ارزیابی امنیت فیزیکی برای مکانهای کار از راه دور

سطح صحیح امنیت فیزیکی برای محل کار از راه دور به سطح تأثیر تجارت (BIL) در مورد آسیب احتمالی افراد، اطلاعات و دارایی شما بستگی دارد. استفاده از BIL به شما کمک می‌کند سطح امنیت را به درستی بدست آورید.

هنگامی که BIL به بالا یا بالاتر ارزیابی می‌شود، قبل از اجرای هرگونه ترتیب کار برای کار از راه دور، باید اطمینان حاصل کنید که اقدامات امنیتی برای هر مکان پیشنهادی مناسب است. برای BIL های پایین‌تر، باید مناسب بودن اقدامات امنیتی را در مکان‌های بالقوه ارزیابی کنید و در صورت لزوم آنها را بهبود ببخشید.

الزامات منطقه امنیتی ممکن است در بعضی از مکان‌ها اعمال شود .مناطق امنیتی به محافظت از اطلاعات و منابع رسمی یا ارزشمند کمک می‌کنند .اکثر مکانها بدون نیاز به تغییرات اساسی در سایت، شرایط منطقه ۲ را برآورده می‌کنند .

❖ گزینه‌های سیستم هشدار امنیتی برای کار از راه دور

در ارزیابی ریسک خود، نیاز به سیستم‌های هشدار امنیتی را در تنظیمات کار از راه دور در نظر بگیرید. در صورت نیاز به سیستم هشدار امنیتی، از سیستمی استفاده کنید که مطابق با AS / NZ 2201.1: 2007 کلاس ۲ یا بالاتر باشد.

۲-۱-۴۳- ارزیابی امنیت فیزیکی برای اطلاعات و دارایی‌های رسمی

قبل از اینکه افراد شما از هر فضای کاری خارج از دفتر سنتی استفاده کنند، بیاموزید که چگونه از اطلاعات و دارایی‌های رسمی که ممکن است در آنجا ذخیره یا استفاده شود محافظت می‌کنید.

❖ **اطلاعات رسمی**

برای کسب اطلاعات رسمی، به این پاسخ دهید تا به شما کمک کند.

- آیا می‌توانید از نظر امنیتی که برای محافظت در محیط کار ذخیره می‌کنید، سطح امنیتی درستی داشته باشید؟
- آیا می‌توانید فضای کار را به طور مستقل ایمن کنید؟
- چگونه اطلاعات رسمی را از دیده یا شنیده شدن توسط افراد غیر مجاز، از جمله خانواده و فرزندان محافظت می‌کنید؟
- آیا تجهیزات ICT مورد استفاده در فضای کار را می‌توان از سیستم ICT سازمان شما ایمن یا تفکیک کرد؟

اطمینان حاصل کنید که سایت‌های پیشنهادی دارای اعتبار لازم هستند .این معمولاً شامل بازرسی‌های امنیتی سایت است .برای کسب اطلاعات بیشتر، به: اقدامات امنیتی جسمی خود را تأیید کنید.

❖ **دارایی‌های**

بیشتر دارایی‌های استفاده شده در خارج از دفتر قابل حمل هستند و به محض اینکه از محل کار شما خارج شوند بیشتر در معرض خطر هستند .چند نمونه از دارایی‌های قابل حمل عبارتند از:

- وسایل نقلیه
- دستگاه‌های ارتباطی کار و موبایل
- ظروف امنیتی و سایر مبلمان
- سلاح
- حیوانات
- نمونه‌ها، مانند نمونه‌های بیولوژیکی یا شیمیایی
- تجهیزات تخصصی، علمی یا تحقیقاتی
- مواد فرهنگی یا مجموعه‌ای

در نظر بگیرید که چگونه از دارایی‌های سازمان خود در سناریوهای کار با تلفن همراه و از راه دور محافظت می‌کنید.

۲-۲۰- اقدامات امنیتی خود را طراحی و اجرا کنید

هنگامی که افراد شما خارج از دفتر کار می‌کنند، سازمان شما باید:

- اطمینان حاصل کنید که افراد شما به طور مناسب مختصر و آموزش داده می‌شوند تا مطابق با الزامات و روش‌های امنیتی و ایمنی شما باشند
- قبل از تصویب هرگونه ترتیب کار برای کار در خارج از دفتر، خطرات موجود درمورد افراد، اطلاعات و دارایی خود را تا حد قابل قبولی کاهش دهید
- اقدامات امنیتی را انجام دهید که اطمینان در اطلاعات و ترتیبات تقسیم دارایی را فراهم می‌کند.

۲-۱-۴۴- کاهش خطرات برای مردم خود

افسر ارشد امنیتی شما (CSO) و افسران ایمنی و بهداشت شما باید با هم همکاری کنند تا پاسخ‌هایی را کاهش دهند که خطرات مربوط به ایمنی مردم شما را کاهش می‌دهد و امنیت را در هنگام کار دور از دفتر بهبود می‌بخشد .

برای کمک به شما در توسعه پاسخ‌ها، تصمیم بگیرید که از کدام اقدامات امنیتی برای کاهش خطرات شناسایی شده استفاده می‌کنید .شما هم چنین باید:

- اقدامات پیشگیرانه‌ای را که قبل از خروج افراد از دفتر اعمال می‌شود، شناسایی کنید
- اقدامات جزئی برای انجام موارد اضطراری
- نحوه برخورد مردم با مشتری و مردم (در صورت وجود) را بررسی کنید
- اگر افراد شما اطلاعات و تجهیزات دارای علامت محافظ را منتقل می‌کنند، ایمنی و ایمنی خودرو را در بر بگیرید
- ایجاد رویه‌هایی برای گزارش حوادث امنیتی.

❖ **توسعه روش‌های گزارش حوادث**

اگر احساس می‌کنند امنیت آنها به خطر افتاده است، به افراد خود توصیه کنید تا برای کمک با پلیس محلی تماس بگیرند .پس از ایمن شدن آنها، باید این حادثه را به سازمان شما گزارش دهند.

شما باید رویه‌هایی را برای کارگران سیار یا از راه دور برای گزارش حوادث امنیتی در نظر بگیرید .این روش‌ها باید شامل گزارش دهی باشد:

- هر حادثه امنیتی شامل اطلاعات و دارایی‌های سازمان شما
- حوادث دیگر در محل کار آنها.

وقتی در حال انجام رویه‌های خود هستید، توانایی خود را برای پاسخگویی و تحقیق در مورد حوادثی که در خارج از محل زندگی شما اتفاق می افتد، در نظر بگیرید.

گزارش حوادث و انجام تحقیقات امنیتی اطلاعات و مشاوره بیشتری دارد.

❖ **گزینه‌های سیستم هشدار امنیتی برای کار با تلفن همراه**

استفاده از سیستم هشدار امنیتی را در نظر بگیرید .سازمان‌های شما ممکن است از سیستم‌های هشدار قابل حمل برای محافظت از دارایی در سایر سناریوهای کار با تلفن همراه استفاده کنند .به عنوان مثال، ممکن است وسایل نقلیه مجهز به زنگ هشدار و بی حرکتی موتور باشند.

۲-۱-۴۵- مدیریت امنیت ICT

قبل از اینکه اجازه دهید تنظیمات کاری موبایل یا راه دور شروع شود، شرایط امنیتی ICT را برآورده کنید.

قبل از شروع هماهنگی‌ها، سازمان شما باید کلیه الزامات امنیتی ICT را که در راهنمای امنیت اطلاعات نیوزلند (NZISM) مشخص شده است - در خارج از سایت کار می کند، برآورده کند توجه داشته باشید که در دور از سناریوهای اداره، اعمال امنیت ICTبرای تجهیزات دشوار است .با این حال، هنگامی که افراد شما از تجهیزاتی که سازمان شما در اختیار شما قرار داده است استفاده می‌کنند، منطقی است که انتظار داشته باشیم از آنها به همان روشی که در دفتر کار می‌کنند استفاده کنند.

❖ **مرزهای استفاده از تجهیزات ICT را در سیاست‌های خود بگنجانید**

در سیاست‌های خود برای کار با تلفن همراه و از راه دور، باید مرزهای استفاده از تجهیزات سازمان خود را به روشنی مشخص کنید.

شما باید پوشش دهید:

- معنای استفاده شخصی معقول چیست
- آیا اعضای خانواده می‌توانند از تجهیزات استفاده کنند یا خیر
- هرگونه محدودیت یا قانونی که مردم شما برای رعایت آن نیاز دارند.

❖ **اطلاعات دارای علامت محافظ را مدیریت کنید**

شما نباید به افراد خود اجازه دسترسی به اطلاعات دارای علامت محافظ را در رایانه‌های عمومی یا سایر وسایل ارتباطی عمومی ICT، مانند کافی نت‌ها، مراکز تجاری هتل‌ها یا سالن‌های فرودگاه بدهید.

تمام اطلاعات قابل دسترسی در تجهیزات عمومی ICT در معرض خطر است .سازمان شما هیچ کنترلی بر اینکه چه کسی می‌تواند به تجهیزات یا ویژگی‌های امنیتی یا برنامه‌هایی که توسط مالک یا مدیر آن بر روی تجهیزات فعال هستند، دسترسی پیدا کند.

❖ **استفاده از تجهیزات ICT شخصی برای کار را با دقت در نظر بگیرید**

امروزه افراد بیشتری از دستگاه‌های شخصی خود برای اهداف شرکتی یا دستگاه‌های سازمانی خود برای اهداف شخصی استفاده می‌کنند .هر دو سناریو استفاده، خطراتی را برای اطلاعات سازمان شما افزایش می‌دهد .آموزش کاربران برای مدیریت خطرات بسیار مهم است.

قبل از تأیید استفاده از وسایل شخصی، به راهنمایی‌های زیر در مورد کنترل‌های امنیتی BYOD که باید اعمال کنید مراجعه کنید.

NZISM: 21.4.دستگاه های غیر نمایندگی و دستگاه خود را بیاورید(BYOD)

به افراد خود اجازه ندهید از تجهیزات ICT شخصی برای پردازش اطلاعات با سطح تأثیر تجاری (BIL) بالاتر یا بالاتر، یا دارای علامت محافظتی یا بالاتر استفاده کنند. توجه داشته باشید که حتی هنگام خاموش شدن دستگاه‌ها، اطلاعات همچنان در حافظه ذخیره می‌شوند و بنابراین آسیب پذیر هستند. اطمینان حاصل کنید که افراد شما هنگام کار از طریق USB یا دستگاه ذخیره سازی مشابه، خطر از دست رفتن اطلاعات را درک می‌کنند.

۲-۱-۴۶- محافظت از دستگاه‌های تلفن همراه

راهکارهای زیر را برای محافظت از دستگاه‌های تلفن همراه در نظر بگیرید.

دستگاه‌های تلفن همراه شامل رایانه‌های قابل حمل، دستگاه‌های ارتباطی تلفن همراه و USB یا سایر دستگاه‌های ذخیره سازی قابل حمل است.

❖ **دستگاه‌ها را برای استفاده آماده کنید**

- اطمینان حاصل کنید که امنیت و به روزرسانی های برنامه در هر دستگاه نصب شده است و افراد شما می‌دانند که چگونه به روزرسانی های بعدی ما را بر روی دستگاه‌های خود انجام دهند.
- ویژگی‌های امنیتی دستگاه را فعال کنید و از تغییر پین‌ها و رمزهای عبور اطمینان حاصل کنید .همیشه از گذرواژه‌های پیچیده حاوی حروف بزرگ، کوچک، اعداد و نمادها استفاده کنید.

- اطلاعاتی را که برای کاهش خطر قرار گرفتن در معرض اطلاعات لازم نیست حذف کنید.
- از اطلاعات ذخیره شده در دستگاه پشتیبان تهیه کنید .اگر دستگاهی به خطر بیفتد، ممکن است فرصت بازیابی اطلاعات از آن محدود شود.
- در صورت نگه داشتن اطلاعات رمزگذاری شده توسط دستگاه، احتمال سازش را ارزیابی کنید.

❖ **دستورالعمل‌هایی را برای ایمن و ایمن نگه داشتن دستگاه‌ها ارائه دهید**

اطمینان حاصل کنید که هر کاربر دستگاه تلفن همراه به اندازه لازم از دستورالعمل‌های زیر استفاده می‌کند.

- کنترل فیزیکی دستگاه را همیشه حفظ کنید .آن را در مکان‌هایی که ممکن است یک هدف آسان برای سرقت یا دستکاری باشد، بدون مراقبت رها نکنید.
- همیشه هوشیار باشید .هنگام استفاده از دستگاه، اطمینان حاصل کنید که یک مکالمه قابل شنیدن نیست و دیگران اطلاعات صفحه را نمی‌توانند مشاهده کنند.
- از قرار دادن وسایل در موقعیت‌هایی که احتمالاً گفتگوی حساس یا خصوصی وجود دارد، خودداری کنید .اگر نمی‌توانید از این وضعیت جلوگیری کنید، دستگاه را خاموش کرده و در صورت امکان، باتری را جدا کنید.
- اگر کنترل فیزیکی دستگاه را از دست داده‌اید (به عنوان مثال، هنگامی که دستگاه خارج از جلسه امن است)، قبل از استفاده مجدد از آن، از افراد امنیتی ICT خود راهنمایی بخواهید.
- از دستگاه‌های سازمانی با تمام اقدامات امنیتی مربوطه استفاده کنید .فقط در شرایطی که سیاست‌های BYOD اجازه می‌دهد و اقدامات امنیتی مناسب وجود دارد، از یک وسیله شخصی برای مشاغل رسمی استفاده کنید.
- اگر نگران خطر ردیابی هستید، هر قابلیت GPS را غیرفعال کنید .برای امنیت بیشتر، دستگاه را خاموش کرده و در صورت امکان، باتری را جدا کنید.
- هر ویژگی یا قابلیتی را که نیازی ندارید غیرفعال کنید .به عنوان مثال، خدمات بی سیم، بلوتوث و موقعیت مکانی را غیرفعال کنید .قبل از انجام مکالمات محرمانه، انجام این کار را در نظر بگیرید.
- همیشه یکپارچگی هر رسانه ذخیره سازی جدید را با افراد امنیتی ICT خود قبل از اتصال به دستگاه تأیید کنید .همه رسانه‌های ذخیره سازی باید مرتباً از نظر تهدید اسکن شوند.

❖ **اطمینان حاصل کنید که استفاده از ایمیل ایمن است**

برای کمک به ایمن نگه داشتن ایمیل‌ها، دستورالعمل‌های روشنی مطابق با خط مشی‌های خود در مورد موضوعات زیر ارائه دهید.

- استفاده از حساب‌های ایمیل خصوصی برای ذخیره یا برقراری ارتباط اطلاعات رسمی.
- ارسال ایمیل از سیستم‌های ایمیل شرکت به حساب‌های ایمیل شخصی، مانند .Gmail این خط مشی به ویژه برای ایمیل‌های دارای طبقه بندی "محدود" یا بالاتر مربوط می‌شود.
- هنگامی که به امنیت ایمیل اضافی و نحوه دستیابی به آن نیاز دارید.
- چگونه خطر بارگیری بدافزار مخفی را کاهش دهیم.
- استفاده از اینترنت را ایمن نگه دارید
- برای جلوگیری از نگرانی امنیتی استفاده از اینترنت، دستورالعمل‌های واضح و منطبق با خط مشی‌های خود در مورد موضوعات زیر ارائه دهید
- استفاده از حالت حریم خصوصی در یک مرورگر اینترنت.
- استفاده از کوکی‌ها.

- غیرفعال کردن تکمیل خودکار برای جلوگیری از ذخیره نام‌های کاربری و گذرواژه‌های مرورگر شما.
- اتصال به شبکه‌های خارجی ساده‌ترین اقدامات احتیاطی این است که به اینترنت با استفاده از نقاط داغ ناشناخته متصل نشوید و در عوض از شبکه‌های تلفن همراه ۳ Gیا ۴ Gاستفاده کنید.

❖ **دستگاه‌ها را پس از استفاده ایمن کنید**

- پس از سفر ایده خوبی است که همه گذرواژه‌های دستگاه را تغییر دهید.
- با هرگونه اطلاعات رمزگذاری نشده در دستگاهی که گم شده است، به عنوان خطرناک رفتار کنید

۲-۱-۴۷- محافظت از مکالمات

- شما باید از اطلاعات مهم خود در برابر شنیدن یا ضبط شدن محافظت کنید.
- شما باید روشهایی را برای محافظت از مکالمات تهیه کنید که شامل اطلاعات حساس یا دارای علامت محافظ باشد.
- ضبط مکالمه بسیار آسان‌تر از ضبط صفحه لپ تاپ است، بنابراین انجام این مکالمات در مکان‌های ناامن بسیار خطرناک است.
- اقدامات زیر ممکن است تهدید به طور تصادفی شنیده یا ضبط شده مکالمات را کاهش دهد.

❖ **از مناطق پر خطر خودداری کنید**

به افراد خود یادآوری کنید که مکالمه‌های پرخطر، از جمله مکالمه تلفنی، نباید در اجاره اتومبیل، تاکسی، شاتل، وسایل نقلیه رسمی، اتاق‌های هتل یا اتاق کنفرانس انجام شود، مگر اینکه تدابیری برای اطمینان از امنیت صوتی در نظر گرفته شده باشد .این مناطق در معرض خطر بالای نظارت صوتی قرار دارند.

همچنین افراد خود را از انجام مکالمات حساس یا مکالمه‌های مربوط به اطلاعات طبقه بندی شده در فضاهای عمومی بسته هنگام نشستن یا ایستادن در یک مکان منصرف کنید، زیرا مکالمات به راحتی شنیده یا ضبط می‌شوند .بحث در مورد اطلاعات طبقه بندی شده در انظار عمومی، هواپیما، سالن‌های فرودگاه، در کافه محلی یا مکان‌های دیگری که افراد شما می‌توانند در آن‌ها مراجعه کنند، این اطلاعات را در معرض خطر جدی قرار می‌دهد و باید دلسرد شود.

❖ **در صورت امکان از امکانات ایمن استفاده کنید**

خطر رهگیری صوتی هنگام مسافرت به خارج از کشور بسیار افزایش می‌یابد .به افراد خود توصیه کنید تا جایی که امکان دارد از امکانات ایمن برای مکالمه یا تماس تلفنی شامل اطلاعات حساس یا طبقه بندی شده استفاده کنند .استفاده از امکانات امن یک دولت متحد در صورتی قابل قبول است که امکانات در سطح مناسب اعتبارسنجی شده و اجازه داده شود اطلاعات مورد بحث با آن دولت به اشتراک گذاشته شود.

❖ **از یک فضای باز استفاده کنید**

وقتی هیچ امکان ایمنی در دسترس نیست و مکالمه یا تماس تلفنی ضروری است، افراد خود را به یافتن یک مکان عمومی باز مانند پارک یا فضای باز راهنمایی کنید .سپس آنها باید هنگام راه رفتن صحبت کنند، مراقب باشید که مکالمه توسط ناظران معمولی شنیده نشود. پارک‌ها و مناطق آزاد بیشترین محافظت را از نظارت صوتی گاه به گاه دارند" .صدای سفید"، مانند آب جاری از چشمه‌ها، همچنین ممکن است ضبط مکالمه از راه دور بدون تجهیزات خاص را برای کسی سخت کند.

❖ **از اطلاعات طبقه بندی شده محافظت کنید**

"مناطق امن صوتی" برای ایمن نگه داشتن مکالمات مربوط به اطلاعات طبقه بندی شده استفاده می‌شود.

در خارج از این مناطق، ممکن است جلوگیری از گوش دادن به دشمنان مصمم، از جمله سرویس‌های اطلاعاتی خارجی باشد. شما فقط باید اجازه دهید مکالمات مربوط به اطلاعات طبقه بندی شده در خارج از مناطق امن صوتی انجام شود، زیرا این امر برای یک عملیات حیاتی است. قبل از اجازه هرگونه مکالمه در خارج از مناطق امن صوتی، برای کسب اطلاعات، از مبدع اطلاعات مشاوره بگیرید قبل از اجازه هرگونه مکالمه در خارج از مناطق امن صوتی، برای اطلاعات، از سرویس اطلاعات امنیتی نیوزلند و سازمان مبدأ مشاوره بگیرید.

۲-۱-۴۸-

محافظت از اطلاعات

شما باید از اطلاعاتی که دور از دفتر کار شما استفاده می‌شود یا به مکان دیگری منتقل می‌شود محافظت کنید .برای اطلاعات دارای علامت محافظ نیز باید از الزامات مربوط به دست زدن استفاده کنید.

❖ **امنیت اطلاعات رسمی در تأسیسات خصوصی**

ممکن است در هنگام کار افراد در تأسیسات خصوصی، مانند تأسیسات تجاری یا مشتری، تأمین اطلاعات کافی برای شما دشوار باشد. بعید به نظر می‌رسد شما بتوانید بر کنترل‌های امنیتی کلیدی مانند سیستم‌های هشدار یا کلید زنی کنترل داشته باشید.

تا زمانی که سازمان شما کنترل کاملی روی فضا نداشته باشد، باید با امکانات به عنوان مناطق امنیتی منطقه ۱ برای اطلاعات و ذخیره دارایی رفتار کنید.

❖ **ذخیره اطلاعات دارای علامت محافظ**

اطلاعات دارای علامت محافظ نباید در خارج از دفاتر شما ذخیره شود، مگر اینکه این موارد را اجرا کرده باشید:

- پروتکل مدیریت امنیت اطلاعات
- پروتکل مدیریت برای امنیت فیزیکی
- الزامات پشتیبانی از جمله اعتباربخشی هرگونه ICT و ترتیبات امنیتی فیزیکی

شما نباید اجازه دهید اطلاعات TOP SECRET در خارج از محل زندگی شما ذخیره شود، مگر اینکه برای عملیاتی حیاتی باشد .سرویس اطلاعات امنیتی نیوزلند باید تمام ذخیره اطلاعات TOP SECRET را تأیید کند.

❖ **انتقال اطلاعات به خارج از دفتر**

غیرمجاز است که از مردم انتظار داشته باشد که اطلاعات را به طور مداوم در اختیار داشته باشند، اگر این اطلاعات را به شخص خود منتقل نکنند. با این حال، باید استفاده از رسانه‌های ICT قابل جابجایی، مانند درگاه‌های USB و هارد دیسک‌های قابل حمل را برای حمل اطلاعات زیادی محدود کنید، زیرا به راحتی از بین می‌روند. اطلاعات هنگام انتقال بسیار در معرض خطر است .قبل از اینکه به افراد خود اجازه دهید اطلاعات را به مکان‌های دوردست منتقل کنند، همه گزینه‌ها را در نظر بگیرید.

برخی از گزینه‌های مورد بررسی عبارتند از:

- دسترسی ایمن از راه دور به شبکه‌های ICT شما (در صورت امکان اتصال)
- انتقال اطلاعات به نزدیکان دولت نیوزیلند یا مراکز قضایی با استفاده از پیک‌های تأیید شده یا شبکه‌های امن
- ذخیره اطلاعات در یک دستگاه قابل حمل مورد تأیید اداره امنیت ارتباطات دولت - دستگاهی که کنترل‌های منطقی اضافی را برای جلوگیری از دسترسی غیر مجاز فراهم می‌کند.

- هنگامی که نمی‌توانید حمل و نقل جایگزین ترتیب دهید، در نظر بگیرید که در هنگام استراحت در سفر، اطلاعات را باید در امکانات مناسب دولت نیوزلند یا دولت نیوزلند تأیید کنید.

برای اطلاعات بیشتر به این آدرس بروید:

- الزامات رسیدگی به اطلاعات و تجهیزات دارای علامت محافظ
- مناطق امنیتی

❖ **دفع اطلاعات رسمی به طور ایمن**

سازمان شما باید رویه‌هایی را برای دفع امن اطلاعات رسمی برای همه افرادی که دور از سناریو دفتر کار می‌کنند، فراهم کند.

شما باید اطمینان حاصل کنید که تمام اطلاعات دارای علامت محافظ برای تخریب به محل شما بازگردانده می‌شوند، مگر اینکه تجهیزات تخریب مستقر در محل را تأیید کرده باشید.

برای اطلاعات بیشتر به:

❖ الزامات رسیدگی به اطلاعات و تجهیزات دارای علامت محافظ
- NZISMبهداشت و دفع محصولات
- NZISMمدیریت رسانه، Decommissionو Disposa L

۲-۱-۴۹- محافظت از دارایی‌ها

برای محافظت از دارایی‌های سازمان خود هنگام دور بودن از دفتر، این راهنما را دنبال کنید.

❖ **به ثبت مدیریت دارایی خود اضافه کنید**

دارایی‌های استفاده شده توسط افرادی که دور از دفتر کار می‌کنند را در ثبت مدیریت دارایی خود قرار دهید، حتی اگر ارزش دارایی زیر آستانه‌ای باشد که معمولاً برای کنترل دارایی اعمال می‌کنید.

❖ **حذف مجوز فقط در صورت لزوم**

فقط درصورتی که به افراد برای انجام وظایف خارج از دفتر خود ضروری باشد، اجازه دهید دارایی‌ها را از امکانات شما خارج کنند.

❖ **تعیین حضانت**

قبل از اینکه اجازه دهید دارایی از محل زندگی شما خارج شود، حق حضانت هر دارایی را به شخصی اختصاص دهید .و قبل از استفاده از تجهیزات، ملزم به امضا کردن تجهیزات برای افراد در نظر بگیرید.

❖ **افراد خود را مختصر و اقدامات امنیتی را اجرا کنید**

به افراد خود از مسئولیت‌هایشان در جهت حفاظت از دارایی‌هایی که به آنها سپرده شده است، مشاوره کنید .اطمینان حاصل کنید که آنها از اقدامات امنیتی شما و نحوه حمایت از آنها اطلاع دارند.

اطمینان حاصل کنید که افراد شما دارایی‌های از دست رفته یا آسیب دیده روش گزارش دهی حوادث شما را می‌دانند و آن را دنبال می‌کنند .با هرگونه اطلاعات موجود در دارایی‌های بد جا، گمشده یا مسروقه، به عنوان مصالحه رفتار کنید.

❖ **محافظت از دارایی در وسایل نقلیه**

به افراد خود بگویید دارایی را در وسایل نقلیه نگذارند، مگر اینکه اجتناب ناپذیر باشد یا اقدامات امنیتی جسمی برای محافظت از وسیله نقلیه و محتوای آن اعمال شود.

❖ **محافظت از دارایی‌ها در هتل‌ها**

به افراد خود یادآوری کنید که دارایی‌های باقیمانده در اتاق‌های هتل یا گاوصندوق‌های هتل به ویژه هنگام مسافرت به خارج از کشور در معرض خطر است .قبل از عزیمت افراد برای اقامت در هتل، از ارزیابی و درمان آنها اطمینان حاصل کنید.

❖ **محافظت از دارایی در هواپیما**

هنگام مسافرت، دارایی‌های موجود در چمدان از ایمن‌تر از چمدان‌های چک شده هستند، به شرطی که چمدان‌های دستی در کنترل کارمند باقی بماند.

برای اطلاعات بیشتر، به مناطق امنیتی بروید.

❖ **محافظت از دارایی‌ها در تأسیسات خصوصی**

حتی اگر فضای کاری اختصاصی به شما داده شود، ممکن است نتوانید امنیت دارایی‌های مستقر در محل مشتری را کنترل کنید .در این صورت، خطرات موجود در دارایی‌های خود را به روشی مشابه هر محیط کاری غیر امن خارج از سایت ارزیابی کنید.

اگر دارایی‌هایی دارید که برای تنظیم فعالیت‌های مشتری استفاده می‌شود، ممکن است این دارایی‌ها به حفاظت اضافی نیاز داشته باشند .به عنوان مثال، هنگامی که شما نیاز به محافظت از دارایی در برابر دستکاری یا اقدامات دیگری دارید که فعالیت‌های نظارتی شما را به خطر می‌اندازد.

۲-۱-۵۰- ترتیبات کار از راه دور از خانه

کار از راه دور از خانه منوط به توافق بین مدیریت و کارمند است. توجه داشته باشید که اگر افراد شما از مکانهایی استفاده می‌کنند که مورد تأیید قرار نگرفته‌اند یا ارزیابی ریسک داشته‌اند، باید با تنظیمات آنها به عنوان کار متحرک رفتار کنید.

❖ **دفتر خانه یا سایت کار را ارزیابی کنید**

توافق نامه‌ای برای کار از راه دور به طور معمول شما را ملزم به ارزیابی دفتر خانه یا محل کار می‌کند .شما باید مطابقت با هرگونه ایمنی و بهداشت شغلی و نیازهای منابع انسانی را که از طریق یک فرآیند خود ارزیابی برای سازمان شما اعمال می‌شود، ارزیابی کنید. اطلاعات صحیح را در یک توافق نامه بگنجانید

در یک توافق نامه، باید حداقل موارد زیر را وارد کنید:

- شرایط استخدام
- الزامات ایمنی و بهداشت شغلی
- الزامات امنیتی

این توافق نامه باید شامل فناوری و تجهیزات باشد .ایمنی و امنیت؛ و ارتباط و در دسترس بودن.

❖ **فناوری و تجهیزات**

مشخص کنید کدام فناوری برای دستیابی به اطلاعات از مکان از راه دور مناسب است.

- بررسی کنید که سازمان شما چه تجهیزاتی را فراهم می‌کند، کارگر از راه دور چه تجهیزات را فراهم می‌کند و چه چیزی به اشتراک گذاشته می‌شود (از جمله کنترل‌های خاص مربوط به استفاده از تجهیزات شخصی).
- اگر تجهیزات تهیه می‌کنید، برنامه‌ای از تجهیزات را درج کنید.
- در مورد خرابی یا خرابی تجهیزات، نحوه ارائه کمک فنی را توضیح دهید.

❖ **ایمنی و امنیت**

- ببینید آیا خصوصیات فیزیکی محل کار از راه دور با استانداردهای ایمنی و امنیتی مطابقت دارد یا خیر.
- اطمینان حاصل کنید که کارگران از راه دور اقدامات اضطراری شما را انجام می‌دهند.
- روش‌های خود را برای دفع اطلاعات رسمی به طور ایمن (در صورت وجود) درج کنید.

❖ **ارتباط و در دسترس بودن**

انتظارات خود را برای برقراری ارتباط و در دسترس بودن بیان کنید .به عنوان مثال، کارگران از راه دور باید از طریق تلفن یا ایمیل در یک زمان مشخص قابل تماس باشند. در صورت نیاز به تغییر توافق نامه، از فرایندهایی استفاده خواهید کرد. برای مشاوره در مورد موافقت نامه‌های کاری، به سایت Employment New Zealand بروید: توافق نامه‌های استخدام

❖ **اسناد پشتیبانی**

چک لیست برای کار با تلفن همراه و از راه دور.

۲-۱-۵۱- یافتن مشاوره بیشتر در مورد کار دور از دفتر

مشاوره‌های مرتبط در این سایت موجود است:

- امنیت اطلاعات
- امنیت فیزیکی
- امنیت کارکنان
- سیستم طبقه بندی امنیتی دولت نیوزیلند

مشاوره از موسسه ملی استاندارد و فناوری:(NIST)

- راهنمای مشارکت از راه دور ، دسترسی از راه دور و امنیت دستگاه خود(BYOD)
- همه نشریات

همچنین می‌توانید مرکز امنیت سایبری ملی را امتحان کنید

فصل ۳

امنیت فیزیکی

۳- امنیت فیزیکی

۳-۱- مقدمه

مدیریت خطرات امنیتی سازمان‌ها را قادر می‌سازد تا مردم، اطلاعات و دارایی‌ها را به‌طور مناسب محافظت نمایند برای مدیریت موفق این خطرات امنیتی (RISK MANAGEMENT) سازمان‌ها باید اطمینان حاصل نمایند که امنیت بخشی از فرهنگ‌سازمانی و برنامه‌های عملیاتی آن‌ها است.

هر سازمان دولتی در نیوزلند برای حفاظت از مردم، اطلاعات و دارایی‌ها باید تدابیر امنیتی فیزیکی را در نظر بگیرد. امنیت فیزیکی چندوجهی است و ترکیبی از استانداردهای ایمنی و امنیتی و بهداشت را پشتیبانی می‌کند.

۳-۲- چرا امنیت فیزیکی مهم است

امنیت فیزیکی یکی از اجزای اصلی سلامت و ایمنی شما است. امنیت فیزیکی اقدامات فیزیکی و رویه‌ای را باهم ترکیب می‌کند. این اقدامات برای جلوگیری یا کاهش تهدیدات مردم، اطلاعات و دارایی‌های شما طراحی‌شده است. اقدامات امنیتی فیزیکی مکمل اقدامات امنیتی شما در زمینه‌های دیگر مانند پرسنل، مدیریت اطلاعات، ارتباطات و ICT است.

۳-۱-۱- امنیت فیزیکی قوی به نفع همه است

داشتن امنیت فیزیکی قوی می‌تواند به شما کمک کند

- مردم، مشتریان و مردم خود را ایمن نگه‌دارید
- از دسترسی افراد غیرمجاز به محل، اطلاعات یا دارایی‌های شما جلوگیری کنید
- اعتماد و اطمینان مردم و سازمان‌هایی که به آن‌ها خدمت می‌کنید یا با آن‌ها کار می‌کنید را حفظ کنید
- ارائه خدمات بدون اختلال در صورت افزایش سطح تهدید با فاجعه
- تعهدات خود را تحت قانون ایمنی و بهداشت در محل کار ۲۰۱۵ انجام دهید

۳-۱-۲- تهدیدهای امنیتی فیزیکی چندوجهی است

تهدیدهای امینت فیزیکی می‌تواند از جانب افراد خود یا خارج از سازمان شما (به‌عنوان‌مثال بازدیدکنندگان، پیمانکاران، مردم، گروه‌های خارجی) باشد.

تهدیدها می‌تواند برای افرادی که در دفتر کار یا محل کار شما کار می‌کنند اعمال شود. تهدیدهای مختلف می‌تواند در مواقعی که افراد شما دور از دفتر کار می‌کنند وجود داشته باشد، به‌ویژه هنگامی‌که آن‌ها تنها کار می‌کنند.

تهدیدها عبارت‌اند از:

- جرم، ازجمله جرم شخصی و مالی
- خشونت در محل کار، مانند حمله، آزار و اذیت و حملات انتقام‌جویی، از طرف خودی‌ها و طرف‌های خارجی
- اغتشاشات مدنی، مانند اعتراضات و شورش‌ها
- بالای صنعتی، مانند انفجارها، آتش‌سوزی ساختمان‌ها و فروریزش های ساختاری
- اقدامات تروریستی، مانند بمب‌گذاری، اخاذی، حوادث «پودر سفید» و آدم‌ربایی
- خطرات دیگر مانند افراد آشفته و حوادث رانندگی

در سازمان شما نقص امنیت می‌تواند تصادفی باشد به‌عنوان‌مثال اگر افراد شما نسبت به خطر ایجادشده دم درب هشیار نباشند، ممکن است به افراد غیرمجاز، دسترسی به مناطق امن شمارا بدهند.

۳-۳- الزامات اجباری

الزامات اصلی امنیت فیزیکی که آژانس‌های دولتی موظف به دنبال آن هستند و سایر سازمان‌ها باید بهترین روش را در نظر بگیرند

۳-۱-۳- آنچه را که برای محافظت از آن نیاز دارید درک کنید

افراد، اطلاعات و دارایی‌هایی را که سازمان شما برای محافظت از آن‌ها نیاز دارد و مکان آن‌ها را شناسایی کنید. خطرات امنیتی (تهدیدها و آسیب‌پذیری‌ها) و تأثیر تجارت در ضرر و زیان مردم، اطلاعات یا دارایی‌ها را ارزیابی کنید. از درک خود استفاده کنید تا:

- از مردم خود در مقابل تهدید به خشونت محافظت کنید و در صورت بروز اتفاق مضر از آن‌ها حمایت کنید.
- از افراد عمومی که با سازمان شما تعامل دارند محافظت کنید.
- برای به حداقل رساندن یا از بین بردن خطرات موجود در دارایی‌های اطلاعاتی خود، اقدامات امنیتی فیزیکی در نظر بگیرید.

۳-۱-۴- امنیت فیزیکی خود را طراحی کنید

در اوایل مراحل برنامه‌ریزی، انتخاب، طراحی و اصلاح امکانات امنیتی فیزیکی را در نظر بگیرید. تدابیر امنیتی را طراحی کنید که خطرات سازمان شمارا تهدید می‌کند و بااشتهای شما سازگار است. اقدامات امنیتی شما باید مطابق با تعهدات مربوط به بهداشت و ایمنی باشد.

۳-۱-۵- اقدامات امنیتی خود را تائید کنید

تائید کنید که اقدامات امنیتی فیزیکی شما به‌درستی اجراشده و برای اهداف مناسب است. برای اطمینان از تائید فعالیت مناطق امنیتی، مراحل صدور گواهینامه و اعتبار سنجی را به اتمام برسانید.

۳-۱-۶- امنیت خود را به‌روز نگه‌دارید

اطمینان حاصل کنید که از تهدیدات و آسیب‌پذیری‌های در حال به‌روز بدون، مطلع هستید و به‌طور مناسب پاسخ می‌دهید. اطمینان حاصل کنید که اقدامات امنیت فیزیکی شما به‌طور مؤثر حفظ می‌شود تا برای اهداف مناسب باقی بماند.

۳-۴- پروتکل مدیریت برای امنیت فیزیکی

سازمان خود را با امنیت فیزیکی قوی حفظ کنید. خطرات افراد، اطلاعات و دارایی‌های سازمان خود را کاهش دهید. برای دستیابی به یک فرهنگ امنیتی قوی، اطمینان حاصل کنید که اقدامات امنیتی فیزیکی شما شناخته‌شده و دنبال می‌شود.

این پروتکل:

- مراحلی را که سازمان شما برای بهبود امنیت فیزیکی شما باید طی کند توضیح می‌دهد.
- چرخه مدیریت امنیت فیزیکی را تعریف می‌کند.
- الزامات اجباری برای سازمان‌های دولت نیوزلند را مشخص می‌کند.

اگر مدیر اجرایی، مدیر ارشد امنیت (CSO) مدیر ارشد امنیت اطلاعات (CISO) مدیر ارشد یا مدیر خط هستید، مطمئن شوید که:

- چرخه مدیریت را درک کنید

- الزامات اجباری را برآورده کنید

اگر شما یک سازمان بخش خصوصی هستید، پذیرش داوطلبانه الزامات اجباری امنیت فیزیکی شمارا بهبود می‌بخشد.

۳-۱-۷- امنیت فیزیکی چیست

امنیت فیزیکی یکی از اجزای اصلی رژیم بهداشت و ایمنی شماست. امنیت فیزیکی ترکیبی از اقدامات چسمی و رویه‌ای است که برای جلوگیری یا کاهش تهدیدات مردم، اطلاعات و دارایی شما طراحی‌شده است. اقدامات امنیت شما در زمینه‌های دیگر مانند پرسنل، مدیریت اطلاعات، ارتباطات و ICT است.

۳-۱-۸- امنیت فیزیکی قوی به نفع همه است

داشتن امنیت فیزیکی قوی می‌تواند به شما کمک کند

- مردم، مشتریان و مردم خود را ایمن نگه‌دارید.
- از دسترسی افراد غیرمجاز به محل، اطلاعات یا دارایی‌های شما جلوگیری کنید.
- اعتماد و اطمینان مردم و سازمان‌هایی که به آن‌ها خدمت می‌کنید یا با آن‌ها کار می‌کنید را حفظ کنید.
- ارائه خدمات بدون اختلال در صورت افزایش سطح تهدید با فاجعه
- تعهدات خود را تحت قانون ایمنی و بهداشت در محل کار ۲۰۱۵ انجام دهید.

۳-۱-۹- تهدیدها و خطرات لازم برای مدیریت را بدانید

تهدیدهای امنیتی فیزیکی می‌تواند از جانب افراد خود یا خارج از سازمان شما (به‌عنوان‌مثال بازدیدکنندگان، پیمانکاران، مردم، گروه‌های خارجی) باشد. تهدیدها می‌تواند برای افرادی که در دفتر کار یا محل کار شما کار می‌کنند اعمال شود. تهدیدهای مختلف می‌تواند در مواقعی که افراد شما دور از دفتر کار می‌کنند وجود داشته باشد، به‌ویژه هنگامی‌که آن‌ها تنها کار می‌کنند.

تهدیدها عبارت‌اند از:

- جرم، ازجمله جرم شخصی و مالی
- خشونت در محل کار، مانند حمله، آزار و اذیت و حملات انتقام‌جویی، از طرف خودی‌ها و طرف‌های خارجی
- اغتشاشات مدنی، مانند اعتراضات و شورش‌ها
- بالای صنعتی، مانند انفجارها، آتش‌سوزی ساختمان‌ها و فروریزش های ساختاری
- اقدامات تروریستی، مانند بمب‌گذاری، اخاذی، حوادث «پودر سفید» و آدم‌ربایی
- خطرات دیگر مانند افراد آشفته و حوادث رانندگی

در سازمان شما نقص امنیت می‌تواند تصادفی باشد به‌عنوان‌مثال اگر افراد شما نسبت به خطر ایجادشده دم درب هشیار نباشند، ممکن است به افراد غیرمجاز، دسترسی به مناطق امن شمارا بدهند.

۳-۱-۱۰- چرخه عمر امنیت فیزیکی را بفهمید

برای محافظت از افراد، اطلاعات و دارایی‌های سازمان خود چرخه حیات امنیت فیزیکی را بشناسید و دنبال کنید.

مراحل چرخه زندگی مراحلی را نشان می‌دهد که باید طی کنید تا درک کنید از چه چیزی باید محافظت کنید. خطرات افراد، اطلاعات و دارایی‌های خود را ارزیابی کنید. اقدامات امنیتی مناسب را طراحی کنید. تائید کنید که این اقدامات به‌درستی اجراشده است و آن‌ها را به‌مرور حفظ کنید.

۳-۱-۱۱- رویکرد مبتنی بر ریسک برای امنیت فیزیکی در پیش بگیرید

زمینه منحصربه‌فرد سازمان شما و تهدیدات احتمالی تعیین می‌کند که به کدام اقدامات امنیت فیزیکی نیاز دارید. وقتی رویکردی مبتنی بر ریسک را در پیش می‌گیرید، می‌توانید از اقدامات امنیتی فیزیکی مناسب برای سازمان خود اطمینان حاصل کنید.

شما باید افراد، اطلاعات، دارایی‌های فیزیکی و عملکردهای مورد محافظت را شناسایی کنید. سپس باید تهدیدهای سازمان خود را در نیوزلند و خارج از کشور تعیین کنید.

شما باید ارزش و حساسیت اطلاعات و دارایی خود را کاملاً بفهمید تا خطرات امنیت فیزیکی خود را دقیق ارزیابی کنید.

استفاده از سطوح تأثیر کسب‌وکار (Bils) به ارزیابی تأثیر بالقوه اگر مردم خود را، اطلاعات و یا دارایی‌ها، آسیب‌دیده‌اند به خطر بیافتد و یا در دسترسی نیست. مثلاً:

- اگر مشتریان نسبت به مردم شما تهاجمی بودند
- اگر اموال سازمان شما به سرقت رفته باشد
- اگر کسی در سیستم امنیتی شما دست‌کاری کرده و خارج از ساعت به دفتر شما دسترسی غیرمجاز پیداکرده است.

برای هر سناریوی تهدید، خطرات زیر را در نظر بگیرید:

- عموم
- افراد، دارایی، عملیات، اعتبار، امور مالی یا فرایندهای تجاری شما
- نیوزلند به‌عنوان یک کل

۵-۳- فرهنگ امنیتی ایجاد کنید

همه افراد در سازمان شما به فرهنگ امنیتی شما کمک می‌کنند. هیچ سرمایه‌گذاری در امنیت فیزیکی بدون فرهنگ امنیتی مناسب مؤثر نخواهد بود.

از افراد و شرکای خود اطمینان حاصل کنید:

- خطرات امنیتی را درک کنید.
- سیاست‌های امنیت فیزیکی خود را درک کنید
- رفتارهای امنیتی صحیح را اتخاذ کنید
- در مورد مسائل امنیتی یا حوادث صحبت کنید

برای کمک به ایجاد فرهنگ امنیتی قوی، ارتباطات، آموزش و پشتیبانی از آگاهی امنیتی را فراهم کنید و اطمینان حاصل کنید که سیاست‌های امنیت فیزیکی شما به افراد و همه افرادی که با آن‌ها کار می‌کنید، ابلاغ می‌شود.

باید مردم را تشویق کرد که تگرانی های نوظهور یا نزدیک به خطاها را گزارش دهند و به‌عنوان شهروندان شرکتی خوب شناخته شوند نه مشکل‌ساز

افسر ارشد امنیتی شما (CSO) مطابق باسیاست کلی محافظتی شما، مسئول امنیت فیزیکی سازمان شما است.

۳-۱-۱۲- امنیت فیزیکی خود را برنامه‌ریزی کنید

یک طرح امنیت فیزیکی برای سازمان خودتنظیم کنید که:

- با سطح خطر امنیتی در محیط فیزیکی شما مطابقت دارد
- با نیازهای تجاری و تعهدات قانونی شما سازگار است
- بر اساس چارچوب کلی و برنامه‌ریزی برای امنیت سازمان شما است
- تعهدات تحت قانون ایمنی بهداشت در محل کار ۲۰۱۵ را پوشش می‌دهد

برنامه‌ریزی مؤثر امنیت فیزیکی

- در مواردی که مجموعه‌ای از اطلاعات و دارایی‌های فیزیکی و غلظت بالاتر از افراد را در اختیاردارید، خطرات بیشتری را دربرمی گیرد.
- نیازهای خاص محل کار مختلف سازمان شمارا تأمین می‌کند
- شامل اقدامات مقیاس‌پذیر برای برآوردن سطح افزایش تهدیدات و انطباق تغییرات در سطح تهدید ملی است.
- شامل سیستمی از کنترل‌ها و موانع برای کمک به سازمان شما در جلوگیری، شناسایی، تأخیر و پاسخگویی به هرگونه تهدید خارجی یا داخلی است
- خطرات مرتبط با امکانات مشترک و الزامات امنیتی برای کار در خارج از دفتر را برطرف می‌کند.

۳-۶- الزامات اجباری امینت فیزیک را برآورده کنید

الزامات اجباری

۳-۱-۱۳- آنچه را که برای محافظت از آن نیاز دارید درک کنید

افراد، اطلاعات و دارایی‌هایی را که سازمان شما برای محافظت از آن‌ها نیاز دارد و مکان آن‌ها را شناسایی کنید. خطرات امنیتی (تهدیدها و آسیب‌پذیری‌ها) و تأثیر تجارت در ضرر و زیان مردم، اطلاعات یا دارایی‌ها را ارزیابی کنید. از درک خود استفاده کنید.

با پیروی از الزامات اجباری و مراحل مربوطه به چرخه زندگی فیزیکی که در زیر توضیح داده‌شده، سازمان خود را با امنیت فیزیکی قوی حفظ کنید.

۳-۱-۱۴- آنچه را که برای محافظت از آن نیاز دارید درک کنید

قبل از اینکه بتوانید اقدامات امنیتی فیزیکی مناسبی را اعمال کنید، باید درک کنید که برای محافظت از چه چیزی نیاز دارید. شاید لازم باشد از آن‌ها محافظت کنید

- افراد، اطلاعات و دارایی‌های شما
- مردم یا مشتریان
- منابع فرهنگی

۳-۱-۱۵- چگونه از امکانات شما استفاده خواهد شد

شما باید بفهمید که چگونه از امکانات شما استفاده می‌شود، چه کسی از آن‌ها استفاده می‌کند، چه کسی ممکن است از آن‌ها بازدید کند و چه چیزهایی در آن‌ها ذخیره می‌شود. به یاد داشته باشید که هرگونه اطلاعات طبقه‌بندی‌شده یا دارایی را که ذخیره می‌کنید و الزامات قانونی را که باید برآورده کنید، درج کنید.

۳-۱-۱۶- آیا افراد شما دور از دفتر کار می‌کنند

شرایطی را در نظر بگیری که افراد شما ممکن است هنگام کار در خارج از دفتر کار کنند.

آیا آن‌ها در خانه کار خواهند کرد؟ در مکان‌های دورافتاده؟ در ساختمان شخص دیگری؟ خارج از کشور؟

۳-۱-۱۷- آیا نیازهای بهداشتی و ایمنی را در نظر گرفته‌اید

طبق قانون ایمنی و بهداشت در محل کار ۲۰۱۵، سازمان باید:

- تمام اقدامات منطقی را برای به حداقل رساندن خطر صدمه به کارمندان، مشتریان و مردم انجام دهید
- اطمینان حاصل کنید که برنامه‌های امنیتی فیزیکی آن‌ها خطر آسیب رساندن به مشتریان و مردم را برطرف می‌کند.

۳-۱-۱۸- آیا سازمان شما در مکان‌یابی مشترک است

اگر در مکان‌یابی مشترک قرار دارید، با همکاری طرفین دیگر بتوانید درک مشترکی از مسائل مربوط به امنیت فیزیکی و الزامات امنیتی یکدیگر داشته باشد.

۳-۱-۱۹- خطرات امنیت فیزیکی خود را ارزیابی کنید

هنگامی‌که خطرات منحصربه‌فرد سازمان خود را ارزیابی می‌کنید، می‌توانید تعیین کنید که برای کاهش خطرات در حد قابل قبولی، به کدام اقدامات امنیتی جسمی نیاز دارید.

شما باید بدانید که در کجا آسیب‌پذیر هستید و چگونه سازمان شما تحت تأثیر نقض امنیت قرار می‌گیرد. در اینجا چند سؤال برای پاسخ دادن وجود دارد.

- در چه ساعاتی افراد وارد، عزیمت و کار در هر سایت می‌شوند؟
- چند نفر در هر سایت کار می‌کنند؟
- کدام اشخاص ثالث به امکانات شما دسترسی دارند؟
- خطرات مرتبط با مجموعه اطلاعات و دارایی‌های فیزیکی که در دست دارید؟
- خطرات مرتبط با غلظت بالاتر مردم در مناطق خاص چیست؟
- سازمان شما در هر سایت کدام فعالیت‌ها را انجام می‌دهد؟
- آیا تهدیداتی ناشی از فعالیت‌های شما وجود دارد؟

- چه تهدیدهایی از محل زندگی و همسایگان شما ناشی می‌شود؟

احتمال و تأثیر هر یک از ریسک‌ها را ارزیابی کنید تا به شما کمک کند درک کنید که در کجا باید اقدامات بیشتری انجام دهید. برای هر خطری که نمی‌توانید به‌طور دقیق ارزیابی کنید، با منابع خارجی مانند پلیس محلی یا سایر مقامات تماس بگیرید. اگر با سازمان‌های دیگر مکان‌یابی می‌کنید، خطرات امنیتی ترکیبی را در نظر بگیری و برای ارزیابی آن‌ها باهم کارکنید.

به یاد داشته باشید که:

- خطرات هر سایتی را که به‌طور جداگانه استفاده می‌کنید ارزیابی کنید، زیرا لازم است برنامه‌های امنیتی خاص سایت را تهیه کنید.
- خطرات امنیت فیزیکی را در فهرست (های) ثبت خطر سازمان خود بگنجانید.

۳-۷- امنیت فیزیکی خود را طراحی کنید

در اوایل مراحل برنامه‌ریزی، انتخاب، طراحی و اصلاح امکانات فیزیکی را در نظر بگیرید. تدابیر امنیتی را طراحی کنید که خطرات سازمان شمارا تهدید می‌کند و بااشتهای شما سازگار است. اقدامات امنیتی شما باید مطابق با تعهدات مربوط به بهداشت و ایمنی باشد.

۳-۱-۲۰- امنیت فیزیکی را در مراحل اولیه خود طراحی کنید

ازآنجاکه اقدامات امنیتی فیزیکی اگر بعداً انجام شود می‌تواند گران‌تر و کارآمدتر باشد، در اولین مراحل-ترجیحاً در مراحل طراحی و طراحی- شرایط امنیتی فیزیکی خود را در نظر بگیرید. هر زمان که هستید این استراتژی را اعمال کنید.

- برنامه‌ریزی سایت‌ها یا ساختمان‌های جدید
- انتخاب سایت‌های جدید
- برنامه‌ریزی تغییرات در ساختمان‌های موجود
- برای سایت‌ها یا ساختمان‌های پرخطر، ممکن است لازم باشد زودتر با سازمان‌های تخصصی مانند سرویس اطلاعات امنیتی نیوزلند (NZSIS) و اداره امنیت ارتباطات دولتی (GCSB) مشورت کنید.

۳-۱-۲۱- قبل از انتخاب سایت، خطرات امنیت فیزیکی را ارزیابی کنید

برای بررسی مناسب بودن سایت، عوامل زیر را ارزیابی کنید

- محله
- اندازه محیط ایستادن
- دسترسی به سایت و پارکینگ
- ایجاد نقاط دسترسی
- مناطق امنیتی

۳-۱-۲۲- برنامه‌های امنیتی سایت را تهیه کنید

برای کمک به شما از ارزیابی خطر خاص سایت خود استفاده کنید

- برنامه‌های امنیتی خاص سایت را تهیه کنید
- شامل الزامات امنیتی در سایر برنامه‌های توسعه سایت باشد

سازمان شما باید برای همه سایت‌های جدید، تأسیسات در دست‌ساخت و تسهیلاتی که تحت بازسازی اساسی قرار دارند، یک طرح امنیت سایت داشته باشد. این طرح باید با حداقل استانداردهای امنیتی سازمان شما برای انواع خاصی از امکانات موافقت کند.

برای هر طرح امنیتی سایت، اطمینان حاصل کنید که اقدامات امنیتی فیزیکی

- تأخیر کافی را فراهم کنید تا بتوانید پاسخ‌های برنامه‌ریزی‌شده را تحت تأثیر قرار دهید
- نیازهای تجاری را برآورده می‌کند
- سایر روش‌های عملیات را تکمیل و پشتیبانی می‌کند
- اقدامات لازم برای محافظت از حریم خصوصی دیداری و شنیداری را در بربگیرید
- بی‌دلیل با مردم دخالت نکنید.

۸-۳- از مناطق امنیتی برای بازتاب سطح تأثیرات تجاری استفاده کنید

تدابیر امنیتی اضافی برای مناطقی اعمال می‌شود که اطلاعات دارای مارک محافظتی و سایر منابع رسمی یا ارزشمند پردازش، اداره و ذخیره می‌شوند. به این مناطق «مناطق امنیتی» گفته می‌شود. مناطق بر اساس BIL ها ساخته‌شده‌اند و هر یک از آن‌ها دارای حداقل کنترل‌های امنیتی هستند که سازمان شما باید اجرا کند. اگر سازمان شما با افزایش سطح تهدید روبه‌رو است، از ارزیابی ریسک خود استفاده کنید تا اقدامات اضافی را در هر منطقه آسیب‌دیده انجام دهید. افزایش سطح تهدید می‌تواند به دلیل دخالت خارجی، خشونت باانگیزه سیاسی، فعالیت مجرمانه یا حملات سایبری باشد.

۳-۱-۲۳- منطقه ۱: منطقه دسترسی عمومی

این‌ها مناطق امن نیستند ازجمله ترتیبات کاری خارج از دفتر آن‌ها کنترل دسترسی محدودی به اطلاعات و دارایی‌های فیزیکی را فراهم می‌کنند، درصورتی‌که هرگونه خسارت منجر به تأثیر تجاری کم یا متوسط شود. آن‌ها همچنین محافظت محدودی را برای افراد فراهم می‌کنند.

نمونه‌هایی از مناطق دسترسی عمومی عبارت‌اند از:

- محوطه ساختمان و سرسرای عمومی
- مناطق مصاحبه و میزتحریر
- مناطق کار موقت خارج از دفتر که آژانس هیچ کنترلی بر دسترسی آن‌ها ندارد
- کارهای میدانی، ازجمله بیشتر کارهای مبتنی بر وسیله نقلیه
- قطعات دسترسی عمومی در امکانات چند ساختمان

۳-۱-۲۴- منطقه ۲: منطقه کاری

این مناطق دارای امنیت کم هستند که دارای برخی کنترل‌ها هستند. آن‌ها کنترل دسترسی به اطلاعات و دارایی‌های فیزیکی را فراهم می‌کنند، درصورتی‌که هرگونه ضرر درنتیجه تأثیر تجاری بسیار بالا باشد. آن‌ها همچنین برخی از محافظت از مردم را فراهم می‌کنند. این مناطق اجازه دسترسی نامحدود به افراد و پیمانکاران شمارا می‌دهد. دسترسی عمومی یا بازدیدکننده محدودشده است.

نمونه‌هایی از مناطق کاری عبارت‌اند از:

- محیط‌های عادی اداری
- محل کار معمولی خارج از دفتر یا خانه که در آن می‌توانید دسترسی به مناطق مورداستفاده برای مشاغل خود را کنترل کنید
- مناطق مصاحبه و میز جلو که افراد شما از مشتری و مردم جداشده‌اند
- پایگاه‌های نظامی و مناطق کاری در کنار فرودگاه با حصار امنیتی در اطراف محیط و ورودی‌های کنترل‌شده
- کار مبتنی بر وسیله نقلیه درجایی که وسیله نقلیه دارای یک ظرف امنیتی، زنگ هشدار و ایموبلایزر باشد

- مناطق نمایشگاه با کنترل امنیتی و دسترسی عمومی کنترل‌شده

۳-۱-۲۵- منطقه ۳: محدودیت کاری

این مناطق امنیتی با کنترل‌های امنیتی بالا هستند. آن‌ها کنترل دسترسی به اطلاعات و دارایی‌های فیزیکی را فراهم می‌کنند، درصورتی‌که ضرر و زیان منجر به تأثیر تجاری شود. آن‌ها همچنین از افراد محافظت می‌کنند. دسترسی افراد و پیمانکاران شما محدود به افرادی است که نیاز به دسترسی به منطقه دارند. افرادی که دسترسی مستمر دارند باید دارای یک مجوز امنیتی مناسب باشند. باید اسکورت شوند، یا از نزدیک کنترل شوند و برای دسترسی به منطقه نیاز تجاری داشته باشند.

نمونه‌هایی از مناطق ممنوع:

- مناطق امن در ساختمان شما که دارای کنترل دسترسی اضافی برای افراد شما هستند (مانند اتاق سرور IT)
- مناطق نمایشگاه با دارایی‌های بسیار ارزشمند
- مناطقی با اشیا (Items) باارزش بالا یا موارد فرهنگی که در معرض نمایش نیستند.

۳-۱-۲۶- منطقه ۴: منطقه امنیتی

این‌ها مناطق امنیتی با سطح امنیت بالاتری هستند. آن‌ها کنترل دسترسی به اطلاعاتی را که هرگونه خسارت منجر به تأثیر در تجارت تا حد شدید می‌شود فراهم می‌کنند و دارایی‌های فیزیکی که هرگونه خسارت منجر به تأثیر آن می‌شود تا فاجعه‌بار است. آن‌ها همچنین از افراد محافظت می‌کنند. دسترسی افراد شما با تائید شناسه و دسترسی به کارت کاملاً کنترل می‌شود. افرادی که دسترسی مستمر دارند باید دارای یک مجوز امنیتی مناسب باشند. بازدیدکنندگان و پیمانکاران باید از نزدیک کنترل شوند و برای دسترسی به منطقه نیاز تجاری دارند.

نمونه‌هایی از مناطق امنیتی عبارت‌اند از:

- مناطق امن در داخل ساختمان شما که دارای کنترل دسترسی اضافی برای افراد شما هستند.
- مناطق نمایشگاهی با دارایی‌های بسیار ارزشمند، با کنترل‌های محافظت از دارایی‌های خاص و دسترسی عمومی از نزدیک کنترل‌شده
- مناطقی که برای نگهداری اشیاء باارزش بالا یا موارد فرهنگی که در معرض نمایش نیستند استفاده می‌شود.

۳-۱-۲۷- منطقه ۵: منطقه با امنیت بالا

این مناطق امنیتی با بالاترین سطح کنترل امنیتی هستند. آن‌ها کنترل دسترسی به اطلاعات را فراهم می‌کنند درصورتی‌که هرگونه خسارت منجر به تأثیر تجاری تا فاجعه‌بار شود. دسترسی افراد شما با تائید شناسه دسترسی به کارت کاملاً کنترل می‌شود. افرادی که دسترسی مستمر دارند باید دارای یک مجوز امنیتی مناسب باشند. بازدیدکنندگان و پیمانکاران باید از نزدیک شوند و برای دسترسی به منطقه نیاز تجاری دارند.

نمونه‌هایی از مناطق با امنیت بالا عبارت‌اند از:

- مناطقی که اطلاعات محرمانه، حساس و محفوظ را ذخیره می‌کنند
- امکانات جامعه اطلاعاتی نیوزلند

۳-۹- روش خوبی را برای طراحی امنیت فیزیکی اعمال کنید

۳-۱-۲۸- امنیت توسط طراحی

اقدامات امنیت فیزیکی قادر به کاهش طیف وسیعی از خطرات است. بااین‌حال، با توجه به‌وقت و عزم کافی، یک فرد غیرمجاز می‌تواند تقریباً از هرگونه اقدام امنیتی فیزیکی استفاده کند.

۳-۱-۲۹- بازداشتن

افراد غیرمجاز را از تلاش برای دستیابی غیرمجاز به تأسیسات خود منصرف کنید. اقداماتی را که افراد غیرمجاز تصور می‌کنند بیش‌ازحد دشوار است و یا برای شکست دادن آن‌ها به ابزار و آموزش خاصی نیاز دارند، اجرا کنید.

۳-۱-۳۰- تشخیص

افراد غیرمجاز را در اسرع وقت تشخیص دهید. اقدامات لازم را برای بررسی اینکه آیا اقدامی غیرمجاز اتفاق افتاده یا رخ‌داده است، اجرا کنید.

۳-۱-۳۱- تأخیر انداختن

تلاش دسترسی غیرمجاز را تا زمانی که ممکن باشد به تأخیر بیاندازید تا اجازه دهید یک پاسخ امنیتی مؤثر فعال شود. اقداماتی را برای کند کردم پیشرفت یک رویداد مضر اجرا کنید.

۳-۱-۳۲- پاسخ دادن

یک پاسخ مؤثر در مدت‌زمان مناسب با اقدامات تأخیر، فعالیت پیش‌بینی‌شده یک شخص غیر مجار را خنثی می‌کند. اقداماتی را برای جلوگیری، مقاومت یا کاهش تأثیر حمله یا رویداد آماده کنید.

۳-۱-۳۳- بازیابی

اقدامات لازم برای بهبودی از یک حادثه امنیتی را انجام دهید. برنامه‌ریزی کنید تا به دنبال وقوع حادثه، به‌موقع عملیات را به حالت عادی نزدیک کنید.

۳-۱۰- امنیت در عمق «از چندین لایه امنیتی استفاده کنید»

یک مفهوم کلیدی در امنیت فیزیکی «امنیت در عمل» است. یک سیستم چندلایه که در آن اقدامات امنیتی برای حمایت و تکمیل یکدیگر ترکیب می‌شوند. با قرار دادن مناطق در داخل مناطق می‌توانید این مفهوم را اعمال کنید. این لایه‌بندی باعث افزایش کل زمان تأخیر و ایجاد موانع اضافی می‌شود. هر فرد غیرمجاز که بخواهد به مناطق بالاتر دسترسی پیدا کند، با افزایش سطح کنترل روبه‌رو می‌شود.

۳-۱۱- از محصول مورد تائید NZSIS استفاده کنید

سازمان‌های دولتی باید از موارد موجود در فهرست محصولات تائید شده NZSIS (APL) برای حفاظت از مردم، اطلاعات و دارایی‌ها استفاده کنند. اطلاعات موجود در این لیست طبقه‌بندی‌شده است. برای کسب اطلاعات بیشتر با تیم PSR تماس بگیرید.

۳-۱-۳۴- به تمام مناطقی که ممکن است امنیت فیزیکی شما نقض شود، رسیدگی کنید

تدابیر امنیتی خود را برای رفع خطرات و آسیب‌پذیری‌های مهم امنیت فیزیکی خود، ازجمله تهدیدات امنیت سایبری، فرهنگ امنیت فیزیکی و محصولات و فرآیندهای امنیتی، طراحی کنید.

۳-۱-۳۵- تمام قوانین و استانداردهای مربوطه را بدانید و از آن‌ها پیروی کنید

طراحی اقدامات امنیتی فیزیکی شما باید مطابق با قانون ایمنی و بهداشت در محل کار ۲۰۱۵، قانون حریم خصوصی ۱۹۹۳، قانون ساختمان ۲۰۰۴ و هرگونه مقررات مربوط باشد. این طرح باید مطابق با هر کنوانسیون بین‌المللی مربوطه باشد (به‌عنوان‌مثال، کنوانسیون سازمان ملل متحد علیه شکنجه و سایز رفتارها یا مجازات بی‌رحمانه، غیراساسی یا تحقیرآمیز) طرح شما همچنین باید با یادداشت‌های فنی NZSIS برای مناطق ۳ و ۴ یا ۵ منطقه) و کتابچه راهنمای امنیت اطلاعات نیوزلند (NZISM) مطابقت داشته باشد. شما همچنین باید بررسی کنید که آیا خطرات ایمنی می‌تواند ناشی از اقدامات امنیتی شما باشد یا خیر و سپس برنامه‌ای برای مدیریت این خطرات مطابق با قوانین مربوطه داشته باشید.

۳-۱-۳۶- برنامه‌های تداوم کسب‌وکار و بهبود شرایط را به مشاغل خود اضافه کنید.

الزامات امنیت فیزیکی که در مرحله شناسایی می‌کنید باید در برنامه‌های تداوم کسب‌وکار و بازیابی بلایای طبیعی نیز باشد، تا امنیت مداوم در صورت اختلال در کسب‌وکار را تضمین کنید.

۳-۱-۳۷- اعمال پیشگیری از جرم از طریق طراحی محیطی ((CPTED

از CPTED استفاده کنید تا مشخص کنید که کدام جنبه از محیط را به بخشی جدایی‌ناپذیر از برنامه‌ریزی تسهیلات خود تبدیل کنید.CPTED فیزیکی شما می‌تواند بر رفتار افراد تأثیر بگذارد و سپس محیط فیزیکی خود را برای به حداقل رساندن جرم طراحی کنید.

۳-۱-۳۸- برای ایمن‌سازی امکانات مشترک همکاری کنید

اگر سازمان شما محل اقامت را با سازمان‌های دیگر به اشتراک می‌گذارد، ارزیابی خطرات را انجام داده و اقدامات امنیتی فیزیکی را به‌طور مشترک برای رفع خطرات جمعی اعمال کنید. هنگام ارزیابی ریسک، خطرات ناشی از اجاره مشترک در هر مرکز مشترک را ارزیابی کنید.

۳-۱-۳۹- در نظر بگیرید که اقدامات امنیتی برای یک منطقه چگونه می‌تواند بر مناطق دیگر تأثیر بگذارد

هنگام تدوین تدابیر امنیتی فیزیکی، نمایه‌های تهدید مناطق درون سازمان خود را در نظر بگیرید. به‌عنوان‌مثال، آیا اقدامات امنیتی فیزیکی در یک منطقه بر امنیت یا عملیات مناطق دیگر تأثیر می‌گذارد؟

۳-۱-۴۰- خطرات امنیتی فیزیکی را برای افرادی که دور از دفتر کار می‌کنند ارزیابی کنید

وقتی سیاست‌ها و رویه‌هایی را برای افرادی که از راه دور کار می‌کنند تدوین می‌کنید، هرگونه افزایش خطرات امنیتی برای افراد، اطلاعات و دارایی‌های فیزیکی خود را در نظر بگیرید.

۳-۱-۴۱- طراحی امنیت فیزیکی خود را قبول کنید

قبل از اینکه بتوانید اقدامات امنیتی فیزیکی خود را اجرا کنید، رئیس ارشد امنیت (CSO) یا سایر افراد مجاز باید این طرح امنیتی را بپذیرند.

- برای هدف مناسب است

- نیازهای خاص سازمان شمارا برطرف خواهد کرد

قبل از اینکه برنامه امنیت فیزیکی خود را برای ورود به سیستم ارسال کنید، آیا همه خطرات و آسیب‌پذیری‌های خود را در مرحله ارزیابی خطر کاهش داده‌اید یا خیر

۳-۱-۴۲- اقدامات امنیتی فیزیکی خود را اجرا کنید

با تأمین‌کنندگان، مستاجرین و صاحب‌خانه خودکار کنید تا اطمینان حاصل کنید که آن‌ها شرایط امنیت شمارا برآورده می‌کنند. در قراردادها و مشارکت‌های خود امنیت فیزیکی خوبی ایجاد کنید. به یادداشته باشید که کلیه اقدامات یا نتایج مربوطه را که در برنامه‌های امنیت سایت شما مشخص‌شده است، در خلاصه‌های طراحی ساختمان، درخواست مناقصه و قراردادها ذکر کنید.

۳-۱-۴۳- روند برنامه‌ریزی و ساخت خود را مدیریت کنید

شما باید خطرات موجود در برنامه‌ریزی و چرخه عمر ساختمان را در نظر بگیرید. اطمینان حاصل کنید که اقدامات امنیتی فیزیکی شما هنگام ایجاد ساختمان جدید، بازسازی یا دارایی منتقل‌شده از یک محل کار یا منطقه به مکان دیگر، انجام می‌شود. فرایند اجرا را درست از زمان بازنشستگی یا نابودی دارایی‌ها و اطلاعات انجام دهید

۳-۱-۴۴- اقدامات امنیتی خود را تائید کنید

تائید کنید که اقدامات امنیتی فیزیکی شما به‌درستی اجراشده و برای اهداف مناسب است. برای اطمینان از تائید فعالیت مناطق امنیتی، مراحل صدور گواهینامه و اعتبار سنجی را به اتمام برسانید.

۳-۱-۴۵- اقدامات امنیتی فیزیکی خود را معتبر ارزیابی کنید

اعتبار سنجی اقدامات امنیتی فیزیکی سازمان شما به معنای فهمیدن اینکه آیا آن‌ها به‌درستی اجراشده‌اند یا مناسب اهداف هستند.

۳-۱-۴۶- اعتماد و پاسخگویی را از طریق اعتبار سنجی فراهم کنید

سازمان امور مالیاتی شما تصمیم می‌گیرید که آیا اقدامات برای خطرات سازمان شما مناسب است یا خیر. این خطرات ممکن است از سایتی به سایت دیگر متفاوت باشد. مرحله اعتبار سنجی به مدیران ارشد اطمینان می‌دهد که امینت فیزیکی به‌خوبی مدیریت می‌شود، خطرات به‌درستی شناسایی و کاهش می‌یابد و مسئولیت‌های حاکمیت برآورده می‌شود.

۳-۱-۴۷- اطمینان حاصل کنید که گواهی‌شده و معتبر هستید

مراحل صدور گواهینامه و اعتباربخشی موردنیاز برای نوع اقدامات امنیت فیزیکی را که انجام می‌شود، انجام دهید.

۳-۱-۴۸- اطمینان حاصل کنید که مناطق معتبر هستند

برای فضاهای فیزیکی، مراحل صدور گواهینامه و اعتبار سنجی موردنیاز منطقه امنیتی را دنبال کنید. علاوه بر حفظ امنیت سازمان، اعتباربخشی به سازمان‌هایی می‌دهد که با اطمینان در امنیت خودکار می‌کنند.

۳-۱-۴۹- برای اطلاعات دارای علامت محافظ، الزامات امنیتی را برآورده کنید

تدابیر امنیتی اضافی در مورد اطلاعات دارای محافظتی برای ایمن نگه‌داشتن این اطلاعات مهم و ارزشمند اعمال می‌شود. اطمینان حاصل کنید که با الزامات امنیتی فیزیکی اطلاعات و تجهیزات دارای محافظ مشخص‌شده در الزامات مناطق امنیتی ۳ تا ۵ آشنا هستید.

۳-۱-۵۰- امنیت خود را به‌روز نگه‌دارید

اطمینان حاصل کنید که از تهدیدات و آسیب‌پذیری‌های در حال به‌روز بودن مطلع هستید و به‌طور مناسب پاسخ می‌دهید. اطمینان حاصل کنید که اقدامات امنیتی جسمی شما به‌طور مؤثر (Maintained) حفظ می‌شود تا برای اهداف مناسب باقی بماند.

۳-۱۲- بهره‌برداری و نگهداری کنید

۳-۱-۵۱- اقدامات امنیتی فیزیکی خود را افزایش دهید

بخش مهمی از حفظ امنیت ارائه آموزش و پشتیبانی آگاهی از امنیت است. سیاست‌های امنیت فیزیکی خود را با افراد خود و با افرادی که سازمان شما با آن‌ها کار می‌کند ارتباط برقرار کنید. در صورت تغییر ترتیبات امنیتی فیزیکی به آن‌ها اطلاع دهید و در صورت امکان دلیل آن را بگویید باید مردم را تشویق کرد که نگرانی‌های نوظهور یا نزدیک به خطاها را گزارش دهند و به‌عنوان شهروندان شرکتی خوب شناخته شوند نه مشکل‌ساز.

۳-۱-۵۲- تهدیدات و آسیب‌پذیری‌های در حال تحویل را تحلیل کنید

ایمن نگه‌داشتن افراد، اطلاعات و دارایی‌های شما شامل فعالیت مداوم برای شناسایی و مدیریت تهدیدات و آسیب‌پذیری‌های تکامل‌یافته است.

برای مدریت آسیب‌پذیری‌های خود در امینت فیزیکی، اقدام زیر را انجام دهید

- سیستم‌ها، دارایی‌ها و افراد خود را کنترل کنید
- برای کشف وقایع مشکوک یا غیرمجاز، رویدادها و فرایندها را مشاهده کنید
- برای در امان ماندن از نقاط ضعف یا ضعف در لایه‌های امنیتی خود فعال باشید
- آسیب‌پذیری‌هایی را که فوری‌ترین خطر را برای سازمان شما ایجاد می‌کنند، تجزیه‌وتحلیل، اولویت‌بندی کنید و گزارش دهید
- برای اتمام، اصلاحات را اعمال و پیگیری کنید

۳-۱-۵۳- اقدامات امنیتی فیزیکی خود را به‌روز نگه‌دارید

برای مؤثر بودن، اقدامات امنیتی فیزیکی شما باید خطرات واقعی شمارا نشان دهد. به‌روز باشید و آماده شوید.

- به‌طور فعالانه سیستم‌های کنترل دسترسی کاربر خود را حفظ کنید (به‌عنوان‌مثال آزمایش هشدارهای فشار، بررسی باتری‌ها هر ۶ ماه)
- روش‌های خود را آزمایش کنید تا مطمئن شوید که برای هدف مناسب هستند.

۳-۱-۵۴- به حوادث امنیتی فیزیکی پاسخ دهید

شما باید حوادث امنیتی را به‌خوبی مدیریت کنید تا تأثیر آن‌ها را کاهش دهید. هدف این است که هم تأثیر هر حادثه‌ای کاهش یابد و هم سریع بهبود یابد.

پاسخ به حوادث امنیتی باید بخشی از برنامه امنیتی شما باشد.

۳-۱-۵۵- پاسخ دهید و بهبود یابید

وقتی حادثه‌ای اتفاق می‌افتد، مراحل پاسخگویی به حادثه را دنبال کنید. برای کاهش تأثیر سریع اقدام کنید و به سازمان خود کمک کنید تا در اسرع وقت بهبود یابد. همچنین ممکن است لازم باشد اعتمادبه‌نفس هرکسی را که تحت تأثیر یک حادثه قرارگرفته است بازگردانید.

۳-۱-۵۶- ضبط و ارزیابی

جزئیات مربوط به هر حادثه یا از دست رفتن را ضبط کنید و میزان سازش آسیب را ارزیابی کنید.

۳-۱-۵۷- برقراری ارتباط

اطمینان حاصل کنید که حوادث امنیتی را به‌طرف های آسیب‌دیده و هر مقام مربوطه منتقل می‌کنید. شاید لازم باشد به مردم هشدار دهید تا از آسیب بیشتر خودداری کنند یا گزارشی در مورد حادثه ارائه دهند.

۳-۱-۵۸- تحقیق کنید، در صورت لزوم اقدام کنید و بیاموزید

پس از یک حادثه امنیتی، باید تحقیق کنید. در صورت لزوم اقدامات بیشتری را انجام دهید. اطمینان حاصل کنید که سازمان شما از این حادثه درس می‌گیرد، بنابراین می‌توانید اقدامات امنیتی خود را بهبود ببخشید

۳-۱-۵۹- توانایی خود را ارزیابی کنید

از یک فرایند ارزیابی مبتنی بر شواهد سالانه برای اطمینان از مناسب بودن توانایی امنیتی سازمان خود استفاده کنید. در صورت درخواست، گزارش اطمینان را از طریق تیم محافظت از امنیت موردنیاز به دولت ارائه دهید. سیاست‌ها و برنامه‌های خود را هر ۲ سال یا در صورت لزوم تغییر درتهدید یا محیط کار، زودتر مرور کنید.

۳-۱-۶۰- اقدامات امنیتی فیزیکی خود را مرتباً مرور کنید

برای اطمینان از مناسب بودن اهداف امنیتی خود، مرتباً بررسی کنید. تغییراتی را در استفاده از امکانات، سازمان یا محیط تهدید خود شناسایی کنید. برای اطلاع از پیشرفت‌ها از این اطلاعات استفاده کنید.

۳-۱-۶۱- بررسی‌های دوره‌ای انجام دهید و از انطباق آن اطمینان حاصل کنید

اقدامات امنیتی فیزیکی خود را مرتباً کنترل، بررسی و ممیزی کنید. شما باید بدانید که

- سیاست‌های امنیتی فیزیکی شما دنبال می‌شود
- کنترل‌های امنیتی فیزیک شما طبق برنامه کار می‌کنند
- هرگونه تغییر یا پیشرفت لازم است

۳-۱-۶۲- تغییرات در محیط امنیتی خود را شناسایی کنید

آماده‌باشید که هر زمان محیط امنیتی شما تغییر می‌کند چرخه حیات امنیت فیزیکی خود را دوباره راه‌اندازی کنید. برای اطلاع از تغییرات و پیشرفت‌ها، این سؤالات را در نظر بگیرید

- آیا شما از اطلاعات و دارایی‌های خود به روش دیگری استفاده می‌کنید؟
- آیا از امکانات خود به روش دیگری استفاده می‌کنید؟

- آیا افراد شما به شیوه دیگری کار می‌کنند؟
- آیا در حال برنامه‌ریزی برای بهبود خدمات امنیتی داخلی یا خارجی هستید؟
- آیا تهدیدات امنیتی و آسیب‌پذیری‌های جدید را شناسایی کرده‌اید؟

۳-۱-۶۳- با خیال راحت بازنشسته شوید

هنگامی‌که دیگر به ساختمان، امکانات، اطلاعات یا دارایی شما نیازی نیست، اطمینان حاصل کنید که پیامدهای امنیتی را در مرحله غیرفعال سازی در نظر گرفته‌اید. برنامه‌ای برای از بین بردن، استفاده مجدد، یا دفع امکانات، اطلاعات یا دارایی‌های خود به‌طور ایمن داشته باشید. مثلاً:

- گاوصندوق‌ها یا کابینت‌های بایگانی حاوی اطلاعات طبقه‌بندی‌شده
- چاپگرها / دستگاه‌های چندمنظوره

۳-۱-۶۴- اطلاعات و تجهیزات دارای علامت محافظ را به‌درستی نابود کنید

برای از بین بردن اطلاعات و تجهیزات دارای علامت محافظ، باید تجهیزات تخریب مورد تائید NZSIS یا خدمات تخریب مورد تائید NZSIS استفاده کنید، به‌طوری‌که ضایعات قابل‌بازسازی یا استفاده نیستند.

۳-۱۳- امنیت فیزیکی

۳-۱-۶۵- رویکرد مبتنی بر ریسک را در پیش بگیرید

زمینه منحصربه‌فرد سازمان شما و تهدیدات احتمالی تعیین می‌کند که به کدام اقدامات امنیتی فیزیکی نیاز دارید.

وقتی رویکردی مبتنی بر ریسک را در پیش می‌گیرید، می‌توانید از اقدامات امنیتی فیزیکی مناسب برای سازمان خود اطمینان حاصل کنید.

۳-۱-۶۶- آنچه را که برای محافظت از آن نیاز دارید شناسایی کنید

افراد، اطلاعات، دارایی‌های فیزیکی و عملکردهایی را که برای محافظت از آن‌ها نیاز دارید شناسایی کنید. سپس تهدیدهای پیش روی سازمان خود را تعیین کنید. تهدیدها را در داخل نیوزلند و خارج از کشور بگنجانید (اگر منافع خارج از کشور دارید)

۳-۱-۶۷- تأثیر نقض امنیت را ارزیابی کنید

برای ارزیابی تأثیر احتمالی اگر افراد، اطلاعات یا دارایی‌های شما آسیب‌دیده، به خطر بیفتند یا در دسترس نباشند، از سطح تجارت (BIL) استفاده کنید. مثلاً:

- اگر مشتریان نسبت به مردم شما تهاجمی بودند
- اگر اموال سازمان شما به سرقت رفته باشد
- اگر کسی در سیستم امنیتی شما دست‌کاری کرده و خارج از ساعت به دفتر شما دسترسی غیرمجاز پیداکرده است.
- اگر شخصی دسترسی غیرمجاز به محل شما پیداکرده و اطلاعات ارزشمندی را به سرقت برد

برای هر سناریوی تهدید خطرات زیر را در نظر بگیرید:

- عموم
- افراد، دارایی، عملیات، اعتبار، امور مالی یا فرایندهای تجاری شما
- نیوزلند به‌عنوان یک کل

برای اطلاعات بیشتر

- استفاده از سطوح دسترسی تجاری
- مدیریت ریسک –دستورالعمل‌ها- ISO 31000:2018
- مدیریت ریسک – کتاب راهنما-HB 167:2006

۳-۱-۶۸- فرهنگ امنیتی ایجاد کنید

همه افراد در سازمان شما به فرهنگ امنیتی شما کمک می‌کنند. هیچ سرمایه‌گذاری در امنیت فیزیکی بدون فرهنگ امنیتی مناسب مؤثر نخواهد بود.

- از افراد و شرکای خود اطمینان حاصل کنید
- سیاست‌های امنیت فیزیکی خود را درک کنید
- رفتارهای امنیتی صحیح را اتخاذ کنید
- در مورد مسائل امنیتی یا حوادث صحبت کنید

برای کمک به ایجاد فرهنگ قوی، ارتباطات، آموزش و پشتیبانی از آگاهی امنیتی را فراهم کنید و اطمینان حاصل کنید که سیاست‌های امنیت فیزیکی شما به افراد و همه افرادی که با آن‌ها کار می‌کنید، ابلاغ می‌شود. باید مردم را تشویق کرد که نگرانی‌های نوظهور یا نزدیک به خطاها را گزارش کنند و به‌عنوان شهروندان شرکتی خوب شناخته شوند نه مشکل‌ساز افسر ارشد امنیت شما (CSO) مطابق باسیاست کلی محافظتی شما، مسئول امینت فیزیکی سازمان شما است. امنیتی فیزیکی خود را برنامه‌ریزی کنید

یک طرح امنیتی فیزیکی برای سازمان خودتنظیم کنید که:

- با سطح خطر امنیت در محیط فیزیکی شما مطابقت دارد
- با نیازهای تجاری و تعهدات قانونی شما ساز کار است
- بر اساس چارچوب کلی و برنامه‌ریزی برای امنیت سازمان شما است
- تعهدات شما تحت قانون ایمنی و بهداشت در محل کار ۲۰۱۵ را پوشش می‌دهد

۳-۱-۶۹- برنامه‌ریزی مؤثر فیزیکی

در مواردی که مجموعه‌ای از اطلاعات و دارایی‌های فیزیکی و غلطت بالاتر از افراد را در اختیاردارید، خطرات بیشتری را دربرمی گیرد نیازهای خاص محل کار متخلف سازمان شمارا تأمین می‌کند. شامل اقدامات مقیاس‌پذیر برای برآوردن سطح افزایش تهدید و انطباق تغییرات در سطح تهدید ملی است شامل سیستمی از کنترل‌ها و موانع برای کمک به سازمان شما در جلوگیری، شناسایی، تأخیر و پاسخگویی به هرگونه تهدید (خارجی یا داخلی) است خطرات مرتبط با امکانات مشترک و الزامات امنیتی برای کار در خارج از دفتر را برطرف می‌کند

۳-۱-۷۰- برنامه‌ریزی امنیت فیزیکی

امنیت فیزیکی خود را متناسب با نیازهای سازمان خودتنظیم کنید

یک طرح امنیتی فیزیکی برای سازمان خودتنظیم کنید که:

- با سطح خطر امنیتی در محیط فیزیکی شما مطابقت دارد
- با نیازهای تجاری و تعهدات قانونی شما سازگار است
- بر اساس چارچوب کلی و برنامه‌ریزی برای امنیت سازمان شما است
- تعهدات شما تحت قانون ایمنی و بهداشت در محل کار ۲۰۱۵ را پوشش می‌دهد

۳-۱-۷۱- چه مواردی را باید در یک برنامه مؤثر بگنجانید

برنامه‌ریزی مؤثر امنیت فیزیکی

- در مواردی که مجموعه‌ای از اطلاعات و دارایی‌های فیزیکی و غلظت بالاتر از افراد را در اختیاردارید، خطرات بیشتری را دربرمی گیرد
- نیازهای خاص محل کار مختلف سازمان شمارا تأمین می‌کند
- شامل اقدامات مقیاس‌پذیر برای برآوردن سطح افزایش تهدید و انطباق تغییرات در سطح ملی است
- شامل سیستمی از کنترل‌ها و موانع برای کمک به سازمان شما در جلوگیری، شناسایی، تأخیر و پاسخگویی به هرگونه تهدید (داخلی یا خارجی) است
- خطرات مرتبط با امکانات مشترک و الزامات امنیتی برای کار در خارج از دفتر را برطرف می‌کند

۳-۱۴- امنیت فیزیکی

برای محافظت از افراد، اطلاعات و دارایی‌های سازمان خود چرخه حیات امنیت فیزیکی را بشناسید و دنبال کنید.

- امنیت فیزیکی
- چرخه عمر امنیت فیزیکی را بفهمید

۳-۱-۷۲- چرخه عمر امنیت فیزیکی را بفهمید

با رعایت چرخه حیات امینت فیزیکی، امنیت بدنی قوی ایجاد و حفظ کنید.

۳-۱-۷۳- آنچه را که برای محافظت از آن نیاز دارید درک کنید

قبل از اینکه بتوانید اقدامات امنیت بدنی مناسبی را اعمال کنید، باید درک کنید که برای محافظت از چه چیزی نیاز دارید. به ارزش افراد، اطلاعت و دارایی‌های محیط خود فکر کنید.

۳-۱-۷۴- ارزیابی تهدید

۳-۱-۷۵- امنیت فیزیکی را در مراحل اولیه خود طراحی کنید

اقدامات امنیتی فیزیکی اگر بعداً انجام شود، می‌تواند گران‌تر و کم اثر باشد. بنابراین الزامات امنیت فیزیکی خود را در اولین مراحل – ترجیحاً در مراحل طراحی- در نظر بگیرید

۳-۱۵- برنامه‌ریزی سایت

اقدامات امنیتی خاص

۳-۱-۷۶- طراحی امنیت فیزیکی خود را قبول کنید

۳-۱-۷۷- اقدامات امنیتی فیزیکی خود را اجرا کنید

در طول این مرحله، شما اقدامات امنیتی فیزیکی موردتوافق را اجرا می‌کنید، ازجمله سیاست‌ها، فرایندها و اقدامات فنی

۳-۱-۷۸- اقدامات امنیتی فیزیکی خود را معتبر ارزیابی کنید

اعتبار سنجی اقدامات امنیتی فیزیک سازمان شما به معنای فهمیدن اینکه آیا آن‌ها به‌درستی اجراشده‌اند یا مناسب اهداف هستند.

۳-۱-۷۹- تائید و تائید اعتبار مناطق امنیتی

۳-۱-۸۰- برای ایمن ماندن کار و نگهداری کنید

مهم است که اقدامات امنیتی خود را به‌طور مناسب انجام دهید و حفظ کنید، بنابراین آن‌ها همچنان به محافظت شما نیاز دارند.

۳-۱-۸۱- اقدامات امنیتی فیزیکی خود را مرتباً مرور کنید

برای اطمینان از مناسب بودن اهداف امنیتی خود، مرتباً بررسی کنید. تغییراتی را در استفاده از امکانات، سازمان یا محیط تهدید خود شناسایی کنید.

۳-۱-۸۲- اطلاعات و دارایی‌ها را به‌طور ایمن بازنشسته کنید

هنگامی‌که دیگر به ساختمان، امکانات، اطلاعات یا دارایی شما نیازی نیست، اطمینان حاصل کنید که پیامدهای امنیتی را در مرحله غیرفعالی سازی در نظر گرفته‌اید. برنامه‌ای برای از بین بردن، استفاده مجدد یا دفع امکانات، اطلاعات یا دارایی‌های خود به‌طور ایمن داشته باشید.

۳-۱-۸۳- آنچه را که برای محافظت از آن نیاز دارید درک کنید

قبل از اینکه بتوانید اقدامات امنیتی فیزیکی مناسبی را اعمال کنید، باید درک کنید که برای محافظت از چه چیزی نیاز دارید.

شاید لازم باشد از آن‌ها محافظت کنید:

- افراد، اطلاعات و دارایی‌های شما
- مردم و مشتریان
- منابع فرهنگی

۳-۱-۸۴- آنچه را که برای محافظت از آن نیاز دارید درک کنید

افراد، اطلاعات و دارایی‌هایی را که سازمان شما برای محافظت از آن‌ها نیاز دارد و مکان آن‌ها را شناسایی کنید. خطرات امنیتی (تهدیدها و آسیب‌پذیری‌ها) و تأثیر تجارت در ضرر و زیان مردم، اطلاعات یا دارایی‌ها را ارزیابی کنید. از درک خود استفاده کنید

۳-۱-۸۵- چگونه از امکانات شما استفاده خواهد شد

شما باید بفهمید که چگونه از امکانات شما استفاده می‌شود، چه کسی از آن‌ها استفاده می‌کند، چه کسی ممکن است از آن‌ها بازدید کند و چه چیزهایی در آن‌ها ذخیره می‌شود.

به یاد داشته باشید که هرگونه اطلاعات طبقه‌بندی‌شده یا دارایی را که ذخیره می‌کنید و الزامات قانونی را که باید برآورده کنید، درج کنید.

۳-۱-۸۶- آیا افراد شما دور از دفتر کار می‌کنند؟

شرایطی را در نظر بگیرید که افراد شما ممکن است هنگام کار در خارج از دفتر کار کنند.

آیا آن‌ها در خانه کار خواهند کرد؟ در مکان‌های از راه دور؟ در ساختمان شخص دیگری؟ خارج از کشور؟

۳-۱-۸۷- آیا نیازهای بهداشتی و ایمنی را در نظر گرفته‌اید؟

طبق قانون ایمنی و بهداشت در محل کار ۲۰۱۵، سازمان‌ها باید:

- تمام اقدامات منطقی را برای به حداقل رساندن خطر صدمه به کارمندان، مشتریان و مردم انجام دهید.
- اطمینان حاصل کنید که برنامه‌های امنیتی فیزیکی آن‌ها خطر آسیب رساندن به مشتریان و مردم را برطرف می‌کند.

۳-۱-۸۸- آیا سازمان شما در مکان‌یابی مشترک است؟

اگر در مکان‌یابی مشترک قرار دارید، با همکاری طرفین دیگر بتوانید درک مشترکی از مسائل مربوط به امنیت فیزیکی و الزامات امنیتی یکدیگر داشته باشد.

۳-۱-۸۹- امنیت فیزیکی خود را ارزیابی کنید

هنگامی‌که خطرات منحصربه‌فرد سازمان خود را ارزیابی می‌کنید، می‌توانید تعیین کنید که برای کاهش خطرات به میزان قابل قبولی، به کدام اقدامات امنیتی جسمی نیاز دارید.

۳-۱-۹۰- آنچه را که برای محافظت از آن نیاز دارید درک کنید

افراد، اطلاعات و دارایی‌هایی را که سازمان شما برای محافظت از آن‌ها نیاز دارد و مکان آن‌ها را شناسایی کنید. خطرات امنیتی (تهدیدها و آسیب‌پذیری‌ها) و تأثیر تجارت در ضرر و زیان مردم، اطلاعات یا دارایی‌ها را ارزیابی کنید. از درک خود استفاده کنید

۳-۱-۹۱- آسیب‌پذیری‌های خود را بشناسید

شما باید بدانید در کجا آسیب‌پذیر هستید و چگونه سازمان شما تحت تأثیر نقض امنیت قرار می‌گیرد

در اینجا چند سؤال مهم برای پاسخ دادن وجود دارد:

- ساعات کار افراد در هر سایت چیست؟ چه موقع آن‌ها وارد می‌شوند و می‌روند؟
- چند نفر در هر سایت کار می‌کنند؟
- کدام اشخاص ثالث به امکانات شما دسترسی دارند؟
- خطرات مرتبط با مجموعه اطلاعات و دارایی‌های فیزیکی که در دست دارید چیست؟
- خطارت مرتبط با غلظت بالاتر مردم در مناطق چیست؟
- سازمان شما در هر سایت کدام فعالیت‌ها را انجام می‌دهد؟
- آیا تهدیداتی ناشی از فعالیت‌های شما وجود دارد؟
- چه تهدیدهایی از محل زندگی و همسایگان شما ناشی می‌شود؟

احتمال و تأثیر هر یک از ریسک‌ها را ارزیابی کنید تا به شما کمک کند درک کنید که درکجا باید اقدامات بیشتری انجام دهید. برای هر خطری که نمی‌توانید به‌طور دقیق ارزیابی کنید، با منابع خارجی مانند پلیس محلی یا سایر مقامات تماس بگیرید.

اطلاعات بیشتر:

- ارزیابی تهدید

۳-۱۶- امنیت فیزیکی را در نقشه سایت‌ها و ساختمان‌ها ایجاد کنید

برای اطمینان از مقرون‌به‌صرفه بودن و مقاوم بودن، امنیت فیزیکی را در مراحل مفهوم در نظر بگیرید. هر زمان که هستید این استراتژی را اعمال کنید:

- برنامه‌ریزی سایت‌ها یا ساختمان‌های جدید

- انتخاب سایت‌های جدید
- برنامه‌ریزی تغییرات در ساختمان‌های موجود

برای سایت‌ها یا ساختمان‌های پرخطر، ممکن است لازم باشد زودتر با سازمان‌های تخصصی مانند سرویس اطلاعات امنیتی نیوزلند (NZSIS) و اداره امنیت ارتباطات دولتی (GCSB) مشورت کنید.

۳-۱-۹۲- قبل از انتخاب سایت، خطرات امنیت فیزیکی را ارزیابی کنید

برای بررسی مناسب بودم سایت، عوامل زیر را ارزیابی کنید:

- محله
- اندازه محیط ایستادن
- دسترسی به سایت و پارکینگ
- ایجاد نقاط دسترسی
- مناطق امنیتی

۳-۱-۹۳- خطرات موجود در افراد را شناسایی کنید

طبق قانون ایمنی و بهداشت در محل کار ۲۰۱۵، سازمان‌ها باید:

- تمام اقدامات احتیاطی قابل‌قبول عملی را انجام دهید تا خطر آسیب به کارمندان، مشتریان و مردم به حداقل برسد.
- اطمینان حاصل کنید که برنامه‌های امنیتی فیزیکی آن‌ها خطر آسیب رساندن به مشتریان و مردم را برطرف می‌کند.

برای انطباق با این قانون، خطرات مربوط به مردم را که می‌تواند ناشی از اقدامات شما برای حفاظت از اطلاعات و دارایی‌های فیزیکی باشد، متوجه افراد شوید. برای هرگونه خطری که شناسایی می‌کنید، تدابیری در نظر بگیرید که آن‌ها را تا حد قابل قبولی کاهش دهید.

۳-۱-۹۴- از مشتریان و مردم در برابر آسیب محافظت کنید

طبق قانون ایمنی و بهداشت در محل کار ۲۰۱۵ سازمان‌ها باید:

- از مشتریان و مدرم در برابر آسیب‌های ناشی از فعالیت‌های آن‌ها محافظت کنید
- اقدامات منطقی عملی را برای محافظت از همه افراد در محل زندگی آن‌ها و در نزدیکی محل آن‌ها انجام دهید.

بعضی‌اوقات اقدامات امنیتی که شما برای محافظت از مردم خود استفاده می‌کنید ممکن است از مشتریان و مردم نیز محافظت کند. اگر شما یک مدیرمسئول ایمنی و واکنش‌های اضطراری هستید، برای اطمینان از اینکه اقدامات ایمنی را طراحی می‌کنید که نیازهای امنیتی سازمان شمارا تکمیل می‌کنند، از کارمندان امنیتی خود مشاوره بگیرید.

۳-۱-۹۵- خطرات موجود در منابع فرهنگی را شناسایی کنید

اگر سازمان شما ازنظر فرهنگی دارای دارایی قابل‌توجهی است، ممکن است مجبور باشید با خطرات امنیتی که برای سایر سازمان‌ها وجود ندارد مقابله کنید. علاوه بر انجام ارزیابی ریسک، با سازمان‌های دولتی و غیردولتی مشابه تماس بگیرید تا بررسی کنید آیا طیف وسیعی از خطرات و کنترل‌ها را در نظر گرفته‌اید یا خیر.

۳-۱-۹۶- ارزیابی خطرات ناشی از همکاری مشترک با سازمان‌های دیگر

اگر در مکان‌یابی یا اجاره مشترک با سازمان‌های دیگر هستید، خطرات امنیتی ترکیبی را در نظر بگیرید و برای ارزیابی آن‌ها باهم کارکنید. سپس اقدامات امنیتی حفاظتی را به‌طور مشترک برای رفع خطرات جمعی اعمال کنید. به یاد داشته باشید که خطرات سازمان را نیز در نظر داشته باشید.

۳-۱-۹۷- از برنامه‌های امنیتی سازمان خود استفاده کنید

از ارزیابی ریسک امنیت فیزیکی خود برای آگاهی از مؤلفه‌های امنیت فیزیکی برنامه امنیت کلی سازمان خود استفاده کنید.

به یاد داشته باشید:

- خطرات هر ساختمان را که به‌طور جداگانه استفاده می‌کنید ارزیابی کنید، زیرا لازم است برنامه‌های امنیتی خاص ساختمان را تهیه کنید.
- مشخصات تهدیدهای مختلف واحدهای تجاری جداگانه در سازمان خود را در نظر بگیرید
- خطرات امنیتی فیزیکی را در فهرست‌های ثبت خطر سازمان خود بگنجانید.
- مدیریت ریسک امنیتی HB 167:2006

۳-۱-۹۸- انتخاب ساختمان

خطرات امنیت فیزیکی خود را در طی مراحل انتخاب ساختمان ارزیابی کنید

در اوایل مراحل انتخاب سایت، مدیر ارشد امنیتی خود و سایر افراد امنیتی را درگیرد کنید. شما باید اطمینان حاصل کنید که یک سایت بالقوه می‌تواند نیازهای امنیت سازمان شمارا برآورده کند.

۳-۱-۹۹- ساختمان را ارزیابی کنید

عوامل امنیتی فیزیکی زیر را ارزیابی کنید تا در صورت مناسب بودن ساختمان بررسی کنید

۳-۱-۱۰۰- آیا محله خطری دارد؟

نمونه‌هایی از مسائل مربوط به همسایگی که ممکن است تصمیم شما برای استفاده از یک ساختمان را تحت تأثیر قرار دهد.

- سطح و نوع فعالیت مجرمانه در منطقه
- تأثیر خطرات به همسایگان (یا سازمان‌ها، مشاغل و ساکنان)
- تأثیر از دید بیش‌ازحد عملیات سازمان شما

۳-۱-۱۰۱- آیا فضای کافی برای فضای ایستادن وجود دارد؟

برای محافظت از ساختمان در برابر تهدیدات، ممکن است به یک‌فاصله ایستا مشخص نیاز داشته باشید. در بعضی از محیط‌های شهری دستیابی به فاصله ایستا مؤثر می‌تواند دشوار باشد.

به یاد داشته باشید که هرگونه تهدیدی که عابر پیاده و وسایل نقلیه ایجاد می‌کنند را در نظر بگیرید

۳-۱-۱۰۲- آیا ساختمان نیازهای دسترسی و پارکینگ شمارا برآورده می‌کند؟

دسترسی را از طریق فضای ایستاده و تأسیسات بررسی و ارزیابی کنید.

- دسترسی برای تردد عابر پیاده، وسایل حمل‌ونقل اتومبیل چگونه است؟
- آیا سایت به‌راحتی مشاغل عادی را در خود جای‌داده است؟
- چگونه پارکینگ را در محیط کنترل و کنترل می‌کنید؟

۳-۱-۱۰۳- آیا می‌توانید تمام نقاط دسترسی را ایمن کنید؟

اطمینان حاصل کنید که تمام نقاط دسترسی ساختمان می‌توانند ایمن باشند، ازجمله:

- ورودی‌ها
- خارج می‌شود
- ورودی و خروجی هوا
- مجاری سرویس

۳-۱-۱۰۴- آیا ساختمان مناطق امنیتی شمارا در خود جای‌داده است؟

آیا ساختمان می‌تواند مناطق امنیتی موردنیاز شما (مناطقی را که در ارزیابی ریسک خود شناسایی کرده‌اید) فراهم کند؟

آیا می‌توانید امنیت را به‌صورت عمیق در سایت پیاده‌سازی کنید؟

۳-۱-۱۰۵- آیا ساختمان در معرض خطری طبیعی است؟

در مورد خطرات ناشی از بلایای طبیعی در منطقه و راهکارهای تخفیف برای استفاده از آن‌ها، به مشاوره تخصصی بپردازید. برای اطلاع از خطرات طبیعی یک سایت، با مقام محلی خود تماس بگیرید.

اگر سازمان شما ساختمانی را انتخاب می‌کند که در معرض خطر یک بلایای طبیعی است، محصولات امنیتی را انتخاب کنید که از خطرات مربوط به امنیت فیزیکی محافظت کند.

۳-۱۷- ارزیابی تهدید

تهدیدهای امنیتی فیزیکی خود را ارزیابی کنید تا بتوانید کنترل‌های صحیح را در اختیار داشته باشید.

تهدیدات ممکن است کل سازمان شما را تحت تأثیر قرار دهد یا مختص یک ساختمان یا منطقه باشد. تهدیدهای خاص می‌تواند برای افراد، مشتریان و مردم شما اعمال شود. به یاد داشته باشید که تهدیدهای موجود در مورد دارایی‌های فردی را نیز ارزیابی کنید.

از ارزیابی تهدیدات خود برای آگاهی از ارزیابی کلی خطر سازمان خود استفاده کنید.

۳-۱-۱۰۶- در صورت نیاز با کارشناسان تماس بگیرید

در صورت عدم تخصص صحیح برای ارزیابی تهدید، با منابع خارجی مانند پلیس محلی و سایر مقامات تماس بگیرید تا به شما کمک کنند.

اگر برای تکمیل ارزیابی تهدید خود به اطلاعات سرویس اطلاعات امنیتی نیوزلند (NZSIS) نیاز دارید، با مدیر تعامل PSR تماس بگیرید.

۳-۱-۱۰۷- ارزیابی کنید که ممکن است امکانات شما به محافظت بیشتری نیاز داشته باشد

برخی تهدیدها برای تأسیسات احتمال آسیب رساندن به مردم، اطلاعات یا دارایی‌های فیزیکی را افزایش می‌دهد. برای کاهش این تهدیدات باید کنترل‌های اضافی یا بالاتر را در نظر بگیرید. در اینجا چند سال آورده شده است تا شما را در موقعیت‌هایی که ممکن است سازمان شما نیاز به محافظت بیشتر از امکانات داشته باشد، به فکر بیاندازید.

- مردم چقدر می‌دانند که از امکانات شما برای چه کاری استفاده می‌شود؟ آیا برنامه‌های بحث برانگیزی در امکانات شما اجرا می‌شود؟
- آیا سطح بالایی از جرم و جنایت در محله وجود دارد؟
- آیا افراد شما در معرض خشونت از جانب مشتریان قرار دارند؟
- آیا امکانات شما در معرض خشونت عمومی ناشی از اعتراضات است؟

- آیا تروریسم تهدید احتمالی است؟
- آیا امکانات مشترکی دارید؟ به عنوان مثال می‌توان به امکانات یکبار مصرف، اجاره مشترک با مستاجرهای پرخطر خصوصی و مناطق کاری در سازمان خود با برنامه‌های متنوع اشاره کرد.
- اطلاعات و دارایی‌های فیزیکی امکانات شما چقدر ارزش دارد؟ آیا آنها برای گروههای امنیتی از جمله سرویسهای اطلاعاتی خارجی، گروه‌های دارای انگیزه و افراد معتمد جذاب خواهند بود؟
- اطلاعات بیشتر در مورد مدیریت خطرات:
- بخش ۴ HB 167: 2006 مدیریت ریسک امنیتی

۱۸-۳- امنیت فیزیکی

اقدامات امنیتی بدنی اگر بعداً انجام شود، می‌تواند گران‌تر و کم اثر باشد. بنابراین الزامات امنیتی فیزیکی خود را در اولین مراحل - ترجیحاً در مراحل طراحی و طراحی - در نظر بگیرید.

❖ **امنیت فیزیکی**

- چرخه عمر امنیت فیزیکی را بفهمید
- امنیت فیزیکی را در مراحل اولیه خود طراحی کنید

۳-۱-۱۰۸- امنیت فیزیکی را در مراحل اولیه خود طراحی کنید

۳-۱-۱۰۹- امنیت فیزیکی خود را طراحی کنید

در اوایل مراحل برنامه ریزی، انتخاب، طراحی و اصلاح امکانات امنیتی فیزیکی را در نظر بگیرید. تدابیر امنیتی را طراحی کنید که خطرات سازمان شما را تهدید می‌کند و با نیازهای شما سازگار است. اقدامات امنیتی شما باید مطابق با تعهدات مربوط به بهداشت و ایمنی باشد.

۳-۱-۱۱۰- برنامه ریزی ساختمان

سازمان‌ها باید ارزیابی کنند که آیا محیط امنیتی فیزیکی به عنوان بخشی از ارزیابی منظم ریسک امنیتی آنها قابل قبول است یا خیر. برای کمک به شما از ارزیابی خطر خاص ساختمان خود استفاده کنید: تهیه برنامه‌های امنیتی خاص ساختمان شامل الزامات امنیتی در سایر برنامه‌های توسعه ساختمان است.

۳-۱-۱۱۱- اعمال خوب را اعمال کنید

روش‌های خوبی که باید هنگام طراحی امنیت فیزیکی خود دنبال کنید.

- بازدارنده، ردیابی، تأخیر، پاسخ، بازیابی
- پیشگیری از جرم از طریق طراحی محیطی
- مناطق امنیتی
- امنیت در عمق
- حفاظت فیزیکی از اطلاعات
- قوانین و استانداردهای مربوطه

۳-۱-۱۱۲- اقدامات امنیتی خاص

- راهنمای توصیف استفاده از اقدامات امنیتی خاص.
- استفاده از محصولات مورد تأیید NZSIS

- کنترل‌های دسترسی محیطی
- ساخت و ساز ساختمان
- سیستم‌های هشدار
- گزینه‌های هشدار فردی
- سیستم‌های کنترل دسترسی
- قابلیت همکاری سیستم دزدگیر و سایر سیستم‌های مدیریت ساختمان
- قفل‌ها، سیستم‌های کلیدی و درها
- تلویزیون مداربسته
- روشنایی امنیتی
- ظروف و کابینت‌های امنیتی
- اتاق‌ها، گاوصندوق‌ها و اتاق‌های نگهداری ایمن
- کنترل بازدید کننده
- پذیرندگان و نگهبانان
- سایر اقدامات امنیتی جسمی

۳-۱-۱۱۳- طراحی امنیت فیزیکی خود را قبول کنید

قبل از اینکه بتوانید اقدامات امنیتی جسمی خود را اجرا کنید، افسر ارشد امنیتی (CSO) یا سایر افراد مجاز باید طرح امنیتی پیشنهادی را بپذیرند.

۳-۱-۱۱۴- برنامه ریزی ساختمان

سازمان‌ها باید ارزیابی کنند که آیا محیط امنیتی فیزیکی به عنوان بخشی از ارزیابی منظم ریسک امنیتی آنها قابل قبول است یا خیر.

برای کمک به شما از ارزیابی خطر خاص ساختمان خود استفاده کنید:

- برنامه‌های امنیتی خاص ساختمان را تهیه کنید
- شامل الزامات امنیتی در سایر برنامه‌های توسعه ساختمان باشد

۳-۱-۱۱۵- در اوایل مراحل برنامه ریزی با کارشناسان امنیتی مشورت کنید

از آنجا که اقدامات امنیتی فیزیکی در صورت ارائه در مرحله بعد ممکن است هزینه و هزینه کمتری داشته باشند، در اولین مراحل برنامه ریزی ساختمانها یا ساختمانهای جدید، یا تغییر در ساختمانهای موجود، الزامات امنیتی خود را با مشورت با مدیر ارشد امنیتی (CSO) ارزیابی کنید. برای ساختمانها یا ساختمانهای پر خطر، زود با آژانسهای مربوطه مانند سرویس اطلاعات امنیتی نیوزیلند (NZSIS)، اداره امنیت ارتباطات دولتی (GCSB) یا سایر آژانس‌های تخصصی مشورت کنید.

۳-۱-۱۱۶- برنامه‌های امنیتی ساختمان ایجاد کنید

تدابیر امنیتی را برای ساختمانها و ساختمانهای جدید در اسرع وقت، ترجیحاً در مراحل طراحی و طراحی در نظر بگیرید. یک طرح امنیتی ساختمان اقدامات مقابله‌ای را برای مقابله با خطرات شناسایی شده برای عملکرد و منابع سازمان شما در ساختمان ثبت می‌کند.

سازمان شما باید برنامه‌های امنیتی ساختمان را برای موارد زیر آماده کند:

- ساختمان‌های جدید

- ساختمان‌های greenfield
- امکانات در دست ساخت
- امکانات تحت بازسازی اساسی.

برای هر طرح امنیتی ساختمان، باید اطمینان حاصل کنید که اقدامات امنیتی فیزیکی شما:

- تأخیر کافی را فراهم کنید تا بتوانید پاسخهای برنامه ریزی شده را تحت تأثیر قرار دهید
- نیازهای تجاری را برآورده می‌کند
- سایر روشهای عملیاتی را تکمیل و پشتیبانی می‌کند
- اقدامات لازم برای محافظت از حریم خصوصی دیداری و شنیداری را در بر بگیرید
- بی دلیل با مردم دخالت نکنید.

به یاد داشته باشید که در مورد وظایف مختلف سازمان شما در یک مرکز قرار دارد، بنابراین می‌توان این مکان‌ها را برای محافظت مناسب ایجاد کرد.

۳-۱-۱۱۷- چه مواردی را باید در برنامه امنیتی ساختمان بگنجانید

در برنامه خود، پاسخ سؤالات گروههای زیر را مستند کنید.

۳-۱-۱۱۸- مکان و مالکیت

- مکان و ماهیت ساختمان چگونه است؟
- آیا سازمان شما دارای مالکیت منفرد یا مشترک، یا اجاره ساختمان است؟

۳-۱-۱۱۹- مردم

- افراد شما در چه ساعاتی در ساختمان کار خواهند کرد؟
- چه کسی از این ساختمان بازدید خواهد کرد (به عنوان مثال، مردم، ارائه دهندگان خدمات)؟
- در چه ساعاتی برای عموم یا سایر بازدیدکنندگان باز هستید؟

۳-۱-۱۲۰- اطلاعات دارای علامت محافظ

- چه اطلاعاتی با علامت محافظ در هر قسمت از ساختمان ذخیره، پردازش، پردازش شده یا به طریقی دیگر استفاده خواهد شد؟ برای این اطلاعات به کدام اقدامات محافظتی نیاز دارید؟
- کدام اقدامات محافظتی برای بحث‌ها و جلسات حساس (از جمله جلساتی که شامل اطلاعات دارای علامت محافظ هستند) لازم است؟

۳-۱-۱۲۱- دارایی‌ها و منابع ICT

- کدام دارایی‌ها و منابع فناوری اطلاعات و ارتباطات (ICT) در ساختمان وجود دارد؟ (شامل داده‌ها، نرم افزارها، سخت افزارها، ایستگاه‌های کاری، سرورها، فریم‌ها و کابل‌ها و دستگاه‌های قابل حمل مانند لپ تاپ‌ها و تبلت ها، اما نه محدود به آنها).

۳-۱-۱۲۲- ساختمان کامل، مناطق درون ساختمان، اقدامات مقیاس پذیر

- به طور کلی کدام اقدامات محافظتی برای ساختمان مورد نیاز است؟
- چه اقدامات حفاظتی برای مناطق خاص در محل مورد نیاز است؟ به عنوان مثال، بخشی از یک طبقه که اطلاعاتی با طبقه بندی بالاتر از بقیه ساختمان را در خود جای دهد.
- چگونه اقدامات امنیتی خود را برای رسیدن به افزایش سطح تهدید مقیاس بندی می‌کنید؟

۳-۱-۱۲۳- از برنامه‌های امنیتی خود نیز محافظت کنید

به یاد داشته باشید که برنامه‌های امنیتی ساختمان شما حاوی اطلاعات ارزشمندی در مورد امنیت و عملکرد سازمان شما است. تأثیر هرگونه خسارت یا صدمه به برنامه خود را ارزیابی کنید و در صورت لزوم یک علامت محافظ اعمال کنید.

۳-۱-۱۲۴- الزامات امنیتی را در خلاصه‌ها و قراردادها بگنجانید

تمام تدابیر امنیتی مربوطه را از برنامه‌های امنیتی ساختمان خود در خلاصه طراحی ساختمان و درخواست مناقصه و قراردادها بگنجانید، بنابراین آنها در امکانات تکمیل شده گنجانده می‌شوند.

۳-۱-۱۲۵- اطلاعات بیشتر:

- سیستم طبقه بندی امنیتی دولت نیوزیلند
- الزامات رسیدگی به اطلاعات و تجهیزات دارای علامت محافظ
- قسمت ۱ - هفت کیفیت مکان‌های امن و قسمت ۲ - طراحی پیاده سازی
- دستورالعمل‌های ملی پیشگیری از جرم از طریق طراحی محیط (وزارت دادگستری، ۲۰۰۵)
- طراحی جرم: پیشگیری از جرم از طریق طراحی محیطی

۳-۱-۱۲۶- بازدارنده، ردیابی، تأخیر، پاسخ، بازیابی

اقدامات امنیتی فیزیکی با هدف حفاظت از مردم، اطلاعات و دارایی‌ها در برابر مصالحه یا آسیب از طریق تکنیک‌های زیر انجام می‌شود.

۳-۱-۱۲۷- بازداشتن

افراد غیرمجاز را از تلاش برای دستیابی غیر مجاز به تاسیسات خود منصرف کنید. اقداماتی را که افراد غیرمجاز تصور می‌کنند خیلی دشوار است و یا برای شکست دادن آنها به ابزار و آموزش ویژه احتیاج دارند، اجرا کنید.

۳-۱-۱۲۸- تشخیص

دسترسی غیرمجاز را در اسرع وقت تشخیص دهید. اقدامات لازم را برای بررسی اینکه آیا اقدامی غیرمجاز اتفاق افتاده یا رخ داده است، اجرا کنید.

۳-۱-۱۲۹- تأخیر انداختن

تلاش دسترسی غیرمجاز را تا زمانی که ممکن باشد به تأخیر بیندازید تا اجازه دهید یک پاسخ امنیتی مثمر فعال شود. اقداماتی را برای کند کردن پیشرفت یک رویداد مضر اجرا کنید.

۳-۱-۱۳۰- پاسخ دادن

یک پاسخ مؤثر در مدت زمان مناسب با اقدامات تأخیر، فعالیت پیش بینی شده یک شخص غیر مجاز را خنثی می‌کند. اقداماتی را برای جلوگیری، مقاومت یا کاهش تأثیر حمله یا رویداد آماده کنید.

۳-۱-۱۳۱- بازیابی

اقدامات لازم برای بهبودی از یک حادثه امنیتی را انجام دهید. برنامه ریزی کنید تا به دنبال وقوع حادثه، به موقع و به موقع عملیات را به حالت عادی نزدیک کنید.

۳-۱۹- پیشگیری از جرم از طریق طراحی محیطی

پیشگیری از جرم از طریق طراحی محیطی (CPTED) باید بخشی جدایی ناپذیر از برنامه ریزی تأسیسات شما باشد. برای بکارگیری اصول CPTED، مشخص کنید کدام جنبه از محیط فیزیکی می‌تواند بر رفتار افراد تأثیر بگذارد و سپس از این دانش برای طراحی محیطی استفاده کنید که جرم را به حداقل برساند. اقدامات امنیتی خود را همیشه بر اساس ارزیابی خطر سازمان خود قرار دهید، زیرا CPTED به تنهایی ممکن است تمام نیازهای امنیتی شما را برآورده نکند.

۳-۱-۱۳۲- اطلاعات بیشتر در مورد CPTED:

بسیاری از نشریات با CPTED در حوزه‌های مسکن خصوصی و مناطق عمومی سروکار دارند، اما این اصول برای سازمان‌های دولتی نیز به یک اندازه اعمال می‌شوند.

- رهنمودهای ملی پیشگیری از جرم از طریق طراحی محیطی، وزارت دادگستری، ۲۰۰۵
- طراحی جرم: پیشگیری از جرم از طریق طراحی محیط زیست موسسه جرم شناسی استرالیا
- پیشگیری از جرم از طریق طراحی محیطی (ویرایش سوم، ۲۰۱۳) توسط تیموتی کرو MS جرم شناسی - دانشگاه ایالتی فلوریدا، تجدید نظر شده توسط لارنس فنلی.

۳-۱-۱۳۳- مناطق امنیتی

از مناطق امنیتی استفاده کنید تا امنیت خود را با خطرات پیش روی افراد، اطلاعات یا دارایی خود مطابقت دهید. تدابیر امنیتی اضافی در مناطقی اعمال می‌شود که اطلاعات دارای علامت محافظ و سایر منابع رسمی یا ارزشمند پردازش، اداره، بحث و ذخیره می‌شوند. به این مناطق "مناطق امنیتی" گفته می‌شود. مناطق امنیتی براساس سطح تأثیرات تجاری (BIL) تنظیم شده‌اند و هر یک از آنها دارای حداقل کنترل‌های امنیتی هستند که سازمان شما باید اجرا کند.

اگر سازمان شما با افزایش سطح تهدید روبرو شده است، از ارزیابی ریسک خود استفاده کنید تا ببینید چه اقدامات اضافی در هر منطقه آسیب دیده نیاز دارید. افزایش سطح تهدید می‌تواند به دلیل دخالت خارجی، خشونت با انگیزه سیاسی، فعالیت مجرمانه یا حملات سایبری باشد. رعایت حداقل استانداردهای منطقه، هنگامی که اطلاعات یا دارایی‌ها را به اشتراک می‌گذارید، به سازمان‌های دیگر اطمینان می‌دهد.

۳-۱-۱۳۴- مناطق مختلف را درک کنید

۳-۱-۱۳۵- منطقه ۱: مناطق دسترسی عمومی

این‌ها مناطق امن نیستند از جمله ترتیبات کاری خارج از دفتر. آن‌ها کنترل دسترسی محدودی به اطلاعات و دارایی‌های فیزیکی را فراهم می‌کنند، در صورتی که هرگونه خسارت منجر به تأثیر تجاری کم یا متوسط شود. آن‌ها همچنین محافظت محدودی را برای افراد فراهم می‌کنند.

نمونه‌هایی از مناطق دسترسی عمومی عبارتند از:

- محوطه ساختمان و سرسرای عمومی
- مناطق مصاحبه و میز تحریر
- مناطق کار موقت خارج از دفتر که آژانس هیچ کنترلی بر دسترسی آنها ندارد.
- کارهای میدانی، از جمله بیشتر کارهای مبتنی بر وسیله نقلیه
- قطعات دسترسی عمومی در امکانات چند ساختمانی (به عنوان مثال کافه‌ها یا مغازه‌ها).

۳-۱-۱۳۶- موارد استفاده مجاز

در منطقه ۱ می‌توانید:

- اطلاعات و دارایی‌های فیزیکی مورد نیاز برای تجارت با BIL های پایین تا متوسط را ذخیره کنید
- از اطلاعات و دارایی‌های فیزیکی با BIL زیاد یا بسیار زیاد استفاده کنید (ذخیره سازی توصیه نمی‌شود اما در صورت غیر قابل اجتناب مجاز است)
- فقط در شرایط استثنایی با تأیید آژانس مبدأ، از اطلاعات و دارایی‌های فیزیکی با BIL بالاتر از حد بالا استفاده کنید (ذخیره سازی مجاز نیست).

۳-۱-۱۳۷- منطقه ۲: مناطق کاری

این مناطق دارای امنیت کم هستند که دارای برخی کنترل‌ها هستند. آن‌ها کنترل دسترسی به اطلاعات و دارایی‌های فیزیکی را فراهم می‌کنند، در صورتی که هرگونه خسارت منجر به تأثیر تجاری شود بسیار زیاد است. آن‌ها همچنین برخی از محافظت از مردم را فراهم می‌کنند. مناطق منطقه ۲ اجازه دسترسی نامحدود به افراد و پیمانکاران شما را می‌دهد. دسترسی عمومی یا بازدید کننده محدود شده است.

نمونه‌هایی از مناطق کاری عبارتند از:

- محیط‌های عادی اداری
- محل کار معمولی خارج از دفتر یا خانه که در آن می‌توانید دسترسی به مناطق مورد استفاده برای مشاغل خود را کنترل کنید
- مناطق مصاحبه و میز جلو که افراد شما از مشتری و مردم جدا شده‌اند
- پایگاه‌های نظامی و مناطق کار در کنار فرودگاه با حصار امنیتی در اطراف محیط و ورودی‌های کنترل شده
- کار مبتنی بر وسیله نقلیه در جایی که وسیله نقلیه دارای یک ظرف امنیتی، زنگ هشدار و ایموبیلایزر باشد
- مناطق نمایشگاه با کنترل امنیتی و دسترسی عمومی کنترل شده.

۳-۱-۱۳۸- موارد استفاده مجاز

در منطقه ۲ می‌توانید:

- ذخیره اطلاعات و دارایی‌های فیزیکی با BIL تا بسیار زیاد
- از اطلاعات و دارایی‌های فیزیکی با BIL شدید استفاده کنید، (اما این اطلاعات به طور معمول نباید در منطقه ذخیره شود و باید از ظروف امنیتی تأیید شده استفاده کنید)
- فقط در شرایط استثنایی از اطلاعات و دارایی‌های فیزیکی دارای BIL فاجعه بار استفاده کنید تا با تأیید آژانس مبدأ، اقدامات عملیاتی را برآورده کنید. ذخیره سازی مجاز نیست

۳-۱-۱۳۹- منطقه ۳: مناطق کاری محدود

این مناطق امنیتی با کنترل‌های امنیتی بالا هستند. آن‌ها کنترل دسترسی به اطلاعات و دارایی‌های فیزیکی را فراهم می‌کنند، در صورتی که ضرر و زیان منجر به تأثیر تجاری شود. آن‌ها همچنین از افراد محافظت می‌کنند. دسترسی افراد و پیمانکاران شما محدود به افرادی است که نیاز به دسترسی به منطقه دارند. افرادی که دسترسی مستمر دارند باید دارای یک مجوز امنیتی مناسب باشند. بازدیدکنندگان باید اسکورت شوند، یا از نزدیک کنترل شوند و برای دسترسی به منطقه نیاز تجاری داشته باشند.

نمونه‌هایی از مناطق ممنوع:

- مناطق امن در ساختمان شما که دارای کنترل دسترسی اضافی برای افراد شما هستند (مانند اتاق‌های سرور IT)
- مناطق نمایشگاه با دارایی‌های بسیار ارزشمند
- مناطقی با اشیا items با ارزش بالا یا موارد فرهنگی که در معرض نمایش نیستند.

۳-۱-۱۴۰- موارد استفاده مجاز

در منطقه ۳ می‌توانید:

- اطلاعات یا دارایی‌های فیزیکی را با حداکثر BIL ذخیره کنید
- از اطلاعات با BIL فاجعه بار استفاده کنید (اما این اطلاعات معمولاً نباید در منطقه ذخیره شوند).

۳-۱-۱۴۱- منطقه ۴: مناطق امنیتی

این‌ها مناطق امنیتی با سطح امنیت بالاتری هستند. آن‌ها کنترل دسترسی به اطلاعاتی را که در هر صورت منجر به تأثیر تجاری تا حد شدید می‌شود فراهم می‌کنند و دارایی‌های فیزیکی را که در آن هرگونه خسارت منجر به تأثیر یک تجارت می‌شود و فاجعه بار است. آن‌ها همچنین از افراد محافظت می‌کنند. دسترسی افراد شما با تأیید شناسه و دسترسی به کارت کاملاً کنترل می‌شود. افرادی که دسترسی مستمر دارند باید دارای یک مجوز امنیتی مناسب باشند. بازدید کنندگان و پیمانکاران باید از نزدیک کنترل شوند و برای دسترسی به منطقه نیاز تجاری دارند.

نمونه‌هایی از مناطق امنیتی عبارتند از:

- مناطق امن در داخل ساختمان شما که دارای کنترل دسترسی اضافی برای افراد شما هستند
- مناطق نمایشگاه با دارایی‌های بسیار ارزشمند با کنترل خاص محافظت از دارایی‌ها و دسترسی عمومی که از نزدیک کنترل می‌شود.
- مناطقی که برای نگهداری اشا با ارزش بالا یا موارد فرهنگی که در معرض نمایش نیستند استفاده می‌شود.

۳-۱-۱۴۲- موارد استفاده مجاز

در منطقه ۴ می‌توانید:

- اطلاعات را با حداکثر BIL ذخیره کنید
- از اطلاعات با BIL فاجعه بار استفاده کنید اما این اطلاعات معمولاً نباید در منطقه ذخیره شود.

۳-۱-۱۴۳- منطقه ۵: مناطق با امنیت بالا

این مناطق امنیتی با بالاترین سطح کنترل امنیتی هستند. آن‌ها کنترل دسترسی به اطلاعات را فراهم می‌کنند در صورتی که هر گونه خسارت منجر به تأثیر تجاری تا فاجعه بار شود. دسترسی افراد شما با تأیید شناسه و دسترسی به کارت کاملاً کنترل می‌شود. افرادی که دسترسی مستمر دارند باید دارای یک مجوز امنیتی مناسب باشند. بازدید کنندگان و پیمانکاران باید از نزدیک کنترل شوند و برای دسترسی به منطقه نیاز تجاری دارند.

نمونه‌هایی از نماطق با امنیت بالا عبارتند از:

- مناطقی که اطلاعات محرمانه، خساس یا فشرده را ذخیره می‌کنند.
- امکانات جامعه اطلاعاتی نیوزلند

۳-۱-۱۴۴- موارد استفاده مجاز

در منطقه ۵ شما می‌توانید اطلاعاتی را که با Top Secret مشخص شده است، اطلاعات فشرده یا مقادیر زیادی اطلاعاتی که در صورت جمع شدن دارای BIL فاجعه بار هستند، ذخیره کنید.

۳-۲۰- الزامات منطقه را اعمال کنید

الزامات منطقه حداقل سطح اطمینان را در برابر:

- اطلاعات در معرض خطر، آسیب دیده یا در دسترس نیستند.
- دارایی‌های فیزیکی در معرض خطر قرار گرفته، از بین رفته یا آسیب دیده است.

۳-۱-۱۴۵- الزامات منطقه امنیتی

این حداقل نیازها ممکن است برای محافظت از افراد، اطلاعات و دارایی‌های فیزیکی شما کافی نباشد. از ارزیابی ریسک خود برای بررسی اینکه به کدام کاهش‌های اضافی نیاز دارید استفاده کنید. سازمان شما برای کنترل خطرات شناسایی شده شما باید از کنترل‌های امنیتی درست استفاده کند.

۳-۱-۱۴۶- امنیت در عمق

برای افزایش حفاظت، یک سیستم چند لایه از اقدامات امنیتی را طراحی کنید. لایه بندی اقدامات امنیتی جسمی به این معنی است که امنیت افراد، اطلاعات و دارایی شما با از بین رفتن یا نقض هیچ لایه‌ای به میزان قابل توجهی کاهش نمی‌یابد. با طراحی اقدامات امنیتی که برای پشتیبانی و تکمیل یکدیگر ترکیب شوند، دسترسی غیر مجاز برای یک متجاوز خارجی یا یک کارمند را دشوار خواهید کرد. این روش "امنیت در عمق" نامیده می‌شود.

برای اطمینان عمیق از امنیت، سازمان شما باید:

- از ترکیبی از اقدامات برای محافظت و کنترل دسترسی به افراد، اطلاعات، دارایی‌های فیزیکی و اماکن خود استفاده کنید
- محصولات امنیتی فیزیکی را انتخاب کنید که از سطح مناسب محافظت برخوردار باشند (همانطور که ارزیابی ریسک شما تعیین می‌کند).

۳-۱-۱۴۷- دستیابی به امنیت در عمق

برای دستیابی به امنیت در عمق، مناطق را لایه بندی کنید، از منطقه ۱ کار کنید و با هر منطقه جدید محافظت کنید.

نمودار زیر ترکیبی از مناطق امنیتی را برای دستیابی عمیق به امنیت نشان می‌دهد.

۳-۱-۱۴۸- نمودار ۱ – دستیابی به امنیت در عمق با لایه بندی مناطق امنیتی

از آنجا که سطح امنیت مطابق با مناطق افزایش می‌یابد، با هر لایه جدیدی که اضافه می‌کنید تأخیرهای طولانی‌تری ایجاد خواهید کرد. تأخیر تجمعی به شما فرصت بیشتری می‌دهد تا به هرگونه تلاش برای ورود غیرمجاز به مناطق داخلی پاسخ دهید.

نمودار زیر نشان می‌دهد که چگونه امنیت در عمق می‌تواند تأخیر کافی برای پاسخ مؤثر امنیتی را فراهم کند.

نمودار ۲- جدول زمانی حادثه امنیتی

با افزایش سطح منطقه، اقدامات امنیتی محافظتی شما باید به تدریج تغییر کند تا از اطلاعات و دارایی‌های فیزیکی محافظت شود. تعداد مناطق مورد نیاز شما به سطوح مختلف اطمینان و تفکیک مورد نیاز بستگی دارد. گاهی اوقات امکان قرارگیری مناطق بالاتر در مناطق پایین وجود ندارد. در آن موارد، تقویت دیواره‌های خارجی مناطق بالاتر را در نظر بگیرید. منطقه ۱ باید شامل اقدامات محافظت از محیط باشد. به عنوان مثال، کاهش انفجار، محافظت از تروریسم و غیره.

شما باید حداقل و حداکثر مناطق مورد نیاز در امکانات خود را تنظیم کنید. به عنوان مثال، سازمان‌هایی با:

- BIL های کم و متوسط ممکن است فقط به منطقه ۱ یا منطقه ۲ نیاز داشته باشند
- BIL ها تا، و از جمله، از بالا به خیلی زیاد ممکن است به منطقه ۱ و منطقه ۲ نیاز داشته باشند
- BIL تا حداکثر و از جمله ممکن است به مناطق ۱ تا ۴ نیاز داشته باشد *
- BIL تا فاجعه بار و از جمله آنها ممکن است به مناطق ۱ تا ۵ نیاز داشته باشد **

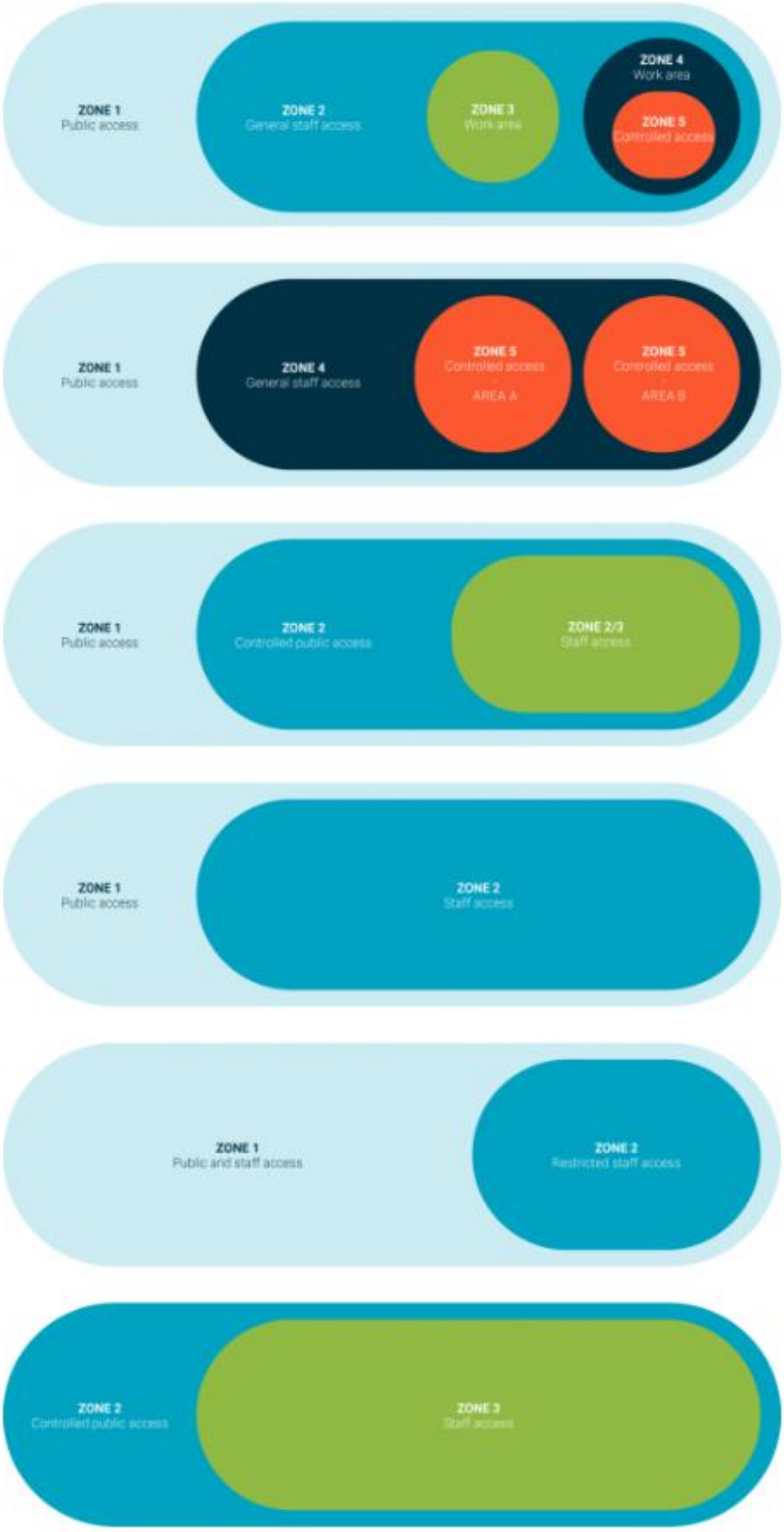
* از مناطق ۳ یا ۴ برای همه مناطق دسترسی کارکنان عمومی به جای منطقه ۲ استفاده کنید.

** برای دسترسی عموم کارکنان از منطقه ۴ استفاده کنید.

برای کسب اطلاعات بیشتر در مورد BIL ها، به Applying the Business Impact Levels بروید.

نمودار ۳ برخی از روش‌های مختلف را نشان می‌دهد که می‌توانید برای ایجاد حفاظت بیشتر، مناطق را لایه بندی کنید.

۳-۱-۱۴۹- نمودار ۳ - ترکیب مناطق امنیتی برای افزایش حفاظت


ZONE 1
Public access
ZONE 2
General staff access
ZONE 3
Work area
ZONE 4
Work area
ZONE 5
Controlled access
ZONE 1
Public access
ZONE 4
General staff access
ZONE 5
Controlled access
AREA A
ZONE 5
Controlled access
AREA B
ZONE 1
Public access
ZONE 2
Controlled public access
ZONE 2/3
Staff access
ZONE 1
Public access
ZONE 2
Staff access
ZONE 1
Public and staff access
ZONE 2
Restricted staff access
ZONE 2
Controlled public access
ZONE 3
Staff access

۳-۱-۱۵۰- ایمن سازی اطلاعات و دارایی‌های محافظت شده در مناطق امنیتی

سازمان شما باید حداقل اطلاعات امنیتی را برای اطلاعات و دارایی‌های محافظت شده رعایت کند.

۳-۱-۱۵۱- مناطق ۳ تا ۵

برای محافظت از اطلاعات و دارایی‌های مشخص شده با BIL شدید یا فاجعه بار برای امنیت ملی، به الزامات مندرج در جدول ۱ مراجعه کنید.

همچنین هنگام ساخت مناطق امنیتی برای ذخیره اطلاعات TOP SECRET یا اطلاعات جمع شده با BIL فاجعه بار، باید "یادداشت فنی NZSIS - امنیت فیزیکی مناطق ۵ منطقه" را رعایت کنید. اطلاعات در یادداشت فنی طبقه بندی می‌شود. برای کسب اطلاعات بیشتر با تیم PSR تماس بگیرید.

اگر به هر دلیلی سازمان شما نتواند این شرایط را برآورده کند، باید برای تهیه هرگونه اطلاعات TOP SECRET یا تجمیع اطلاعات با BIL فاجعه بار، از مبدأ مواد برای هر سایت تأیید بگیرید.

هنگامی که در حال ساخت منطقه ۳ یا ۴ منطقه‌ای هستید که اطلاعات دارای علامت محافظ را در خود ذخیره می‌کند، باید از "یادداشت فنی NZSIS - امنیت فیزیکی مناطق امن" پیروی کنید. این اطلاعات طبقه بندی شده است. برای کسب اطلاعات بیشتر با تیم PSR تماس بگیرید.

۳-۲۱- حفاظت فیزیکی از اطلاعات

۳-۱-۱۵۲- محافظت از موارد منفرد یا اطلاعات محدود

سازمان شما باید از اسناد جداگانه مطابق با پروتکل مدیریت برای امنیت اطلاعات و الزامات مربوط به آن محافظت کند.

ممکن است مواد با علامت گذاری محفظه‌ای، مانند کلمه رمز یا SCI، به کنترل‌های امنیتی اجباری اضافی نیاز داشته باشند.

با توجه به سطح تأثیر تجاری (BIL)، از اطلاعات چاپی و الکترونیکی محافظت فیزیکی کنید.

"مقدار محدودی از اطلاعات" به معنای گروهی از اطلاعات است که منجر به BIL بالاتر نمی‌شود یا نیاز به مارک محافظتی بالاتر از مجموعه اطلاعاتی که از آن می‌آید، دارد.

۳-۱-۱۵۳- رابطه بین BIL ها و سطح طبقه بندی

در بعضی مواقع، ممکن است بین طبقه بندی امنیتی اطلاعات رسمی و BIL ها رابطه وجود داشته باشد. هنگام بررسی محرمانه بودن اسناد یا پرونده‌های فردی، طبقه بندی‌های امنیتی مستقیماً با BIL ها مطابقت دارند. با این حال، این لزوماً در مورد مجموعه دارایی‌ها صدق نمی‌کند. به عنوان مثال، در مجموعه دارایی‌های دارای سطح تأثیر تجاری ۴ برابر، ممکن است هر مورد منفرد به عنوان محرمانه علامت گذاری نشود.

با این وجود، مارک محافظتی یا محرمانه بودن دارایی تنها عاملی نیست که باید هنگام تهیه BIL در نظر بگیرید. قبل از اعمال BIL باید تمام عوامل مؤثر بر امنیت دارایی را در نظر بگیرید. BIL ها همچنین باید یکپارچگی و در دسترس بودن را در نظر بگیرند.

جداول زیر پیوندهای احتمالی بین علائم محافظتی و BIL های اسناد منفرد یا اطلاعات محدود را به طور خلاصه بیان می‌کند.

- علامت گذاری سند فردی
- سطح تأثیر تجاری
- طبقه بندی نشده (ممکن است علامت گذاری نشده باشد)
- ۱ کم
- با اطمینان
- ۲ متوسط
- حساس یا محدود شده است
- ۳ بالا
- محرمانه
- ۴ بسیار بالا
- راز
- ۵ افراطی
- فوق سری
- ۶ فاجعه بار

۳-۱-۱۵۴- محافظت از اطلاعات جمع شده

منظور از اطلاعات جمع، مجموعه‌ای از اطلاعات رسمی دارای علامت محافظتی یا طبقه بندی نشده است. به عنوان مثال، مجموعه اطلاعات الکترونیکی.

وقتی اطلاعات جمع می‌شوند، اغلب ارزش بیشتری پیدا می‌کنند و نیاز به محافظت بیشتری دارند.

سازمان شما باید اقدامات امنیتی فیزیکی را برای کاهش خطرات مرتبط با اطلاعات جمع آوری شده اعمال کند.

برای راهنمایی بیشتر، به این موارد بروید:

استفاده از سطوح تأثیر تجاری

۳-۱-۱۵۵- محافظت از اطلاعات با BIL فاجعه بار

TOP SECRET یا اطلاعات جمع شده‌ای که در صورت نقض امنیت آن می‌تواند به امنیت ملی نیوزلند آسیب برساند، فقط در منطقه مجاز توسط سرویس اطلاعات امنیتی نیوزلند (NZSIS) ذخیره می‌شود. قبل از استفاده از منطقه و بعد از هرگونه تغییر در آن، به گواهینامه آنها احتیاج دارید.

اگر امکانات مناسبی ندارید یا هزینه ایجاد امکانات توجیه پذیر نیست، می‌توانید آژانس دیگری را برای نگهداری اطلاعات TOP SECRET خود تنظیم کنید. با این حال، اگر سازمان شما اطلاعات را در اختیار دارد، باید کانتینرهای امنیتی برای نگهداری اطلاعات تهیه کنید و دسترسی به ظروف را کنترل کنید

۳-۱-۱۵۶- قوانین و استانداردهای مربوطه

طراحی اقدامات امنیتی فیزیکی شما باید مطابق با اقدامات زیر و هرگونه مقررات یا کدهای مرتبط باشد:

- بهداشت و ایمنی در قانون کار ۲۰۱۵
- حریم قانون ۱۹۹۳
- قانون ساختمان ۲۰۰۴.

۳-۱-۱۵۷- استانداردها، کتاب‌های راهنما و کدها

هنگامی که سازمان شما اقدامات امنیتی فیزیکی را اجرا می‌کند، از استانداردها، کتاب‌های راهنما و کدهای زیر برای راهنمایی خود استفاده کنید.

۳-۲۲- استانداردها

۳-۱-۱۵۸- استانداردهای استرالیا و نیوزیلند (AS و NZS)

- AS 3555.1: 2003 عناصر ساختمانی - آزمایش و رتبه بندی برای مقاومت در برابر نفوذگرها
- AS / NZS 2343: 1997 پانل‌ها و عناصر مقاوم در برابر گلوله
- AS 1725: 2003 شمشیربازی و دروازه‌های امنیتی پارچه‌ای با زنجیر
- AS / NZS 3016: 2002 نصب و راه اندازی برق - نرده‌های امنیتی برقی
- AS / NZS 2201.5: 2008 سیستم‌های هشدار متجاوز - سیستم‌های انتقال دزدگیر
- AS / NZS 2201.1: 2007 سیستم‌های هشدار متجاوز - محل کارفرما - طراحی، نصب، راه اندازی و نگهداری
- AS 2201.3: 1991 سیستم‌های هشدار متجاوز - دستگاه‌های تشخیص برای استفاده داخلی
- AS 2201.2: 2004 سیستم‌های هشدار متجاوز - مراکز نظارت
- AS 4145.2: 2008 قفل و سخت افزار درب و پنجره - قفل مکانیکی درب و پنجره در ساختمان‌ها
- AS / NZS 4801: 2001 سیستم‌های مدیریت ایمنی و بهداشت شغلی
- AS / NZS 3809: 1998 گاوصندوق‌ها و اتاق‌های محکم

۳-۱-۱۵۹- استانداردهای انگلیس (BS)

- دستورالعمل PAS 69: 2013 برای مشخصات و نصب موانع امنیتی خودرو
- BS EN 14450: 2005 - واحدهای ذخیره سازی ایمن. الزامات، طبقه بندی‌ها و روش‌های آزمایش مقاومت در برابر سرقت. کابینت‌های ایمن را ایمن کنید
- نرده‌های BS 1722–14: 2016 - مشخصات نرده‌های پانل فولادی مش باز
- نرده‌های BS 1722–12: 2016 - مشخصات نرده‌های استیل محکم

۳-۱-۱۶۰- سازمان بین المللی استاندارد سازی (ISO)

- ISO / IEC 27002: 2006 فناوری اطلاعات - تکنیک‌های امنیتی - آیین نامه مدیریت امنیت اطلاعات
- ISO 31000: 2018 مدیریت ریسک - دستورالعمل‌ها

۳-۱-۱۶۱- استاندارد صنعتی ژاپن (JIS)

- JIS S 1037 - تست آتش استاندارد

۳-۱-۱۶۲- استانداردهای UL

- UL 72 - آزمایش مقاومت در برابر آتش تجهیزات حفاظت از سوابق
- UL 687 - گاوصندوق‌های مقاوم در برابر سرقت

۳-۱-۱۶۳- استانداردهای آمریکا و کانادا

- FIPS FIPS 201
- CAN / ULC-S319 سیستم‌های کنترل دسترسی الکترونیکی

۳-۱-۱۶۴- کتاب‌های راهنما

- HB 327: 2010 ارتباط و مشاوره در مورد ریسک
- طراحی جرم: پیشگیری از جرم از طریق طراحی محیطی
- دستورالعمل‌های IES-G-1-03 در مورد روشنایی امنیتی برای افراد، املاک و فضاهای عمومی
- HB 328: 2009 Mailroom Security
- حریم خصوصی و دوربین مداربسته: راهنمای قانون حریم خصوصی برای مشاغل، آژانس‌ها و سازمان‌ها
- راهنمای امنیت اطلاعات نیوزلند (NZISM) - ضد عفونی و دفع محصولات - دفع رسانه‌ها
- NZISM - تلفن‌ها و سیستم‌های تلفنی
- HB 167: 2006 مدیریت ریسک امنیتی

۳-۱-۱۶۵- کدها

- قانون ساختمان نیوزیلند

۳-۱-۱۶۶- راهنمایی برای ایجاد مناطق ۳، ۴ یا ۵

هنگام طبقه بندی مناطق ۳، ۴ یا ۵، مواد طبقه بندی شده زیر شما را راهنمایی می‌کنند. برای کسب اطلاعات بیشتر با تیم PSR تماس بگیرید.

- لیست محصولات تأیید شده NZSIS (APL)
- یادداشت فنی NZSIS - اتاق امن کلاس A
- یادداشت فنی NZSIS - اتاق امن کلاس B
- یادداشت فنی NZSIS - اتاق امن کلاس C
- یادداشت فنی NZSIS - امنیت فیزیکی مناطق مقاوم به نفوذ
- یادداشت فنی NZSIS - امنیت فیزیکی مناطق امن
- یادداشت فنی NZSIS - امنیت فیزیکی مناطق ۵ منطقه

۳-۱-۱۶۷- امنیت فیزیکی

راهنمای زیر استفاده از اقدامات امنیتی خاص را توصیف می‌کند.

- امنیت فیزیکی
- چرخه عمر امنیت فیزیکی را بفهمید
- امنیت فیزیکی را در مراحل اولیه خود طراحی کنید
- اقدامات امنیتی خاص

به یاد داشته باشید که امنیت فیزیکی ترکیبی از اقدامات فیزیکی و رویه‌ای است .شما باید سیاست‌هایی تدوین کنید که اقدامات امنیتی جسمی شما را پشتیبانی کند و استفاده از آنها را کنترل کند.

۳-۱-۱۶۸- استفاده از محصولات مورد تأییدNZSIS

با استفاده از محصولات امنیتی تأیید شده از سرویس اطلاعات ویژه نیوزلند (NZSIS) از افراد، اطلاعات و دارایی‌های سازمان خود محافظت کنید NZSIS .محصولات امنیتی را مورد آزمایش و تأیید قرار می‌دهد که: محافظت از اطلاعات دارای علامت محافظ با سطح تأثیر تجاری (BIL) بالا یا بالاتر، از تلفات گسترده زندگی جلوگیری می‌کند و به آزمایشات تخصصی نیاز دارد.

۳-۱-۱۶۹- کنترل های دسترسی محیطی

محدود کردن دسترسی به امکانات شما با کنترل دسترسی محیطی می‌تواند به سازمان شما کمک کند تا تهدیدات را کاهش دهد .برخی از انواع کنترل دسترسی محیطی عبارتند از: حصارها و دیوارها موانع عبور عابر پیاده موانع وسیله نقلیه.

۳-۱-۱۷۰- ساخت و ساز ساختمان

قبل از اینکه سازمان شما هرگونه محل اجاره را اجاره کند یا احداث کند، روش‌ها و مواد ساخت را ارزیابی کنید تا بفهمید آیا از محافظت شما کمک می‌کند .افزایش سطح امنیت ساختمان پس از آن ممکن است گران یا غیرممکن باشد.

۳-۱-۱۷۱- سیستم های هشدار

سیستم‌های هشدار می‌توانند هشدار زودهنگام در مورد دسترسی غیرمجاز به امکانات شما را بدهند .با این حال، یک سیستم هشدار فقط زمانی ارزش دارد که شما از آن در کنار سایر اقدامات طراحی شده برای شناسایی تلاش برای نفوذ، تأخیر در پیشرفت یک متجاوز و فرصت دادن به شما برای پاسخگویی استفاده کنید.

۳-۱-۱۷۲- گزینه های هشدار فردی

هشدارهای فردی می‌توانند از مردم و وسایل نقلیه در برابر آسیب محافظت کنند .در برخی شرایط، ایجاد سیستم‌های هشدار دهنده یا اقدامات دیگر در کل امکانات ممکن است تمام محافظت مورد نیاز مردم و دارایی شما را ایجاد نکند.

۳-۱-۱۷۳- سیستم های کنترل دسترسی

برای جلوگیری از دسترسی غیر مجاز از سیستم‌های کنترل دسترسی استفاده کنید .سیستم کنترل دسترسی یک معیار یا گروهی از اقدامات است که به منظور اجازه عبور از پرسنل مجاز، وسایل نقلیه و تجهیزات از موانع محافظ، جلوگیری از دسترسی غیر مجاز است.

۳-۱-۱۷۴- قابلیت همکاری سیستم دزدگیر و سایر سیستم های مدیریت ساختمان

سیستم‌های قابل همکاری باید با دقت طراحی شوند تا از ایجاد آسیب پذیری جلوگیری شود. اجرای قابلیت همکاری بین سیستم‌های هشدار امنیتی (SAS) و سایر سیستم‌های مدیریت ساختمان می‌تواند تهدید دسترسی و نفوذ غیرمجاز سیستم را افزایش دهد.

۳-۱-۱۷۵- قفل ها ، سیستم های کلیدی و درها

سخت افزار مناسب را برای محافظت از اطلاعات و دارایی‌های خود انتخاب کنید .سازمان شما باید با استفاده از قفل‌ها و سخت افزارهای تجاری یا درجه تجاری یاNZSIS ، تمام نقاط دسترسی به محل کار شما را از جمله درها و پنجره‌های قابل استفاده ایمن کند.

۳-۱-۱۷۶- تلویزیون مداربسته

استفاده از دوربین مداربسته را در نظر داشته باشید وقتی سازمان شما در حال توسعه "امنیت عمیق" برای یک سایت است . دوربین مداربسته یک عامل بازدارنده بصری برای دسترسی غیرمجاز، سرقت یا خشونت است.

۳-۱-۱۷۷- روشنایی امنیتی

استفاده از روشنایی برای افزایش امنیت فیزیکی در سایت شما .روشنایی می‌تواند سهم مهمی در امنیت فیزیکی داشته باشد.

۳-۱-۱۷۸- صندوق ها و کابینت های امنیتی

ظروف و کابینت‌های مناسب را برای ایمن نگه داشتن اطلاعات و دارایی انتخاب کنید .شما باید اطلاعات رسمی، دارایی‌های فیزیکی ارزشمند و پول را در ظروف متناسب با سطح تأثیر تجاری آنها (BIL) ایمن کنید.

۳-۱-۱۷۹- اتاق ها ، گاوصندوق ها و اتاق های نگهداری ایمن

استفاده از اتاق‌های امن، گاوصندوق‌ها، یا خزانه‌ها را به جای ظروف برای محافظت از مقادیر زیادی از اطلاعات رسمی یا دارایی‌های فیزیکی ارزشمند در نظر بگیرید .استفاده از اتاق‌های امن اتاق‌های امن برای ذخیره مقدار زیادی اطلاعات رسمی مناسب هستند.

جدول انتخاب گاوصندوق‌ها یا خزانه‌ها برای محافظت از دارایی‌های ارزشمند فیزیکی (PDF 39 KB)

- **آخرین به روزرسانی**25/06/2018 **:**

جدول برای کمک به انتخاب انواع ایمن و خزانه برای ذخیره ایمن اطلاعات یا دارایی‌ها.

۳-۱-۱۸۰- کنترل بازدید کننده

برای کنترل دسترسی بازدید کننده به امکانات خود، فرآیندهای روشن و سازگار را دنبال کنید .منظور از ویزیتور، هر کسی در یک مرکز یا منطقه است که: کارمند نباشد، به عنوان بازدید کننده دسترسی عادی به مرکز یا مرکز داده شده است.

۳-۱-۱۸۱- پذیرندگان و نگهبانان

بازدید کنندگان را کنترل کرده و تهدیدات را با پذیرشگران و نگهبانان دفع کنید اگر سازمان شما به طور منظم با عموم یا مشتری ارتباط برقرار می‌کند، باید پذیرنده یا نگهبان داشته باشید تا از بازدید کنندگان استقبال، کمک و راهنمایی کنند.

۳-۲۳- سایر اقدامات امنیتی فیزیکی

بررسی کنید که سایر اقدامات امنیتی فیزیکی ممکن است سازمان شما برای رفع خطرات خاص لازم باشد .برای کمک به شما در مورد اینکه کدام اقدامات امنیتی فیزیکی به بهترین وجه شرایط خاص شما را برآورده می‌کند، از مثالهای زیر استفاده کنید

۳-۱-۱۸۲- استفاده از محصولات مورد تأییدNZSIS

با استفاده از محصولات امنیتی تأیید شده از سرویس اطلاعات ویژه نیوزلند (NZSIS) از افراد، اطلاعات و دارایی‌های سازمان خود محافظت کنید.

- NZSISمحصولات امنیتی را آزمایش و تأیید می‌کند که:

- از اطلاعات دارای علامت محافظ با سطح تأثیر تجاری (BIL) بالاتر یا بالاتر محافظت کنید

- جلوگیری از تلفات گسترده زندگی
- نیاز به آزمایش تخصصی دارد.

اگر یک سازمان دولتی هستید، باید از محصولات مورد تأیید NZSIS برای تأمین نیازهای منطقه امنیتی و کاهش خطرات شناسایی شده در ارزیابی ریسک استفاده کنید. این موارد تأیید شده در فهرست محصولات تأیید شده NZSIS (APL) ذکر شده است .اطلاعات موجود در این لیست طبقه بندی شده است .برای کسب اطلاعات بیشتر با تیم PSR تماس بگیرید. اگر سازمان شما می‌خواهد از محصولات مورد تأیید NZSIS و تجهیزات تجاری مشابه برای نیازهای امنیتی سطح پایین استفاده کند، مدیر ارشد امنیتی (CSO) شما باید ابتدا از NZSIS مشاوره دریافت کند.

۳-۱-۱۸۳- ساخت و ساز ساختمان

قبل از اینکه سازمان شما هرگونه محل اجاره را اجاره کند یا احداث کند، روش‌ها و مواد ساخت را ارزیابی کنید تا بفهمید آیا از محافظت شما کمک می‌کند.

افزایش سطح امنیت ساختمان پس از آن ممکن است گران یا غیرممکن باشد.

۳-۱-۱۸۴- ساخت و ساز داخلی در مقابل ساختمان تجاری

به طور معمول، ساختمان‌ها با کد ساختمان نیوزلند ساخته می‌شوند. برخی از ساختمانهای قدیمی ممکن است این کد را نداشته باشند. ساخت وسازهای داخلی از دسترسی غیر مجاز محافظت کمی می‌کند. نفوذ برای سرقت متداول‌ترین نوع دسترسی غیر مجاز است. دسترسی مخفی ماهر به طور معمول در شرایط داخلی بسیار دشوار است.

دفاتر تجاری استاندارد معمولاً از محیط پیرامونی بیشتری نسبت به ساختمانهای داخلی محافظت می‌کنند. با این حال، دیوارهای داخلی، سقف‌های کاذب و سایر روش‌های معمول ساختمان توانایی شما را در محافظت از اطلاعات و دارایی‌های فیزیکی کاهش می‌دهد. اکثر فضاهای اداری تجاری فقط برای محافظت از دارایی‌ها و اطلاعات با سطح تأثیر تجاری (BIL) متوسط یا پایین مناسب هستند.

۳-۱-۱۸۵- اضافه کردن حفاظت اضافی با سخت شدن ساختمان

اگر ارزیابی ریسک شما نشان می‌دهد برای رفع خطرات خاص باید عناصر ساختمانی اضافه کنید، سخت شدن ساختمان ممکن است تا حدی سطح تخفیف را ایجاد کند.

چند نمونه از سخت شدن ساختمان عبارتند از:

- اقدامات کاهش انفجار
- حمله قهری و مقاومت بالستیک
- جاده‌ها و مسیرهای دسترسی عمومی
- روشنایی (علاوه بر روشنایی امنیتی)
- تخفیف وسیله نقلیه خصمانه
- عناصر پیشگیری از جرم از طریق طراحی محیطی (CPTED).

۳-۱-۱۸۶- استانداردهای مربوط به نیوزیلند

- AS 3555.1: 2003 عناصر ساختمان - آزمایش و رتبه بندی مقاومت در برابر نفوذگر - پانل‌های مقاوم در برابر نفوذ. این استاندارد راهنمایی در مورد مقاومت بسیار بالا در برابر متجاوز، مانند خزانه‌های با امنیت بالا را ارائه می‌دهد.

- AS / NZS 2343: 1997 پانل‌ها و عناصر مقاوم در برابر گلوله

۳-۱-۱۸۷- با استفاده از ساخت و ساز دال به دال

ساخت و ساز دال به دال از دسترسی از طریق سقف‌های کاذب جلوگیری می‌کند. دیوارها مستقیماً به کف و به پایین طبقه بعدی یا سازه سقف متصل می‌شوند.

۳-۱-۱۸۸- جایی که باید از ساختار دال به دال استفاده کنید

سازمان شما باید از ساخت و ساز دال به دال در محیط مناطق امنیتی، از جمله تمام نقاط دسترسی استفاده کند. برای جزئیات بیشتر در مورد روش‌های ساخت ورق به دال، به یادداشت فنی NZSIS - امنیت فیزیکی مناطق مقاوم در برابر نفوذ مراجعه کنید. این یادداشت طبقه بندی شده است. برای کسب اطلاعات بیشتر با تیم PSR تماس بگیرید. تغییرات ساختاری می‌تواند بر یکپارچگی ساختمان‌ها تأثیر بگذارد، بنابراین قبل از اجرای ساخت و ساز از دال به دال، به دنبال مهندسی سازه باشید.

۳-۱-۱۸۹- وقتی می‌توانید بدون ساخت و ساز دال به دال بروید (با دقت)

نقاط دسترسی شما برای منطقه ۱ و منطقه ۲ ممکن است بین ساعات کاری و بعد از ساعت متفاوت باشد. به عنوان مثال، از نقاط داخلی (مانند مبادی ورودی کنترل شده دفتر) در ساعات کاری تا محیط ساختمان یا ساختمان بعد از ساعت (مانند درب اصلی).

هنگامی که نقطه دسترسی خارج از ساعت دارای ساخت دال به دال است، می‌توانید از نقاط دسترسی منطقه ۲ در ساعات کاری بدون ساخت دال به دال استفاده کنید. روش دیگر، شما می‌توانید یک لایه مقاوم در برابر نفوذگر، مانند مش فولادی، در سقف نصب کنید تا در صورت نیاز به تاخیرهای نفوذ برای اتاق‌های خاص، مشکل پانل‌های سقف کاذب قابل جابجایی را برطرف کنید. توجه داشته باشید که این اقدامات هیچ گونه محافظتی در مورد شنیدن بیش از حد ایجاد نمی‌کند، بنابراین در مواردی که به امنیت گفتاری نیاز دارید نباید از آنها استفاده کنید. همچنین می‌توانید از تکنیک‌های ساختمانی مشهود برای دستکاری استفاده کنید تا نشانه‌ای از دسترسی غیرمجاز ارائه دهید.

۳-۱-۱۹۰- ساخت محوطه ۳ و منطقه ۴

برای کسب اطلاعات در مورد ساخت مناطق ۳ و منطقه ۴ برای ذخیره اطلاعات دارای علامت محافظ یا تجمع اطلاعات با سطح تأثیر تجاری (BIL) با خسارت بسیار زیاد، به یادداشت فنی NZSIS - امنیت فیزیکی مناطق امن مراجعه کنید. از آنجا که این یادداشت فنی یک سند طبقه بندی شده است، برای اطلاعات بیشتر با تیم PSR تماس بگیرید

۳-۱-۱۹۱- ساخت منطقه ۵ محیط

برای اطلاعات در مورد ساخت مناطق ۵ منطقه برای ذخیره اطلاعات TOP SECRET یا تجمیع اطلاعات با سطح تأثیر تجاری (BIL) خسارت فاجعه بار، به یادداشت فنی NZSIS - امنیت فیزیکی مناطق ۵ مراجعه کنید. از آنجا که این یادداشت فنی یک سند طبقه بندی شده است، برای اطلاعات بیشتر با تیم PSR تماس بگیرید.

فصل ۴

امنیت پرسنل

۴- چرا امنیت پرسنل اهمیت دارد

امنیت پرسنل از طریق پشتیبانی سازمان، از افراد، اطلاعات و دارایی شما محافظت می‌کند:

- خطر آسیب رساندن به مردم، مشتریان و شرکای خود را کاهش دهید
- خطر از بین رفتن، آسیب دیدن یا به خطر افتادن اطلاعات یا دارایی‌های خود را کاهش دهید
- به افرادی که به اطلاعات و دارایی‌های رسمی یا مهم شما دسترسی دارند اعتماد بیشتری داشته باشید
- ارائه خدمات و کار موثرتر

تهدیدهای داخلی از طرف کارمندان گذشته، یا حال حاضر، پیمانکاران یا شرکای تجاری ما ناشی می‌شود .آن‌ها می‌توانند از دانش درونی خود سو استفاده کنند و یا به صدمه به مردم، مشتریان، دارایی یا اعتبار ما آسیب برسانند .تمرکز امنیت کارکنان بر کاهش خطرات مرتبط با تهدیدات داخلی است.

"تهدید داخلی" یا "خودی"، هر شخصی است که از دسترسی قانونی خود به دارایی‌های یک سازمان برای آسیب رساندن به امنیت سازمان خود یا نیوزیلند، خواسته یا ناخواسته، از طریق جاسوسی، تروریسم، سو استفاده یا قصد بهره برداری از آنها را دارد. افشای غیرمجاز اطلاعات یا از بین رفتن یا تخریب یک منبع (یا قابلیت).

اقدامات خودی مشترک شامل موارد زیر است:

- افشای غیرمجاز اطلاعات رسمی، خصوصی یا انحصاری
- کلاهبرداری یا پردازش فساد
- دسترسی غیرمجاز به سیستمهایICT
- جاسوسی اقتصادی یا صنعتی
- سرقت
- خشونت یا آسیب جسمی به دیگران.

بسیاری از نقض‌های امنیتی ناخواسته است و ناشی از عدم آگاهی یا توجه به اقدامات امنیتی، حواس پرتی یا فریب خوردن کمک ناخواسته به شخص ثالث است

❖ الزامات اجباری

الزامات اصلی امنیتی پرسنل که دستگاههای دولتی مأمور باید رعایت کنند و سایر سازمانها باید بهترین روش را در نظر بگیرند.

❖ فرد مناسب را استخدام کنید

اطمینان حاصل کنید که همه افرادی که برای سازمان شما کار می‌کنند (کارمندان، پیمانکاران و کارکنان موقت) که به اطلاعات و دارایی‌های دولت نیوزلند دسترسی دارند:

- هویت آنها مشخص شده است
- حق کار در نیوزیلند را دارند
- برای دسترسی مناسب هستند

موافقت می‌کنید که با سیاست‌ها، استانداردها، پروتکل‌ها و الزامات دولت که از مردم، اطلاعات و دارایی‌ها در برابر آسیب محافظت می‌کند، پیروی کنید.

❖ **اطمینان از مناسب بودن مداوم آنها**

از مناسب بودن مداوم همه افرادی که برای سازمان شما کار می‌کنند اطمینان حاصل کنید .این مسئولیت شامل رسیدگی به هرگونه نگرانی است که ممکن است در شایستگی شخص برای ادامه دسترسی به اطلاعات و دارایی‌های دولت تأثیر بگذارد.

❖ **عزیمت آنها را مدیریت کنید**

عزیمت افراد را مدیریت کنید تا هرگونه خطر برای افراد، اطلاعات و دارایی‌های ناشی از افرادی که از سازمان شما خارج می‌شوند، محدود شود .این مسئولیت شامل اطمینان از بازگشت هرگونه حق دسترسی، مجوزهای امنیتی و دارایی‌ها و درک افراد از تعهدات مداوم خود است.

❖ **مجوزهای امنیتی ملی را مدیریت کنید**

اطمینان حاصل کنید که افراد قبل از اینکه به اطلاعات، دارایی‌ها یا مکان‌های کاربری محرمانه، محرمانه و دسترسی پیدا کنند، از سطح امنیت ملی مجاز برخوردار هستند.

شایستگی مداوم کلیه دارندگان مجوزهای امنیت ملی برای داشتن مجوز را مدیریت کرده و هرگونه تغییر در مورد ترخیص آنها را به NZSIS اطلاع دهید

۱-۴- پروتکل مدیریت برای امنیت پرسنل

این پروتکل چرخه مدیریت ریسک امنیت پرسنل(PERSEC) ، چرخه مدیریت امنیت پرسنل و نحوه ارتباط آنها با الزامات امنیتی پرسنل اجباری PSR را توضیح می‌دهد.

اگر شما یک مدیر اجرایی، مدیر ارشد امنیت(CSO) ، مدیر ارشد یا مدیر خط هستید که چرخه حیات PERSEC را می‌فهمید و شرایط را برآورده می‌کنید به شما کمک می‌کند:

- برای محافظت از سازمان خود، اقدامات امنیتی قوی را در پیش بگیرید
- فرهنگی را تشویق کنید که در آن همه رفتارهای امنیتی درست را اتخاذ کنند.

❖ **مزایای امنیت قوی پرسنل را درک کنید**

اگرچه اغلب گفته می‌شود که مردم بزرگترین سرمایه یک سازمان هستند، اما همچنین می‌تواند یک نقطه ضعف باشد.

امنیت پرسنل از طریق پشتیبانی سازمان، از افراد، اطلاعات و دارایی شما محافظت می‌کند:

- خطر آسیب رساندن به مردم، مشتریان و شرکای خود را کاهش دهید
- خطر از بین رفتن، آسیب دیدن یا به خطر افتادن اطلاعات یا دارایی‌های خود را کاهش دهید
- به افرادی که به اطلاعات و دارایی‌های رسمی یا مهم شما دسترسی دارند اعتماد بیشتری داشته باشید
- ارائه خدمات و کار موثرتر

تهدیدهای داخلی از طرف کارمندان گذشته، یا حال حاضر، پیمانکاران یا شرکای تجاری ما ناشی می‌شود .آن‌ها می‌توانند از دانش درونی خود سو استفاده کنند و یا به صدمه به مردم، مشتریان، دارایی یا اعتبار ما آسیب برسانند .تمرکز امنیت کارکنان بر کاهش خطرات مرتبط با تهدیدات داخلی است.

"تهدید داخلی" یا "خودی"، هر شخصی است که از دسترسی قانونی خود به دارایی‌های یک سازمان برای آسیب رساندن به امنیت سازمان خود یا نیوزیلند، خواسته یا ناخواسته، از طریق جاسوسی، تروریسم، سو استفاده یا قصد بهره برداری از آنها را دارد. افشای غیرمجاز اطلاعات یا از بین رفتن یا تخریب یک منبع (یا قابلیت).

اقدامات خودی مشترک شامل موارد زیر است:

- افشای غیرمجاز اطلاعات رسمی، خصوصی یا انحصاری
- کلاهبرداری یا پردازش فساد
- دسترسی غیرمجاز به سیستمهایICT
- جاسوسی اقتصادی یا صنعتی
- سرقت
- خشونت یا آسیب جسمی به دیگران.

بسیاری از نقض‌های امنیتی ناخواسته است و ناشی از عدم آگاهی یا توجه به اقدامات امنیتی، حواس پرتی یا فریب خوردن کمک ناخواسته به شخص ثالث است.

❖ رویکردی مبتنی بر ریسک برای امنیت پرسنل داشته باشید

اجرای اقدامات امنیتی پرسنل می‌تواند پرهزینه و مخل باشد .تدابیر امنیتی شما باید با توجه به زمینه امنیتی سازمان، تهدیدات احتمالی و اشتهای مخاطره در نظر گرفته شود.

یک رویکرد مبتنی بر ریسک برای امنیت محافظ، تضمین می‌کند که خطرات، اقدامات و سرمایه گذاری‌های امنیتی پرسنل برای خطرات سازمان شما مناسب است.

❖ فرهنگ امنیتی ایجاد کنید

همه افراد سازمان به فرهنگ امنیتی آن کمک می‌کنند .فرهنگ سازمانی تأثیر مستقیمی بر امنیت دارد .اگر مردم نگرش ضعیفی نسبت به امنیت داشته باشند، حتی با بهترین فرایندها و ابزارهای امنیتی، سازمان شما همچنان در معرض خطر خواهد بود.

شما باید فرهنگی را ایجاد کنید که همه افراد خطرات امنیتی پیش روی سازمان را درک کنند، رفتارهای امنیتی صحیحی را در پیش گرفته و همکاران خود را به همان کار تشویق کنند.

ایجاد فرهنگ امنیتی مؤثر پرسنل به معنای سوار شدن همه افراد است .مسئولیت‌های مربوط به امنیت پرسنل در کل سازمان شما گسترش می‌یابد.

رئیس اجرایی شما مسئولیت کلی امنیت محافظت در سازمان شما را بر عهده دارد.

افسر ارشد امنیتی شما مسئول سیاست حفاظت از امنیت، نظارت بر اقدامات امنیتی محافظتی و فعالیت‌های ارزیابی است که از پیشرفت‌های مداوم خبر می‌دهد.

❖ چرخه مدیریت خطرات امنیتی پرسنل را دنبال کنید

چرخه مدیریت ریسک امنیتی پرسنل نشان می‌دهد چگونه سازمان خود را باید در سطح سازمانی در شناسایی و مدیریت خطرات امنیتی پرسنل.

چرخه در حال انجام شامل سه فعالیت اصلی است.

- خطرات امنیتی پرسنل خود را ارزیابی کنید
- خطرات امنیتی پرسنل خود را مدیریت کنید

ارزیابی کنید که چگونه به طور مؤثر خطرات امنیتی پرسنل خود را مدیریت می‌کنید.

❖ خطرات امنیتی پرسنل خود را ارزیابی کنید

شما باید منابع بالقوه خطرات امنیتی پرسنل را که سازمان شما با آن روبرو است، نحوه بروز آنها و انواع تهدیدهای آنها را شناسایی کنید .ارزیابی ریسک شما باید نقش‌ها یا گروه‌هایی از افراد را شناسایی کند که به دلیل دسترسی به اطلاعات یا دارایی‌های حساس، ارزشمند یا طبقه بندی شده، پتانسیل بیشتری برای ایجاد آسیب دارند.

نمونه‌هایی از خطرات سازمان شما می‌تواند نشت ناخواسته، سرقت مالکیت معنوی، کلاهبرداری یا سود مجرمانه باشد.

❖ خطرات امنیتی پرسنل خود را مدیریت کنید

هر مرحله از چرخه حیات پرسنل چالش‌های متفاوتی را نشان می‌دهد .شما باید از زمان شروع استخدام / تدارکات، هنگام استخدام یا تعامل شخصی و تا لحظه ترک وی - احتمالاً حتی پس از ترک کار، امنیت پرسنل را در نظر داشته باشید .اقدامات مناسبی را برای مقابله با خطرات امنیت پرسنل در هر یک از این مراحل اجرا کنید

برای مدیریت خطرات امنیتی پرسنل، باید تدابیر امنیتی را که شناسایی کرده‌اید به طور مستمر و مداوم در مورد همه افراد شاغل در سازمان خود اعمال کنید.

ارزیابی کنید که چگونه به طور مؤثر خطرات خود را مدیریت می‌کنید

تهدیدهای پیش روی سازمان با گذشت زمان تغییر می‌کند .این بدان معناست که شما باید بررسی کنید که آیا درک شما از منابع خطرات امنیتی پرسنل دقیق و به روز است.

شما همچنین باید بررسی کنید که آیا ترتیبات و اقدامات امنیتی شما هنوز مؤثر و مناسب هستند .مشخص کنید چه چیزی خوب کار می‌کند و چه چیزی مناسب نیست و ترتیبات خود را متناسب با آن تنظیم کنید.

❖ چرخه عمر امنیت پرسنل را بفهمید

چرخه عمر امنیت پرسنل مسائل مشخص و اقدامات امنیتی شما باید در هر مرحله از زمان یک فرد را با سازمان شما در نظر نشان می‌دهد.

❖ الزامات امنیتی پرسنل اجباری

سازمان‌های دولتی باید چهار الزام امنیتی اجباری پرسنل را داشته باشند:

۱) فرد مناسب را استخدام کنید
۲) از تناسب مداوم آنها اطمینان حاصل کنید
۳) عزیمت آنها را مدیریت کنید
۴) مجوزهای امنیت ملی را مدیریت کنید.

در مجموع، این الزامات کمک می‌کند تا اطمینان حاصل شود که دسترسی به اطلاعات و دارایی فقط به افراد مناسب داده می‌شود .به عنوان بخشی از اقدامات خوب، ما توصیه می‌کنیم که سازمانهای بخش خصوصی نیز الزامات اجباری امنیت پرسنل را اتخاذ کنند.

❖ **فرد مناسب را استخدام کنید**

اطمینان حاصل کنید که همه افرادی که برای سازمان شما کار می‌کنند (کارمندان، پیمانکاران و کارکنان موقت) که به اطلاعات و دارایی‌های دولت نیوزیلند دسترسی دارند: • هویت آنها مشخص شده است • حق کار در نیوزیلند دارند • برای دسترسی مناسب هستند • موافقت با با سیاست‌ها، استانداردها، پروتکل‌ها و الزامات دولت که از مردم، اطلاعات و دارایی‌ها در برابر آسیب محافظت می‌کند، پیروی کنید.

❖ **با فرآیندهای قوی استخدام، خطر را به حداقل برسانید**

به کارگیری یا قراردادن یک فرد مناسب در یک نقش مناسب بهترین راه برای به حداقل رساندن خطر است.

تو باید:

- خطرات امنیتی پرسنل مرتبط با هر نقش را درک کنید
- بررسی‌های قبل از استخدام / قبل از نامزدی خود را متناسب با سطح خطر نقش انجام دهید.

برای تأیید هویت، صلاحیت و توانایی شخصی که در حال استخدام یا درگیر کردن هستید، از چک‌های قبل از استخدام استفاده کنید.

❖ **انتظارات صحیح را در القای تنظیم کنید**

روند القای شما باید شامل آموزش آگاهی از امنیت باشد .افراد شما باید از ابتدا بدانند که مسئولیت‌هایشان چیست و چگونه می‌توانند به آنها پاسخ دهند.

❖ **اطمینان از مناسب بودن مداوم آنها**

از مناسب بودن مداوم همه افرادی که برای سازمان شما کار می‌کنند اطمینان حاصل کنید .این مسئولیت شامل رسیدگی به هرگونه نگرانی است که ممکن است در شایستگی شخص برای ادامه دسترسی به اطلاعات و دارایی‌های دولت تأثیر بگذارد.

تغییراتی را که می‌توانند بر مناسب بودن تأثیر بگذارند، کنترل کنید

مردم و شرایط آنها با گذشت زمان تغییر می‌کند .افرادی که در زمان استخدام خود مناسب هستند ممکن است ناامید شوند، با مشکلات مالی روبرو شوند، رفتارهای پرخطر داشته باشند یا به مرور با اقدامات امنیتی بی دقت شوند. اطمینان حاصل کنید که سیستم‌ها و رویه‌هایی را برای نظارت بر رفتار یا سایر تغییرات و رویدادهایی که می‌تواند بر افراد تأثیر بگذارد، ایجاد کرده‌اید.

❖ **تغییرات نقش را مدیریت کنید**

معمول است که افراد در یک نقش وارد یک سازمان می‌شوند و سپس با مسئولیت بیشتر و نمایه ریسک بالاتر به نقش دیگری می‌روند .عدم اتمام بررسی‌های مناسب برای نقش جدید به دلیل اینکه شخص برای سازمان "شناخته شده" است، خطر بروز مشکلات را افزایش می‌دهد. قبل از تأیید در نقش، اطمینان حاصل کنید که تمام بررسی‌های لازم قبل از استخدام و / یا بررسی‌های مناسب برای انجام کار در سطح لازم انجام شده است .

❖ **عزیمت آنها را مدیریت کنید**

عزیمت افراد را مدیریت کنید تا هرگونه خطر برای افراد، اطلاعات و دارایی‌های ناشی از افرادی که از سازمان شما خارج می‌شوند، محدود شود. این مسئولیت شامل اطمینان از بازگشت هرگونه حق دسترسی، مجوزهای امنیتی و دارایی‌ها و درک افراد از تعهدات مداوم خود است.

❖ رویکرد برنامه ریزی شده‌ای را برای عزیمت انجام دهید

هنگامی که شخصی در حال ترک است، فرصت بیشتری برای آسیب رساندن به عمد یا به طور تصادفی سازمان شما پیدا می‌کند و می‌تواند این کار را با عواقب کمتری انجام دهد .به عنوان مثال، هنگامی که شخصی شغل خود را ترک می‌کند، ممکن است احساس کند کمتر به اقدامات امنیتی محدود می‌شود .

- برای مدیریت عزیمت یک رویکرد برنامه ریزی شده را در پیش بگیرید.
- اجازه و توانایی شخص را برای دسترسی به منابع الکترونیکی، اسناد و سایتهای فیزیکی خود حذف کنید .این مرحله به ویژه در موارد ترک اجباری مهم است.
- اطمینان حاصل کنید که تمام کارتهای شناسایی و کارتهای دسترسی برگشت داده شده‌اند (از جمله هر ابزاری که امکان دسترسی از راه دور به سیستمهای اطلاعاتی را فراهم می‌کند).
- اطمینان حاصل کنید که کلیه اموال متعلق به سازمان شما پس داده شده است.
- هرگونه تعهدات مداوم در مورد افراد سازمان، اطلاعات یا دارایی‌های خود را به شخص یادآوری کنید .به ویژه درباره مالکیت معنوی یا اطلاعات رسمی به آنها یادآوری کنید.

❖ مجوزهای امنیتی ملی را مدیریت کنید

اطمینان حاصل کنید که افراد قبل از اینکه به اطلاعات، دارایی‌ها یا مکان‌های کاربری محرمانه، محرمانه و دسترسی پیدا کنند، از سطح امنیت ملی مجاز برخوردار هستند .شایستگی مداوم کلیه دارندگان مجوزهای امنیت ملی برای داشتن مجوز را مدیریت کرده و هرگونه تغییر در مورد ترخیص آنها را به NZSIS اطلاع دهید.

❖ مجوزهای امنیتی ملی را مدیریت کنید

هرکسی که نیاز به دستیابی به مطالبی دارد که به طور محافظت شده در راز محرمانه، راز یا مشخص شده است، ابتدا باید توسط رئیس اجرایی شما یا نماینده او مجوز تصویب امنیت ملی را بدست آورد. سطح پاکسازی براساس طبقه بندی امنیتی اطلاعات، دارایی‌ها یا مکان‌های کاری است که فرد برای انجام وظایف خود به آنها نیاز دارد - نه بر اساس درجه، ارشد یا وضعیت.

برای مدیریت مجوزهای امنیت ملی، سازمان شما باید:

- موقعیت‌هایی را که نیاز به دسترسی به اطلاعات، دارایی‌ها یا مکان‌های کاربری محرمانه، رازدار و TOP SECRET دارند، شناسایی، ثبت و بررسی کنید
- قبل از اعطای مجوز امنیت ملی، یک توصیه از NZSIS دریافت کنید
- قبل از اینکه به وی اجازه دسترسی دهید، از سطح صحیح ترخیص اطمینان حاصل کنید
- اطمینان از شایستگی مداوم کلیه دارندگان ترخیص برای ادامه تصدیق امنیت ملی.
- سازمان شما همچنین باید موارد زیر را به NZSIS اطلاع دهد:
- تصمیم برای اعطای یا رد مجوز امنیت ملی
- تصمیم منجر به تغییر در مجوز امنیت ملی

نگرانی‌هایی که ممکن است در شایستگی فرد برای بدست آوردن یا حفظ سطح مناسب ترخیص تأثیر بگذارد دارنده ترخیص کالا که سازمان شما را ترک می‌کند یا با شما قرارداد بسته است. برای کسب اطلاعات به مجوزهای امنیت ملی مراجعه کنید.

آیا شما امنیت پرسنل را از زمان بکارگیری وی تا زمان ترک محل کارش مدیریت می‌کنی؟

بکارگیری فرد درست و شایسته

غربالگری قبل از اشتغال، اساس و پایه امنیت فردی است

- تایید هویت، ملیت
- آزمایش جسمانی
- حق اشتغال در زلاندنو
- چک صلاحیت
- چک‌های مرجع
- چک اعتبار
- چک سابقه جرم
- چک پلیس
- اعطا مجوز امنیت کشور
- چک مواد مخدر و الکل

انتظارات درست و بجا را تعیین کنید

مهم است که تمامی افراد جدید الورود سیاست‌ها و رویه‌های عملی امنیتی شما را بشناسند. این کار درحد ممکن و پس از پیوستن به‌شما صورت‌گیرد. سازمان‌ها باید رفتارهای فرد را مورد پایش قرار دهند

- القاء سازمانی
- آگاهی‌بخشی و آموزش امنیت
- راه‌اندازی برنامه‌های مدیریتی در جایی که مخاطره فردی مورد شناس واقع شده
- راه‌اندازی برنامه‌های مدیریتی براساس
- پیشنهادات اعطای مجوز شایستگی
- توجیه‌های امنیتی معین

تغییرات قانون

حصول اطمینان از تناسب کنونی در کار

مردم و شرایط آنها طی گذشت زمان تغییر می‌کند سازمان‌ها باید رفتارهای فرد مورد پایش قرار دهندتا بتواند روی مردم در راستای کاستن از مخاطره آسیب رساندن به مردم و کسب‌وکارتان تاثیر بگذارد

- گزارش بازرسی رخداد امنیتی
- آگاهی و هشدار قطع
- قاعده‌بندسازی چک‌های پلیس زلاندنو
- چک اعتبار به شکل قاعده‌مند
- گزارش بغییر قابل ملاحظه در شرایط
- گزارش پیمان در قرارداد مشکوک
- نشانگر تهدید داخلی و مطالعه اشتغال
- توضیح مختصری از سفربین‌المللی
- گزارش شرایط تغییرات فردی
- گزارش قراردادهای مشکوک
- مدیریت دسترسی اضطراری به مواد دارای طبقه‌بندی
- تغییرات در سطح مجوز امنیت
- مرور مجوزهای امنیتی
- آموزش سالانه امنیت
- توجیهات امنیتی

خروجشان را مدیریت کنید

از مخاطرات سازمان که هنگام ترک سازمان توسط افراد واقع می‌گرددبکاهید

- ورقه‌ای عبور امنیتی را جمع کنید
- حقوق دسترسی را بگیرید
- مطمئن شوید که دارایی لازم عودت داده شد
- سند قانونی رازداری
- از پرسش سوال خارج شوید/توقف مصاحبه
- مجوز امنیتی را انتقال یا باطل نمایید
- سرویس اطلاعاتی زلاندنو را مطلع نمایید

مدیریت ریسک امنیت کارکنان

سازمان شما باید به طور مداوم توانایی خود را در مدیریت خطرات ناشی از تهدیدهای داخلی بهبود بخشد. این امر به چرخه ارزیابی خطرات امنیتی پرسنل ، مدیریت این خطرات و ارزیابی اثربخشی اقدامات امنیتی شما نیاز دارد.

رئیس اجرایی باید از اجرای موفقیت آمیز امنیت حفاظتی در آژانس خود اطمینان حاصل کند.

رئیس ارشد امنیت بر سیاست ها و اقدامات امنیتی محافظتی آژانس نظارت می کند.

۲-۴- رویکرد مبتنی بر ریسک

اجرای اقدامات امنیتی پرسنل می‌تواند پرهزینه یا مخل باشد .تدابیر امنیتی شما باید با توجه به زمینه امنیتی سازمان، تهدیدات احتمالی و اشتهای مخاطره در نظر گرفته شود.

یک رویکرد مبتنی بر ریسک برای امنیت محافظ، تضمین می‌کند که خطرات، اقدامات و سرمایه گذاری‌های امنیتی پرسنل برای خطرات سازمان شما مناسب است.

مدل ما برای مدیریت مداوم ریسک داخلی در سازمانها بر اساس سه فعالیت کلیدی است.

- خطرات امنیتی پرسنل خود را ارزیابی کنید
- خطرات امنیتی پرسنل خود را مدیریت کنید
- ارزیابی کنید که چگونه به طور مؤثر خطرات امنیتی پرسنل خود را مدیریت می‌کنید .

❖ خطرات امنیتی پرسنل خود را ارزیابی کنید

شما باید منابع بالقوه خطرات امنیتی پرسنل را که سازمان شما با آن روبرو است، نحوه بروز آنها و انواع تهدیدهای آنها را شناسایی کنید. ارزیابی ریسک شما باید نقش‌ها یا گروه‌هایی از افراد را شناسایی کند که به دلیل دسترسی به اطلاعات یا دارایی‌های حساس، ارزشمند یا طبقه بندی شده، پتانسیل بیشتری برای ایجاد آسیب دارند.

نمونه‌هایی از خطرات سازمان شما می‌تواند نشت ناخواسته، سرقت مالکیت معنوی، کلاهبرداری یا سود مجرمانه باشد. برای اطلاعات بیشتر به ارزیابی ریسک برای امنیت پرسنل بروید.

❖ خطرات امنیتی پرسنل خود را مدیریت کنید

هر مرحله از چرخه حیات پرسنل چالش‌های متفاوتی را نشان می‌دهد .شما باید از زمان شروع استخدام / تدارکات، هنگام استخدام یا تعامل شخصی و تا لحظه ترک وی - احتمالاً حتی پس از ترک کار، امنیت پرسنل را در نظر داشته باشید .اقدامات مناسبی را برای مقابله با خطرات امنیت پرسنل در هر یک از این مراحل اجرا کنید

برای مدیریت خطرات امنیتی پرسنل، باید تدابیر امنیتی را که شناسایی کرده‌اید به طور مستمر و مداوم در مورد همه افراد شاغل در سازمان خود اعمال کنید. برای کسب اطلاعات بیشتر به مدیریت Insider Risk بروید.

❖ ارزیابی کنید که چگونه به طور مؤثر خطرات خود را مدیریت می‌کنید

تهدیدهای پیش روی سازمان با گذشت زمان تغییر می‌کند .این بدان معناست که شما باید بررسی کنید که آیا درک شما از منابع خطرات امنیتی پرسنل دقیق و به روز است.

شما همچنین باید بررسی کنید که آیا ترتیبات و اقدامات امنیتی شما هنوز مؤثر و مناسب هستند .مشخص کنید چه چیزی خوب کار می‌کند و چه چیزی مناسب نیست و ترتیبات خود را متناسب با آن تنظیم کنید. برای اطلاعات بیشتر به ارزیابی امنیت پرسنل خود بروید

۳-۴- ارزیابی خطر برای امنیت پرسنل

ارزیابی خطرات مربوط به امنیت پرسنل را انجام دهید تا سازمان شما بتواند تصمیمات خوبی درباره اقدامات امنیتی لازم برای مدیریت خطرات خود اتخاذ کند.

اجرای اقدامات امنیتی صحیح پرسنل می‌تواند به شما کمک کند تا از فعالیتهای مختلف، از کلاهبرداری کارکنان گرفته تا اقدامات خشونت آمیز یا جاسوسی، پیشگیری یا جلوگیری کنید. ارزیابی ریسک به مدیران امنیتی کمک می‌کند تا با رهبران ارشد در مورد خطرات امنیتی پرسنل که سازمان شما در معرض آن است ارتباط برقرار کنند.

❖ **انجام یک ارزیابی خطر مؤثر**

فرآیند ارزیابی ریسک شما باید شما را قادر به شناسایی خطرات مرتبط با هر نقش در سازمان خود کند و همچنین کنترل‌های امنیتی که باید در هر مرحله از چرخه حیات پرسنل استفاده کنید.

برای انجام ارزیابی خطر برای امنیت پرسنل:

۱) مشخص کنید سازمان شما چه اطلاعات و دارایی‌های مهمی را در اختیار دارد.
۲) تهدیدات موجود در اطلاعات و دارایی‌های خود را شناسایی کنید (براساس نقش، قصد و توانایی کسانی که می‌توانند تهدیدها را انجام دهند).
۳) احتمال وقوع تهدیدات در سازمان خود را ارزیابی کنید.
۴) در صورت بروز تهدیدات، تأثیر سازمان خود را ارزیابی کنید.
۵) اقدامات مقابله‌ای امنیتی موجود خود را از نظر تهدیدات بررسی کنید - آیا احتمالاً مؤثر هستند؟
۶) اقدامات جدیدی را برای کاهش خطرات امنیتی خود پیشنهاد کنید (در صورت لزوم).

نتایج را در ارزیابی ریسک خود فاکتور کنید.

هر دو سال یک بار ارزیابی خطرات مربوط به امنیت پرسنل را مطابق با استانداردهای زیر موجود در استاندارد نیوزلند انجام دهید.

- ISO 31000: 2018مدیریت ریسک - دستورالعمل‌ها
- HB 167: 2006 -مدیریت ریسک امنیتی - کتاب راهنما

۴-۴- ایجاد فرهنگ امنیتی

همه افراد سازمان به فرهنگ امنیتی آن کمک می‌کنند .فرهنگ سازمانی تأثیر مستقیمی بر امنیت دارد .اگر مردم نگرش ضعیفی نسبت به امنیت داشته باشند، حتی با بهترین فرایندها و ابزارهای امنیتی، سازمان شما همچنان در معرض خطر خواهد بود.

مراحل زیر به ایجاد یک فرهنگ امنیتی مثبت و پایدار و کاهش خطرات امنیتی پرسنل در سازمان شما کمک می‌کند.

❖ **از بالا تعهد بگیرید**

مدیر ارشد اجرایی و تیم ارشد باید متعهد به اقدامات و روشهای امنیتی مثر باشند .آن‌ها همچنین باید بهترین اقدامات را در سازمان سازمان دهند.

❖ **آگاهی امنیتی ایجاد کنید**

اگر مردم خطرات امنیتی قابل اعتمادی را که سازمان شما با آن روبرو است، درک کنند، بسیار بیشتر درگیر فرهنگ امنیتی شما می‌شوند .افزایش آگاهی به مردم کمک می‌کند درک کنند که آنها مسئولیت‌های امنیتی مهمی دارند و می‌دانند این مسئولیت‌ها چیست.

❖ **در مورد امنیت ارتباطات شفاف منتشر کنید**

همه به سیاست‌ها و رویه‌های روشنی نیاز دارند که:

- دلایل دستورالعمل‌های امنیتی سازمان خود را توضیح دهید
- رئوس مطالبات قانونی، نظارتی و انطباق
- اطمینان حاصل کنید که مردم مسئولیت‌های خود را درک می‌کنند.

❖ **رفاه کارکنان پشتیبانی**

از جمله برنامه محرمانه کمک به کارمندان، امکان پشتیبانی را برای افراد فراهم کنید .قبل از اینکه به یک مشکل جدی تبدیل شوند، آن‌ها را تشویق کنید که مسائل شخصی را گزارش و رسیدگی کنند.

❖ **رفتارهای نگران کننده را مدیریت کنید**

مدیران برای شناسایی، پشتیبانی و مدیریت افرادی که رفتارهای نگران کننده‌ای از آنها را برای انجام امنیت، عملکرد ضعیف یا رفتار غیرقابل قبول نشان می‌دهند، به ابزارها و سیاست‌هایی نیاز دارند.

❖ **از فرهنگ سرزنش پرهیز کنید**

افرادی که نگرانی‌های قانونی امنیتی را مطرح می‌کنند باید تشویق شوند و به عنوان یک شهروند خوب شرکتی دیده شوند تا مشکل ساز.
گزارش نگرانی‌های جدید یا گمشدن های نزدیک باید به عنوان راهی برای کمک به همکارانی که ممکن است در معرض خطر باشند، تلقی شود نه اینکه آنها را دچار مشکل کند.

۵-۴- خطراتی را که افراد برای سازمان شما به وجود می‌آورند درک کنید

اگرچه اغلب گفته می‌شود که مردم بزرگترین سرمایه یک سازمان هستند، اما همچنین می‌تواند یک نقطه ضعف باشد. تهدیدهای داخلی از طرف کارمندان گذشته، یا حال حاضر، پیمانکاران یا شرکای تجاری ما ناشی می‌شود .آن‌ها می‌توانند از دانش درونی خود سو استفاده کنند و یا به صدمه به مردم، مشتریان، دارایی یا اعتبار ما آسیب برسانند.

"تهدید داخلی" یا "خودی"، هر شخصی است که از دسترسی قانونی خود به دارایی‌های یک سازمان برای آسیب رساندن به امنیت سازمان خود یا نیوزیلند، خواسته یا ناخواسته، از طریق جاسوسی، تروریسم، سو استفاده یا قصد بهره برداری از آنها را دارد. افشای غیرمجاز اطلاعات یا از بین رفتن یا تخریب یک منبع (یا قابلیت). مطالعات نشان داده است که بیشتر افراد داخلی که امنیت را زیر پا می‌گذارند، هنگام شروع به کار، قصد سو icious‌قصد ندارند .در عوض، ممکن است شل شوند و یا به عنوان واکنشی نسبت به وقایع بعدی "بد" شوند.

❖ **روش‌های رایج ممکن است یک فرد داخلی امنیت را نقض کند**

اقدامات خودی مشترک می‌تواند شامل موارد زیر باشد:

- افشای غیرمجاز اطلاعات رسمی، خصوصی یا انحصاری
- کلاهبرداری یا پردازش فساد
- دسترسی غیرمجاز به سیستمهایICT
- جاسوسی اقتصادی یا صنعتی
- سرقت، خشونت یا آسیب جسمی به دیگران.

❖ **دلایل رایج ممکن است یک فرد داخلی امنیت را نقض کند**

انگیزه خودی اغلب به دلیل ترکیبی از عوامل و فشارها است، مانند:

- انتقام از کارفرما یا همکاران
- عدم اطمینان در مورد ادامه کار آنها
- طمع یا سود مالی
- ایدئولوژی سیاسی یا مذهبی
- ایگو یا بدنامی
- اجبار، سو استفاده یا سو استفاده از طرف شخص ثالث خارجی.

هنگامی که موارد داخلی مورد بررسی قرار می‌گیرند، کشف الگویی از رفتارهای گذشته در مورد امنیت نادر نیست .در برخی موارد، افراد مورد توجه مدیران قبلی قرار گرفته‌اند.

❖ **نقض امنیت ناخواسته**

نقض امنیت ناخواسته یا قصورهای نزدیک می‌تواند ناشی از موارد زیر باشد:

- عدم آگاهی یا توجه به اقدامات امنیتی
- حواس پرتی بودن
- بامزه بودن
- گول خوردن کمک ناخواسته به شخص ثالث (مهندسی اجتماعی).

۶-۴- چرا امنیت پرسنل اهمیت دارد

امنیت پرسنل از طریق پشتیبانی سازمان، از افراد، اطلاعات و دارایی شما محافظت می‌کند:

- خطر آسیب رساندن به مردم، مشتریان و شرکای خود را کاهش دهید
- خطر از بین رفتن، آسیب دیدن یا به خطر افتادن اطلاعات یا دارایی‌های خود را کاهش دهید
- به افرادی که به اطلاعات و دارایی‌های رسمی یا مهم شما دسترسی دارند اعتماد بیشتری داشته باشید
- ارائه خدمات و کار موثرتر

تهدیدهای داخلی از طرف کارمندان گذشته، یا حال حاضر، پیمانکاران یا شرکای تجاری ما ناشی می‌شود .آن‌ها می‌توانند از دانش درونی خود سو استفاده کنند و یا به صدمه به مردم، مشتریان، دارایی یا اعتبار ما آسیب برسانند .تمرکز امنیت کارکنان بر کاهش خطرات مرتبط با تهدیدات داخلی است.

"تهدید داخلی" یا "خودی"، هر شخصی است که از دسترسی قانونی خود به دارایی‌های یک سازمان برای آسیب رساندن به امنیت سازمان خود یا نیوزیلند، خواسته یا ناخواسته، از طریق جاسوسی، تروریسم، سو استفاده یا قصد بهره برداری از آنها را دارد. افشای غیرمجاز اطلاعات یا از بین رفتن یا تخریب یک منبع (یا قابلیت).

اقدامات خودی مشترک شامل موارد زیر است:

- افشای غیرمجاز اطلاعات رسمی، خصوصی یا انحصاری
- کلاهبرداری یا پردازش فساد
- دسترسی غیرمجاز به سیستمهایICT

- جاسوسی اقتصادی یا صنعتی
- سرقت
- خشونت یا آسیب جسمی به دیگران.

بسیاری از نقض‌های امنیتی ناخواسته است و ناشی از عدم آگاهی یا توجه به اقدامات امنیتی، حواس پرتی یا فریب خوردن کمک ناخواسته به شخص ثالث است.

۴-۶-۱- فرد مناسب را استخدام کنید

بررسی‌های قبل از استخدام پایه و اساس امنیت خوب پرسنل است .آن‌ها خطر آسیب رساندن شخص معتمد به سازمان یا تجارت شما را کاهش می‌دهند.

- چک‌های قبل از استخدام به شما اجازه می‌دهد:
- هویت، واجد شرایط بودن، شایستگی و توانایی شخصی را که درحال استخدام هستید تأیید کنید

دریابید که آیا یک متقاضی اطلاعات مهم را پنهان کرده است یا خود را اشتباه معرفی کرده است.

بررسی‌های قبل از استخدام را در مورد افرادی که در نظر دارید استخدام کنید انجام دهید، از جمله تغییر نقش در کارمندان فعلی، پیمانکاران، کارکنان کوتاه مدت و افراد دیگری .به دلیل سابقه کار یا سابقه کار فرد از چک‌های قبل از استخدام صرف نظر نکنید.

❖ **فرد مناسب را استخدام کنید**

اطمینان حاصل کنید که همه افرادی که برای سازمان شما کار می‌کنند (کارمندان، پیمانکاران و کارکنان موقت) که به اطلاعات و دارایی‌های دولت نیوزیلند دسترسی دارند: • هویت آنها مشخص شده است • حق کار در نیوزیلند دارند • برای دسترسی مناسب هستند • موافقت با با سیاست‌ها، استانداردها، پروتکل‌ها و الزامات دولت که از مردم، اطلاعات و دارایی‌ها در برابر آسیب محافظت می‌کند، پیروی کنید.

❖ **بررسی‌های صحیح قبل از استخدام را انجام دهید**

سه نوع چک اصلی قبل از استخدام عبارتند از:

- بررسی‌های پایه‌ای که باید برای همه نقش‌ها انجام دهید
- چک‌های اختیاری برای استفاده در هنگام شناسایی افزایش خطر امنیتی
- بررسی‌های اجباری دارندگان مجوزهای امنیت ملی.

برخی از سازمان‌ها ممکن است به دلیل ماهیت کار خود، بررسی‌های پایه بیشتری داشته باشند .به عنوان مثال، بررسی پلیس برای نقش در سازمان‌هایی که خدمات را برای کودکان ارائه می‌دهند اجباری است. بررسی‌های اساسی برای همه نقش‌ها انجام دهید

❖ **شما باید چک‌های قبل از استخدام زیر را برای هر شخص انجام دهید.**

- هویت آنها را تأیید کنید
- ملیت آنها را تأیید کنید
- حق کار در نیوزیلند را تأیید کنید
- منابع آنها را با کارفرمای قبلی خود بررسی کنید

- بررسی سوابق کیفری را انجام دهید.

می‌توانید چک‌های قبل از استخدام خود را انجام دهید یا شخص ثالثی مانند آژانس استخدام را بخواهید که همه یا بعضی از آنها را برای شما انجام دهد.

به یاد داشته باشید که ابتدا رضایت متقاضی را جلب کنید .طبق قانون حریم خصوصی، قبل از اینکه شما یا شخص ثالث اطلاعات را از داوران یا منابع دیگر جمع آوری کنید، باید کتباً رضایت بگیرید .همچنین باید به برنامه بگویید که چگونه از اطلاعات جمع آوری شده استفاده خواهید کرد.

اگر از شخص ثالثی استفاده می‌کنید، مطمئن شوید که در مورد بررسی‌های آنها و با چه استانداردی کاملاً شفاف هستید .خوب است که درخواست کنید:

- تأیید آنها بررسی‌های درخواستی شما را انجام داده‌اند
- کپی چک‌های مرجع

❖ **هویت آنها را تأیید کنید**

شما باید بررسی کنید که افراد همان کسانی هستند که می گویند هستند .برای تأیید هویت شخصی، بخواهید یک سند اصلی مانند گذرنامه یا شناسنامه وی را ببینید.

توجه داشته باشید که:

- برخی از افراد ممکن است نام مستعار داشته باشند (به عنوان مثال، نام خانوادگی قبلی)
- برخی افراد ممکن است با نام کوچک شناخته شوند
- قراردادهای نامگذاری بین فرهنگ‌ها متفاوت است.

اگر در مستندات هویت فردی اختلاف غیرقابل توجیهی یافتید، از تیم منابع انسانی خود راهنمایی بخواهید.

❖ **شواهد استاندارد هویت را برآورده کنید**

هنگامی که مشغول بررسی هویت هستید، باید استاندارد شواهد تعیین شده توسط وزارت امور داخلی (DIA) را داشته باشید.

- شواهد استاندارد هویت
- DIAمشاوره مفیدی در مورد بررسی و تأیید اسناد هویتی، مانند شناسنامه و گذرنامه ارائه می‌دهد.
- برای بررسی شواهد اسناد هویتی ، برگه های اطلاعات DIA را مشاهده کنید

❖ **ملیت آنها را تأیید کنید**

تأیید ملیت شخص از اهمیت بسزایی برخوردار است زیرا ممکن است بر روی اطلاعات، دارایی‌ها و مکان کار وی تأثیر بگذارد.

محدودیت های دسترسی اتباع خارجی را درک کنید

❖ **حق کار در نیوزیلند را تأیید کنید**

اگر فردی را برای کار در سازمان خود در نیوزلند استخدام می‌کنید، مطمئن شوید که وی یا شهروند نیوزلند باشد یا نوع ویزای مناسبی برای کار در نیوزیلند را داشته باشد.

- اطلاعات مربوط به انواع تابعیت را در govt.nz مشاهده کنید

برای افرادی که شهروند نیوزلند نیستند، بررسی کنید که کدام ویزا را دارند و آیا شرایط ویزا به آنها اجازه می‌دهد کار مورد نظر خود را انجام دهند.

- با استفاده از VisaView Immigration NZ ویزای متقاضی خود را بررسی کنید

❖ **اگر برای پست خارج از کشور استخدام می‌کنید**

اگر فردی را برای کار در سازمان خود در یک مکان خارج از کشور استخدام می‌کنید، بررسی کنید که وی حق کار در آن کشور را دارد .به عنوان مثال، اگر سازمان شما در چین دفتر دارد و باید فردی را برای کار در آنجا استخدام کنید، تأیید کنید که فرد واجد شرایط کار در چین است.

برای مشاوره برای کمک به شما در تأیید صلاحیت کار، با سفارت مربوطه تماس بگیرید.

- اطلاعات تماس با سفارتخانه ها را از وزارت امور خارجه و تجارت دریافت کنید

❖ **منابع آنها را با کارفرمای قبلی خود بررسی کنید**

نحوه عملکرد و رفتار یک فرد در گذشته، نشانگر خوبی برای عملکرد و رفتار آینده اوست .بررسی کامل منابع به شما فرصتی می‌دهد:

- بررسی کنید که شخص می‌تواند آنچه را که می گویند انجام دهد
- از شخصیت فرد بینشی کسب کنید.
- بررسی کنید هر داوری وجود دارد:
- اخیر (از آخرین کارفرمای خود)
- مناسب برای نقش
- از یک منبع قانونی (در صورت لزوم در این مورد از تیم منابع انسانی خود کمک بخواهید)

فارغ از هرگونه تعارض منافع (مانند ارتباط نزدیک شخصی با متقاضی).

یادداشت برداری دقیق از هر چک لفظی، مانند مکالمه تلفنی، روش خوبی است .یادداشت‌های خود را برای مراجعه در آینده ثبت کنید.

اگر پس از بررسی منابع، نگرانی دارید، انجام برخی از چک‌های اختیاری قبل از استخدام را نیز در نظر بگیرید.

❖ **در حال بررسی منابع از خارج از کشور**

بررسی منابع خارج از کشور دشوارتر است اما هنوز باید آنها را تا آنجا که می‌توانید دقیق بررسی کنید.

❖ **بررسی سوابق کیفری را انجام دهید**

بررسی سوابق کیفری به شما کمک می‌کند تا موارد زیر را شناسایی کنید:

- محکومیت‌های جنایی که ممکن است شخص را برای این نقش نامناسب کند
- اقداماتی که برای تصمیم گیری در صورت تصمیم گیری برای استخدام شخص ممکن است در محل انجام شود.

قبل از اقدام به بررسی سوابق کیفری، باید رضایت نامه شخص را داشته باشید .همچنین باید تعهدات خود را به عنوان یک کارفرما درک کنید.

- در مورد تعهدات خود با چک سوابق کیفری از Employment NZ اطلاعات کسب کنید

اگر نگران نتایج بررسی سوابق کیفری هستید، برخی از چک‌های اختیاری قبل از استخدام ممکن است به شما کمک کند تا تصویر واضح‌تری از قابلیت اطمینان و مناسب بودن شخص بدست آورید.

❖ گرفتن چک سوابق کیفری در نیوزیلند

در نیوزیلند، وزارت دادگستری بررسی سوابق کیفری را انجام می‌دهد .این حداقل شرط بررسی سوابق کیفری است .اطلاعات دقیق‌تر از طریق بررسی پلیس در دسترس است .سیاست‌ها و رویه‌های سازمان شما باید تعیین کند که چه چک را درخواست می‌کنید.

برای بررسی سوابق کیفری از وزارت دادگستری اقدام کنید

❖ بررسی سوابق کیفری وزارت دادگستری در مقابل بررسی پلیس

بررسی سوابق کیفری وزارت دادگستری فقط شامل محکومیت‌ها می‌شود .بررسی پلیس همچنین می‌تواند شامل اطلاعاتی در مورد هر گونه تماس شخصی با پلیس باشد از جمله:

❖ اتهامات فعال و قرار بازداشت

هرگونه تعامل شخص با پلیسNZ ، از جمله حوادث خشونت خانوادگی و تحقیقات که منجر به محکومیت نشده است

اطلاعات منوط به سرکوب نام در مواردی که اطلاعات برای اهداف بررسی لازم است.

در صورت درخواست مستقیم سوابق کیفری وزارت دادگستری، در حال حاضر رایگان است .در حال حاضر بررسی پلیس ۸،۵۰ دلار به علاوه GST هزینه دارد.

❖ گرفتن چک سوابق کیفری در خارج از کشور

هنگامی که برای افرادی که مقیم خارج از کشور یا مهاجران اخیر هستند، چک‌های قبل از استخدام را انجام می‌دهید، بررسی کنید که آیا شما نیاز به بررسی سابقه کیفری در خارج از کشور دارید. توجه داشته باشید که قوانین مربوط به درخواست سوابق کیفری با توجه به کشورها، و گاهی نیز با ایالت یا سرزمین متفاوت است.

برای مشاوره مفید، راهنمای زیر را از مرکز حمایت از زیرساخت‌های ملی انگلستان مشاهده کنید.

- نحوه دستیابی به بررسی سوابق کیفری در خارج از کشور: راهنمای مرجع سریع

در بعضی جاها، فقط شخصی که سابقه کیفری به آن تعلق دارد می‌تواند برای سوابق خود درخواست کند .در این شرایط، می‌توانید از شخص بخواهید که پرونده خود را درخواست کند و یک نسخه معتبر از آن را به شما بدهد.

❖ مراقب علائم هشدار دهنده باشید

عواملی که به تنهایی یا با هم باعث ایجاد نگرانی در مورد صداقت و مناسب بودن شخص برای کار در سازمان شما می‌شوند، عبارتند از:

- هرگونه درگیری فعلی با فعالیت مجرمانه
- نگهداری اطلاعات در مورد محکومیت‌های کیفری که در قانون سوابق کیفری (Clean Slate) قانون ۲۰۰۴ شامل نمی‌شود
- اظهارات نادرست در CV یا فرم درخواست شغل

- ادعاهای دروغین در مورد شرایط یا دستاوردها
- خلأ های غیر قابل توجیه در سابقه اشتغال یا اقامت متقاضی
- منابع شخصیت نامطلوب
- تضاد علاقه
- رفتار طفره رفتن وقتی از آنها خواسته می‌شود اطلاعاتی را که ارائه داده‌اند تأیید کنند
- رفتار طفره رفتن یا امتناع در هنگام درخواست مرجع یا رضایت برای چک سوابق کیفری یا چک اعتباری.
- حضور در شبکه‌های اجتماعی.

❖ **برای کاهش خطرات شناسایی شده از چک‌های اختیاری استفاده کنید**

هنگامی که خطر امنیتی بیشتری را با نقشی یا ماهیت کار سازمان خود تشخیص می‌دهید، بررسی‌های اضافی لازم است .به عنوان مثال، برای یک مدیر فناوری اطلاعات که دسترسی گسترده‌ای به اطلاعات سازمان شما دارد، ممکن است بخواهید اقدامات بیشتری برای اطمینان از قابل اعتماد بودن آنها انجام دهید. بررسی‌های اضافی که اعمال می‌کنید به عوامل مختلفی از جمله زمینه امنیتی و فرهنگ سازمان شما و محیط کار بستگی دارد.

❖ **تست روان سنجی**

برای آزمایش توانایی‌ها و ویژگی‌های مختلف شخصیتی می‌توانید از تست روان سنجی استفاده کنید .این نوع آزمایش می‌تواند در شرایط زیر مفید باشد:

- شما نگران نتایج حاصل از بررسی‌های اولیه قبل از استخدام هستید
- ارزیابی اینکه کسی توانایی‌ها و ویژگی‌های لازم برای این نقش را دارد دشوار است.
- در مورد آزمایش روان سنجی در وب سایت Employment NZ بیشتر بدانید

❖ **بررسی صلاحیت**

برای کمک به سازمان خود در یافتن صلاحیت مدارک تحصیلی، عضویت در ارگان‌های حرفه‌ای یا گواهینامه‌های تمرین ذکر شده درCV ، از یک بررسی صلاحیت استفاده کنید. اگر صلاحیت برای این کار بسیار مهم است، اجتناب از انجام این چک را برای جلوگیری از آسیب جدی به سازمان خود در نظر بگیرید.

مطمئن شوید که اسناد اصلی را به جای کپی مشاهده می‌کنید .اگر از اصل بودن مدارک مطمئن نیستید، برای تأیید صلاحیت با موسسه آموزشی یا نهاد حرفه‌ای تماس بگیرید.

❖ **بررسی ثبت نام‌های شغلی**

وب سایت Immigration NZ مشاغلی را که نیاز به ثبت در نیوزلند دارند و مشخصات تماس مقاماتی را که می‌توانند ثبت نام یک شخص را تأیید کنند، ذکر کرده است.

- شرایط ثبت نام شغلی را در وب سایت Immigration NZ بررسی کنید

❖ **بررسی صلاحیت‌های دانشگاه**

بعضی از دانشگاه‌ها پایگاه داده‌های تحصیلات تکمیلی خود را به صورت آنلاین در دسترس قرار می‌دهند تا بتوانید نام شخص را جستجو کنید و بررسی کنید چه مدرکی را کسب کرده و چه زمانی .

❖ بررسی صلاحیت‌های خارج از کشور

می‌توانید از سازمان صلاحیت‌های نیوزیلند (NZQA) بخواهید بررسی کنند که آیا صلاحیت از خارج از کشور در نیوزلند شناخته شده است یا قابل مقایسه با صلاحیت نیوزلند است .این سرویس دارای هزینه است و حدود ۲۵ روز کاری به طول می‌انجامد.

درباره خدمات NZQA برای تشخیص صلاحیت های خارج از کشور بیشتر بیاموزید

❖ چک اعتباری

چک اعتباری یک چک تجاری از سوابق عمومی مرتبط با سابقه مالی متقاضی و هرگونه ارتباط با مشاغل است. اگر این نقش دارای یک خطر مالی قابل توجه است یا اینکه یک شخص تفویض مالی می‌کند، باید یک بررسی اعتبار انجام دهید .ابتدا رضایت شخص را جلب کنید. توجه داشته باشید که نتایج چک‌های اعتباری می‌تواند ذهنی باشد .مطمئن شوید که شما:

- یک فرد با تجربه مناسب را برای بررسی نتایج بدست آورید
- خط مشی‌ها و فرایندهایی را برای رسیدگی به هر سوالی که چک ارائه می‌دهد داشته باشید.
- به یاد داشته باشید که براساس قانون سوابق کیفری (Clean Slate) قانون ۲۰۰۴، اگر فرد دوره توانبخشی را به اتمام رسانده باشد (۷ سال بدون محکومیت کیفری)، برخی از جرائم جزئی در چک اعتباری نشان داده نمی‌شوند.
- ورشکستگی ۴ سال پس از ترخیص شخص از سوابق حذف می‌شود.

❖ بررسی پلیس

بررسی پلیس بیش از محکومیت‌ها است .همچنین این موارد را بررسی می‌کند:

- اتهامات فعال و قرار بازداشت

هرگونه تعامل شخص با پلیسNZ ، از جمله حوادث خشونت خانوادگی و تحقیقات که منجر به محکومیت نمی‌شود اطلاعات منوط به سرکوب نام در مواردی که اطلاعات برای اهداف بررسی لازم است. بر اساس قانون کودکان آسیب پذیر ۲۰۱۴، متقاضیان برای برخی از نقش‌ها باید از طریق بازرسی پلیس وارد شوند.

- شرایط قانون کودکان را برای بررسی ایمنی درک کنید

در شرایط دیگر، بررسی پلیس ممکن است اطمینان بیشتری در مورد مناسب بودن شخص برای یک نقش به شما بدهد. قبل از اقدام به بازرسی پلیس، اطمینان حاصل کنید که رضایت شخص را به صورت کتبی دریافت کرده و تعهدات خود را به عنوان کارفرما دنبال کنید.

- درباره تعهدات خود با بررسی سوابق کیفری در وب سایت Employment NZ اطلاعات کسب کنید

❖ درخواست بررسی پلیس

برای درخواست بازرسی پلیس، سازمان شما باید در اداره بازرسی پلیس ثبت شود.

- درخواست بازرسی پلیس

❖ درخواست چک سابقه کیفری استرالیا

اگر سازمان شما برای بررسی پلیس NZ ثبت شده است، می‌توانید از خدمات بررسی سابقه کیفری استرالیا درخواست کنید.

- از پلیس NZ درخواست بررسی تاریخچه پلیس ملی استرالیا کنید

❖ **بررسی مواد مخدر و الکل**

این ممکن است بخشی از سیاست سازمان شما باشد که آزمایش مواد مخدر و الکل برای نقشهایی را انجام می‌دهد:

- شامل کار در مناطق حساس به ایمنی است
- به طور مستقیم بر ایمنی افراد دیگر تأثیر می‌گذارد.

شما همچنین می‌توانید تصمیم بگیرید که این بررسی‌ها زمانی مناسب است که بررسی‌های پایه نشان می‌دهد شخصی ممکن است در مصرف مواد مخدر یا الکل مشکلی داشته باشد.

قبل از تصمیم گیری برای انجام آزمایش مواد مخدر و الکل، به عنوان قوانین حریم خصوصی و استخدام، مشاوره حقوقی دریافت کنید

- راهنمایی در مورد مواد مخدر ، الکل و کار را از Employment NZ مشاهده کنید

❖ **برای دارندگان تصویب امنیت ملی بررسی‌های اجباری انجام دهید**

روند تأیید برای افرادی که نیاز به مجوز امنیت ملی دارند شامل بررسی‌های اجباری است و توسط سرویس اطلاعات امنیتی نیوزلند (NZSIS) انجام می‌شود.

قبل از اتمام مراحل بررسی، در مورد به کارگیری یک فرد محتاط باشید تا از مشکلات احتمالی اشتغال جلوگیری کنید .

❖ **راهنمایی بیشتر**

- استخدام و مدیریت دارندگان مجوزهای امنیت ملی

❖ **هرگونه نگرانی از چک‌های قبل از استخدام را برطرف کنید**

اگر نگرانی ناشی از چک‌های قبل از استخدام دارید، باید:

ارزیابی کنید که چگونه خطرات ممکن است بر نقشی که فرد ممکن است برای آن کار کند تأثیر بگذارد

بررسی کنید که آیا می‌توانید خطرات را به یک سطح قابل قبول و قابل کنترل کاهش دهید.

❖ **نمونه سناریوها**

❖ **صلاحیت تأیید نمی‌شود**

شما نمی‌توانید صلاحیت لازم برای یک نقش را تأیید کنید، بنابراین تصمیم می‌گیرید که خطر بسیار زیاد باشد و آن شخص را رد کنید.

❖ **چک اعتباری بدهی اندکی را نشان می‌دهد**

یک چک اعتباری بدهی کمی از سالها قبل را نشان می‌دهد، اما این نقش شامل مدیریت امور مالی نیست، بنابراین شما تصمیم می‌گیرید که استخدام شخص ایمن باشد (با فرض اینکه از نتیجه چک‌های دیگر خود راضی هستید).

❖ **آنچه را کشف می‌کنید ضبط کنید**

به یاد داشته باشید که همه را ضبط کنید:

- نگرانی‌هایی که در چک‌های قبل از استخدام پیش می‌آید
- ارزیابی خطر شما انجام می‌شود

- تصمیماتی که برای کاهش یا مدیریت خطرات می‌گیرید.

❖ **در صورت لزوم برنامه مدیریت ریسک ایجاد کنید**

اگر فردی را با ریسک‌های مشخص استخدام کردید، با او همکاری کنید تا یک برنامه مدیریت ریسک منفرد ایجاد کنید .از این طرح برای حمایت از شخص در کار خود، درمان خطرات و حفظ امنیت سازمان خود استفاده کنید.

۴-۶-۲-انتظارات درستی را تعیین کنید

در مورد امنیت انتظارات مشخصی را تعیین کنید .کارمندان جدید، کارمندان در حال تغییر نقش و پیمانکاران، باید سیاست‌های امنیتی و اقدامات شما را در اسرع وقت پس از عضویت در سازمان خود درک کنند.

❖ **فعالیت‌های پایه برای تعیین انتظارات درست**

یک القا به سازمان خود، از جمله ارزش‌های خود، آیین نامه رفتار، اقدامات بهداشتی و ایمنی و انتظارات امنیتی انجام دهید . آموزش آگاهی از امنیت متناسب با خطرات امنیتی سازمان خود و همچنین خطرات شناسایی شده برای نقشهای فردی را ارائه دهید .اطمینان حاصل کنید که همه از مسئولیت‌های خود در زمینه امنیت آگاه هستند.

❖ **فعالیت‌های اختیاری را باید در نظر گرفت**

اگر فردی که استخدام می‌کنید دارای خطرات امنیتی خاص است، یک برنامه مدیریت خطر شخصی ایجاد کنید .از این طرح برای حمایت از کارمند در کار خود، درمان خطرات و حفظ امنیت سازمان خود استفاده کنید.

❖ **فعالیت‌هایی برای دارندگان ترخیص امنیت ملی**

برای کارکنانی که مجوز تأمین امنیت ملی را دریافت می‌کنند، باید یک خلاصه امنیت ارائه دهید .برای کمک به آنها در درک مسئولیت‌های خود از جلسات توجیهی استفاده کنید، بنابراین آن‌ها می‌توانند اطلاعات خود را حفظ کنند و اطلاعات و دارایی شما را ایمن نگه دارند. اگر به یک کارمند با شرایط (صلاحیت) ترخیص داده شود، شما باید یک طرح مدیریت ریسک برای رسیدگی به این مدارک تهیه کنید.

۴-۶-۳-از تناسب مداوم آنها اطمینان حاصل کنید

بررسی‌های مؤثر قبل از استخدام خطر تهدیدات برای افراد، اطلاعات و دارایی‌های شما را کاهش می‌دهد .با این حال، افراد و شرایط آن‌ها می‌تواند تغییر کند .تغییرات می‌توانند در طول زمان یا به طور ناگهانی به عنوان واکنش به یک واقعه اتفاق بیفتند. سازمان شما باید اطمینان حاصل کند که افراد برای دسترسی به اطلاعات و دارایی‌های شما مناسب هستند.

❖ **اطمینان از مناسب بودن مداوم آنها**

از مناسب بودن مداوم همه افرادی که برای سازمان شما کار می‌کنند اطمینان حاصل کنید .این مسئولیت شامل رسیدگی به هرگونه نگرانی است که ممکن است در شایستگی شخص برای ادامه دسترسی به اطلاعات و دارایی‌های دولت تأثیر بگذارد.

از آنجا که افراد و شرایط آن‌ها می‌توانند با گذشت زمان تغییر کنند، شما باید تغییرات و حوادثی را که می‌تواند بر افراد تأثیر بگذارد کنترل کنید. آموزش امنیت در حال انجام به شما کمک می‌کند تا افراد، اطلاعات و دارایی‌های شما از آسیب در امان باشند.

❖ **حداقل اطمینان را برای اطمینان از مناسب بودن مداوم انجام دهید**

حداقل، سازمان شما باید:

- فرایندی برای گزارش دهی افراد در مورد حوادث امنیتی و قصورهای نزدیک داشته باشید
- حوادث امنیتی را بررسی کنید
- به روز رسانی و آموزش آگاهی از امنیت مداوم را ارائه دهید.

❖ گزارش و پاسخگویی به حوادث امنیتی

شما باید سیستمی برای گزارش دادن و پاسخگویی به حوادث احتمالی و واقعی امنیتی داشته باشید .مدیریت حوادث به سازمان شما کمک می‌کند تا:

- حاوی اثرات
- عواقب را مدیریت کنید
- در اسرع وقت بهبود یابد
- از آنچه اتفاق می افتد بیاموزید.

حداقل شما باید:

- یک روش رسمی گزارش و پاسخگویی به حوادث امنیتی ایجاد کنید
- کلیه موارد امنیتی پرسنل را به افراد مناسب سازمان خود گزارش دهید
- هرکسی را از مسئولیت‌های خود و روش گزارش دهی حوادث امنیتی آگاه سازید.

ارتباط خوب بین مدیران و کارکنان، همراه با انتظارات و رویه‌های امنیتی روشن، ایجاد نگرانی در افراد و گزارش تغییرات و حوادث را برای افراد آسان می‌کند. مدیران و همکاران در بهترین وضعیت برای مشاهده تغییر در رفتار یا نگرش فرد قرار دارند .افراد خود را تشویق کنید آنچه را که مشاهده می‌کنند گزارش دهند و انجام این کار را به صورت محرمانه برای آنها آسان کند.

❖ راهنمایی بیشتر

- گزارش حوادث و انجام تحقیقات امنیتی
- به روز رسانی و آموزش آگاهی از امنیت مداوم را ارائه دهید

آموزش امنیت در حال انجام به امنیت و امنیت افراد، اطلاعات و دارایی شما کمک می‌کند .همچنین فرهنگ امنیتی شما را ارتقا می‌بخشد .وقتی درک مردم خود را از اقدامات و فرآیندهای امنیتی افزایش می‌دهید، "فاکتور مراقبت" آن‌ها و "فاکتور انجام" آن‌ها را افزایش می‌دهید - امنیت به عهده همه است.

❖ بررسی‌های مستمر اضافی را برای نقش‌های بیشتر انجام دهید

هنگامی که یک خطر امنیتی افزایش یافته مربوط به نقشی یا ماهیت کار سازمان خود را شناسایی می‌کنید، بررسی‌های مداوم اضافی لازم است .بررسی‌هایی که انجام می‌دهید به عوامل مختلفی از جمله زمینه و فرهنگ امنیتی سازمان شما و محیط کار بستگی دارد.

❖ بررسی برای در نظر گرفتن

بررسی‌های اضافی که می‌توانید برای اطمینان از مناسب بودن مداوم در نظر بگیرید شامل موارد زیر است:

- الزام مردم به گزارش هرگونه تغییر قابل توجه در شرایط شخصی (به عنوان مثال، طلاق، شریک جدید، ورشکستگی، تابعیت خارجی، یا بدهی جدید و قابل توجه)
- مردم را ملزم می‌کند که هر گونه تماس مشکوک را گزارش دهند
- تشویق مردم به گزارش هر گونه سو ظن در مورد "تهدید داخلی"
- انجام یک نظرسنجی نامزدی برای درک میزان رضایت و اشتیاق افراد شما
- توجیه مردم در مورد خطرات مربوط به سفرهای بین المللی
- نیاز به بررسی منظم پلیس دارد
- انجام چک‌های مالی یا اعتباری منظم
- نیاز به آزمایش مواد مخدر و الکل دارد
- بررسی منظم تضاد منافع
- گرفتن کپی از گواهینامه‌های تمرین سالانه.

❖ **تغییرات قابل توجه در شرایط شخصی را گزارش دهید**

تغییرات قابل توجهی در شرایط شخصی می‌تواند از زمینه‌های مختلف ناشی شود: روابط، امور مالی، سلامتی، مسائل کاری، سو مصرف مواد، یا علایق و ارتباطات جدید. این تغییرات می‌تواند افراد را تحت فشار قرار دهد .آن‌ها می‌توانند غیر منطقی یا نامناسب عمل کنند، یا در معرض سو استفاده دیگران قرار بگیرند.

گزارش تغییرات قابل توجه در شرایط به شما کمک می‌کند تا خطر شخصی را مدیریت کنید:

- امنیت خود را عمداً یا ناخواسته نقض کنید
- توسط یک طرف خارجی مجبور به نقض امنیت شما می‌شود.

افراد شما باید بدانند که کدام تغییرات در شرایط را باید گزارش دهند و به چه کسانی گزارش دهند .اگر مطمئن نیستید که تغییرات قابل توجهی باید گزارش شود، با منابع انسانی و تیم‌های امنیتی خود مشورت کنید.

❖ **تماس یا رفتار مشکوک را گزارش دهید**

مقامات خارجی، سرویس‌های اطلاعاتی خارجی و گروه‌های تجاری، سیاسی یا انگیزه دهنده مسائل می‌توانند انرژی قابل توجهی را برای دستیابی به اطلاعات (به عنوان مثال اطلاعات سیاسی، اقتصادی، علمی، فناوری و نظامی) اختصاص دهند. اطلاعات کوچک می‌توانند در ایجاد یک تصویر ارزشمند نقش داشته باشند .اطمینان حاصل کنید که افراد شما می‌فهمند که یک مکالمه یا تماس به ظاهر بی گناه، مانند یک ایمیل، ممکن است بخشی از تمرین جمع آوری اطلاعات گسترده‌تری باشد. تماس‌ها می‌توانند رسمی (به عنوان بخشی از نقش شخص) اجتماعی یا اتفاقی باشند و در زمینه‌های متنوعی برقرار شوند.

هنگامی که یک تماس رسمی یا اجتماعی از هر نظر مشکوک، مستمر، غیرمعمول یا مداوم به نظر می‌رسد، افراد شما باید یک گزارش تماس را تکمیل کنند .این تماس می‌تواند با موارد زیر باشد:

- سفارت یا مقامات دولت خارجی در نیوزیلند
- مقامات خارجی یا اتباع خارج از نیوزیلند، از جمله نمایندگان تجارت یا تجارت
- هر فرد یا گروهی، صرف نظر از ملیت، که به دنبال به دست آوردن اطلاعات رسمی یا تجاری حساس است که "نیاز به دانستن" معتبری ندارند.

تلاش برای به دست آوردن اطلاعات ممکن است شامل تکنیک‌هایی از جمله فیشینگ یا باتلاق باشد.

❖ **افراد را در مورد خطرات مربوط به سفرهای بین المللی مختصر معرفی کنید**

وقتی افراد شما به خارج از کشور سفر می‌کنند، می‌توانند توسط سرویس‌های جاسوسی خارجی هدف قرار گیرند تا به مطالب طبقه بندی شده دسترسی پیدا کنند.

برای محافظت از سازمان خود و منافع نیوزیلند، ارائه مشاوره یا اطلاع رسانی در مورد خطرات و اقدامات امنیتی لازم برای مردم را در نظر بگیرید .هنگام بازگشت، درمورد تأیید اطلاعات آنها را بررسی کنید تا هر گونه تماس مشکوک، مداوم، غیرمعمول یا مداوم (SOUP) به نظر برسد.

کارمندان، پیمانکاران و افراد دوم باید:

- قبل از سفر با افسر ارشد امنیتی خود مشورت کنید تا آیا توجیهی امنیتی لازم است یا خیر
- بدانید که عوامل خارجی برای جمع آوری اطلاعات از چه روشی استفاده می‌کنند
- درک کنید که چگونه از اطلاعات و دارایی‌های سازمان خود محافظت کنید
- بدانید که آنها باید از چه اطلاعاتی محافظت کنند
- بدانید چه اطلاعاتی می‌توانند به اشتراک بگذارند و تجارت کنند
- از نحوه مدیریت تجهیزات الکترونیکی آگاه باشید.

❖ **مشاوره بیشتر**

مشاوره امنیتی برای مقامات دولت نیوزلند که برای تجارت از خارج از کشور سفر می کنند

❖ **برای دارندگان تصویب امنیت ملی بررسی کنید**

برای افرادی که دارای گواهینامه امنیت ملی هستند، علاوه بر بررسی‌های مداوم عمومی که شما باید انجام دهید، باید:

- سالانه به روز رسانی آگاهی از امنیت را ارائه دهید
- جلسات امنیتی را انجام دهید
- اطمینان حاصل کنید که آنها هرگونه تغییر در شرایط شخصی خود را گزارش می‌دهند
- اطمینان حاصل کنید که آنها هر گونه تماس مشکوک را گزارش می‌دهند
- مدیریت هرگونه دسترسی اضطراری به مطالب طبقه بندی شده
- گزارش تغییرات سطح ترخیص امنیتی آنها
- مجوزهای امنیتی آنها را بررسی کنید.

❖ **راهنمایی بیشتر**

- استخدام و مدیریت دارندگان مجوزهای امنیت ملی
- راهنمای مدیریت دارندگان مجوزهای امنیت ملی

❖ **تغییرات نقش را مدیریت کنید**

معمول است که افراد در یک نقش وارد یک سازمان می‌شوند و سپس با مسئولیت بیشتر و نمایه ریسک بالاتر به سمت نقش دیگری حرکت می‌کنند .عدم اتمام بررسی‌های مناسب برای نقش جدید به دلیل اینکه شخص برای سازمان شما "شناخته شده" است، خطر بروز مشکلات را افزایش می‌دهد.

قبل از اینکه فردی را در نقش جدید تأیید کنید، اطمینان حاصل کنید که همه چک‌های لازم قبل از استخدام و / یا بررسی مناسب بودن شرایط را تا سطح مورد نیاز برای نقش جدید انجام دهید.

۴-۶-۴- پیمانکاران مدیریت

دسترسی پیمانکار به اطلاعات و دارایی‌های شما با خطرات امنیتی مشابه برای کارمندان ثابت و برخی از خطرات اضافی همراه است.

خطر اصلی این است که یک پیمانکار فعلی یا سابق به طور تصادفی یا سو استفاده از دسترسی مورد اعتماد خود برای صدمه زدن به افراد، مشتریان، دارایی‌ها و اطلاعات یا شهرت سازمان شما سو استفاده کند .این خطر به عنوان "تهدید داخلی" شناخته می‌شود.

برای محافظت از اطلاعات و دارایی‌های خود:

- از همان اقدامات امنیتی پرسنل با پیمانکاران مانند کارمندان ثابت استفاده کنید
- اقدامات اضافی را برای مقابله با چالش‌های امنیتی که پیمانکاران می‌توانند ارائه دهند، در نظر بگیرید.

❖ **چالش‌های امنیتی اضافی با پیمانکاران**

چالش‌های زیر در پیمانکاران مشترک است.

❖ **در حال اخذ تعهد نسبت به اقدامات امنیتی خود**

اگر شما یک پیمانکار را به فرهنگ امنیتی خود القا نکنید یا آنها را احساس کنید عضوی از تیم هستند، ممکن است تعهد آنها به اقدامات امنیتی شما زیاد نباشد.

❖ **دانستن منافع رقابتی**

یک پیمانکار ممکن است قبل، در حین و بعد از قراردادش با شما برای یک رقیب کار کند .اگر در مورد تضاد منافع نپرسید، نمی‌توانید خطرات را ارزیابی کنید یا آنها را مدیریت کنید.

❖ **تمدید یا تمدید قرارداد**

اگر قرارداد را بدون بررسی مجدد یا تأیید مجدد پیمانکار تمدید یا تمدید کنید، نمی‌توانید به راحتی خطرات جدید ناشی از تغییر در محیط کار یا زندگی پیمانکار را شناسایی کنید.

❖ **انتقال پیمانکاران از یک وظیفه به وظیفه دیگر**

اگر شما یک پیمانکار را از یک وظیفه دیگر با مشخصات امنیتی بالاتر بدون بررسی‌های صحیح و تحویل امنیت انتقال دهید، خطر بروز مشکلات را افزایش می‌دهید.

❖ **راهنمایی برای کمک به شما در مدیریت پیمانکاران**

برای مقابله با تهدیدات داخلی و چالش‌های اضافی با پیمانکاران، مراحل و نکاتی را در راهنمای ما برای استخدام و مدیریت پیمانکاران دنبال کنید (در بخش اسناد پشتیبانی در زیر موجود است)

۴-۶-۵-عزیمت آنها را مدیریت کنید

مدیریت عزیمت افراد به خوبی از امنیت و اعتبار سازمان شما محافظت می‌کند.

❖ **عزیمت آنها را مدیریت کنید**

عزیمت افراد را مدیریت کنید تا هرگونه خطر برای افراد، اطلاعات و دارایی‌های ناشی از افرادی که از سازمان شما خارج می‌شوند، محدود شود .این مسئولیت شامل اطمینان از بازگشت هرگونه حق دسترسی، مجوزهای امنیتی و دارایی‌ها و درک افراد از تعهدات مداوم خود است.

هنگامی که شخصی سازمان شما را ترک می‌کند، دانش خود را در مورد عملیات تجاری، مالکیت معنوی، اطلاعات رسمی و آسیب پذیری های امنیتی شما حفظ می‌کند .مدیریت خوب عزیمت آنها خطر سو استفاده از این دانش را کاهش می‌دهد.

فارغ از اینکه شخصی به انتخاب خود ترک می‌کند یا نه، یک تجربه مثبت خروج خطر سو استفاده از دانش خود در مورد عملیات، مالکیت معنوی، اطلاعات رسمی یا هرگونه ضعف امنیتی را کاهش می‌دهد.

❖ **حداقل فعالیت‌های عزیمت**

حقوق دسترسی را بردارید

قبل از اینکه شخصی از سازمان شما خارج شود، باید دسترسی او را به منابع الکترونیکی، منابع فیزیکی و سایت‌های فیزیکی از بین ببرید.

❖ **کارت‌های امنیتی را جمع کنید**

اطمینان حاصل کنید که فرد درحال عزیمت کلیه کارتهای شناسایی و کارتهای دسترسی را از جمله ابزارهایی که به آنها امکان دسترسی از راه دور به سیستمهای مدیریت اطلاعات شما را می‌دهد، پس می‌دهد.

❖ **اطمینان حاصل کنید که دارایی‌ها پس داده می‌شوند**

یک شخص در حال عزیمت باید کلیه املاکی را که به سازمان شما تعلق دارد پس دهد .از مالکیت معنوی یا اطلاعات رسمی خود مراقبت ویژه‌ای داشته باشید.

❖ **اقدامات اختیاری برای در نظر گرفتن**

اگر خطر بالاتری را در ارتباط با نقشی خاص یا شرایط شخص تشخیص دادید، از او بخواهید که:

- توضیحات یا مصاحبه خروج را کامل کنید
- سند محرمانه بودن را امضا کنید.

❖ **مصاحبه‌های خروج را انجام دهید**

علاوه بر عملکرد گسترده‌تر، مصاحبه‌های خروج به شما این امکان را می‌دهد که تعهدات خود را در مورد محافظت از اطلاعات سازمان خود به شخص در حال ترک یادآوری کنید.

مصاحبه‌های خروج نیز فرصت خوبی برای اجازه دادن به فرد آسیب دیده است:

- درباره دلایل ترک آنها، و نگرش آنها نسبت به سازمان و افراد خود صحبت کنید
- هرگونه گذر یا کارت دسترسی را در دست بگیرید.

❖ **در صورت بالا بودن خطر از محرمانه بودن استفاده کنید**

برای حفاظت از اطلاعات انحصاری یا مالکیت معنوی سازمان شما ممکن است یک راز محرمانه باشد.

❖ **فعالیت‌هایی برای دارندگان ترخیص امنیت ملی**

هنگامی که شخصی که دارای مجوز امنیت ملی است از سازمان شما خارج می‌شود، شما باید فعالیت‌های اساسی را انجام دهید و همچنین:

- مصاحبه خروج انجام دهید
- اجازه امنیتی خود را منتقل یا لغو کنید
- آن‌ها را از هرگونه جلسات توجیهی اطلاعات حساس که برگزار می‌کنند توضیح دهید
- به سرویس اطلاعات امنیتی نیوزلند اطلاع دهید.

۷-۴- اخذ مجوز امنیت ملی

اگر کاندیدای تصویب امنیت ملی هستید، در این بخش به شما یک مرور کلی از روند بررسی می‌دهد و به شما می‌گوید مسئولیت‌ها و حقوق شما چیست.

❖ **مروری بر روند بررسی**

فرآیند بررسی به سازمان شما کمک می‌کند تا تصمیم بگیرد که آیا به شما مجوز اعطا می‌کند .آن‌ها باید بدانند که می‌توانند در دسترسی به اطلاعات، دارایی‌ها و مکان‌های کاری که می‌توانند بر امنیت نیوزیلند تأثیر بگذارند به شما اعتماد کنند.

اگر واجد شرایط بازرسی هستید، توسط سرویس اطلاعات امنیتی نیوزلند (NZSIS) تأیید خواهید شد .آن‌ها تمام نامزدهای تصفیه را بررسی می‌کنند.

سازمان شما با شما یک تماس بررسی می‌کند - شخصی در سازمان شما که می‌تواند در روند بررسی به شما کمک کند .روند بررسی شش مرحله دارد و می‌تواند چندین ماه طول بکشد.

چهار سطح امنیتی وجود دارد، به شرح زیر:

- محرمانه
- راز
- فوق سری
- راز ویژه

سازمان شما براساس بالاترین طبقه بندی اطلاعات، دارایی‌ها و محل کار مورد نیاز شما، تصمیم می‌گیرد که به کدام سطح از ترخیص نیاز دارید .سطح تصفیه براساس درجه، سابقه یا وضعیت شما نیست.

❖ **چک کردن چقدر طول می‌کشد؟**

مدت زمانی که از درخواست شما گرفته تا تصمیم نهایی در مورد ترخیص شما طول می‌کشد به موارد زیر بستگی دارد:

- شما و داوران شخصیت شما چقدر سریع اطلاعات را ارائه می‌دهند
- بررسی NZSIS در زمینه شما چقدر باید انجام دهد
- چه تعداد برنامه دیگر در حال پردازش هستند.

۱) سازمان شما صلاحیت شما برای بررسی را بررسی می‌کند

در مرحله ۱، سازمان شما در صورت واجد شرایط بودن برای بررسی و تصدیق مجوز فعالیت می‌کند .اگر واجد شرایط و مناسب باشید، سازمان شما برای شروع بررسی خود به NZSIS تقاضا می‌کند .خودتان نمی‌توانید درخواست ترخیص کنید.

سازمان شما همچنین ممکن است در صورت نیاز برخی از بررسی‌های امنیتی خود را در این مرحله انجام دهد .به عنوان مثال، آن‌ها ممکن است مرجع یا بررسی صلاحیت را انجام دهند.

برای بررسی صلاحیت شما، سازمان شما نیاز به پاسخ به سؤالات زیر دارد.

❖ آیا شما تابعیت یا وضعیت ویزا مناسبی دارید؟

به طور معمول شما باید یک شهروند نیوزیلند باشید یا دارای ویزای رزیدنت کلاس باشید .تابعیت شما شاخص وفاداری شما به نیوزیلند است.

سازمان شما ممکن است قوانین سختگیرانه دیگری در مورد اینکه چه کسی می‌تواند به وی اجازه بدهد داشته باشد.

برای بررسی صلاحیت خود از ابزار خودآزمایی ما استفاده کنید

❖ آیا NZSIS می‌تواند پیش زمینه شما را به اندازه کافی بررسی کند؟

NZSISباید بتواند جزئیاتی را که در مورد سابقه خود ارائه می‌دهید بررسی کند .در بیشتر موارد، پیشینه‌ها باید برای دوره مورد نظر یا تا سن ۱۸ سالگی قابل بررسی باشند.

بررسی پس زمینه	سطح پاکسازی
۵ سال	**محرمانه**
۱۰سال	**راز**
۱۰ سال	**فوق سری**
۱۵ سال	**راز ویژه**

اگر زمان خود را برای زندگی در خارج از کشور گذرانده‌اید NZSIS :می‌تواند سابقه شما را زمانی که شما در استرالیا، کانادا، انگلستان یا ایالات متحده آمریکا زندگی کرده‌اید بررسی کند .اگر بیشتر زندگی بزرگسالی خود را در خارج از این کشورها گذرانده‌اید، با تماس با سازمان تأیید سازمان خود اطمینان حاصل کنید که معیارهای پیشینه قابل بررسی را برآورده می‌کنید.

می‌توانید از ابزار خودآزمایی واجد شرایط بودن ما استفاده کنید تا بفهمید احتمالاً سابقه شما قابل بررسی است یا خیر.

- صلاحیت خود را برای تصویب امنیت ملی بررسی کنید

برای کسب اطلاعات بیشتر در مورد این مرحله از بررسی، به بخش ۱ راهنمای قابل چاپ ما مراجعه کنید: دریافت مجوز امنیت ملی .در انتهای این صفحه در بخش اسناد پشتیبانی آن را پیدا خواهید کرد.

۲) شما بصورت آنلاین ثبت نام می‌کنید و رضایت می‌دهید

در مرحله ۲، شما بصورت آنلاین ثبت نام می‌کنید و موافقت خود را با NZSIS انجام می‌دهید تا بررسی‌های قبلی انجام دهد.

برای کسب اطلاعات بیشتر در مورد ثبت نام، به بخش ۲ راهنمای قابل چاپ ما مراجعه کنید: دریافت مجوز امنیت ملی .در انتهای این صفحه در بخش اسناد پشتیبانی آن را پیدا خواهید کرد.

۳) پرسشنامه بررسی را تکمیل می‌کنید

در مرحله ۳، شما یک پرسشنامه بررسی آنلاین را تکمیل و ارسال می‌کنید.

اطلاعاتی که در پرسشنامه می‌دهید فقط برای اهداف بررسی استفاده می‌شود.

هرچه زودتر پرسشنامه را تکمیل کنید، NZSISزودتر می‌تواند روند بررسی را شروع کند.

اطلاعاتی که برای جمع آوری پرسشنامه بررسی نیاز دارید

برای راهنمایی دقیق برای کمک به شما در جمع آوری اطلاعات مناسب برای پرسشنامه بررسی، یکی از راهنماهای زیر را بخوانید.

- دریافت مجوز امنیتی محرمانه
- گرفتن مجوز امنیتی مخفی
- اخذ مجوز امنیتی بسیار محرمانه
- اخذ مجوز امنیتی ویژه بسیار محرمانه

برای کسب اطلاعات بیشتر در مورد مرحله پرسشنامه بررسی، به بخش ۳ راهنمای قابل چاپ ما مراجعه کنید: اخذ مجوز امنیت ملی .در انتهای این صفحه در بخش اسناد پشتیبانی آن را پیدا خواهید کرد.

۴) اطلاعات شما را NZSISارزیابی کرده و پیشینه شما را بررسی می‌کند

در این مرحله، NZSISاطلاعاتی را که در پرسشنامه داده‌اید ارزیابی می‌کند و پیشینه شما را بررسی می‌کند.

آن‌ها فقط در صورت رضایت شما سابقه شما را بررسی می‌کنند .هرچه سطح ترخیص کالا بیشتر باشد، عمق بررسی‌های آنها بیشتر است.

NZSISبرای تأیید جزئیاتی که در پرسشنامه آورده‌اید، ممکن است با افراد و سازمانها تماس بگیرد .آن‌ها همچنین ممکن است شما یا داوران شما را به شرکت در مصاحبه در صورت لزوم دعوت کنند.

برای کسب اطلاعات بیشتر در مورد مصاحبه‌ها، به قسمت ۴ راهنمای قابل چاپ ما مراجعه کنید: دریافت مجوز امنیت ملی .در انتهای این صفحه در بخش اسناد پشتیبانی آن را پیدا خواهید کرد.

در مرحله ۴، NZSISبدنبال پاسخ سؤالات questions زیر خواهد بود.

- **آیا قابل اعتماد و مسئولیت پذیر هستید؟**

NZSIS به دنبال شواهدی است که نشان می‌دهد شما:

- وفادار، صادق و قابل اعتماد هستند
- به مسئولیت خود در مورد ایمن نگه داشتن اطلاعات طبقه بندی شده احترام بگذارید

در تصمیمات شما درباره اطلاعات طبقه بندی شده، بدون هیچ گونه تأثیر نامناسب، از قضاوت مناسب استفاده خواهد کرد.

❖ **آیا خطری دارید؟**

NZSIS ارزیابی می‌کند که آیا خطری وجود دارد که شما تصمیم بگیرید (یا متقاعد شوید) از استفاده نامناسب از دسترسی خود استفاده کنید .آن‌ها به بخشهای زیر زندگی شما نگاه می‌کنند:

- سازمان‌ها یا افرادی که به آنها وفادار هستید، ممکن است بر شما نفوذ داشته باشند یا با کسانی که ارتباط دارید
- روابط و رفتارهای شخصی
- موقعیت مالی
- مصرف الکل و مواد مخدر
- تاریخ و رفتار جنایی
- نگرش‌ها و نقض‌های امنیتی
- وضعیت سلامت روان

برای جزئیات بیشتر، به :معیارهای ارزیابی امنیت و دستورالعمل های داوری مراجعه کنید

۵) توصیه‌های خود را به NZSIS ارائه می‌دهد

در مرحله پنجم، NZSIS به شما توصیه می‌کند که آیا شما برای داشتن یک ترخیص کالا مناسب هستید یا خیر.

اگر NZSIS نگرانی دارد، ابتدا آنها را با شما در میان می‌گذارند.

۶) سازمان شما درباره ترخیص شما تصمیم می‌گیرد

آخرین مرحله زمانی است که سازمان شما تصمیم می‌گیرد که به شما مجوز اعطا کند و اگر چنین است، در چه سطحی.

هنگامی که سازمان شما تصمیم خود را اتخاذ کرد، به شما اطلاع داده می‌شود.

❖ **مسئولیت‌های شما به عنوان یک نامزد بررسی**

شما به عنوان یک کاندیدا مسئولیت‌های زیر را دارید.

❖ **جزئیات کامل و صادقانه را بیان کنید**

شما باید در فرآیند بررسی با ارائه اطلاعات به طور کامل و صادقانه همکاری کنید:

- فرم‌هایی را که از شما خواسته شده پر کنید، تکمیل کنید
- در یک مصاحبه به سؤالات پاسخ دهید (اگر از شما خواسته می‌شود که یک سؤال داشته باشید)
- اسناد شخصی و شواهد دیگری برای کمک به تأیید جزئیات خود ارائه دهید
- به هر گونه سؤال در طول فرآیند پاسخ دهید.

اگر کاملاً صادق نباشید، ممکن است سازمان شما در قابلیت اعتماد شما شک کند و این می‌تواند در تصمیم گیری در مورد اعطای مجوز به شما تأثیر بگذارد یا خیر.

اگر درج اطلاعاتی را فراموش کردید، بلافاصله با تماس گیرنده تماس بگیرید.

❖ **همه محکومیت‌ها و انحرافات کیفری را افشا کنید**

اگر محکومیت و انحراف کیفری دارید، باید همه آنها را به NZSIS اعلام کنید، از جمله محکومیت‌های تاریخی و جرائم راهنمایی و رانندگی که به طور معمول با قانون پاک تخته سنگ ۲۰۰۴ معاف هستند.

از آنجا که تصویب شما برای امنیت ملی مهم است، NZSISحق قانونی دارد که طبق اقدامات زیر پرونده کامل کیفری شما را درخواست کند:

- بند ۲۵ قانون حقوق بشر ۱۹۹۳
- بخش ۱۹ (۳) (د) (من) قانون پاک تخته سنگ ۲۰۰۴.

❖ **حقوق شما به عنوان یک نامزد بررسی**

شما به عنوان یک کاندیدا از حقوق زیر برخوردار هستید.

❖ **حقوق تحت قانون حقوق بشر**

وقتی شغلی شامل امنیت ملی نیوزیلند است، بخش ۲۵ قانون حقوق بشر ۱۹۹۳ به NZSIS اجازه می‌دهد تا برخی از عواملی را که ممکن است تبعیض آمیز تلقی شود، در نظر بگیرد NZSIS .فقط در صورتی که این عوامل را به یک مسئله امنیتی مرتبط سازد، آن‌ها را در نظر خواهد گرفت.

❖ **عواملی که NZSIS می‌تواند در نظر بگیرد**

- اعتقادات مذهبی یا اخلاقی
- نظر سیاسی
- سلامت روان
- شرکا یا اقوام خاص
- منشأ ملی

❖ **عواملی که NZSIS نمی‌تواند در نظر بگیرد**

- جنسیت
- گرایش جنسی
- قومیت
- ناتوانی جسمی
- وضعیت تأهل
- سن (مگر اینکه زیر ۲۰ سال باشید)

❖ **حق انصاف رویه‌ای**

عدالت رویه‌ای بدان معناست که NZSIS باید از روندی منصفانه و مناسب برای تصمیم گیری در مورد توصیه شما برای ترخیص استفاده کند یا خیر.

NZSISباید کل زندگی و طیف وسیعی از تجربیات شما را در نظر بگیرد - بنابراین آنها شما را به عنوان یک فرد منحصر به فرد دقیق ارزیابی می‌کنند.

بررسی امنیتی شامل بررسی بیشتر سابقه شما از آنچه قبلاً تجربه کرده‌اید است .هرچه سطح تصفیه بالاتر باشد، بررسی NZSIS بیشتر است .با این حال، روند بررسی:

- برای احترام به حریم خصوصی و حیثیت شما طراحی شده است
- اجازه نمی‌دهد که شما به طور غیرقانونی مورد تبعیض قرار بگیرید
- تا آنجا که ممکن است از حقوق شما به عنوان یک نامزد محافظت می‌کند.

NZSISبه شما این فرصت را می‌دهد تا قبل از اینکه توصیه خود را به سازمان خود ارائه دهند، در مورد هر گونه نگرانی آنها صحبت کنید.

اگر فکر می‌کنید با شما منصفانه رفتار نشده است، با تماس گیرنده خود صحبت کنید.

❖ اطلاعات بیشتر

انصاف رویه ای - حق شما برای یک روند عادلانه

❖ حق شکایت

پس از پایان مراحل بررسی، در صورت عدم رضایت می‌توانید به بازرس کل اطلاعات و امنیت (IGIS) شکایت کنید:

- چگونه NZSIS فرآیند بررسی را انجام داد
- پیشنهادی که NZSIS ارائه داده است

کارگروه فنی- تخصصی

۴-۷-۱- نیاز به تصویب نامه امنیت ملی را شناسایی کنید

این بخش راهنمایی‌هایی برای کمک به سازمانهای دولتی است که می‌توانند بفهمند چه کسی در سازمان آنها نیاز به تصویب امنیت ملی دارد و چه زمانی این کار را انجام نمی‌دهد.

❖ مجوزهای امنیتی ملی را مدیریت کنید

اطمینان حاصل کنید که افراد قبل از اینکه به اطلاعات، دارایی‌ها یا مکان‌های کاربری محرمانه، محرمانه و دسترسی پیدا کنند، از سطح امنیت ملی مجاز برخوردار هستند .شایستگی مداوم کلیه دارندگان مجوزهای امنیت ملی برای داشتن مجوز را مدیریت کرده و هرگونه تغییر در مورد ترخیص آنها را به NZSIS اطلاع دهید.

❖ کار کردن در مورد اینکه چه کسی و در چه سطحی به ترخیص نیاز دارد

اگر شخصی نیاز به دسترسی به اطلاعات، دارایی‌ها یا مکان‌های کاری دولت داشته باشد که برای نقش خود در "اعتماد"، "حساس" یا "محدود" مشخص شده است، نیازی به تصویب ندارد .با این حال، اصل "نیاز به دانستن" هنوز هم اعمال می‌شود .این بدان معناست که دسترسی شما به افرادی که نیاز عملیاتی دارند و بررسی‌های امنیتی پرسنل شما را پشت سر گذاشته‌اند، محدود می‌کنید.

اگر شخصی برای نقش خود به اطلاعات، دارایی‌ها یا مکان‌های کاری طبقه بندی شده مانند "رازدار"، "راز" یا "راز برتر" احتیاج داشته باشد، باید در سطح مناسب دارای مجوز باشد.

برای بررسی اینکه آیا شخصی به ترخیص نیاز دارد و در چه سطحی است:

- وظایف موقعیت را تجزیه و تحلیل کنید
- بالاترین سطح اطلاعات طبقه بندی شده، دارایی‌ها یا مکان‌های کاری را که فرد به آنها نیاز دارد، شناسایی کند
- شناسایی اینکه آیا فرد به مجموعه‌ای از اطلاعات طبقه بندی شده یا دارایی دسترسی دارد) مجموعه‌های فیزیکی و مجموعه اطلاعات در سیستم‌های(ICT
- مشخص کنید که فرد برای چه مدت به ترخیص نیاز دارد (به عنوان مثال آیا این نقش کوتاه مدت است یا دائمی؟).

به یاد داشته باشید که در طول این مراحل با کارمندان امنیتی خود مشورت کنید.

❖ تهدیدهایی که روند بررسی در برابر آنها محافظت می‌کند

روند بررسی به کاهش تهدیدات امنیت ملی از منابع زیر کمک می‌کند .

افرادی که:

- ممکن است در معرض فشار اشخاص ثالث با اهداف مضر قرار داشته باشد
- صادق نبوده یا فقدان صداقت را نشان داده‌اند
- به دلیل شرایطشان غیرقابل اعتماد بوده‌اند یا ممکن است غیرقابل اعتماد باشند
- سرویس‌های اطلاعاتی خارجی
- گروه‌های تروریستی
- افرادی که مایلند دموکراسی پارلمانی ما را از طریق ابزارهای سیاسی، صنعتی یا خشونت آمیز براندازند یا تضعیف کنند.

❖ ارزیابی سطح دسترسی برای اطلاعات طبقه بندی شده در سیستم‌های ICT

هر کسی که به دسترسی به یک سیستم ICT نیاز دارد که دارای اطلاعات طبقه بندی شده یا دارایی‌های مشخص شده با نام "محرمانه" یا بالاتر است، باید دارای تصفیه‌ای باشد که با بالاترین مارک محافظتی اطلاعات نگهداری شده در سیستم مطابقت داشته باشد.

❖ اگر سیستمی مجموعه‌ای از اطلاعات را در خود جای دهد

مجموعه اطلاعات (اطلاعات جمع شده) می‌توانند از اطلاعات تکمیل شده از آنها با ارزش‌تر باشند .هنگامی که در حال دستیابی به سطوح دسترسی هستید، اطمینان حاصل کنید که مقدار یا حساسیت مجموعه اطلاعاتی را که در سیستم‌های ICT خود نگهداری می‌کنید، در نظر می‌گیرید .شما باید اطمینان حاصل کنید که سطح دسترسی خطر آسیب رسیدن به دلیل سو استفاده از مجموعه اطلاعات را منعکس می‌کند.

به عنوان مثال، اگر مجموعه‌ای از اطلاعات محدود شده در یک سیستم داشته باشید و درصورت محرمانه بودن در نظر گرفته شود، کاربران آن سیستم باید اطلاعات محرمانه داشته باشند.

❖ اگر سیستمی دارای اطلاعات محفظه حساس (SCI) باشد

اگر سیستمی دارای SCI باشد، هرکسی که به سیستم دسترسی پیدا می‌کند باید از نظر امنیتی و توجیهی مورد نیاز برای محفظه‌ها برخوردار باشد.

سیستم‌های ICT دارای SCI باید توسط اداره امنیت ارتباطات دولت (GCSB) معتبر شناخته شوند.

ما به شما توصیه می‌کنیم از GCSB برای کمک به شما در زمینه ترقی و شرایط شهروندی برای دسترسی به سیستم‌های ICT با SCI کمک بگیرید.

❖ اگر سیستمی اطلاعاتی را نشان دهد که فقط با چشم نیوزلند مشخص شده‌اند(NZEO)

مارک NZEO نشان می‌دهد که دسترسی به اطلاعات برای شهروندان نیوزیلندی با مجوز مناسب بر اساس نیاز محدود شده است.

اگر یک سیستم ICT دارای اطلاعاتی با علامت NZEO باشد، نمی‌توانید به کسی که شهروند نیوزلند نیست دسترسی داشته باشید مگر اینکه:

- فرد معافیت NZEO دارد، یا
- کنترل‌های فنی برای جلوگیری از دسترسی افراد غیرمجاز به مواد NZEO انجام شده است.

❖ محدودیت‌های دسترسی اتباع خارجی را درک کنید

شما نمی‌توانید به اتباع خارجی اجازه دسترسی دهید:

- هرگونه اطلاعات، دارایی یا مکان کار با NZEO مشخص شده است مگر اینکه از چشم پوشی از NZEO برخوردار باشد
- مواد طبقه بندی شده که از کشوری دیگر به نیوزیلند منتقل شده است مگر اینکه آن کشور دسترسی کتبی را تأیید کرده باشد.

این قوانین حتی اگر فرد دارای مجوز امنیت ملی در سطح مناسب باشد نیز اعمال می‌شود برخی موارد استثنا در شرایط محدودی اعمال می‌شوند.

❖ **گزینه‌های خود را برای نقش‌های کوتاه مدت در نظر بگیرید**

اگر برای نقشی که نیاز به تصویب دارد، به پوشش کوتاه مدت یا موقت نیاز دارید، تغییر یک دارنده ترخیص موجود از داخل سازمان خود را در نظر بگیرید. اگر برای انجام یک کار کوتاه مدت نیاز به تصویب جدید دارید، با تیم بررسی امنیتی NZSIS در مورد اینکه آیا فرد می‌تواند به موقع برای رفع نیازهای شما پاک شود صحبت کنید.

❖ **جذب نیروهایی که نیاز به مجوزهای امنیتی ملی دارند**

وقتی سازمان شما موقعیتی را تبلیغ می‌کند که نیاز به مجوز دارد، روش خوب این است که:

- به مردم بگویید که برای تصفیه نیاز به بررسی دارند
- شامل خلاصه‌ای از معیارهای صلاحیت یا پیوندی به ابزار خودآزمایی واجد شرایط بودن
- در صورت عدم اطمینان از واجد شرایط بودن یا روند بررسی، مردم را به تماس با شما تشویق کنید.

جلو بودن و نزدیک بودن در مورد واجد شرایط بودن و آنچه درگیر گرفتن مجوز است ممکن است به این معنی باشد که تعداد کمتری برنامه برای این نقش دریافت می‌کنید.

- **اطلاعات بیشتر**
- فرد مناسب را استخدام کنید

❖ **صدور مجوز از شرایط اشتغال**

این یک روش خوب است که گرفتن و نگهداری از مجوز را شرط استخدام قرار دهید.

در حالت ایده آل، شما این گزینه را در تبلیغات خود به نامزدهای احتمالی اعلام خواهید کرد .اگر این کار را نکرده‌اید، قبل از اینکه به کاندیدای منتخب خود پیشنهاد دهید به او بگویید و این شرط را در قرارداد کار وی بگنجانید (یا قرارداد خدمات در صورت پیمانکار یا ارائه دهنده خدمات) این روش را برای نامزدهای داخلی یا ترتیبات اعزام نیز اعمال کنید.

۴-۷-۲-صلاحیت بررسی را بررسی کنید

قبل از اینکه سازمان شما درخواست تأییدیه برای تصویب امنیت ملی را ارسال کند، باید صلاحیت و شایستگی نامزد را بررسی کنید. افسر ارشد امنیتی (CSO) شما مسئول این موارد است:

- اطمینان حاصل کنید که بررسی صلاحیت و مناسب بودن انجام شده است
- ارسال درخواست‌های بررسی به سرویس اطلاعات امنیتی نیوزلند (NZSIS)

❖ **تابعیت یا وضعیت ویزا آنها را بررسی کنید**

برای واجد شرایط بودن برای بررسی، فرد باید تابعیت نیوزلند یا دارنده ویزای کلاس اقامت باشد.

در شرایط نادر، سایر نامزدها ممکن است برای بررسی امنیتی در نظر گرفته شوند .با این وجود، قبل از درخواست تأیید مراحل مختلفی درگیر است. رئیس اجرایی یا سازمان امنیت عمومی شما باید ابتدا شرایط نادر را با بررسی NZSIS در میان بگذارید .در

صورت موافقت بررسیNZSIS ، می‌توانید یک پرونده تجاری را برای بررسی تأیید و ارسال کنید (رئیس اجرایی شما باید پرونده تجاری را قبل از ارسال تأیید کند) .تنها در صورتی که NZSIS پرونده تجاری را بپذیرد، بررسی می‌تواند ادامه یابد.

❖ اطمینان حاصل کنید که پیشینه آنها قابل بررسی است

قبل از اینکه سازمان شما درخواست تأیید را ارسال کند، مطمئن شوید که هر داوطلب بررسی حداقل شرایط لازم برای پیشینه بررسی را داشته باشد. در بیشتر موارد، پیشینه فرد باید برای مدت زمان لازم یا تا ۱۸ سالگی قابل بررسی باشد. در برخی شرایط، ارزیابی اینکه آیا فرد حداقل شرایط را دارد، دشوار است .برای راهنمایی، پاسخ سؤالات متداول را بعد از جدول زیر مشاهده کنید.

بررسی پس زمینه	سطح پاکسازی
۵ سال	**محرمانه**
۱۰ سال	**راز**
۱۰ سال	**فوق سری**
۱۵ سال	**راز ویژه**

❖ اگر داوطلب خیلی جوان باشد تا بتواند سابقه کافی قابل بررسی داشته باشد، چه می‌شود؟

اگر یک داوطلب بررسی به دلیل سن کافی سن قابل بررسی را نداشته باشد، باز هم واجد شرایط بازرسی است .تیم بررسی NZSISممکن است توصیه کند که برای مدت زمان کوتاه‌تر مجوز صادر شود. به عنوان مثال، اگر داوطلب ۲۰ سال باشد، فقط در سن ۱۸ سالگی بررسی می‌شود حتی اگر شرط قابل بررسی برای ۵ سال باشد .توصیه تیم بررسی NZSIS این خواهد بود که شما فقط ۲ سال مجوز اعطا کنید.

❖ اگر یک کاندیدا زمان زیادی را در خارج از کشور زندگی کرده باشد، چه می‌کنید؟

زمان استرالیا، کانادا، انگلستان و ایالات متحده آمریکا قابل بررسی است .زمان در کشورهای دیگر به طور کلی قابل بررسی نیست .تیم بررسی NZSIS می‌تواند به شما اطلاع دهد که آیا آنها کاندیداها را قابل بررسی می‌دانند یا خیر.

اگر نامزدها در خارج از کشور برای یک سازمان دولتی نیوزلند کار کرده باشند، اگر این سازمان اطمینان دهد که فرد را مطابق با الزامات امنیتی محافظ دارندگان ترخیص مدیریت کرده است، می‌تواند زمان حضور آنها در کشورهای دیگر را بررسی کند.

برای مشاوره با تیم بررسی NZSIS تماس بگیرید ovr@nzsis.govt.nz

❖ اگر داوطلب را از خارج از کشور جذب می‌کنید، چه می‌کنید؟

اگر در خارج از کشور استخدام می‌کنید، فرد همچنان باید شرایط پیشینه قابل بررسی را داشته باشد.

❖ مناسب بودن آنها برای داشتن ترخیص کالا را بررسی کنید

قبل از اینکه سازمان شما درخواست تأیید را ارسال کند، باید به شخص اعتماد داشته باشید و توانایی او را داشته باشید تا یک توصیه مطلوب برای تصویب را بدست آورید.

برای کمک به شما در بررسی مناسب بودن آنها، سوابق سازمان خود را (مانند سوابق عملکرد یا انضباطی) مرور کنید .به دنبال هر رکوردی باشید که نشان دهد نامزد نامناسب است .به عنوان مثال، سوابق مربوط به:

- عدم صداقت

- سو رفتار
- نقض قانون رفتار برای خدمات دولتی

همچنین باید قدرت شخصیت و صداقت فرد را ارزیابی کنید .اگر شک دارید که آیا می‌توانید به آنها در دسترسی به اطلاعات طبقه بندی شده، دارایی‌ها یا محل کار اعتماد کنید، درخواست بررسی را ارائه نکنید. NZSIS معیارها و دستورالعمل‌های زیر را هنگام بررسی دامنه نامزدها برای تصویب امنیت اعمال می‌کند.

- معیارهای ارزیابی امنیت و دستورالعمل های داوری

❖ در صورت لزوم معیارهای صلاحیت خود را اعمال کنید

اگر ارزیابی ریسک نشان داد که سازمان شما برای تصمیم گیری در مورد اینکه برای چه کسی درخواست تأیید می‌کنید، به معیارهای سختگیرانه تری نیاز دارد، این معیارها را در مرحله بررسی صلاحیت خود در کنار چک‌های اجباری توصیف شده در این صفحه اعمال کنید.

۴-۷-۳-برای تصویب درخواست بررسی کنید

مدیر ارشد امنیتی یک سازمان دولتی موظف است درخواست‌های تأیید مجوزهای امنیتی ملی را با استفاده از سیستم درخواست دامپزشکی آنلاین (OVR) به سرویس اطلاعات امنیتی نیوزلند (NZSIS) ارائه دهد. OVR یک سیستم مبتنی بر وب اتوماتیک و ایمن است .فقط افراد مجاز به OVR دسترسی دارند. اطلاعاتی که داوطلبان در پرسشنامه تأیید می‌دهند فقط برای اهداف بررسی قابل استفاده است .سازمان شما می‌تواند برای اطمینان از کامل بودن اطلاعات، برنامه‌ها را در OVR بررسی کند، اما شما نمی‌توانید برای هر هدف دیگری به اطلاعات دسترسی پیدا کنید یا از آنها استفاده کنید.

قبل از ارسال درخواست برای بررسی، باید مطمئن شوید که فرد واجد شرایط برای بررسی است و احتمالاً توصیه مطلوبی را برای تصویب کسب می‌کند. مطمئن شوید که صلاحیت و شایستگی فرد را بررسی کرده‌اید

قبل از اینکه اجازه دسترسی به اطلاعات طبقه بندی شده، دارایی‌ها یا مکان‌های کار را به دست آورید، به یاد داشته باشید تا زمانی که سازمان شما یک توصیه بررسی و مجوز تأیید را دریافت کند، صبر کنید.

❖ درخواست بررسی فوری

قبل از ارائه درخواست بررسی فوری، با تیم بررسی NZSIS تماس بگیرید .اگر NZSIS موافقت کرد می‌توانید با درخواستی پیش بروید، مطمئن شوید که موارد زیر را درج می‌کنید:

- شرح مختصری از شرایط فوری بودن بررسی
- هنگامی که شما نیاز به پاسخ از NZSIS توسط.

فقط درصورت تأیید فوری باید این کار را انجام دهید .نمونه‌هایی از چنین شرایطی ممکن است شامل موارد زیر باشد:

- ارسال یا استقرار در خارج از کشور
- مشارکت در پرونده‌های قضایی مربوط به امنیت
- حضور در دوره‌هایی که برای آنها ترخیص لازم است.

آگاه باشید که اولویت بندی یک درخواست بررسی احتمالاً باعث تأخیر سایر درخواست‌ها می‌شود.

❖ **اعطای دسترسی اضطراری به مطالب طبقه بندی شده**

در مواقع اضطراری، مدیر اجرایی شما ممکن است به شخصی که قبلاً دارای مجوز تصفیه شده است اجازه دسترسی به اطلاعات، دارایی‌ها یا مکان‌های کاری را یک سطح بالاتر از تراز فعلی خود بدهد .برای کسب اطلاعات بیشتر در مورد دسترسی اضطراری، به این موارد بروید

۴-۷-۴-در مورد اعطای مجوز تصمیم بگیرید

بعد از اینکه سازمان شما از طرف سرویس اطلاعات امنیتی نیوزلند (NZSIS) توصیه تأیید شد، باید آن را بررسی کنید، در مورد اعطای مجوز امنیت ملی تصمیم بگیرید و به NZSIS بگویید که چه تصمیمی گرفته‌اید. همچنین باید اطمینان حاصل کنید که داوطلبان راستی آزمایی می‌دانند حقوقشان چیست.

❖ **دریافت توصیه بررسی**

هنگامی که NZSIS بررسی نامزد شما برای تصویب امنیت ملی را به پایان رساند، آن‌ها توصیه کتبی خود را به افسر ارشد امنیتی (CSO)یا نماینده آنها ارائه می‌دهند.

NZSISممکن است موارد زیر را توصیه کند:

- ترخیص در سطح درخواست شما
- ترخیص در سطح پایین‌تر
- ترخیص با توصیه‌های خاص ("صلاحیت") برای مدیریت آن
- شما مجوز اعطا نمی‌کنید (که تصویب در هر سطح مناسب نیست).

❖ **اقدام به توصیه بررسی**

به یاد داشته باشید که سازمان شما نباید در سطح بالاتر از آنچه برای بررسی درخواست کرده‌اید، مجوز اعطا کند.

وقتی مجوز اعطا می‌کنید، شما سازمان حمایت کننده آن دارنده مجوز هستید.

❖ **برای ترخیص در سطح درخواستی شما**

اگر NZSIS تصویب نامه‌ای را در سطح درخواست شده شما توصیه می‌کند و سازمان شما تصمیم می‌گیرد این مجوز را اعطا کند، باید دارنده مجوز را ارائه دهید:

- خلاصه‌ای از مسئولیت‌های آنها برای محافظت از اطلاعات طبقه بندی شده، دارایی‌ها و محل کار
- شرایط لازم برای گزارش هرگونه تغییر در شرایط یا تماس‌های مشکوک
- جزئیات برنامه آموزش آگاهی از امنیت سازمان شما.

❖ **برای ترخیص در سطح پایین‌تر**

اگر NZSIS نگرانی‌هایی داشته باشد که ممکن است منجر به توصیه ترخیص در سطح پایین‌تری از آنچه سازمان شما درخواست کرده است شود، آن‌ها ممکن است به سازمان امنیت داخلی شما توصیه کنند از دسترسی فرد به اطلاعات طبقه بندی شده، دارایی‌ها یا مکانهای کاری بالاتر از سطح تصویب توصیه شده، خارج شود.

اگر ترخیص کالا از شرط اشتغال باشد، سازمان امنیت و همکاری شما باید به منابع انسانی نتیجه دهد.

سپس سازمان شما می‌تواند شرایط استخدام را تأیید کند یا تصمیم بگیرد که آیا پیشنهاد کار را پس می‌گیرید، فرد را مجدداً استخدام می‌کنید یا کار وی را پایان می‌دهید.

توجه: یک داوطلب بررسی حق دارد در صورت عدم رضایت از توصیه بررسی، شکایت کند .اگر کاندیدایی شکایت کرد، قبل از اقدامی صبر کنید تا روند شکایت به پایان برسد .در صورت نیاز به مشاوره حقوقی مراجعه کنید.

❖ **با صلاحیت در مورد ترخیص**

سازمان شما باید از هر گونه توصیه خاص ("صلاحیت") که NZSIS برای مدیریت خطرات امنیتی مرتبط با یک داوطلب بررسی ارائه می‌دهد پیروی کند. اگر تصمیم گرفتید که خطرات را بپذیرید و مدیریت کنید، با دارنده مجوز برای تهیه یک برنامه مدیریت ریسک امنیتی برای مدیریت خطرات همکاری کنید.

❖ **برای عدم تصویب**

هنگام دریافت توصیه‌های نامطلوب از NZSIS در مورد نامزد، سازمان شما نباید مجوز تصویب کند .برای کسب اطلاعات بیشتر با تیم بررسی NZSIS تماس بگیرید.

❖ **اعطای مجوز برای یک تبعه خارجی**

اگر سازمان شما تصمیم به اعطای مجوز به یک تبعه خارجی می‌دهد، بهتر است به دست آوردن تابعیت نیوزلند تا تاریخ معین شرط حفظ ترخیص خود باشید .این امر به اطمینان از وفاداری آنها به نیوزیلند کمک می‌کند.

❖ **مشاوره NZSIS در مورد تصمیمات و تغییرات**

سازمان شما باید در مورد هر تصمیمی که در وضعیت تصویب انجام می‌دهید به NZSIS اطلاع دهد .هر زمان تصفیه شد باید به آنها بگویید:

- اعطا شده یا رد شده است
- کاهش یافته یا ارتقا یافته است
- معلق یا از سر گرفته شده
- انتقال یا اهرم (با سازمان دیگری به اشتراک گذاشته شده است)
- تمدید شده
- لغو شد

❖ **مشاوره دادن به داوطلبان راستی آزمایی در مورد حق شکایت آنها**

CSOیا نماینده سازمان شما باید در مورد حق شکایت به داوطلبان راستی آزمایی کند .یک نامزد بررسی حق دارد در صورت عدم رضایت از بازرس کل اطلاعات و امنیت، شکایت کند:

- چگونه NZSIS فرآیند بررسی را انجام داد
- پیشنهادی که NZSIS ارائه داده است

۴-۷-۵-انتظارات صحیح را تنظیم کنید (برای دارندگان ترخیص)

یک مدیر دارنده ترخیص کالا باید به وضوح با آنها ارتباط برقرار کند تا انتظارات درستی از نقش آنها داشته باشد .دارنده مجوز باید سیاست‌ها و اقدامات امنیتی سازمان شما را درک کند و هنگام تغییر از آنها آگاه باشد. سازمان شما باید در زمان اعطای مجوز، و حداقل هر ۵ سال، آموزش / توجیهات آگاهی از امنیت را در اختیار دارندگان مجوز قرار دهد .پنج سال شرط اعتبارسنجی مجدد تصدیق دارنده ترخیص است .جلسات توجیهی باید جزئیات مسئولیت دارندگان تصفیه را شرح دهد.

یک دارنده مجوز تصفیه باید مسئولیت‌های خاصی را که به عنوان دارنده مجوز امنیت ملی دارند، درک کند و تصدیق کند .مدیر آنها باید با آنها توضیح دهد که آیا ادامه کار آنها منوط به حفظ ترخیص در سطح مناسب است.

راه‌های اطمینان از آگاهی و آموزش عبارتند از:

- ایجاد برنامه‌های مدیریت ریسک امنیتی پرسنل
- ارائه توجیهات اضافی با دارنده مجوز مربوط به سطح امنیت و نقش آنها.

❖ **دارنده ترخیص کالا را کنترل و ارزیابی کنید**

برای کمک به تعیین انتظارات از همان ابتدا، دارندگان ترخیص کالا باید بدانند که آنها به طور منظم مورد ارزیابی قرار می‌گیرند زیرا مناسب بودن آنها برای داشتن یک ترخیص کالا می‌تواند با گذشت زمان تغییر کند.

❖ **یک برنامه مدیریت خطر امنیتی ایجاد کنید**

هنگامی که یک توصیه بررسی از NZSIS با توصیه‌های خاص ("صلاحیت") برای مدیریت ریسک امنیتی دریافت می‌کنید، باید یک برنامه مدیریت ریسک امنیتی را با دارنده مجوز تنظیم کنید و یک نسخه از برنامه را به NZSIS ارائه دهید.

❖ **جلسات امنیتی را در صورت لزوم انجام دهید**

انواع توجیهاتی که ممکن است هنگام شروع یا برای اهداف خاص به افراد داده شود عبارتند از:

- جلسات توجیهی سفر و سفر خارج از کشور و توجیهات ایمنی شخصی هنگام مسافرت با مشاغل رسمی یا اهداف شخصی
- جلسات توجیهی و خلاصه نویسی برای دسترسی به مطالبTOP SECRET
- جلسات توجیهی و خلاصه توضیحات برای اجازه دسترسی به اطلاعات یا منابع منعکس شده از نظر محافظتی که دارای تأیید هستند، به صورت مجزا یا دارای محافظت از رمز ورود **توجه:** برخی از این جلسات را باید NZSIS یا GCSB ارائه دهند
- جلسات توجیهی خاص برای مقاصد پرخطر
- جلسات توجیهی برای دسته بندی‌های خاص استخدام، به عنوان مثال، مسائل امنیتی منحصر به فرد کارکنان فناوری اطلاعات(IT) ، دانشمندان و دیگران
- جلسات توجیهی متناسب با پیمانکاران، کارمندان موقت، بازدید کنندگان و خانواده‌های کارکنان
- جلسات توجیهی متناسب با نیازهای خاص امنیتی فرد به عنوان بخشی از یک برنامه مدیریت مداوم
- جلسات توجیهی مدیریت ریسک به طور کلی و توجیهات امنیتی محافظتی به طور خاص

۴-۷-۶-اطمینان از مناسب بودن مداوم آنها (برای دارندگان ترخیص)

سازمان شما باید امنیت پرسنل را در سراسر استخدام دارنده مجوز امنیت ملی در نظر بگیرد .در حالی که فرایندهای استخدام و عزیمت فرصت‌های مشخصی را برای مدیریت خطرات مرتبط با یک دارنده مجوز ارائه می‌دهند، چالش برانگیزترین و مهمترین مرحله چرخه حیات امنیتی پرسنل مدیریت دارنده مجوز در طول کار آنها است.

❖ **خلاصه مسئولیت‌های شما**

سازمان شما باید به دارندگان ترخیص کالا کمک کند تا مسئولیت‌های خود را برآورده کنند و اطمینان حاصل کند که آنها برای داشتن ترخیص کالا مناسب هستند .برای انجام این مسئولیت‌ها:

- در مورد امنیت ارتباطات شفاف منتشر کنید
- آموزش و بروزرسانی آگاهی از امنیت را ارائه دهید
- جلسات امنیتی را در صورت لزوم انجام دهید
- دارندگان ترخیص کالا را برای هر سفر بین المللی آماده کنید
- اطمینان حاصل کنید که دارندگان ترخیص، تغییر در شرایط شخصی خود را گزارش می‌دهند
- اطمینان حاصل کنید که دارندگان ترخیص هرگونه تماس و رفتار مشکوک را گزارش می‌دهند
- هرگونه تغییر در شرایط شخصی دارنده ترخیص را گزارش دهید
- گزارش و پاسخگویی به حوادث امنیتی، از جمله تماس‌های مشکوک
- دسترسی اضطراری به اطلاعات طبقه بندی شده، دارایی‌ها و مکان‌های کار را مدیریت کنید
- گزارش تغییرات سطح امنیتی دارنده مجوز
- مرتباً مجوزها را بررسی کرده و تغییرات شرایط شخصی را بررسی کنید .

❖ **در مورد امنیت ارتباطات شفاف منتشر کنید**

سازمان شما باید اطمینان حاصل کند که دارندگان ترخیص کالا به سیاستها و روشهای روشنی دسترسی دارند:

- شرایط امنیتی خود را توضیح دهید
- طرح کلیه موارد قانونی، نظارتی و انطباق.

❖ **آموزش و بروزرسانی آگاهی از امنیت را ارائه دهید**

با ارائه به روزرسانی و آگاهی از امنیت، می‌توانید به یک دارنده ترخیص در انجام وظایف خود کمک کنید .آموزش باید حداقل سالی یک بار انجام شود.

❖ **جلسات امنیتی را در صورت لزوم انجام دهید**

در صورت لزوم، باید با دارندگان ترخیص، جلسات امنیتی یا خلاصه توضیحات امنیتی بیشتری را انجام دهید. برای کسب اطلاعات بیشتر در مورد توجیهات امنیتی، مراجعه کنید به انتظارات صحیح را تنظیم کنید

❖ **دارندگان ترخیص کالا را برای سفرهای بین المللی آماده کنید**

وقتی دارندگان ترخیص کالا به دلایل شغلی یا شخصی به خارج از کشور سفر می‌کنند، با هدف قرار دادن منافع نیوزیلند توسط سرویس‌های اطلاعاتی خارجی هدف قرار می‌گیرند.

دارندگان ترخیص کالا به دلایل مختلفی، از جمله نیوزیلند، ممکن است مورد توجه سرویس‌های اطلاعاتی خارجی قرار گیرند:

- موضع گیری در مورد مسائل و توافق نامه‌های بین المللی مانند تجارت
- چشم انداز و اهداف استراتژیک در سیاست‌های داخلی
- نوآوری در علم و فناوری
- کشاورزی، صنایع اولیه و سایر بخشهایی که توجه قابل توجه سرمایه گذاران خارجی را به خود جلب می‌کنند
- قابلیت‌های دفاعی و اطلاعاتی

به یاد داشته باشید که دارندگان ترخیص شما می‌توانند در نیوزیلند در کنفرانس‌ها یا هنگام میزبانی از هیئت‌های بین المللی در معرض همان خطرات قرار گیرند. سازمان شما مسئول مدیریت هر گونه خطرات در سفرهای بین المللی و اطمینان از ارائه توجیهات سفر برای سفرهای مرتبط با کار است. برای کمک به آماده سازی دارندگان ترخیص برای سفر، مطمئن شوید که آنها راهنمای زیر را بخوانند :مشاوره برای مقامات دولت نیوزلند که برای تجارت به خارج از کشور سفر می کنند

❖ برنامه‌های سفر بین المللی برای دارندگان ترخیص چه زمان گزارش شود

اگر یک دارنده مجوز، جلسات توجیهی اطلاعات حساس (SCI) را برگزار کند، برای سفر به کشورهای مشخص شده به تأیید اضافی نیاز دارد.

برای مشاوره بیشتر با این آدرس تماس بگیریدpsr@protectivesecurity.govt.nz :

❖ اطمینان حاصل کنید که دارندگان پروانه گزارش تغییرات قابل توجهی در شرایط شخصی دارند

اطمینان حاصل کنید که دارندگان ترخیص سازمان شما هرگونه تغییر قابل ملاحظه‌ای را در شرایط شخصی خود گزارش می‌دهند، بنابراین می‌توانید بررسی کنید که آیا بر قابلیت اطمینان و توانایی حفظ ترخیص آنها تأثیر دارد.

برای راهنمایی بیشتر در مورد ارزیابی ادامه دارایی یک دارنده مجوز در صورت بروز حادثه امنیتی، تغییر در شرایط شخصی یا مسئلهHR ، به راهنمایی‌های زیر مراجعه کنید :ارزیابی و اقدام در مورد تغییرات شرایط دارنده مجوز .

❖ معنی "تغییر قابل توجه" چیست

تغییرات زیر در شرایط دارنده ترخیص قابل توجه است و باید به مدیر ارشد سازمان سازمان (CSO) گزارش شود.

- شروع یا پایان دادن به یک رابطه شخصی نزدیک
- زندگی در یا سفر به کشورهای خارجی
- اقوام دارای اهمیت امنیتی در کشورهای خارجی زندگی می‌کنند
- تغییر در تابعیت یا تابعیت
- تغییر در شرایط مالی (به عنوان مثال، افزایش چشمگیر ثروت یا بدهی)
- تغییر در شرایط بهداشتی یا پزشکی (به عنوان مثال، یک وضعیت پزشکی جدی می‌تواند رفتار دارنده مجوز را تغییر دهد یا مشکلات مالی ایجاد کند و داروهای تجویزی می‌توانند بر قضاوت افراد تأثیر بگذارند)
- مشارکت در فعالیت مجرمانه
- درگیر شدن با هر فرد، گروه، جامعه یا سازمانی که ممکن است نگران کننده امنیت باشد

- رویه‌های انضباطی یا حوادث امنیتی
- هرگونه تغییر در شرایط دیگر که ممکن است نگران کننده سازمان شما باشد.

❖ گزارش تغییرات قابل توجه در CSO شما

دارندگان ترخیص شما باید بلافاصله هرگونه تغییر قابل ملاحظه در شرایط شخصی خود را به CSO شما و به مدیر آنها (در صورت لزوم) گزارش دهند .این نیاز گزارش دهی به کاهش هرگونه تعارض منافع احتمالی کمک می‌کند.

اگر سازمان امنیت داخلی شما مطمئن نیست که آیا تغییر در شرایط شخصی پیامدهای قابل توجهی در مورد تصدیق دارنده دارد یا خیر، آن‌ها باید مشاوره بگیرند.

برای مشاوره، با این آدرس تماس بگیریدpsr@protectivesecurity.govt.nz :

اگر افراد دیگر در سازمان شما از تغییر قابل توجهی در شرایط دارنده مجوز آگاه شوند - تغییری که ممکن است در شایستگی آنها در حفظ مجوز یا رعایت استانداردهای امنیتی سازمان شما تأثیر بگذارد - آن‌ها باید این تغییر را به سازمان امنیت داخلی شما گزارش دهند.

شکل تغییر شرایط

❖ شناخت و ارزیابی تغییر قابل توجه در شرایط

وقتی از اوایل تغییر شرایط مطلع شوید، معمولاً برخورد با این مسئله را آسان می‌کند و از تبدیل شدن آن به یک مسئله امنیتی جلوگیری می‌کند .سپس می‌توانید خطرات موجود در دارنده ترخیص و سازمان خود را کاهش دهید.

❖ وقتی سازمان شما از تغییر قابل توجهی آگاه است چه کاری باید انجام دهید

هنگامی که یک تغییر قابل توجه در شرایط شناسایی یا گزارش می‌شود، سازمان شما باید ارزیابی خطر را بر اساس اینکه آیا دارنده ترخیص کالا می‌تواند به یک ترخیص ادامه دهد، انجام دهد .اگر در مورد ادامه ترخیص کالا تردید دارید، سازمان شما باید آن را به حالت تعلیق درآورد یا لغو کند تا زمانی که خطر کاهش یابد یا ارزیابی شود که دیگر وجود ندارد.

هنگامی که سازمان شما باید یک تغییر مهم را به NZSIS اطلاع دهد

هنگامی که تغییر شرایط قابل توجه تلقی می‌شود یا احتمال خطر برای امنیت ملی را تهدید می‌کند، سازمان شما باید بررسی NZSISرا مطلع کند.

NZSISممکن است لازم باشد که سازمان شما درخواست تأیید جدید برای دارنده مجوز را ارائه دهد .اگر NZSIS راضی باشد که نگهدارنده ترخیص کالا برای حفظ ترخیص کالا مناسب است، توصیه مثبتی می‌کند .مشاوره مدیریت ریسک ممکن است شامل اقدامات خاصی باشد که سازمان شما باید انجام دهد.

اطمینان حاصل کنید که دارندگان ترخیص کالا از تماس مشکوک خبر می‌دهند

دارنده تصفیه باید هرگونه تماس مشکوک یا درخواست دسترسی به اطلاعات طبقه بندی شده سازمان شما، دارایی‌ها یا محل کار را به CSO خود گزارش دهد.

مواردی از تماس یا درخواست مشکوک شامل تماس با موارد زیر است:

- مقامات خارجی و اتباع خارجی
- گروه‌ها یا افراد جنایتکار
- افراد مشکوک دیگر
- در حال تکمیل گزارش تماس مشکوک

دارندگان ترخیص کالا باید از زمانی که یک تماس رسمی یا اجتماعی مشکوک، مستمر، مداوم یا غیرمعمول (SOUP) است، یک گزارش تماس را تکمیل کنند .این تماس می‌تواند با موارد زیر باشد:

❖ **سفارت یا مقامات دولت خارجی در نیوزیلند**

مقامات خارجی یا اتباع خارج از نیوزیلند، از جمله نمایندگان تجارت یا تجارت

هر فرد یا گروهی، صرف نظر از ملیت، که به دنبال به دست آوردن اطلاعات رسمی یا تجاری حساس است که "نیاز به دانستن" معتبری ندارند.

- فرم گزارش تماس بگیرید.

❖ **ارزیابی گزارش مشکوک تماس**

سازمان شما باید همه گزارش‌های مشکوک مخاطب را ارزیابی کند تا بررسی کند که آیا شما نیاز دارید:

- گزارش‌های تماس از سایر افراد مربوطه را جمع آوری کرده و آنها را ارزیابی کنید
- NZSIS را برای تماس‌هایی که ممکن است پیامدهای امنیت ملی داشته باشند، راهنمایی کنید
- انجام تحقیقات داخلی (مراجعه به گزارش حوادث و انجام تحقیقات امنیتی)
- با پلیس NZ تماس بگیرید (به زیر مراجعه کنید)

بعضی اوقات ممکن است تماس‌های مشکوک یک دارنده تصفیه جنبه جنایی یا تجاری داشته باشد که شامل تعارض منافع یا یک مزیت ناعادلانه بالقوه باشد .سازمان شما باید پروسه روشنی برای بررسی این تماس‌ها داشته باشد و در صورت لزوم، مقامات مربوطه را برای تحقیقات بیشتر مطلع سازد (به عنوان مثال، پلیسNZ ، دفتر تقلب جدی)

❖ **دسترسی اضطراری به اطلاعات طبقه بندی شده، دارایی‌ها و مکان‌های کار را مدیریت کنید**

برای کسب اطلاعات در مورد مدیریت دسترسی اضطراری، به این قسمت بروید :مجوز امنیتی آنها را مدیریت کنید

❖ **گزارش تغییرات سطح امنیتی دارنده مجوز**

برای کسب اطلاعات در مورد گزارش تغییرات، به :مدیریت ترخیص امنیتی آنها بروید

❖ **مرتباً مجوزها را بررسی کرده و تغییرات شرایط شخصی را بررسی کنید**

در حالی که روند تأییدیه برای سازمان شما سطح مشخصی از اطمینان راجع به مناسب بودن شخص برای تصویب به سازمان می‌دهد، این اطمینان فقط مربوط به زمان انجام بررسی است - این مناسبتی در آینده را تضمین نمی‌کند .به همین دلیل، اگر سازمانی هستید که از این مجوز حمایت مالی می‌کنید، باید:

- برای اطمینان از حفظ سطح اطمینان لازم، تمام مجوزهای امنیتی را بررسی کنید
- مرتباً بررسی کنید تا ببینید شرایط دارندگان ترخیص شما تغییر کرده است یا خیر.

برای حمایت از سازمان شما برای مدیریت شایستگی مداوم دارندگان مجوزهای امنیت ملی، فرم‌های ارزیابی سالانه امنیت (ASAF)موجود است. ASAFبرای دارندگان مجوزهای امنیت ملی - این فرم را برای دارندگان مجوز ارسال کنید تا در سالگرد یا تاریخی که سازمان تعیین کرده است، تکمیل شوند. ASAFبرای مدیران دارندگان مجوزهای امنیت ملی - این فرم را برای مدیران خط ارسال کنید تا پس از دریافت فرم تکمیل شده از دارنده مجوز امنیت ملی، آن را تکمیل کنند.

ASAFبرای تیم های امنیتی یا افسر ارشد امنیتی - این فرم برای تیم‌های امنیتی است که برای بررسی هر دو فرم کامل شده در بالا استفاده می‌کنند .از آن برای ارزیابی هرگونه نگرانی یا شناسایی نیاز به اجرای برنامه‌های مدیریتی برای دارندگان ترخیص استفاده کنید. از این فرم‌ها در نسخه PDF قابل ویرایش خود استفاده کنید یا از نسخه‌های word برای انطباق با نیازهای سازمان خود استفاده کنید. اگر سازمان شما دیگر اطمینان لازم را ندارد، به یاد داشته باشید که می‌توانید در هر مرحله تصفیه را بررسی، تعلیق، لغو یا برداشت کنید.

۴-۷-۷-حفظ امنیت ملی خود

این بخش به شما کمک می‌کند مسئولیت‌های خود را به عنوان یک دارنده مجوز امنیت ملی درک کنید، بنابراین می‌توانید آنها را برآورده کرده و برای نگهداری مجوز مناسب باشید.

❖ **اینکه چرا برای داشتن ترخیص کالا مناسب است، مهم است**

داشتن ترخیص ممکن است یک نیاز اساسی برای نقش شما یا شرط اشتغال شما باشد .به نفع شما و سازمان شماست که برای تصفیه مجوز مناسب باشید.

❖ **مسئولیت‌های شما**

برای حفظ ترخیص، باید مسئولیت‌های خود را به عنوان دارنده ترخیص انجام دهید. اطمینان حاصل کنید که مسئولیت‌های خود را می‌خوانید و می‌فهمید، یا شخصی را در آژانس خود راهنمایی کنید تا به شما در درک آنها کمک کند.

۱) به "اصل نیاز به دانستن" احترام بگذارید

"اصل نیاز به دانستن" فقط در مورد دسترسی یا اشتراک اطلاعات و منابع طبقه بندی شده با افرادی است که سطح صحیح تصفیه را دارند و برای انجام کار خود به دسترسی نیاز دارند.

اگر شخصی از شما درخواست دسترسی می‌کند اما سطح تصفیه صحیحی ندارد، باید "نه" بگویید .اگر فردی سطح ترخیص صحیحی دارد اما برای انجام وظیفه خود نیازی به دسترسی به اطلاعات ندارد، باید "نه" بگویید.

۲) گزارش تغییر در شرایط شخصی خود

تغییرات زیر را باید به محض وقوع به آژانس خود گزارش دهید .سپس آژانس شما می‌تواند خطرات را ارزیابی کرده و در صورت نیاز برای کاهش آنها اقدام کند.

- شما یک رابطه شخصی نزدیک را شروع یا خاتمه می‌دهید
- شما به یک کشور خارجی سفر می‌کنید
- هر یک از بستگان نزدیک شما به یک کشور خارجی نقل مکان می‌کند
- شما قصد تغییر تابعیت یا کشور محل اقامت خود را دارید
- شرایط مالی شما تغییر می‌کند
- شرایط سلامتی یا پزشکی شما تغییر می‌کند

- شما به طور تصادفی یا عمدی درگیر فعالیت جنایی هستید
- شما با افراد یا گروه‌هایی درگیر می‌شوید که ممکن است امنیت را تحت تأثیر قرار دهند
- شما در یک روند انضباطی هستید
- شما امنیت را زیر پا گذاشته‌اید و یا حادثه امنیتی ایجاد کرده‌اید
- شما در شرایط شخصی تغییرات دیگری نیز دارید که آژانس شما به شما گفته است گزارش دهید.

۳) گزارش تغییرات در شرایط دیگران

به سازمان خود اجازه دهید در مورد رفتارها یا حوادث مربوط به افرادی که با آنها کار می‌کنید آگاه شود و به آنها امکان می‌دهد تا روش‌هایی را برای حمایت از آن شخص و حفظ فرهنگ امنیتی سازمان در نظر بگیرند.

۴) برنامه‌های سفر به خارج از کشور را با آژانس خود در میان بگذارید

قبل از رزرو سفرهای خارج از کشور، برنامه‌های سفر خود را با آژانس خود در میان بگذارید.

۵) گزارش تماس‌ها و درخواست‌های مشکوک

شما باید برای دسترسی به اطلاعات و منابع آژانس خود، تماس و درخواست مشکوک را گزارش کنید.

۶) خطرات ناشی از استفاده از شبکه‌های اجتماعی خود را به حداقل برسانید

باید درمورد ارسال مطالب خود در شبکه‌های اجتماعی، از جمله شبکه‌های مرتبط با کار مانندLinkedIn ، بسیار مراقب باشید.

۷) قانون و خط مشی را درک و مطابقت داشته باشید

برای حفظ ترخیص کالا از گمرک، باید موارد زیر را بفهمید:

- الزامات قانون جرایم ۱۹۶۱
- سیاست امنیتی آژانس شما
- الزامات مندرج در راهنمای "حفظ مجوز امنیت ملی خود."

۸) در بررسی‌های منظم شرکت کنید

NZSIS شایستگی شما برای داشتن مجوز را بررسی می‌کند - معمولاً هر پنج سال اگر NZSIS یا آژانس شما نگران رفتار شما باشد یا خطرات خاص دیگری وجود داشته باشد، بررسی ممکن است زودتر انجام شود.

۹) الزامات هر طرح مدیریت خطر امنیتی را برآورده کنید

اگر توصیه بررسی برای ترخیص شما شامل توصیه‌های خاصی ("صلاحیت") باشد، آژانس شما باید یک طرح مدیریت ریسک امنیتی را با شما توافق کرده باشد.

۴-۷-۸-مجوز امنیتی آنها را مدیریت کنید

مدیریت دارنده ترخیص امنیت ملی شامل نظارت بر رفتارهای مربوط به آن، گزارش دادن و پاسخگویی به حوادث امنیتی مربوط به آنها، مدیریت دسترسی اضطراری آنها به اطلاعات، دارایی‌ها یا مکان‌های کاری و مدیریت تغییرات در سطح ترخیص امنیتی آنها است.

شما همچنین باید بدانید که بررسی، تمدید، اشتراک (استفاده از اهرم فشار) یا انتقال مجوز شامل چه مواردی است .

❖ **نظارت بر رفتارهای نگران کننده**

اگر یک دارنده ترخیص کالا را مدیریت می‌کنید، باید رفتار او را کنترل کنید تا نگرانی‌های مربوط به امنیت، عملکرد ضعیف یا رفتار غیرقابل قبول را داشته باشد .نظارت همچنین به معنی مشاهده علائمی است که می‌تواند فرد را غیرقابل اعتماد یا مستعد فشار معرفی کند .اگر دارنده مجوز:

- زیر ۲۰ سال است (شخصیت آنها هنوز شکل می‌گیرد)
- مایل نیست در مورد مسائل صحبت کند، اما به وضوح ناراضی است
- دوستان کمی دارد و به نظر می‌رسد با همکاران خود بیگانه است.

هنگام در نظر گرفتن این عوامل احساس دیدگاه لازم است .و به یاد داشته باشید که در وظایف معمول "وظیفه مراقبت" خود به عنوان مدیر عمل کنید. اگر یک مسئله رفتاری را کشف کردید، باید از طریق ابزارها و سیاست‌های سازمان خود، از طریق هر فرآیند حل و فصل، دارنده مجوز را شناسایی، پشتیبانی و مدیریت کنید.

❖ **گزارش و پاسخگویی به حوادث امنیتی**

مدیریت مؤثر حوادث و تحقیقات امنیتی بخشی اساسی از امنیت خوب است.

سازمان شما باید سوابق همه موارد را ثبت کند:

- نقض امنیت، از جمله نقض سیاست و رویه‌های سازمان که منجر به مصالحه در منافع ملی می‌شود
- نقض امنیت، مانند نقص تصادفی یا غیر عمدی در رعایت الزامات رسیدگی به اطلاعات یا دارایی‌های طبقه بندی شده
- تخلفات امنیتی، از جمله اقدامی عامدانه که منجر به ایجاد مصالحه در اطلاعات طبقه بندی شده، دارایی‌ها یا مکان‌های کاری می‌شود یا می‌تواند منجر شود.

❖ **جزئیات نقض امنیت دارندگان ترخیص را به NZSIS ارائه دهید**

اگر فکر می‌کنید یک دارنده تصفیه امنیت را نقض کرده است، رئیس ارشد امنیتی شما (CSO) باید وضعیت را ارزیابی کند و پاسخ را شناسایی کند، که ممکن است شامل مشاوره به سرویس اطلاعات امنیتی نیوزلند (NZSIS) یا اداره امنیت ارتباطات دولتی (GCSB) باشد.

❖ **نقض امنیت چیست؟**

❖ **بررسی علت**

"بررسی علت"، بازبینی یک دارنده مجوز است هنگامی که سازمان شما نگرانی‌های امنیتی را شناسایی می‌کند که می‌تواند بر شایستگی آن برای حفظ مجوز تأثیر بگذارد NZSIS .بررسی را انجام می‌دهد.

سازمان شما می‌تواند در پاسخ به هرگونه نگرانی امنیتی درباره یک دارنده مجوز، بررسی علت را آغاز کند.

نگرانی‌های امنیتی معمولاً به تغییرات قابل توجهی در شرایط شخصی، نگرش یا رفتار دارنده مجوز مربوط می‌شود.

نگرانی در مورد دارنده ترخیص کالا از این قرار است:

- دارنده ترخیص کالا
- همکاران یا ناظران دارنده ترخیص کالا

- هر شخص دیگری که منطقی معتقد باشد شرایط شخصی، نگرش یا رفتار دارنده تصفیه تغییر کرده است.

❖ **در صورت لزوم دسترسی را متوقف کنید**

اگر سازمان شما به دلیل نقض امنیت در حال بررسی یک دارنده ترخیص کالا است، سازمان امنیت عمومی شما باید دسترسی آنها به اطلاعات طبقه بندی شده، دارایی‌ها یا مکانهای کار را تا زمان انجام تحقیقات (که ممکن است شامل بررسی علت) باشد، به حالت تعلیق درآورد.

❖ **در صورت لزوم مجوز را لغو کنید**

صرف نظر از هرگونه توصیه برای بررسی علل، مدیر اجرایی شما حق دارد اگر بخاطر نگرانی‌های امنیتی، نقض یا نقض آن بیش از حد مکرر یا به اندازه کافی جدی باشد، مجوز امنیت ملی را لغو کند.

❖ **اطلاعات بیشتر**

گزارش حوادث و انجام تحقیقات امنیتی

❖ **دسترسی اضطراری به اطلاعات طبقه بندی شده، دارایی‌ها یا مکان‌های کاری را مدیریت کنید**

گاهی اوقات شرایط اضطراری ممکن است نیاز عملیاتی فوری به دارنده مجوز برای دسترسی به اطلاعات طبقه بندی شده، دارایی‌ها یا مکانهای کاری بالاتر از سطح تصفیه آنها را ایجاد کند .رئیس اجرایی یا نماینده آن‌ها می‌توانند این امر را اعطا کنند .در صورت تفویض اختیار، باید کتباً ثبت شود.

❖ **منظور از "دسترسی اضطراری" است**

دسترسی اضطراری به این معنی است که سازمان شما یک نیاز عملیاتی ضروری و ضروری را برای دسترسی به اطلاعات خاص، دارایی‌ها یا مکان‌های کاری تأیید کرده است و زمان کافی برای تکمیل بررسی‌های تأیید و صدور مجوز در سطح بالاتر وجود ندارد.

دسترسی اضطراری باید:

- فقط به اطلاعات مشخص شده، دارایی‌ها یا محل کار مورد نیاز برای موارد اضطراری
- فقط برای مدت اضطراری
- با اعمال بسیار دقیق اصل نیاز به دانستن اداره می‌شود
- بیش از یک سطح بالاتر از سطح فعلی شخص ارائه نشده است*
- تحت نظارت مدیری با اختیارات مناسب.

دسترسی اضطراری به اطلاعات محفظه حساس (SCI) باید توسط GCSB تأیید شود. به عنوان مثال، اگر مجوز فعلی یک دارنده مجوز محرمانه باشد، مدیر او (با یک مجوز مناسب) ممکن است بر او نظارت کند تا مواد SECRET را تا زمان اضطرار مشاهده کند.

❖ **الزامات ضبط، خلاصه و توضیحات**

مدیر باید ثبت کند که دسترسی اضطراری اعطا شده است و دارنده مجوز را به طور مناسب شرح دهد.

دارنده ترخیص کالا باید تصدیق کند که مدیر آنها قبل از اینکه به وی اجازه داده شود، آن‌ها را مختصر معرفی کرده است .سازمان شما باید این تأیید را به صورت کتبی ثبت کند. سازمان شما همچنین باید با پایان یافتن وضعیت اضطراری، دارنده مجوز را شرح دهد.

❖ **محدودیت استفاده از دسترسی اضطراری**

- برای اعطای دسترسی به دارنده مجوز، نباید از دسترسی اضطراری استفاده کنید:
- برای اهداف اداری یا مدیریتی (مانند کمک به آنها برای کسب موقعیت)

هنگامی که آنها مشغول انجام وظایف مجدد هستند در حالی که منتظر توصیه بررسی امنیتی هستند (از جمله طبقه بندی مجدد) به اطلاعات طبقه بندی شده، دارایی‌ها یا مکان‌های کاری که دارای تأییدیه یا علامت گذاری مجزا هستند. شما نباید به هر کسی که دارای مجوز نیست، دسترسی اضطراری به اطلاعات، دارایی‌ها یا مکان‌های کاری را که با نام "محرمانه" یا بالاتر مشخص شده‌اند، اعطا کنید.

❖ **تغییر در سطح تصفیه امنیت را مدیریت کنید**

گاهی اوقات سطح یا وضعیت ترخیص کالا از گمرک دارنده تغییر می‌کند .سازمان‌های سازمانی سازمان شما باید هر زمان که مجوز تصویب می‌شود به NZSIS بگویید:

- اعطا شده یا رد شده است
- به روز شده یا تنزل یافته است
- تعلیق یا تمدید
- انتقال یا اهرم (با سازمان دیگری به اشتراک گذاشته شده است)
- تمدید شده
- لغو شد.

❖ **مجوزها را پس از ۵ سال بررسی کنید**

تصویب نامه امنیت ملی پس از ۵ سال منقضی می‌شود (یا اگر سازمان شما آن را برای مدت کوتاه‌تری اعطا کرده باشد) یا زمانی که دارنده ترخیص کار خود را ترک کند، زودتر از این اعتبار می‌گذرد. مدیر دارنده مجوز وظیفه مدیریت فرایند برای اطمینان از ادامه ترخیص را دارد، حتی اگر سطح ترخیص تغییر کند.

❖ **تمدید مجوز**

برای تمدید مجوز، سازمان امور مالیاتی شما ابتدا باید شایستگی مداوم دارنده مجوز را برای داشتن مجوز ارزیابی کند .اگر نتیجه ارزیابی مثبت باشد، سازمان‌های امنیت داخلی می‌توانند درخواست تأیید امنیت را به NZSIS ارسال کنند و آنها تصویب نامه را بررسی می‌کنند.

قبل از اینکه درخواست تأیید امنیت را ارائه دهند، سازمان امنیت و همکاری شما باید به توانایی دارنده مجوز برای دریافت توصیه مطلوب از NZSIS اعتماد و اطمینان داشته باشد .برای انجام چنین ارزیابی، سازمان‌های سیاسی شما باید قضاوت خود را انجام دهند و تمام اطلاعات موجود را به طور عینی مشاهده کنند. سازمان شما باید تمدید ترخیص توسط NZSIS را برای حفظ تداوم ترخیص از اوایل آغاز کند، مگر اینکه شخص:

دیگر در موقعیتی نیست که نیاز به ترخیص داشته باشد، یا

شغل دولت نیوزیلند را ترک کرده است.

❖ **ترخیص را تمدید کنید**

سازمان شما ممکن است یک بار مجوز را حداکثر تا ۶ ماه تمدید کند، در مجموع تا ۱۲ ماه.

❖ **نمونه سناریوها**

روند تمدید قبل از انقضا ترخیص کامل نخواهد شد

۱) دارنده ترخیص شما در حال تمدید ترخیص است اما به نظر نمی‌رسد قبل از انقضا ترخیص از نو تمدید شود، بنابراین شما ترخیص را برای ۶ ماه تمدید می‌کنید.

۲) دارنده ترخیص شما در خارج از کشور مستقر شده است، بنابراین آن‌ها نمی‌توانند فرم‌های تمدید خود را تکمیل کنند .انتظار می‌رود که آنها ۶ ماه دیگر بازگردند، بنابراین شما ترخیص را برای ۶ ماه تمدید می‌کنید .بعد از ۵ ماه، متوجه می‌شوید که دارنده ترخیص به زودی بر نمی‌گردد و هنوز نمی‌تواند فرم‌های خود را پر کند .سپس ترخیص آنها را برای ۶ ماه دیگر تمدید می‌کنید.

این ترخیص دوباره قابل تمدید نیست زیرا به حداکثر زمان تمدید خود یعنی ۱۲ ماه رسیده است.

❖ **ترخیص کالا قبل از پایان قرارداد منقضی می‌شود**

قرار است ترخیص منقضی شود اما قرارداد دارنده ترخیص برای ۳ هفته بیش از تاریخ انقضا اجرا می‌شود .دارنده ترخیص کالا پس از پایان قراردادش به ترخیص نیاز ندارد، بنابراین به جای تمدید مجوز، آن را برای ۱ ماه تمدید می‌کنید.

❖ **شما می‌خواهید برای بار دوم مجوز را تمدید کنید**

مجوز تصفیه شما توسط سازمان حمایت مالی ۱ ماه تمدید شده است .بعداً، سازمان حامی مالی مجوز را برای ۶ ماه دیگر تمدید می‌کند .این دو افزونه به ۷ ماه اضافه می‌شود، بنابراین ۵ ماه دیگر برای سازمان از هر ۱۲ ماه دیگر برای هر برنامه تمدید باقی مانده است .

❖ **قوانینی که باید بخاطر بسپارید**

سازمان شما فقط می‌تواند قبل از انقضا a مجوز و در صورت عدم صلاحیت مجوز، مدت تمدید را اعطا کند. برای اطمینان از اینکه نگهدارنده مجوز برای تمدید مجوز مناسب است، باید دقت کافی خود را انجام دهید. شما باید در طول مدت برنامه افزودنی به مدیریت دارنده ترخیص کالا ادامه دهید. اگر این مجوز با سازمان دیگری به اشتراک گذاشته شده است (اهرم اعتبار)، قبل از تمدید مجوز، باید ترتیب اشتراک گذاری را مرور کنید .پس از تمدید مجوز، شما باید سازمان دیگر را مطلع کنید.

❖ **ترخیص را منتقل کنید**

ممکن است سازمان شما بتواند مجوز را از یک سازمان حمایت کننده به سازمان شما منتقل کند .برای انجام این کار، ترخیص موردنیاز برای شخصی که به آن منتقل می‌شود باید در همان سطح یا پایین‌تر از ترخیص کالا از قبل باشد. سازمان‌های دولتی نمی‌توانند در سطح بالاتر تصویب کنند بدون اینکه قبلاً از NZSIS توصیه تأیید شده باشند. برای اطلاعات بیشتر در مورد انتقال ترخیص، به :مدیریت عزیمت آنها بروید.

❖ **تصویب (اهرم) تصویب**

اگر سازمان شما قصد دارد با یک دارنده مجوز تحت حمایت مالی سازمان دیگری کار کند یا آن را به خدمت بگیرد، ممکن است بتوانید به جای گرفتن مجوز جدید، از آن مجوز استفاده کنید. این وضعیت ممکن است زمانی بوجود آید که زمان دارنده تصفیه بین سازمانها تقسیم شود. هر دو سازمان قبل از موافقت با توافق نامه تقسیم بندی، باید مورد قبول بودن خطرات را در نظر بگیرند.

❖ **مسئولیت‌های مشترک شما**

اگر موافقت می‌کنید تصویب کنید، هر دو سازمان باید:

- مسئولیت اشتراک نگرانی‌های امنیتی در مورد شخص را بپذیرید
- توافق کنید که چگونه ترخیص را مدیریت می‌کنید و مسئولیت هر کدام را بر عهده دارید
- درمورد هرگونه تغییر در شرایط دارنده مجوز، از یکدیگر آگاه شوید
- اطمینان حاصل کنید که دارنده پروانه جلسات امنیتی مناسب را دریافت می‌کند.

❖ **حمایت مالی از مسئولیت‌های سازمان**

- قبل از اینکه اطلاعات شخصی وی را با سازمان دیگر به اشتراک بگذارید، از دارنده مجوز اجازه بگیرید.
- اگر توصیه اصلی بررسی دارنده مجوز روتین بود، این امر را به سازمان دیگر اطلاع دهید.
- اگر توصیه اصلی بررسی معمول بود اما همراه با اطلاعات، صلاحیت‌ها، محدودیت‌ها یا یافته‌های نامطلوب بود، پیشنهاد اصلی بررسی را با سازمان دیگر به اشتراک بگذارید.
- اگر برنامه‌هایی برای مدیریت ریسک برای دارنده مجوز در نظر گرفته‌اید، آن برنامه‌ها را با سازمان دیگر به اشتراک بگذارید.
- به بازرسی آزمایشی NZSIS اطلاع دهید که می‌خواهید تصویب نامه‌ای را به اشتراک بگذارید و به آنها بگویید با چه کسی آن را به اشتراک می‌گذارید.
- در صورت لغو یا تعلیق ترخیص کالا، باید تنظیم اشتراک را نیز به حالت تعلیق درآورید یا لغو کنید.
- در صورت انقضا ترخیص کالا، باید ترتیب اشتراک را لغو کنید.
- اگر ترخیص کالا را کاهش دهید، باید سازمان دیگر را مطلع کنید.
- اگر مجوز را به سازمان دیگری منتقل کنید، سازمان حامی مالی جدید باید بازبینی و تأیید ترتیب اشتراک را پذیرفت.

❖ **مدیریت ترتیبات اشتراک - سناریوهای نمونه**

یک دارنده ترخیص کالا با سازمان‌های مختلف قرارداد دارد

یک دارنده ترخیص همزمان با سازمان‌های مختلف دارای دو قرارداد است و برای هر شغل به ترخیص نیاز دارد. دارنده ترخیص ۱ روز در هفته در سازمان A و ۴ روز در هفته در سازمان B کار می‌کند. این دو سازمان توافق می‌کنند که سازمان B باید سازمان حامی مالی باشد و سازمان A برای ۱ روز در هفته، مجوز تصویب نامه با آنها را تصویب می‌کند .سازمان الف می‌داند که هر گونه تغییر در شرایط قرارداد را به سازمان ب اطلاع دهد.

❖ **یک دارنده ترخیص کالا در یک دوره کوتاه مدت است**

سازمان A دارنده ترخیص را حمایت مالی می‌کند و موافقت خود را با اعزام کوتاه مدت به سازمان ب اعلام می‌کند. هر دو سازمان موافقت می‌کنند که مجوز را برای مدت زمان اعزام به اشتراک بگذارند. هنگامی که ارسال پیام به پایان می‌رسد، سازمان A ترتیب اشتراک را لغو می‌کند.

❖ **وقتی فرد از کشور دیگری ترخیص فعلی داشته باشد**

اگر می‌خواهید با شخصی با مجوز امنیتی از استرالیا، کانادا، انگلستان یا ایالات متحده کار کنید، با تیم بررسی امنیتی NZSIS در تماس باشید تا در مورد وضعیت صحبت کنید.

❖ **در صورت لزوم به سطح تصفیه بالاتر ارتقا دهید**

اگر وظایف یا وظایف شغل به حدی تغییر کند که یک دارنده ترخیص نیاز به دسترسی به اطلاعات، دارایی‌ها یا مکان‌های کاری طبقه بندی شده در سطح بالاتر از ترخیص فعلی خود داشته باشد، باید در همان سطح بالاتر تحت بررسی امنیتی قرار گیرند.

سازمان شما باید:

- اطمینان حاصل کنید که دارنده واجد شرایط تصفیه در سطح بالاتر است
- از NZSIS بررسی امنیتی کنید
- پس از دریافت توصیه ازNZSIS ، سطح تصویب بالاتر دارنده توسط رئیس اجرایی شما اعطا شود
- دارنده را در مورد هرگونه تعهدات جدید مرتبط با سطح ترخیص بالاتر آنها مطلع کنید
- با طرحی برای مدیریت نگرانی‌ها یا الزامات در پیشنهاد بررسی NZSIS موافقت کنید.

❖ **در صورت لزوم به سطح ترخیص کالا از گمرک کاهش دهید**

یک نگهدارنده ترخیص ممکن است به سمت نقشی جدید حرکت کند که نیاز به سطح ترخیص کمتر دارد .این می‌تواند یک حرکت دائمی یا موقت باشد .متناوباً، سازمان شما ممکن است تصمیم بگیرد که یک فرد باید سطح تصفیه پایین‌تری داشته باشد .در این موارد، یک مدیر باید تأیید کند که آیا سطح تراز پایین‌تر بر توافق نامه کاری دارنده تصفیه تأثیر می‌گذارد و چگونه .در صورت نیاز از منابع انسانی یا مشاوره حقوقی بهره مند شوید .

بعداً، اگر به دارنده ترخیص کالا برای انجام وظایف در سطح ترخیص بالاتر نیاز دارید، می‌توانید به آنها اجازه دهید تا زمانی که:

- توصیه اولیه بررسی در آن سطح بالاتر بود
- شما به طور مناسب ترخیص آنها را مدیریت می‌کنید و هیچ نگرانی امنیتی وجود ندارد.

❖ **در صورت عدم تأیید مجوز، یا تا پایان مراحل بازبینی یا درخواست تجدیدنظر، دسترسی را پس بگیرید**

برای کسب اطلاعات بیشتر در مورد برداشتن دسترسی یا مدیریت صحیح مراحل بازبینی یا درخواست تجدیدنظر، به بخشهای زیر مراجعه کنید.

- عزیمت آنها را مدیریت کنید
- حفظ امنیت ملی خود
- انصاف رویه ای
- ارزیابی امنیت پرسنل شما

۴-۷-۹-عزیمت آنها را مدیریت کنید (برای دارندگان ترخیص)

هنگامی که یک دارنده مجوز امنیت ملی خارج می‌شود، آن‌ها دانش خود را در مورد عملیات تجاری سازمان، مالکیت معنوی، اطلاعات طبقه بندی شده و آسیب پذیری های امنیتی سازمان حفظ می‌کنند .مدیریت خوب عزیمت آنها به کاهش خطر سو استفاده از این دانش کمک خواهد کرد.

هنگامی که یک دارنده ترخیص کالا از یک سازمان خارج می‌شود، مدیر آن باید حداقل شرایط خروج را برای یک کارمند و برخی شرایط اضافی را انجام دهد .برای کسب اطلاعات بیشتر در مورد حداقل شرایط عزیمت، به این قسمت بروید :عزیمت آنها را مدیریت کنید.

آن‌ها همچنین باید:

- به آنها تعهدات مداوم خود را یادآوری کنید
- ترخیص امنیتی آنها را منتقل یا لغو کنید
- به سرویس اطلاعات امنیتی نیوزیلند (NZSIS) اطلاع دهید.

یک شخص مجاز مجاز ممکن است مجبور باشد:

- اطلاعات مربوط به دارنده تصفیه را از هرگونه دسترسی به اطلاعات محفظه حساس* (SCI)
- ارزیابی خروجی را با دارنده ترخیص انجام دهید
- تماس بعد از جدایی را با دارنده ترخیص کالا از بین ببرید.

*هنگامی که توسط صاحب SCI مجاز باشد، یک فرد مناسب ممکن است دارنده ترخیص را از او توضیح دهد .اگر هیچ کس در تیم CSO مجاز به انجام این گزارش نیست، CSOیا تیم امنیتی باید برای مشاوره با تیم PSR تماس بگیرند.

تماس باpsr@protectivesecurity.govt.nz :

❖ تعهدات مداوم خود را به آنها یادآوری کنید

مدیر دارنده ترخیص کالا باید دارنده ترخیص را یادآوری کند:

- نیاز به صلاحدید ادامه دار آنها پس از خروج از سازمان
- تعهد مادام العمر آن‌ها برای محافظت از اطلاعات طبقه بندی شده، دارایی‌ها و محل کار.

بدست آوردن تأیید کتبی دارنده ترخیص از این تعهدات، روش خوبی است.

❖ ترخیص امنیتی آنها را منتقل کنید

اگر یک دارنده ترخیص مستقیماً به یک سازمان دولتی دیگر منتقل شود، ممکن است مجوز تصویب آنها با آنها منتقل شود .به طور کلی، یک سازمان باید تصویب امنیتی اعطا شده توسط سازمان دیگر را تا زمانی که روند انتقال صحیح دنبال شود، تشخیص دهد.

❖ پذیرش انتقال ترخیص

رئیس اجرایی سازمان جدید ممکن است انتقال مجوز امنیتی از سازمان دیگری را بپذیرد .این عمل بلافاصله اتفاق خواهد افتاد، مشروط بر اینکه شرایط زیر فراهم شده باشد:

- ترخیص کالا از گمرک اولیه کمتر از ۵ سال است (با این حال، اگر ترخیص اولیه کمتر از ۱۲ ماه از تاریخ انقضا در زمان انتقال است، سازمان جدید باید بلافاصله روند تمدید ترخیص را آغاز کند)
- نیاز به دسترسی به اطلاعات طبقه بندی شده، دارایی‌ها یا محل کار در نقش جدید وجود دارد
- ترخیص منتقل شده در همان سطح یا در سطح کمتری از ترخیص کالا از گمرکی است که در ابتدا توسط NZSIS توصیه شده است

- دارنده ترخیص مستقیماً از یک سازمان دولتی به سازمان دیگر بدون یک دوره مداخله بدون نظارت امنیتی (به عنوان مثال، اقامت در خارج از کشور یا سفر گسترده) حرکت می‌کند
- رئیس اجرایی شما از سازمان سابق دارنده تصفیه اخذ می‌کند:
- توصیه بررسی از) NZSIS این ممکن است دارای توصیه‌های مهم مدیریت خطر امنیتی باشد(
- اطمینان کتبی از شایستگی مداوم دارنده ترخیص برای داشتن ترخیص
- اطلاع از هرگونه تغییر در شرایط شخصی دارنده تصفیه که پس از بررسی آنها اتفاق افتاده است.

❖ **امضای قرارداد رازداری یا قرارداد پس از جدایی**

ممکن است سازمان شما بعنوان بخشی از انتقال به دارنده ترخیص کالا برای امضای توافق نامه محرمانه بودن نیاز داشته باشد .این اقدام برای محافظت از هرگونه اطلاعات طبقه بندی شده، دارایی‌ها و مکان‌های کاری است که ممکن است آنها به عنوان بخشی از نقش جدید خود مورد بحث قرار دهند .همچنین ممکن است لازم باشد با سازمان شما قرارداد پس از جدایی امضا کنند.

❖ **توجیهات مدیریتی برایSCI**

به یاد داشته باشید که جلسات توجیهی SCI منتقل نمی‌شوند .قبل از انتقال، باید از سازمانی که در حال حاضر است، دارنده تصفیه راهنمایی شود .در صورت دسترسی بهSCI ، باید آنها را در مورد سازمانی که در حال انتقال هستند، معرفی کند.

- هنگام انتقال تصویب امنیتی به NZSIS اطلاع دهید
- سازمان شما باید NZSIS را هنگام انتقال ترخیص امنیتی مطلع کند.

❖ **وقتی ترخیص واگذار شده منقضی شود**

تصویب نامه امنیت ملی منتقل شده ۵ سال از تاریخ توصیه اولیه یا از زمانی که سازمان اصلی این مجوز را صادر کرده است، متوقف می‌شود.

❖ **مجوز امنیتی آنها را لغو کنید**

هنگامی که یک دارنده ترخیص کالا از سازمان شما خارج می‌شود، باید ترخیص آن را لغو کرده و به NZSIS اطلاع دهید که دیگر دارنده ترخیص را به کار نمی‌گیرید.

۸-۴- معیارهای ارزیابی امنیت و دستورالعمل‌های داوری

این بخش معیارهای ارزیابی امنیت و رهنمودهای قضاوتی را توضیح می‌دهد که روند بررسی NZSIS برای کمک به ارزیابی قابل اعتماد بودن یک نامزد و داشتن مجوز تصویب امنیت ملی استفاده می‌کند.

- معیارهای ارزیابی امنیتمعیارهای ارزیابی امنیتمعیارهای ارزیابی امنیت

❖ **جنبه‌های حقوقی ارزیابی بررسی امنیتی**

کارهایی که امنیت ملی نیوزیلند را شامل می‌شود، گاهی اوقات باید عواملی را در نظر گرفت که ممکن است در موارد دیگر تبعیض آمیز باشد، همانطور که در بخش ۲۵ قانون حقوق بشر ۱۹۹۳ شناخته شده است.

منع تبعیض در کار به دلایل ذکر شده در زیر در مورد استخدام در زمینه امنیت ملی اعمال نمی‌شود:

- اعتقاد مذهبی یا اخلاقی

- نظر سیاسی
- سلامت روان
- شرکا یا بستگان خاص ازدواج
- منشأ ملی

بعلاوه، اگر شخصی زیر ۲۰ سال باشد، اگر کار به سطح بالاییSECRET ، TOP SECRETیا TOP SECRET SPECIAL نیاز به تصویب امنیت ملی داشته باشد، این قانون نقض قانون نیست.

با این وجود، تبعیض بر اساس موارد زیر غیرقانونی است:

- جنسیت
- گرایش یا اولویت جنسی
- سن (غیر از آنچه در بالا توضیح داده شد)
- قومیت
- ناتوانی جسمی
- وضعیت تأهل.

❖ **روند بررسی امنیتی**

روند تأیید امنیت یک معاینه بر اساس "کل افراد، کل زندگی" برای تعیین مناسب بودن یک نامزد برای داشتن تصویب امنیت ملی است. صلاحیت دسترسی به مواد محافظت شده مشخص شده بر اساس این رهنمودها ارزیابی مثبت می‌شود. NZSIS باید کل زندگی و طیف وسیعی از تجربیات شما را در نظر بگیرد - بنابراین آنها شما را به عنوان یک فرد منحصر به فرد دقیق ارزیابی می‌کنند. تمام اطلاعات موجود و قابل اعتماد در مورد نامزد، گذشته و حال، مطلوب و نامطلوب، باید برای رسیدن به یک تصمیم گیری در نظر گرفته شود.

در ارزیابی ارتباط هر رفتاری، افسر ارزیابی باید موارد زیر را در نظر بگیرد:

- ماهیت، میزان و جدیت رفتار
- شرایط پیرامون رفتار، از جمله میزان مشارکت آگاهانه و / یا آگاهانه
- تکرار و اخیر بودن رفتار
- سن و بلوغ نامزد در زمان انجام رفتار
- وجود یا عدم توانبخشی و سایر تغییرات مربوط به رفتار
- انگیزه برای رفتار
- پتانسیل فشار، اجبار، استثمار یا فشار
- احتمال ادامه یا عود.

داوطلبان باید بر اساس شایستگی‌های خود ارزیابی شوند و تعیین نهایی بر عهده کارکنان دامپزشکی است. هر گونه تردید در مورد مناسب بودن نامزد باید به نفع منافع ملی حل شود.

❖ **مناسب بودن برای داشتن مجوز**

یک نامزد برای داشتن تصدیق امنیت ملی در هر سطحی که تأسیس شود، تا میزان رضایتمندی مناسب، که نامزد از آن برخوردار است و از سطح مناسبی از صداقت، یعنی صفت منش و اصول اخلاقی برخوردار است، مناسب است.

در چارچوب امنیتی، صداقت به عنوان طیف وسیعی از ویژگی‌های شخصیتی تعریف می‌شود که یک نامزد باید داشته باشد و آنها را نشان دهد تا دولت بتواند به توانایی آن نامزد در محافظت از مواد محافظت شده با اطمینان اعتماد کند.

این ویژگی‌های شخصیت عبارتند از:

- صداقت
- امانت
- وفاداری

ارجاع به تعدادی از زمینه‌های زندگی نامزد، از جمله روابط شخصی، سابقه استخدام، رفتار و رفتار مالی در ارزیابی صداقت یک نامزد کمک می‌کند. آژانس‌ها باید اطمینان داشته باشند که کارکنانی که مسئول مواد محافظتی هستند قبل از صدور مجوز امنیت ملی دارای شخصیتی سالم و پایدار هستند. نامزدها همچنین باید نشان دهند که در برابر زورگویی یا سایر تأثیرات نامطلوب بی جهت آسیب پذیر نیستند.

❖ معیارهای ارزیابی

تعیین نهایی اینکه آیا یک توصیه برای تصویب امنیت ملی با منافع ملی سازگار است یا خیر، باید یک تصمیم کلی عقل سلیم باشد که بر اساس بررسی دقیق همه افراد در زمینه موارد زیر انجام شود:

- دستورالعمل :A وفاداری، تأثیرات و ارتباطات خارجی
- دستورالعمل :B روابط و رفتارهای شخصی
- دستورالعمل :C ملاحظات مالی
- دستورالعمل :D مصرف الکل و مواد مخدر
- دستورالعمل :E تاریخچه و رفتار کیفری
- دستورالعمل :F نگرش‌ها و تخلفات امنیتی
- دستورالعمل :G اختلالات بهداشت روان.

این عوامل ممکن است با یک یا چند ویژگی شخصیتی یک نامزد ارتباط داشته باشد. اگرچه ممکن است اطلاعات نامطلوب مربوط به یک جنبه منفی برای تعیین نامطلوب کافی نباشد، اما اگر اطلاعات موجود الگوی فعلی یا تکرار شونده‌ای را نشان دهند، ممکن است برای تصویب توصیه نشود.

- قضاوت مشکوک
- عدم صداقت
- عدم بلوغ
- غیر قابل اعتماد بودن
- بی مسئولیتی
- آسیب پذیری در برابر نفوذ یا اجبار
- رفتاری بی ثبات از نظر عاطفی.

اطلاعات نامطلوب قابل اعتماد و قابل توجه ممکن است ارزیاب را به توصیه درمورد اعطای مجوز سوق دهد. هنگامی که اطلاعات مربوط به امنیت درباره نامزدی که در حال حاضر دارای مجوز امنیت ملی است و به مواد محافظت شده دسترسی دارد، شناخته می‌شود، افسر ارزیابی کننده باید عوامل زیر را قبل از تعیین اینکه آیا تصویب ادامه توصیه می‌شود، در نظر بگیرد.

آیا شخص:

- داوطلبانه اطلاعات را گزارش داد
- به سؤالات صادقانه و کامل پاسخ داد
- در صورت لزوم به دنبال کمک و راهنمایی حرفه‌ای رفتند
- حل شده یا به نظر می‌رسد احتمالاً مسئله امنیتی را به طور مطلوب برطرف می‌کند
- تغییرات مثبتی در رفتار و اشتغال نشان داده است.

اگر پس از ارزیابی مطالب مربوط به امنیت، ارزیابی کننده تصمیم بگیرد که این ماده به اندازه کافی جدی نیست که بتواند توصیه‌ای را علیه تصویب نامه امنیت ملی تضمین کند، توصیه می‌شود که تصویب نامه را با هشدار اینکه ممکن است حوادث آینده از یک نوع مشابه در آینده ایجاد کنند، توصیه کنید. یک توصیه منفی

۹-۴- دستورالعمل - A وفاداری‌های خارجی

❖ **نگرانی‌ها**

۱) در وفاداری دارنده مجوز امنیت ملی به نیوزلند و تمایل وی برای محافظت از مواد دارای علامت محافظ مربوط به امنیت ملی نیوزلند تردیدی وجود ندارد.

۲) هر کسی که به نمایندگی از دولت نیوزلند کار می‌کند باید به روند دموکراتیک و همچنین روند کار دولت منتخب احترام بگذارد.

اگر نامزدها عقاید سیاسی یا شخصی خود را ناسازگار با سیستم مشروطه و دموکراتیک نیوزیلند بیان کنند، در مورد اینکه آیا آن‌ها می‌توانند به دولت نیوزیلند وفادار بمانند تردیدهایی ایجاد می‌شود.

پذیرفته شده است که در برخی موارد ممکن است تعارض دیدگاه یا حتی مخالفت با وجدان باشد .با این حال، مسئله این است که آیا نامزدها مسئولیت‌های فردی خود را در قبال آژانس استخدام خود، دولت منتخب و منافع عمومی تشخیص می‌دهند؟

۳) هنگامی که یک نامزد به گونه‌ای عمل می‌کند که نشان دهنده اولویت یک کشور خارجی نسبت به نیوزیلند باشد، در این صورت وی ممکن است مستعد عمل به گونه‌ای باشد که برای منافع ملی نیوزلند مضر باشد.

۴) مشارکت در انواع خاصی از مشاغل یا فعالیتهای خارجی در صورت ایجاد تضاد با مسئولیت‌های امنیتی یک نامزد و ایجاد خطر افزایش افشای غیرمجاز اطلاعات محافظت شده امنیتی، نگران کننده امنیت است.

۵) خطر امنیتی ممکن است زمانی وجود داشته باشد که نامزد یا خانواده نزدیک آنها، از جمله زندگی مشترک و سایر اشخاصی که وی ممکن است تحت محبت، نفوذ یا تعهد باشد، شهروندان نیوزیلند نیستند و یا ممکن است تحت فشار قرار گیرند.

این شرایط می‌تواند پتانسیل نفوذ خارجی را نسبت به وفاداری‌های تقسیم شده ایجاد کند که می‌تواند منجر به به خطر افتادن اطلاعات محافظت شده شود.

تماس با شهروندان سایر کشورها یا منافع مالی در سایر کشورها نیز درصورت تعیین امنیت اگر نامزد را احتمالاً در معرض زور، استثمار یا فشار آسیب پذیر سازد، مرتبط است.

شرایطی که می‌تواند نگرانی امنیتی ایجاد کند و ممکن است رد صلاحیت شود

۶) مشارکت، پشتیبانی، آموزش متعهد یا طرفداری از هر عملی از موارد زیر:
- جاسوسی
- خرابکاری
- تروریسم
- خیانت
- خشونت با انگیزه سیاسی
- حمله به سیستم‌های دفاعی نیوزیلند
- اقدامات دخالت خارجی.

۷) ارتباط یا همدردی با افرادی که قصد ارتکاب یا ارتکاب هر یک از اقدامات فوق را دارند.

۸) ارتباط یا همدردی با اشخاص یا سازمانهایی که طرفدار، تهدید، یا استفاده از زور یا خشونت، یا استفاده از هرگونه وسیله غیرقانونی یا خلاف قانون اساسی هستند، در تلاش برای:
- دولت نیوزیلند را سرنگون یا تحت تأثیر قرار دهد
- از انجام وظایف رسمی کارمندان دولت جلوگیری کند
- برای اشتباهات قابل درک ناشی از دولت نیوزیلند مجازات دریافت کنید
- مانع استفاده دیگران از حقوق خود تحت قانون اساسی یا قوانین نیوزیلند شوید.

۹) در صورت تماس با یک عضو خانواده، شرکای تجاری یا همکار حرفه‌ای، دوست یا شخص دیگری که شهروند یا مقیم کشور خارجی است، در صورت افزایش غیر قابل قبول افزایش خطر استثمار خارجی، تحریک، دستکاری، فشار یا اجبار.

۱۰) ارتباط با یک فرد، گروه، دولت یا کشور خارجی که تعارض بالقوه منافع بین تعهد نامزد برای محافظت از مواد محافظت شده و تمایل نامزد برای کمک به یک فرد، گروه یا کشور خارجی با ارائه این اطلاعات ایجاد می‌کند.

۱۱) تقسیم محل زندگی با یک شخص یا افراد، صرف نظر از وضعیت تابعیت، در صورت ایجاد این رابطه در افزایش تحریک خارجی، کیفری، دستکاری، فشار یا اجبار.

۱۲) یک منافع تجاری، مالی یا دارایی قابل توجه در یک کشور خارجی، یا در هر تجارت خارجی یا تحت مالکیت خارجی، که می‌تواند نامزد را در معرض خطر افزایش نفوذ یا بهره برداری خارجی قرار دهد.

۱۳) عدم گزارش، در صورت لزوم، ارتباط با یک شهروند خارجی.

۱۴) ارتباط غیرمجاز و / یا پنهان با یک مأمور، وابسته یا کارمند مظنون یا شناخته شده یک سرویس اطلاعاتی خارجی.

۱۵) مواردی که نمایندگان یا شهروندان یک کشور خارجی برای افزایش آسیب پذیری نامزد در برابر سو litationاستفاده احتمالی، تحریک، دستکاری، فشار یا اجبار در آینده اقدام می‌کنند.

۱۶) رفتار، به ویژه هنگام مسافرت به خارج از نیوزیلند، که ممکن است نامزد را در معرض استثمار، فشار یا اجبار توسط فرد، گروه یا دولت خارجی قرار دهد.

۱۷) استفاده از هرگونه حق، امتیاز یا تعهد تابعیت خارجی پس از تابعیت نیوزلند .این شامل موارد زیر است:

❖ **داشتن گذرنامه خارجی فعلی**
- خدمت سربازی یا تمایل به حمل اسلحه برای یک کشور خارجی
- پذیرش مزایای آموزشی، پزشکی، بازنشستگی، رفاه اجتماعی یا سایر مزایا از یک کشور خارجی
- اقامت در یک کشور خارجی برای برآورده شدن شرایط شهروندی
- استفاده از تابعیت خارجی برای محافظت از منافع مالی یا تجاری در کشور دیگر
- به دنبال یا داشتن سمت سیاسی در یک کشور خارجی است

- رأی دادن در انتخابات خارجی.

۱۸) اقدام برای به دست آوردن یا به رسمیت شناختن تابعیت خارجی توسط یک شهروند نیوزلند.

۱۹) انجام یا تلاش برای انجام وظایف، یا اعمال دیگر، به منظور تأمین منافع شخص خارجی، گروه، سازمان یا دولتی که با منافع ملی نیوزلند مغایرت داشته باشد.

۲۰) هر بیانیه یا اقدامی که نشان دهنده وفاداری با کشوری غیر از نیوزلند باشد، به عنوان مثال، اعلام قصد انصراف از تابعیت نیوزلند، یا انصراف از تابعیت نیوزلند.

۲۱) هرگونه اشتغال یا خدمت، اعم از جبران خسارت یا داوطلبانه، با:

- دولت یک کشور خارجی
- هر شهروند خارجی، سازمان یا نهاد دیگری
- نماینده هر منافع خارجی
- هر سازمان خارجی، داخلی یا بین المللی، از جمله رسانه‌ها، یا شخصی که درگیر تجزیه و تحلیل است،
- بحث، یا انتشار مطالب در
- اطلاعات، دفاع، امور خارجه، فناوری محافظت شده یا امنیت محافظتی
- عدم گزارش یا افشای کامل فعالیت خارجی در صورت لزوم.

۲۲) ارتباط داوطلبانه در حال انجام با افراد یا گروههایی از ماهیت افراطی، یعنی کسانی که عقاید ناسازگار با لیبرال دموکراسی را حمایت یا تبلیغ می‌کنند.

❖ **شرایطی که می‌تواند نگرانی‌های امنیتی را**

کاهش دهد عوامل کاهش دهنده ممکن است در یک یا چند زمینه نگران کننده تأثیر بگذارد

۲۳) نامزد انتخابات از اهداف غیرقانونی یک فرد یا سازمان بی اطلاع بود و با آموختن این اهداف رابطه خود را قطع کرد.

۲۴) درگیری نامزد فقط با جنبه‌های قانونی یا بشردوستانه سازمانی مانند موارد ذکر شده در A8 بود.

۲۵) درگیر شدن در فعالیت‌های مورد نگرانی فقط برای مدت کوتاهی اتفاق افتاده و می‌تواند ناشی از کنجکاوی یا علاقه تحصیلی باشد.

۲۶) درگیری یا ارتباط با چنین فعالیت‌هایی در چنین شرایط غیرمعمولی اتفاق افتاده است، یا مدت زمان زیادی سپری شده است، که احتمال تکرار آن وجود ندارد و در مورد قابلیت اطمینان، قابلیت اطمینان یا وفاداری فعلی داوطلب تردید ایجاد نمی‌کند.

۲۷) ماهیت روابط با اشخاص خارجی، کشوری که این افراد در آن مستقر هستند یا موقعیت‌ها یا فعالیت‌های آن افراد در آن کشور به گونه‌ای است که بعید است نامزد در موقعیتی قرار گیرد که مجبور به انتخاب بین منافع باشد از یک فرد، گروه، سازمان یا دولت خارجی و منافع ملی نیوزیلند است.

۲۸) هیچ تضادی در منافع وجود ندارد، زیرا احساس وفاداری یا تعهد نامزد نسبت به شخص خارجی، گروه، دولت یا کشور بسیار کم است، یا نامزد دارای روابط و وفاداری چنان عمیق و طولانی مدت در نیوزیلند است که می‌توان انتظار داشت برای حل هرگونه تضاد منافع به نفع منافع ملی نیوزیلند.

۲۹) تماس یا برقراری ارتباط با شهروندان خارجی اتفاقی و نادر است و احتمال اینکه بتواند خطر نفوذ یا استثمار خارجی را ایجاد کند وجود ندارد.

۳۰) تماس‌ها و فعالیت‌های خارجی در ارتباط با مشاغل دولت نیوزلند است و یا توسط مأمور امنیت بخش تأیید می‌شود.

۳۱) داوطلب بلافاصله الزامات آژانس را در رابطه با گزارش تماس، درخواست یا تهدید از جانب افراد، گروه‌ها یا سازمان‌ها از یک کشور خارجی رعایت کرده است.

۳۲) ارزش یا روال معمول منافع تجاری، مالی یا دارایی خارجی به حدی است که بعید است منجر به درگیری شود و نمی‌توان از آنها برای تأثیرگذاری، دستکاری یا فشار بر نامزد استفاده کرد.
۳۳) در مواردی که دلایل تملک یا کسب تابعیت دو یا چندگانه یک نگرانی امنیتی نیست، شامل موارد زیر است:

تابعیت دو یا چندگانه صرفاً بر اساس تابعیت یا تولد والدین در یک کشور خارجی است

- ازدواج
- راحتی سفر.

۳۴) این نامزد قادر است وفاداری اولیه خود را نسبت به سایر کشورها به نیوزیلند ابراز کند.
۳۵) استفاده از حقوق، امتیازات یا تعهدات تابعیت خارجی قبل از اینکه کاندیدا به شهروند نیوزلند تبدیل شود یا زمانی که نامزد خردسال بود، اتفاق افتاد.
۳۶) استفاده از گذرنامه خارجی توسط افسر امنیت بخش تأیید می‌شود.
۳۷) گذرنامه خارجی تخریب شده، تسلیم شده و یا در غیر این صورت باطل شده است.
۳۸) شرکت در یک انتخابات خارجی توسط دولت نیوزلند تشویق شد.

❖ **دستورالعمل - B روابط و رفتار شخصی**

نگرانی‌ها

۱) رفتاری که شامل قضاوت مشکوک، عدم صداقت، یا عدم تمایل به پیروی از قوانین و مقررات می‌تواند سوالاتی در مورد قابلیت اطمینان، قابل اعتماد بودن و توانایی محافظت از اطلاعات دارای علامت محافظتی نامزد ایجاد کند.
۲) از اهمیت ویژه‌ای برخوردار است هرگونه عدم ارائه پاسخ‌های صحیح و صریح در طی مراحل بررسی امنیتی یا هرگونه عدم موفقیت در همکاری با روند بررسی امنیتی.

موارد زیر به طور معمول منجر به توصیه نامطلوب برای تصویب امنیت ملی یا خاتمه رسیدگی بیشتر برای ارزیابی بررسی امنیتی می‌شود:

امتناع یا عدم موفقیت بدون دلیل منطقی، انجام یا همکاری با فرآیند بررسی امنیتی، از جمله ملاقات با یک افسر بررسی برای مصاحبه امنیتی، تکمیل فرم‌های امنیتی و / یا رضایت و همکاری با ارزیابی‌های تکمیلی و بررسی‌های دوره‌ای

امتناع یا عدم ارائه پاسخهای کامل، صریح و صادقانه به سؤالات مربوط از یک افسر بررسی یا سایر نمایندگان رسمی در رابطه با بررسی امنیتی.

۳) رفتار جنسی شامل یک جرم کیفری، نشانگر یک شخصیت یا اختلال عاطفی، نشان دهنده فقدان قضاوت یا اختیار فاحش است، یا ممکن است نامزد را تحت تأثیر بی فایده یا زورگویی قرار دهد، بهره برداری یا اجبار می‌تواند سوالاتی در مورد قابلیت اطمینان، قابلیت اطمینان و بلوغ نامزد ایجاد کند..
۴) گرایش یا اولویت جنسی ممکن است به عنوان مبنایی برای ارزیابی مناسب بودن یک نامزد برای تصویب امنیت ملی یا به عنوان یک عامل سلب صلاحیت مورد استفاده قرار نگیرد.

شرایطی که می‌تواند نگرانی امنیتی ایجاد کند و ممکن است رد صلاحیت شود

۵) حذف، پنهان کاری، یا جعل واقعیت‌های مربوطه هنگام تکمیل هرگونه پرسشنامه امنیتی پرسنل، بیانیه تاریخچه شخصی یا فرم مشابهی که برای تعیین مناسب بودن مجوز تصدی امنیت ملی یا ارائه اطلاعات نادرست یا گمراه کننده به افسران بازرسی یا سایر کارکنان درگیر در روند بررسی امنیتی استفاده می‌شود.

۶) اطلاعات نامطلوب معتبر در چندین حوزه قضاوتی که برای تعیین عارضه تحت هیچ دستورالعمل دیگری کافی نیست، اما اگر به عنوان یک کل در نظر گرفته شود، از ارزیابی کل شخص از قضاوت مشکوک، عدم اعتماد، عدم اطمینان، عدم صراحت، عدم تمایل به مطابق با قوانین و مقررات، یا سایر ویژگی‌های نشان می‌دهد که فرد ممکن است به درستی از اطلاعات رسمی محافظت نمی‌کند

۷) اطلاعات نامطلوب معتبری که به صراحت تحت هیچ دستورالعمل دیگری قرار نگرفته‌اند و ممکن است به تنهایی برای تعیین عیب کافی نباشند، اما اگر با همه اطلاعات موجود ترکیب شوند، ارزیابی وفاداری، قابل اعتماد بودن، صداقت، بلوغ یا مشکوک مشکوک را در اختیار شخص قرار می‌دهد. آسیب پذیری در برابر اجبار یا نفوذ.

این موارد شامل موارد زیر است:

رفتار غیر قابل اعتماد یا غیر قابل اعتماد از جمله نقض محرمانه بودن مشتری، انتشار اطلاعات اختصاصی، انتشار غیر مجاز شرکت‌های حساس حساس یا سایر اطلاعات رسمی دولت

- اخلالگرانه، خشن یا سایر رفتارهای نامناسب در محل کار
- الگویی از عدم صداقت یا نقض قوانین
- شواهدی مبنی بر سو استفاده قابل توجه از وقت یا منابع کارفرمایان.

۸) رفتار جنسی از جنبه جنایی، خواه کاندیدا مورد پیگرد قانونی قرار گرفته باشد یا نه.

۹) الگویی از رفتارهای جنسی اجباری، خودتخریبی یا پرخطر که فرد قادر به متوقف کردن آن نیست و یا ممکن است از علائم اختلال شخصیت باشد.

۱۰) رفتار جنسی که باعث می‌شود نامزد در معرض اجبار، استثمار یا فشار قرار گیرد) به دستورالعمل G مراجعه کنید.(

۱۱) رفتار شخصی یا مخفی کردن اطلاعات مربوط به رفتار فرد، که باعث ایجاد آسیب پذیری در بهره برداری، دستکاری یا اجبار می‌شود مانند:

انجام فعالیتهایی که در صورت شناخته شدن، ممکن است بر وضعیت شخصی، شغلی یا اجتماع فرد تأثیر بگذارد

در حالی که در یک کشور دیگر هستید، انجام هر فعالیتی که در آن کشور غیرقانونی باشد یا در آن کشور قانونی باشد اما در نیوزیلند غیرقانونی باشد و ممکن است به عنوان پایه‌ای برای بهره برداری یا فشار توسط خارجی باشد

سرویس امنیتی یا اطلاعاتی یا گروه دیگری.

۱۲) نقض تعهد کتبی یا ثبت شده‌ای که داوطلب نسبت به کارفرما به عنوان شرط استخدام انجام داده است.

۱۳) ارتباط با افرادی که درگیر فعالیت جنایی هستند.

❖ **شرایطی که می‌تواند نگرانی‌های امنیتی را**

کاهش دهد عوامل کاهش دهنده ممکن است در یک یا چند زمینه نگران کننده تأثیر بگذارد

۱۴) این رفتار قبل و یا در دوران نوجوانی رخ داده است و هیچ سندی از رفتار بعدی با ماهیت مشابه وجود ندارد.

۱۵) این رفتار دیگر به عنوان پایه‌ای برای اجبار، استثمار یا تأثیرگذاری عمل نمی‌کند.

۱۶) داوطلب قبل از مواجهه با حقایق، تلاش‌های سریع و حسن نیت را برای اصلاح حذف، پنهان کاری یا جعل انجام داد.

۱۷) امتناع یا عدم همکاری، حذف یا پنهان کاری ناشی از مشاوره نامناسب یا ناکافی افسران دولتی یا مشاوران حقوقی بوده و یا با آنها همراه بوده است.

داوطلب پس از آگاهی از نیاز به همکاری یا ارائه اطلاعات، به طور کامل و صادقانه همکاری کرد.

۱۸) رفتار یا تخلف بسیار جزئی است، یا مدت زمان زیادی سپری شده است، یا رفتار آنقدر کم اتفاق افتاده است، یا در چنین شرایط منحصر به فردی اتفاق افتاده است که احتمال تکرار آن وجود ندارد و قابلیت اطمینان، قابلیت اطمینان یا خوب بودن نامزد را زیر سؤال نمی‌برد. داوری.

۱۹) داوطلب این رفتار را تأیید کرده و مشاوره‌ای برای تغییر رفتار یا اقدامات مثبت دیگری برای کاهش عوامل استرس زا، شرایط یا عواملی که باعث رفتارهای غیرقابل اعتماد، غیر قابل اعتماد یا رفتارهای نامناسب دیگر شده‌اند، کرده است.

شواهدی وجود دارد که این روش درمانیم ثر بوده و چنین رفتاری بعید به نظر می‌رسد.

۲۰) نامزد گام‌های مثبتی برای کاهش یا از بین بردن آسیب پذیری در برابر بهره برداری، دستکاری یا فشار برداشته است.

۲۱) اطلاعات غیرمستند یا از منبع قابل اعتماد بودن سؤال بود.

۲۲) ارتباط با اشخاصی که درگیر فعالیت‌های جنایی هستند متوقف شده یا در شرایطی اتفاق می افتد که اطمینان، اطمینان، قضاوت یا تمایل داوطلب برای رعایت قوانین و مقررات را زیر سؤال نبرد.

توجه: افسر ارزیابی کننده همچنین باید راهنمایی‌های مربوط به رفتار مجرمانه) دستورالعمل (E یا اختلالات بهداشت روانی)دستورالعمل را در تعیین چگونگی حل مشکلات امنیتی ناشی از رفتار جنسی در نظر بگیرد.

❖ دستورالعمل - C ملاحظات مالی

نگرانی‌ها

۱) عدم موفقیت یا ناتوانی در زندگی در حد توان خود، تأمین بدهی‌ها یا تحقق تعهدات مالی، ممکن است نشان دهنده ضعف در کنترل خود، عدم قضاوت یا عدم تمایل به رعایت قوانین و مقررات باشد.

این ممکن است سوالاتی در مورد صداقت، قابل اعتماد بودن، بلوغ و آسیب پذیری یک نامزد در برابر اجبار یا نفوذ ایجاد کند.

۲) نامزدی که بیش از حد تمدید مالی شود ممکن است در معرض خطر بیشتری برای انجام اقدامات غیرقانونی از جمله جاسوسی برای تولید بودجه قرار گیرد.

اگر مشکلات مالی ناشی از رفتار اجباری، به عنوان مثال قمار باشد، این خطر بیشتر می‌شود.

۳) عدم تمایل به پرداخت بدهی در صورت وجود امکانات ممکن است نشان دهنده عدم اعتماد به نفس یا عدم وجدان در مورد تعهدات باشد.

۴) تأثیرگذاری که با منابع شناخته شده درآمد قابل توضیح نیست نیز نگران کننده است زیرا ممکن است درآمد حاصل از رفتار مجرمانه را نشان دهد.

شرایطی که می‌تواند نگرانی امنیتی ایجاد کند و ممکن است رد صلاحیت شود

۵) ناتوانی یا عدم تمایل به تأمین بدهی‌ها

۶) بدهکاری ناشی از هزینه‌های ناعادلانه و غیرمسئولانه و عدم وجود هیچ مدرکی از تمایل یا قصد پرداخت بدهی یا تهیه برنامه واقعی برای پرداخت بدهی.

۷) سابقه عدم انجام تعهدات مالی، از جمله هرگونه سابقه ورشکستگی، عدم رویه دارایی، پیش فرض پرداخت‌ها یا خدمات اعلامیه‌های وصول.
۸) اقدامات مالی فریبکارانه یا غیرقانونی مانند اختلاس، سرقت، کلاهبرداری، فرار مالیاتی یا دیگر نقض عمدی اعتماد.
۹) هزینه مداوم فراتر از توان شخصی، که ممکن است با بدهی بیش از حد، جریان نقدی منفی قابل توجه، نسبت بالای بدهی به درآمد و / یا سایر تجزیه و تحلیل‌های مالی نشان داده شود.
۱۰) مشکلات مالی که مرتبط با سو drug مصرف مواد مخدر، اعتیاد به الکل، اعتیاد به قمار یا سایر مواردی است که رفتار اجباری یا بی ثباتی عاطفی یا روانی را نشان می‌دهد که ممکن است تأثیراتی در بلوغ، قابلیت اعتماد و آسیب پذیری نامزدی در برابر فشار یا فشار داشته باشد) به دستورالعمل‌های D و G مراجعه کنید.(
۱۱) عدم انجام مکرر تعهدات مالیاتی نیوزیلند.
۱۲) ثروت غیر قابل توضیح، همانطور که در سبک زندگی یا استاندارد زندگی نشان داده شده است، افزایش ارزش خالص یا انتقال پول است که با منابع قانونی شناخته شده درآمد نامزد قابل توضیح نیست.
۱۳) قمار اجباری یا اعتیاد آور همانطور که با یک تلاش ناموفق برای متوقف کردن قمار، "تعقیب ضرر" (یعنی افزایش شرط بندی یا بازگشت یک روز دیگر در تلاش برای یکسان سازی) نشان داده شده است، پنهانکاری در ضرر قمار، وام گرفتن پول برای تأمین بودجه قمار یا پرداخت قمار بدهی، درگیری خانوادگی یا سایر مشکلات ناشی از قمار.

شرایطی که می‌تواند نگرانی‌های امنیتی را کاهش دهد عوامل کاهش دهنده ممکن است در یک یا چند زمینه نگران کننده تأثیر بگذارد

۱۴) رفتاری که مدتها پیش اتفاق افتاده، بسیار نادر بوده و یا در چنین شرایطی رخ داده است که بعید است تکرار شود و در مورد قابلیت اطمینان، قابل اعتماد بودن یا قضاوت خوب نامزد مورد تردید قرار نمی‌گیرد.
۱۵) شرایطی که منجر به مشکل مالی شد، عمدتاً از عهده داوطلب خارج بود (به عنوان مثال، از دست دادن شغل، رکود تجاری، فوریت‌های پزشکی غیر منتظره، یا مرگ، طلاق یا جدایی) و نامزد مسئولیت پذیرانه عمل کرد.
۱۶) داوطلب مشاوره‌ای را برای این مشکل دریافت کرده و یا در حال دریافت آن است و یا نشانه‌های روشنی وجود دارد که نشان می‌دهد مشکل در حال حل است و یا تحت کنترل است.
۱۷) نامزد تلاش‌های خیرخواهانه را برای بازپرداخت طلبکاران معوق یا حل و فصل بدهی‌ها آغاز کرد.
۱۸) داوطلب مبنای معقولی برای اختلاف در مشروعیت بدهی دارد و شواهدی از اقدامات برای حل مسئله را ارائه می‌دهد.
۱۹) ثروتمندی نتیجه یک منبع قانونی درآمد بود.

❖ **دستورالعمل - D مصرف الکل و مواد مخدر**

نگرانی‌ها

۱) مصرف بیش از حد الکل معمولاً منجر به اعمال قضاوت مشکوک یا عدم کنترل انگیزه‌ها می‌شود و می‌تواند سوالاتی را درباره قابلیت اطمینان و قابلیت اطمینان یک نامزد و توانایی حفظ اختیار ایجاد کند.
۲) استفاده از داروهای غیرقانونی یا سو استفاده از داروهای تجویز شده می‌تواند سوالاتی در مورد قابلیت اطمینان و صداقت یک نامزد ایجاد کند، هم به دلیل اینکه ممکن است قضاوت را مختل کند و هم اینکه سوالاتی را در مورد توانایی یا تمایل فرد برای مطابقت با قوانین، قوانین و مقررات ایجاد می‌کند.

استفاده از داروهای غیرقانونی یا سو استفاده از داروهای تجویز شده نیز ممکن است باعث شود نامزد در معرض اجبار یا سایر تأثیرات نامطلوب یا فشار قرار گیرد.

۳) مواد مخدر مواد تغییر دهنده خلق و خو و رفتار هستند و شامل داروها، مواد و سایر ترکیبات شیمیایی هستند که در فهرست برنامه‌های سو مصرف مواد مخدر، مواد استنشاقی و سایر مواد مشابه ذکر و ذکر شده‌اند.
۴) سو مصرف مواد مخدر استفاده از داروی غیرقانونی یا استفاده از داروی مجاز به روشی است که از جهت پزشکی مجاز خارج شود.

شرایطی که می‌تواند نگرانی امنیتی ایجاد کند و ممکن است رد صلاحیت شود

۵) حوادث مربوط به الکل در خارج از محل کار، مانند رانندگی در حالی که تحت تأثیر، دعوا، کودک آزاری یا همسر، سایر خشونت‌های خانگی، برهم زدن آرامش یا سایر حوادث نگران کننده است، بدون در نظر گرفتن اینکه آیا کاندیدا سو مصرف الکل تشخیص داده شده است یا وابسته به الکل
۶) حوادث مرتبط با الکل در محل کار، مانند گزارش کار در شرایط مست و کمبود مستی، یا نوشیدن بیش از حد در محل کار.
۷) مصرف عادی یا زیاد الکل تا حدی که قضاوت مختل شود.
۸) تشخیص توسط یک متخصص پزشکی واجد شرایط (مثلاً پزشک، روانشناس بالینی یا روانپزشک) در مورد الکل، یا سو مصرف یا وابستگی به مواد مخدر.
۹) شناسایی الکل یا سو مصرف مواد مخدر یا وابستگی توسط یک مددکار اجتماعی معتبر بالینی که عضو کارکنان یک برنامه درمانی شناخته شده الکل یا مواد مخدر است.
۱۰) پس از تشخیص الکل یا سو مصرف مواد مخدر یا وابستگی و اتمام یک برنامه توانبخشی الکل یا مواد مخدر، عود کنید.
۱۱) اتهامات کیفری مربوط به سو مصرف الکل یا مواد مخدر یا داشتن آن.
۱۲) عدم رعایت هرگونه حکم دادگاه در رابطه با آموزش الکل یا اعتیاد به مواد مخدر، ارزیابی، درمان یا پرهیز از مصرف مواد مخدر.
۱۳) هرگونه سو مصرف مواد مخدر (به بخش D4 مراجعه کنید)
۱۴) آزمایش مثبت برای استفاده غیرقانونی از مواد مخدر.
۱۵) در اختیار داشتن مواد مخدر غیرقانونی، از جمله کشت، فرآوری، ساخت، خرید، فروش یا توزیع یا توزیع مواد مخدر.
۱۶) قصد ابراز شده برای ادامه مصرف غیرقانونی مواد مخدر یا عدم تعهد واضح و قانع کننده برای قطع مصرف مواد مخدر.

❖ **شرایطی که می‌تواند نگرانی‌های امنیتی را**

کاهش دهد عوامل کاهش دهنده ممکن است در یک یا چند زمینه نگران کننده تأثیر بگذارد

۱۷) مدت زمان زیادی سپری شده است، یا رفتار آنچنان نادر بوده است، یا در چنین شرایط غیرمعمولی رخ داده است که بعید است تکرار شود یا در مورد قابلیت اطمینان، قابل اعتماد بودن یا قضاوت خوب داوطلب تردید ایجاد کند.
۱۸) داوطلب در یک برنامه مشاوره یا درمان الکل شرکت می‌کند، سابقه درمان و عود قبلی ندارد و پیشرفت مطلوبی دارد.
۱۹) داوطلب وابستگی یا سو مصرف الکل خود را تصدیق می‌کند و با موفقیت:

مشاوره یا توانبخشی مشروبات الکلی بستری یا سرپایی همراه با هرگونه مراقبت‌های بعدی مورد نیاز

الگوی مشخص و مشخصی از مصرف یا پرهیز اصلاح شده مطابق با توصیه‌های درمانی مانند پایبندی به برنامه‌ای مانند مشروبات الکلی ناشناس یا سازمانی مشابه

پیش بینی مطلوب توسط یک متخصص پزشکی واجد شرایط یا یک مددکار اجتماعی معتبر بالینی که عضو هیات یک برنامه درمانی شناخته شده الکل است، پیش بینی شده است.

۲۰) قصد سو استفاده از هیچ دارویی در آینده مانند:

- جدا شدن از افراد وابسته و ارتباطات مصرف مواد مخدر
- تغییر یا اجتناب از محیط استفاده از مواد مخدر
- یک دوره پرهیز مناسب
- بیانیه امضا شده با بازبینی خودکار برای هرگونه تخلف.

۲۱) سو استفاده از داروهای تجویز شده پس از یک بیماری شدید یا طولانی مدت بود که در طی آن این داروها تجویز شده و سو مصرف به پایان رسیده است.

۲۲) اتمام رضایت بخش یک برنامه درمان دارویی تجویز شده، از جمله نیازهای توانبخشی و مراقبت‌های پس از آن، بدون تکرار سو استفاده، و پیش آگهی مطلوب توسط یک متخصص پزشکی با صلاحیت مناسب یا یک مددکار اجتماعی معتبر بالینی که عضو هیات دارویی شناخته شده است برنامه درمانی

❖ **دستورالعمل - E تاریخچه و رفتار کیفری**

نگرانی‌ها

۱) رفتار مجرمانه ایجاد تردید در مورد قضاوت، قابلیت اطمینان، قابل اعتماد بودن، بلوغ و صداقت فرد می‌کند.

از نظر ماهیت خود، صداقت فرد و توانایی یا تمایل وی در انطباق با قوانین، قوانین و مقررات را زیر سال می‌برد.

۲) شرایطی که می‌تواند نگرانی امنیتی ایجاد کند و ممکن است رد صلاحیت باشد. یک جرم کیفری، یا چندین جرم کمتر، یا محکومیت در دادگاه نیوزیلند یا خارج از کشور، از جمله دادگاه نظامی در مورد یک جرم.

۳) اخراج یا اخراج از نیروی دفاعی نیوزلند یا پلیس نیوزیلند به دلیل سو m رفتار.

۴) ادعای معتبر، اطلاعات، اطلاعات یا پذیرش رفتار مجرمانه، بدون در نظر گرفتن اینکه متهم به طور رسمی متهم شده، به طور رسمی تحت پیگرد قانونی یا محکوم قرار گرفته است.

۵) داوطلب در حال حاضر مشروط یا مشروط است.

۶) نقض آزادی مشروط یا مشروط، یا عدم تکمیل برنامه توانبخشی با حکم دادگاه.

۷) ارتباط داوطلبانه با مجرمان.

❖ **شرایطی که می‌تواند نگرانی‌های امنیتی را**

کاهش دهد عوامل کاهش دهنده ممکن است در یک یا چند زمینه نگران کننده تأثیر بگذارد

۸) زمان زیادی از وقوع رفتار مجرمانه سپری شده است، یا در چنین شرایط غیرمعمولی رخ داده است که بعید به نظر می‌رسد که تکرار شود و قابلیت اطمینان، صداقت، اعتمادپذیری یا قضاوت خوب کاندیدا را مورد تردید قرار ندهد.

۹) فرد تحت فشار قرار گرفته یا مجبور به ارتکاب عمل شده است و این فشارها دیگر در زندگی فرد وجود ندارد.

۱۰) متعاقباً شواهد اقناعی مبنی بر اینکه شخص مرتکب جرمی نشده است یا محکومیت وی را لغو کرده است.

۱۱) شواهدی از توانبخشی موفقیت آمیز وجود دارد که شامل گذر زمان بدون تکرار فعالیت مجرمانه، شواهد پشیمانی یا جبران خسارت، آموزش شغلی یا تحصیلات عالی، سابقه اشتغال خوب یا مشارکت سازنده جامعه است.

۱۲) جرم از نظر ماهیت جزئی یا نظارتی بود که از نظر امنیتی نگران کننده نیست .

❖ **دستورالعمل - F نقض امنیت**

نگرانی‌ها

۱) عدم رعایت عمدی یا سهل انگاری در پیروی از رویه‌ها، قوانین و مقررات مربوط به محافظت از اطلاعات ملی طبقه بندی شده یا سایر اطلاعات انحصاری، شخصی، محافظت شده یا حساس، از جمله در سیستم‌های فناوری اطلاعات و ارتباطات(ICT) ، در مورد قابلیت اطمینان، قضاوت، قابلیت اطمینان یا اطمینان یک نامزد تردید ایجاد می‌کند. تمایل و توانایی برای حفاظت از چنین اطلاعاتی و یک نگرانی جدی امنیتی است.

۲) سیستم‌های ICT شامل کلیه سخت افزارهای رایانه‌ای، نرم افزارها، سیستم عامل‌ها و داده‌های مربوطه است که برای ارتباط، انتقال، پردازش، دستکاری، ذخیره سازی یا محافظت از اطلاعات محافظت شده محافظت می‌شود.

۳) شرایطی که می‌تواند نگرانی امنیتی ایجاد کند و ممکن است باعث عدم صلاحیت شود .دسترسی غیرمجاز به اطلاعات رسمی یا شخصی و استفاده از آنها به روشهای زیر:

- مشاهده
- افشا کردن
- جمع آوری
- ذخیره سازی
- رسیدگی
- تخریب
- دستکاری - اعمال نفوذ
- تغییر.

۴) نادیده گرفتن عمدی رویه‌های آژانس یا دستورالعمل‌های مربوط به دست زدن، استفاده و ذخیره اطلاعات رسمی یا شخصی.

۵) کپی کردن اطلاعات رسمی یا شخصی به روشی که برای پنهان کردن یا حذف طبقه بندی یا سایر علائم محافظتی طراحی شده است.

۶) مشاهده یا بارگیری اطلاعات از یک سیستم ایمن فراتر از نیاز داوطلب به دانستن.

۷) هرگونه عدم رعایت قوانین مربوط به حفاظت از اطلاعات ملی طبقه بندی شده یا سایر اطلاعات حساس.

۸) سهل انگاری یا عادات امنیتی شل که علی رغم مشاوره توسط مدیریت، وجود دارد.

۹) عدم رعایت قوانین یا مقرراتی که منجر به آسیب رساندن به امنیت ملی می‌شود، صرف نظر از این که عمدی یا سهل انگاری بوده است.

۱۰) دسترسی به اطلاعات، نرم افزار، سیستم عامل یا سخت افزار ICT غیرقانونی یا غیر مجاز، از جمله:

- ورود به هر سیستمICT
- تغییر
- تخریب
- دستکاری - اعمال نفوذ
- عدم دسترسی

۱۱) استفاده از هر سیستم ICT برای دستیابی غیرمجاز به سیستم دیگر یا به یک قسمت محفظه در همان سیستم.

۱۲) بارگیری، ذخیره یا انتقال اطلاعات علامت گذاری شده محافظتی روی یا به هر نرم افزار، سخت افزار یا سیستم ICT غیر مجاز.

۱۳) استفاده غیرمجاز از دولت یا سیستم ICT دیگر.

۱۴) معرفی، حذف یا تکثیر سخت افزار، سیستم عامل، نرم افزار یا رسانه از هر سیستم ICT بدون مجوز یا از آن، درصورتی که توسط قوانین، رویه‌ها، دستورالعمل‌ها یا مقررات منع شده باشد.
۱۵) هرگونه سو استفاده ازICT ، خواه عمدی یا سهل انگاری، که منجر به آسیب رساندن به امنیت ملی می‌شود.

توجه: سو استفاده از هر دو سیستم دولتی و خصوصی ICT نگران کننده است.

شرایطی که می‌تواند نگرانی‌های امنیتی را کاهش دهد عوامل کاهش دهنده ممکن است در یک یا چند زمینه نگران کننده تأثیر بگذارد

۱۶) زمان زیادی از این رفتار گذشته است، یا این اتفاق بسیار نادر و یا در چنین شرایط غیرمعمولی رخ داده است، که احتمال تکرار آن وجود ندارد و قابلیت اطمینان، صداقت، قابل اعتماد بودن، یا قضاوت خوب داوطلب را تردید نمی‌کند.
۱۷) داوطلب به مشاوره یا آموزش‌های درمانی بهبودی پاسخ مثبت داده و اکنون نگرش مثبتی نسبت به انجام مسئولیت‌های امنیتی خود نشان می‌دهد.
۱۸) تخلفات امنیتی به دلیل آموزش نادرست یا ناکافی بوده است.
۱۹) این سواستفاده جزئی بوده و فقط در جهت ضرورت یک امر ضروری یا عملیاتی صادقانه انجام شده است که هیچ گزینه به موقع دیگری به راحتی در دسترس نبوده است.
۲۰) این رفتار غیر عمدی یا سهوی بود و به دنبال آن یک تلاش سریع و حسن نیت برای اصلاح اوضاع و اطلاع یک ناظر بود.

❖ **رهنمود - G مسائل بهداشت روان**

نگرانی‌ها

۱) برخی شرایط عاطفی، ذهنی و شخصیتی می‌توانند قضاوت، قابلیت اطمینان، یا قابلیت اعتماد را مختل کنند .برای تشخیص نگرانی تحت این دستورالعمل، تشخیص رسمی اختلال لازم نیست.
۲) هنگام ارزیابی اطلاعات بالقوه رد صلاحیت و تخفیف تحت این دستورالعمل، باید از یک متخصص بهداشت روان (به عنوان مثال، روانشناس بالینی یا روانپزشک) که از آژانس استفاده می‌شود یا مورد قبول و تأیید آژانس است، برخوردار باشد.
۳) شرایطی که می‌تواند نگرانی امنیتی ایجاد کند و ممکن است رد صلاحیت باشد .رفتاری که قضاوت، قابلیت اطمینان یا قابل اعتماد بودن یک نامزد را زیر سؤال ببرد، که تحت هیچ دستورالعمل دیگری شامل آن نمی‌شود، از جمله شامل رفتارهای ناپایدار عاطفی، غیرمسئولانه، ناکارآمد، خشونت، پارانویا یا عجیب و غریب نیست.
۴) نظر یک متخصص بهداشت روان دارای صلاحیت مناسب مبنی بر این که داوطلب شرایطی را دارد که تحت هیچ دستورالعمل دیگری تحت تأثیر قرار نگرفته است که ممکن است قضاوت، قابلیت اطمینان یا قابلیت اطمینان را مختل کند.
۵) داوطلب نتوانسته است از توصیه‌های درمانی مربوط به شرایط عاطفی، روانی یا شخصیتی تشخیص داده شده پیروی کند، به عنوان مثال عدم مصرف داروهای تجویز شده.
۶) هیچ استنباط منفی در مورد داوطلب فقط به دلیل مراجعه به مشاوره بهداشت روان مطرح نیست.
۷) شرایطی که می‌تواند نگرانی‌های امنیتی را کاهش دهد عوامل کاهش دهنده ممکن است در یک یا چند زمینه نگران کننده تأثیر بگذارد

شرایط شناسایی شده به راحتی با درمان قابل کنترل است و کاندیدا انطباق مداوم و مداوم با برنامه درمانی را نشان داده است.

۸) داوطلب داوطلبانه برای شرایطی که قابل درمان است، وارد یک برنامه مشاوره یا درمان شده است و داوطلب در حال حاضر تحت مشاوره یا درمان با پیش آگهی مطلوب توسط یک متخصص بهداشت روان واجد شرایط است.

۹) نظر اخیر یک متخصص بهداشت روان دارای صلاحیت واجد شرایط، استخدام شده یا مورد قبول و تأیید آژانس متقاضی بررسی اینکه شرایط قبلی یک داوطلب تحت کنترل یا بهبود است و احتمال عود یا تشدید آن کم است.

۱۰) بی ثباتی عاطفی گذشته یک شرایط موقتی بود (به عنوان مثال، بیماری ناشی از مرگ، بیماری یا از هم پاشیدگی زناشویی)، اوضاع برطرف شده است و داوطلب دیگر نشانه‌هایی از بی ثباتی عاطفی را نشان نمی‌دهد.

۱۱) هیچ نشانه‌ای از یک مشکل فعلی وجود ندارد.

فصل ۵

امنیت اطلاعات

۵- چرا امنیت اطلاعات مهم است

هر سازمانی به محرمانه بودن، صداقت و در دسترس بودن اطلاعاتی که پردازش، ذخیره و ابلاغ می‌کند متکی است.

❖ **امنیت اطلاعات قوی یک فعالیت تجاری است**

امنیت اطلاعات قوی به سازمان شما کمک می‌کند تا:

- اعتماد و اطمینان عموم، مشتریان و شرکا را حفظ کنید
- اطلاعات مهم خود را ایمن نگه دارید و در دسترس کسانی که به آن نیاز دارند، قرار دهید
- خطرات از دست رفتن، آسیب دیدن یا به خطر افتادن اطلاعات خود را کاهش دهید
- از هزینه‌های بهبودی پس از یک حادثه و همچنین هزینه‌های خرابی و از دست رفتن بهره وری اجتناب کنید
- مطابق با مقررات و قوانین.

❖ **تهدیدها و خطرات در حال افزایش و تکامل هستند**

تهدیدهای مربوط به امنیت اطلاعات شما می‌تواند از داخل و خارج سازمان شما باشد .اطلاعات شما در همه اشکال (به عنوان مثال الکترونیکی، چاپی یا گفتاری) باید به طور مناسب محافظت شود .اطلاعات ذخیره شده و پردازش شده در سیستم‌های IT یا دستگاه‌های تلفن همراه در معرض تهدیدهای خاص سایبری است.

ما امروز بیش از هر زمان دیگری در معرض دید قرار گرفته‌ایم.

- ما مقادیر فزاینده‌ای از اطلاعات الکترونیکی داریم و سازمان‌ها اغلب به شدت به عملکرد آنها وابسته هستند.
- ما دارای فناوری‌های ابری، رسانه‌های اجتماعی، موبایل و سایر فناوری‌های نوظهور هستیم که روش‌های دستیابی به اطلاعات مهم را افزایش داده‌اند.

ما با تهدیدات فزاینده و در حال تکامل روبرو هستیم که شناسایی را به چالش می‌کشد.

بازیگران خارجی و افراد ناخوشایند ناراضی شناخته شده‌اند:

- اطلاعات حساس را در دامنه عمومی افشا یا منتشر کنید
- رمزگذاری کنید و سپس اطلاعات مهم را باج دهید
- فروش اطلاعات به رقبا و طرف‌های علاقه مند
- سرقت مالکیت معنوی(IP)
- با تخریب یا انکار دسترسی به سوابق، سازمان‌ها را به خطر بیندازید.

افراد شما همچنین ممکن است به طور تصادفی اطلاعات شما را به خطر بیندازند زیرا:

- عدم آگاهی از اقدامات امنیتی و دلیل اهمیت آنها
- هنگام دست زدن به اطلاعات سازمانی حواس پرتی یا خود راضی نگه دارید

- دسترسی به احزاب دیگری را که به دنبال اطلاعات برای مقاصد جنایی یا نامناسب هستند، فراهم کنید .به عنوان مثال، حملات "مهندسی اجتماعی" سعی در دستکاری افراد در شکستن کنترل‌های امنیتی عادی دارد، و اغلب خود را از طریق فیشینگ، بهانه گیری، طعمه گذاری، و باتلاق یا سایر روشها به عنوان شخصی مورد اعتماد مبدل می‌کنند.

۵-۱- الزامات اجباری

الزامات اصلی امنیت اطلاعات که ادارات دولتی موظف به رعایت آنها هستند و سایر سازمانها باید بهترین روش را در نظر بگیرند.

❖ **آنچه را که برای محافظت از آن نیاز دارید درک کنید**

اطلاعات و سیستم‌های ICT را که سازمان شما مدیریت می‌کند شناسایی کنید .خطرات امنیتی (تهدیدها و آسیب پذیری ها) و تأثیر تجاری هرگونه نقض امنیت را ارزیابی کنید.

❖ **امنیت اطلاعات خود را طراحی کنید**

در اوایل مراحل برنامه ریزی، انتخاب و طراحی، امنیت اطلاعات را در نظر بگیرید.

تدابیر امنیتی را طراحی کنید که خطرات سازمان شما را تهدید می‌کند و با اشتهای شما سازگار است .اقدامات امنیتی شما باید مطابق با موارد زیر باشد:

- سیستم طبقه بندی امنیتی دولت نیوزیلند
- کتابچه راهنمای امنیت اطلاعات نیوزلند
- هرگونه تعهدات حریم خصوصی، قانونی و نظارتی که تحت آن فعالیت می‌کنید.
- یک چارچوب مناسب مدیریت امنیت اطلاعات متناسب با خطرات خود اتخاذ کنید.

❖ **اقدامات امنیتی خود را تأیید کنید**

تأیید کنید که اقدامات امنیتی اطلاعات شما به درستی اجرا شده و برای اهداف مناسب است. فرآیند صدور گواهینامه و اعتبار سنجی را به اتمام برسانید تا از سیستم‌های ICT خود برای تأیید بهره مند شوید.

❖ **امنیت خود را به روز نگه دارید**

اطمینان حاصل کنید که امنیت اطلاعات شما برای هدف مناسب است:

- نظارت بر رویدادهای امنیتی و پاسخگویی به آنها
- به روز نگه داشتن تهدیدات و آسیب پذیری های در حال تحول
- حفظ دسترسی مناسب به اطلاعات شما.

۵-۲- پروتکل مدیریت امنیت اطلاعات

با اقدامات امنیتی قوی از اطلاعات سازمان خود محافظت کنید .وقتی کنترل‌های امنیتی اطلاعات شما به خوبی طراحی و اجرا شود، خطرات به خطر افتادن اطلاعات خود را کاهش می‌دهید. یک فرهنگ امنیتی قوی را تشویق کنید، بنابراین اقدامات امنیتی اطلاعات شما شناخته شده و دنبال می‌شود.

این پروتکل مراحلی را که سازمان شما برای بهبود امنیت اطلاعات شما باید طی کند توضیح می‌دهد .این یک چرخه زندگی برای مدیریت امنیت اطلاعات تعیین می‌کند، و الزامات اجباری آژانس‌های دولتی نیوزلند را مشخص می‌کند.

درک چرخه حیات امنیت اطلاعات و برآورده سازی الزامات اجباری به شما کمک می‌کند تا از اطلاعات سازمان خود محافظت کنید .اگر اهل هستید این پروتکل را بخوانید:

- رئیس اجرایی، افسر ارشد امنیت (CSO) یا مدیر ارشد امنیت اطلاعات(CISO)
- مدیر ارشد مسئول امنیت اطلاعات، مدیر مسئول مدیریت اطلاعات، مدیر ارشد یا مدیر خط.

این اصول باید همراه با پروتکل مدیریت برای امنیت پرسنل ، پروتکل مدیریت برای امنیت فیزیکی و راهنمایی‌های حاکمیت برای امنیت محافظتی خوانده شوند. به عنوان بخشی از اقدامات خوب، ما توصیه می‌کنیم که سازمانهای بخش خصوصی نیز الزامات اجباری برای امنیت اطلاعات را اتخاذ کنند.

❖ امنیت اطلاعات چیست؟

اطلاعات یک دارایی است و امنیت اطلاعات حفاظتی است که شما برای ایمن نگه داشتن دارایی‌های اطلاعاتی خود از آسیب استفاده می‌کنید .به اطلاعات به معنای وسیع فکر کنید، نه فقط از نظر فناوری اطلاعات .اطلاعات به اشکال مختلفی وجود دارد (به عنوان مثال الکترونیکی، چاپی یا گفتاری) و ممکن است در داخل یا خارج از سازمان شما زندگی کند، از جمله با ارائه دهندگان و مشتریان و در فضای ابری. امنیت اطلاعات مفهوم گسترده‌ای است که شامل امنیت سایبری، امنیت دیجیتال و امنیت ICT نیز می‌شود.

❖ مزایای امنیت اطلاعات قوی را درک کنید

هر سازمانی به محرمانه بودن، صداقت و در دسترس بودن اطلاعاتی که پردازش، ذخیره و ابلاغ می‌کند متکی است .امنیت اطلاعات قوی یک فعالیت تجاری است .این به سازمان شما کمک می‌کند تا:

- اعتماد و اطمینان عموم، مشتریان و شرکا را حفظ کنید
- اطلاعات مهم خود را ایمن نگه دارید و در دسترس کسانی که به آن نیاز دارند، قرار دهید
- خطرات از دست رفتن، آسیب دیدن یا به خطر افتادن اطلاعات خود را کاهش دهید
- از هزینه‌های بهبودی پس از یک حادثه و همچنین هزینه‌های خرابی و از دست رفتن بهره وری اجتناب کنید
- مطابق با مقررات و قوانین.

❖ تهدیدها و خطرات لازم برای مدیریت را بدانید

تهدیدهای مربوط به امنیت اطلاعات شما می‌تواند از داخل و خارج سازمان شما باشد .اطلاعات شما در همه اشکال (به عنوان مثال الکترونیکی، چاپی یا گفتاری) باید به طور مناسب محافظت شود .اطلاعات ذخیره شده و پردازش شده در سیستم‌های IT یا دستگاه‌های تلفن همراه در معرض تهدیدهای خاص سایبری است.

- ما امروز بیش از هر زمان دیگری در معرض دید قرار گرفته‌ایم.
- ما مقادیر فزاینده‌ای از اطلاعات الکترونیکی داریم و سازمان‌ها اغلب به شدت به عملکرد آنها وابسته هستند.
- ما دارای فناوری‌های ابری، رسانه‌های اجتماعی، موبایل و سایر فناوری‌های نوظهور هستیم که روش‌های دستیابی به اطلاعات مهم را افزایش داده‌اند.
- ما با تهدیدات فزاینده و در حال تکامل روبرو هستیم که شناسایی را به چالش می‌کشد.

بازیگران خارجی و افراد ناخوشایند ناراضی شناخته شده‌اند:

- اطلاعات حساس را در دامنه عمومی افشا یا منتشر کنید
- رمزگذاری کنید و سپس اطلاعات مهم را باج دهید
- فروش اطلاعات به رقبا و طرف‌های علاقه مند
- سرقت مالکیت معنوی(IP)
- با تخریب یا انکار دسترسی به سوابق، سازمان‌ها را به خطر بیندازید.

افراد شما همچنین ممکن است به طور تصادفی اطلاعات شما را به خطر بیندازند زیرا:

- عدم آگاهی از اقدامات امنیتی و دلیل اهمیت آنها
- هنگام دست زدن به اطلاعات سازمانی حواس پرتی یا خود راضی نگه دارید
- دسترسی به احزاب دیگری را که به دنبال اطلاعات برای مقاصد جنایی یا نامناسب هستند، فراهم کنید .به عنوان مثال، حملات "مهندسی اجتماعی" سعی در دستکاری افراد در شکستن کنترل‌های امنیتی عادی دارد، و اغلب خود را از طریق فیشینگ، بهانه گیری، طعمه گذاری، و باتلاق یا سایر روشها به عنوان شخصی مورد اعتماد مبدل می‌کنند.

❖ **نقض امنیت می‌تواند غیرقابل شناسایی، اخلالگر و آسیب رسان باشد**

اگر اقدامات امنیتی شما ضعیف باشد، اطلاعات شما در معرض خطر قرار می‌گیرد .می‌توان آن را حذف، کپی، اصلاح، تخریب، منتشر، به اشتراک گذاشت یا بهره برداری کرد. این می‌تواند بدون اینکه سازمان شما از آن آگاه باشد رخ دهد .حتی اگر سازمان شما نسبت به حادثه یا تخلفی هشدار داده شود، تأیید میزان تأثیر ممکن است دشوار باشد.

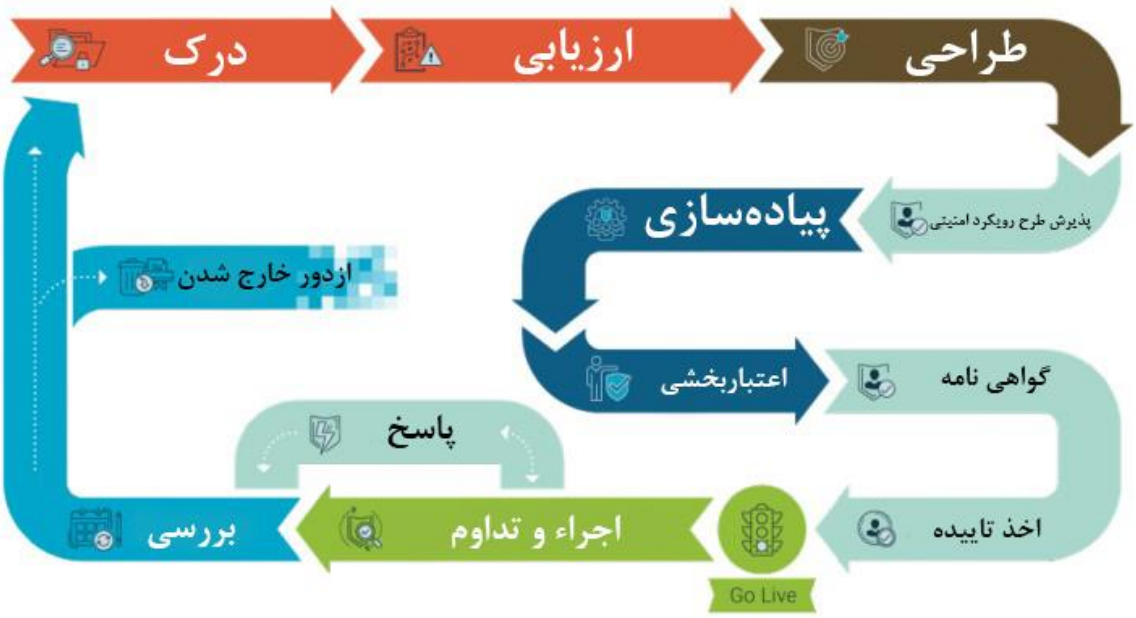
نقض امنیت اطلاعات می‌تواند به طور جدی توانایی شما در تجارت را مختل کند، شما و مشتریان خود را در معرض خطرات بیشتری قرار دهید و به اعتبار شما آسیب برساند .نقض می‌تواند:

- پردازش معاملات یا ارائه خدمات اصلی را دشوار یا غیرممکن می‌کند
- شامل از دست دادن مالکیت معنوی است
- قوانین حاکم بر حریم خصوصی یا سایر اطلاعاتی را که با اعتماد محرمانه است نقض کنید
- شما را در معرض مراحل قانونی احزاب متضرر قرار می‌دهد
- باعث خجالت در سطح بین المللی، ملی یا منطقه‌ای شوید
- اعتماد بین سازمان خود و افرادی که خدمت می‌کنید یا با آنها کار می‌کنید را از بین ببرید.

❖

❖ **چرخه عمر امنیت اطلاعات را بفهمید**

برای محافظت از اطلاعات سازمان خود، چرخه حیات امنیت اطلاعات را بشناسید و دنبال کنید.



مراحل چرخه حیات مراحلی را نشان می‌دهد که شما باید برای درک آنچه برای محافظت از آن نیاز دارید، ارزیابی خطرات موجود در اطلاعات خود، طراحی اقدامات امنیتی مناسب، تأیید صحت اجرای صحیح این اقدامات و حفظ آنها با گذشت زمان انجام دهید.

❖ **رویکرد مبتنی بر ریسک برای امنیت اطلاعات را در پیش بگیرید**

در پاسخ به این تهدیدها، استفاده از یک رویکرد مبتنی بر ریسک که مدیریت صحیح ریسک را اعمال می‌کند، به شما امکان می‌دهد یک چارچوب امنیت اطلاعات را متناسب با زمینه عملیاتی سازمان خود و تهدیداتی که ممکن است با آن روبرو شود، تنظیم کنید.

نباید با همه اطلاعات به یک اندازه رفتار شود .برخی از اطلاعات دارای ارزش یا حساسیت بیشتری هستند و به سطح حفاظت بیشتری نیاز دارند .شما باید ارزش، اهمیت و حساسیت اطلاعات خود را درک کنید .این حداقل نیازهای شما برای محافظت از آن در برابر آسیب را تعیین می‌کند. تاثیر کسب و کار سطح (BILs) ابزاری است که می‌تواند برای ارزیابی ارزش اطلاعات خود را و تأثیر بالقوه اگر اطلاعات شما به خطر بیافتد استفاده می‌شود .همراه با ارزیابی احتمال وقوع، تهدیدها، و آسیب پذیری ها، BILs باید ارزیابی خطر قوی را به شما اطلاع دهد.

تأثیر در سازمان خود را در نظر بگیرید اگر:

- یک پایگاه داده با اطلاعات حساس خراب شد
- یک شخص غیر مجاز به اطلاعات حساس و حساس با رسانه‌ها دسترسی پیدا کرده و آنها را به اشتراک گذاشته است

اطلاعات به طور تصادفی برای اشخاص ثالث منتشر شد.

❖ **یک فرهنگ امنیتی ایجاد کنید که همه آن را بشناسند و از آن استفاده کنند**

هر کس در سازمان شما باید بخشی از فرهنگ امنیتی شما باشد، در غیر این صورت فرایندها و ابزارهای امنیتی شما مbe ثر نخواهد بود .فقط یک پیوست ایمیل مخرب طول می‌کشد تا به طور بالقوه کل سازمان شما را به خطر بیندازد .شما باید اطمینان حاصل کنید که افراد و شرکای خود:

- خطرات امنیتی را درک کنید
- سیاست‌های امنیت اطلاعات خود را درک کنید
- رفتارهای امنیتی صحیح را اتخاذ کنید.

برای سوق دادن همه افراد، ارائه آموزش آگاهی از امنیت و پشتیبانی مداوم از اهمیت بالایی برخوردار است. مدیر ارشد امنیت اطلاعات (CISO)یا سایر مدیران ارشد مسئول امنیت اطلاعات سازمان شما، مطابق با سیاست کلی محافظتی است.

❖ **چارچوبی را برای مدیریت امنیت اطلاعات اتخاذ کنید**

سازمان شما باید چارچوبی برای هدایت و هماهنگی مدیریت امنیت اطلاعات شما ایجاد کند.

چارچوب شما باید:

- متناسب با سطح خطر امنیتی در محیط اطلاعاتی شما باشد
- با نیازهای تجاری و تعهدات قانونی خود سازگار باشید
- با هر چارچوب دیگر حاکم بر امنیت سازمان خود ادغام شوید.

چارچوب شما همچنین باید شامل چگونگی اطمینان شما از سازمان شما باشد:

- سیاست‌ها و فرایندهای امنیتی را می‌فهمد و دنبال می‌کند
- نسبت به تغییر در سیستم‌ها، خطرات یا استانداردها هشدار داده می‌شود
- اطلاعات محافظت شده را به درستی علامت گذاری می‌کند، دسترسی پیدا می‌کند و از آنها طبقه بندی می‌کند
- دسترسی به اطلاعات را مدیریت و کنترل می‌کند.

۵-۱-۱- الزامات اجباری امنیت اطلاعات را برآورده کنید

با پیروی از الزامات اجباری و مراحل چرخه عمر اطلاعات مربوط به توضیحات زیر، سازمان خود را با امنیت اطلاعات قوی ایمن نگه دارید.

❖ **آنچه را که برای محافظت از آن نیاز دارید درک کنید**

اطلاعات و سیستم‌های ICT را که سازمان شما مدیریت می‌کند شناسایی کنید .خطرات امنیتی (تهدیدها و آسیب پذیری ها) و تأثیر تجاری هرگونه نقض امنیت را ارزیابی کنید.

❖ **درک کنید که از چه اطلاعات و سیستم‌های ICT برای محافظت نیاز دارید**

برای اجرای اقدامات امنیتی صحیح، باید بفهمید که چه اطلاعاتی دارید و ارزش آنها چقدر است.

یک موجودی جامع به شما کمک می‌کند تا تعیین کنید که سازمان شما چه نوع اطلاعات و سیستم‌های ICT را شامل می‌شود، از جمله مواردی که از برنامه‌های تداوم تجارت و بازیابی بلایا پشتیبانی می‌کنند.

برای هر نوع اطلاعات یا سیستمICT ، باید موارد زیر را ثبت کنید:

- نحوه استفاده سازمان شما (و هر ارائه دهنده یا شریک)، پردازش، اشتراک یا ذخیره آن
- هرگونه رازداری، صداقت، حریم خصوصی یا الزامات قانونی مربوطه
- چه مدت زمان برای نگهداری و محافظت از اطلاعات نیاز دارید
- حداقل سطح عملکرد سیستم یا دسترسی به اطلاعات سازمان شما برای عملکرد نیاز دارد
- چه شرایط تخریب یا دفع اعمال می‌شود.

❖ ارزش اطلاعات خود را درک کنید

شما باید ارزش، اهمیت و حساسیت اطلاعات خود را درک کنید .این حداقل نیازهای شما برای محافظت از آن در برابر آسیب را تعیین می‌کند. نباید با همه اطلاعات به یک اندازه رفتار شود .برخی از اطلاعات دارای ارزش یا حساسیت بیشتری هستند و به سطح حفاظت بیشتری نیاز دارند .تاثیر کسب و کار سطح (BILs) ابزاری است که می‌تواند برای ارزیابی ارزش اطلاعات خود را و چه تأثیر ممکن است رخ دهد اگر اطلاعات شما به خطر بیافتد استفاده می‌شود.

بر اساس ارزش اطلاعات و تجهیزات خود، شما باید طبقه بندی و علائم محافظتی به آن اختصاص دهید که به افراد شما در مورد نحوه مدیریت و محافظت از اطلاعات در برابر آسیب، اطلاع دهد .همه آژانس‌های دولتی نیوزلند باید این کار را مطابق با سیستم طبقه بندی امنیتی دولت نیوزیلند انجام دهند .

❖ خطرات موجود در امنیت اطلاعات خود را ارزیابی کنید

شما باید درباره آسیب پذیری ها و تهدیداتی که با آنها روبرو هستید و تأثیر آنها بر سازمان خود فکر کنید .برای کمک به شما در ارزیابی خطرات سازمان سیyou الات زیر را در نظر بگیرید.

❖ سازمان شما در کجا آسیب پذیر است؟

مناطقی را شناسایی کنید که سازمان شما ممکن است در برابر نقض امنیت (عمدی یا تصادفی) آسیب پذیر باشد .مشخص کنید که کدام آسیب پذیری ها ممکن است مورد سو استفاده قرار بگیرند و چگونه ممکن است این موارد محدود شود.

❖ با چه تهدیدهایی روبرو هستید؟

تهدیدات احتمالی امنیت اطلاعات خود را شناسایی و ثبت کنید و از به روز بودن این اطلاعات اطمینان حاصل کنید .از خود بپرسید، "چه کسی از دسترسی به اطلاعات سازمان ما سود می‌برد و چه اطلاعاتی می‌خواهند؟"

❖ نقض امنیت چه تاثیری بر سازمان شما خواهد داشت؟

ارزیابی کنید که در صورت نقض امنیت اطلاعات، سازمان شما چگونه تأثیر می‌گذارد .درباره محرمانه بودن، صداقت و در دسترس بودن اطلاعات خود فکر کنید.

شما همچنین باید در هنگام ارزیابی ریسک خود این سؤالات اضافی را در نظر بگیرید:

❖ **آیا خطرات زنجیره تأمین خود را آورده‌اید؟**

زنجیره‌های تأمین عمیق‌تر شده و اتصالات پیچیده‌تر می‌شوند .اطمینان حاصل کنید که هر قسمت از زنجیره تأمین سازمان شما در ارزیابی خطر شما گنجانده شده است .بررسی کنید تأمین کنندگان شما می‌توانند بیان کنند که چه کسی و به چه چیزی متصل هستند و چه وابستگی‌هایی دارند.

❖ **آیا از خطرات ناشی از مجموعه اطلاعات بهره مند شده‌اید؟**

مجموعه اطلاعات (اطلاعات جمع شده) می‌توانند از اطلاعات تکمیل شده با ارزش‌تر باشند، بنابراین ممکن است سازمان شما برای محافظت از آنها به اقدامات امنیتی اضافی نیاز داشته باشد .از خود بپرسید، "اگر مجموعه نقض شود، چه چیزی می‌تواند استنباط شود؟ "اطلاعات جمع شده شامل مجموعه‌ای از اسناد فیزیکی و مجموعه اطلاعاتی است که در سیستم‌های ICT شما ذخیره شده است.

❖ **آیا امنیت موجود شما کافی است؟**

اقدامات امنیتی موجود خود را تجزیه و تحلیل کنید .آن‌ها چقدر می‌توانند از اطلاعات شما در برابر خطرات و تأثیراتی که شناسایی کرده‌اید محافظت کنند؟ اگر اطلاعاتی مانند سوابق مشتری، داده‌های مالی و دارایی معنوی به سرقت رفته باشد، آیا می‌توانید به سرعت و با دقت تشخیص دهید که چه چیزی از دست رفته است و می‌توانید آن را بازیابی کنید؟ برای بهبود امنیت خود باید چه اقدامی انجام دهید؟

❖ **امنیت اطلاعات خود را طراحی کنید**

در اوایل مراحل برنامه ریزی، انتخاب و طراحی، امنیت اطلاعات را در نظر بگیرید .تدابیر امنیتی را طراحی کنید که خطرات سازمان شما را تهدید می‌کند و با اشتهای شما سازگار است .اقدامات امنیتی شما باید مطابق با موارد زیر باشد: • سیستم طبقه بندی امنیتی دولت نیوزیلند • کتابچه راهنمای امنیت اطلاعات نیوزلند • هرگونه تعهدات حریم خصوصی، قانونی و نظارتی که تحت آن فعالیت می‌کنید .یک چارچوب مناسب مدیریت امنیت اطلاعات متناسب با خطرات خود اتخاذ کنید.

❖ **تدابیر مناسب برای امنیت اطلاعات را طراحی کنید**

تدابیر امنیتی اطلاعات شما باید متناسب با خطراتی که سازمان شما شناسایی کرده است و مطابق با اشتهای مخاطره آمیز باشد.

کتابچه راهنمای امنیت اطلاعات نیوزلند (NZISM) بر اساس طبقه بندی اطلاعات شما و مجموعه‌ای از کنترل‌های اضافی برای کمک به شما در درمان خطرات شناسایی شده، کنترل پایه اجباری را برای سازمان‌های دولتی نیوزلند مشخص می‌کند.

❖ **از چندین لایه امنیتی استفاده کنید - "دفاع در عمق"**

با استفاده از چندین لایه مختلف اقدامات امنیتی می‌توان به امنیت مؤثر برای یک دارایی اطلاعاتی دست یافت .از این رویکرد به عنوان "دفاع عمیق" یاد می‌شود - امنیت دارایی با از دست دادن یا نقض هیچ یک از لایه‌های امنیتی، به میزان قابل توجهی کاهش نمی‌یابد.

❖ **به تمام نقاطی که ممکن است امنیت اطلاعات شما نقض شود، رسیدگی کنید**

هنگامی که اقدامات امنیتی خود را طراحی می‌کنید، خطرات و آسیب پذیری های مهم امنیتی اطلاعات خود، از جمله تهدیدات امنیت سایبری، فرهنگ امنیت اطلاعات، محصولات و فرآیندهای امنیتی را برطرف کنید.

❖ **اطمینان حاصل کنید که سازمان شما به تعهدات اجباری خود عمل می‌کند**

طراحی کلیه اقدامات امنیتی شما برای اطلاعات، سیستم‌هایICT ، شبکه‌ها (از جمله دسترسی از راه دور)، زیرساخت‌ها و برنامه‌ها باید قانونی باشد NZISM .منبعی است که آژانس‌های دولتی نیوزلند باید از آن استفاده کنند و سازمان‌های خصوصی می‌توانند از آن برای اطمینان از مطابقت سازمان شما با تعهدات خود استفاده کنند .ارزیابی دقیق اینکه کدام کنترلها در سازمان شما اعمال می‌شوند مهم است.

❖ **معامله بین امنیت نهایی و عملکرد مؤثر را در نظر بگیرید**

رعایت حداقل استانداردها اغلب کافی نیست، اما امنیت نهایی می‌تواند هزینه زیادی را برای شما به همراه داشته باشد .چارچوب امنیت اطلاعات شما باید عملی باشد و در عین حال اطمینان حاصل کند که خطرات حیاتی شما به اندازه کافی برطرف شده است.

❖ **برنامه‌های تداوم کسب و کار و بهبود شرایط را به مشاغل خود اضافه کنید**

الزامات امنیتی مشخص شده در مرحله طراحی نیز باید در برنامه‌های تداوم کسب و کار و بازیابی فاجعه باشد.

پذیرش: طراحی امنیت اطلاعات خود را پذیرفته کنید

قبل از اینکه اقدامات امنیتی خود را اجرا کنید، مدیر ارشد امنیت اطلاعات (یا سایر مقامات اجرایی تعیین شده) شما باید بپذیرد که طرح امنیتی پیشنهادی برای اهداف مناسب است و به الزامات خاص امنیت اطلاعات سازمان شما می‌پردازد.

❖ **اقدامات امنیتی اطلاعات خود را اجرا کنید**

در طول این مرحله، شما باید اقدامات امنیتی و حریم خصوصی مورد توافق را اجرا کنید، از جمله سیاست‌ها، فرایندها و اقدامات امنیتی فنی.

❖ **زنجیره‌های تأمین و راه حل‌های امن بسازید**

با تأمین کنندگان خود کار کنید تا اطمینان حاصل کنید که آنها شرایط امنیتی شما را درک می‌کنند و می‌توانند آن را برآورده کنند .الزامات امنیتی خود را در قراردادهای قراردادی خود قرار دهید.

ضعف‌های امنیتی در تأمین کنندگان می‌تواند اقدامات امنیتی قوی دیگری را در سایر بخشهای تجارت شما به خطر بیندازد .بخاطر بسپارید که خطرات اطلاعاتی مربوط به چرخه عمر توسعه سیستم ICT وجود دارد، مانند دسترسی ارائه دهندگان توسعه و استفاده از داده‌های آزمایش یا سیستم‌های ردیابی نقص.

❖ **تغییرات را آزمایش و کنترل کنید**

آزمایش سیستم باید در حین توسعه و قبل از پذیرش اتفاق بیفتد .همچنین باید اطمینان حاصل کنید که تغییرات مطابق با استانداردهای مربوطه هستند، یک فرایند کنترل تغییر مؤثر داشته باشید.

اقدامات امنیتی خود را تأیید کنید

تأیید کنید که اقدامات امنیتی اطلاعات شما به درستی اجرا شده و برای اهداف مناسب است .فرآیند صدور گواهینامه و اعتبار سنجی را به اتمام برسانید تا از سیستم‌های ICT خود برای تأیید بهره مند شوید.

❖ اقدامات امنیتی خود را تأیید کنید

اقدامات امنیتی سازمان خود را تأیید کنید تا بفهمید آیا به درستی اجرا شده‌اند یا برای اهداف مناسب هستند.

❖ اعتبار سنجی اقدامات امنیتی شما پاسخگویی را فراهم می‌کند

CISO باید تعیین کند که آیا اقدامات برای خطرات سازمان شما قابل قبول است یا خیر .مرحله اعتبارسنجی این اطمینان را به مدیران ارشد می‌دهد که اطلاعات و فناوری مربوط به آن به خوبی مدیریت شده، خطرات به درستی شناسایی و کاهش یافته و مسئولیت‌های حاکمیتی برآورده می‌شوند .

❖ از صدور گواهینامه و اعتباربخشی مناسب اطمینان حاصل کنید

فرآیندهای صدور گواهینامه و اعتباربخشی مناسب را برای نوع اقدامات امنیتی در حال اجرا انجام دهید .سیستم‌های ICT باید فرآیند صدور گواهینامه و اعتباربخشی تعریف شده در NZISM را دنبال کنند .آن‌ها همچنین باید کنترل‌های اجباری را در کتابچه راهنما منعکس کنند .امنیت فیزیکی نیاز به تأییدیه و اعتبار اضافی دارد .برای اطلاعات بیشتر به پروتکل مدیریت برای امنیت فیزیکی مراجعه کنید.

❖ برای ایمن ماندن کار و نگهداری کنید

تهدیدها، آسیب پذیری ها و خطرات با گذشت زمان و با تغییر تقاضای فناوری، تجارت و اطلاعات، تکامل می‌یابند .تدابیر امنیتی باید همگام با این تغییر ادامه یابد تا مرتبط و مؤثر باقی بماند.

❖ تهدیدات و آسیب پذیری های در حال تحول را تحلیل کنید

برای مدیریت آسیب پذیری های امنیت اطلاعات خود، اقدام زیر را انجام دهید.

- سیستم‌ها، شبکه‌ها و فرایندهای خود را برای آسیب پذیری های امنیتی کنترل کنید .رویدادها، پیکربندی‌ها و فرآیندهای سیستم و شبکه را برای شناسایی وقایع مشکوک یا غیرمجاز مشاهده کنید.
- برای در امان ماندن از آسیب پذیری ها یا نقص‌های موجود در محیط فنی خود فعال باشید.
- اقدامات امنیتی خود را در برابر بهترین اقدامات و تهدیدهای امنیتی شناخته شده ارزیابی کنید.
- آسیب پذیری هایی را که فوری‌ترین خطر را برای سازمان شما ایجاد می‌کنند، تجزیه و تحلیل، اولویت بندی کنید و گزارش دهید.
- برای کاهش خطر به خطر افتادن اطلاعات خود، اصلاحات را اعمال و پیگیری کنید.

❖ اقدامات امنیتی اطلاعات خود را به روز نگه دارید

اقدامات امنیتی شما فقط در صورت مؤثر بودن خطرات واقعی شما مثر است .برای به روز بودن اقدام زیر را انجام دهید.

- سیستم‌های کنترل دسترسی کاربر خود را حفظ کنید.
- از تجهیزات ICT سازمان خود محافظت کنید.
- در هنگام معرفی فرایندها، سیستم‌ها و قابلیت‌های جدید، برنامه‌های تداوم کسب و کار و بازیابی خطرات خود را آزمایش کنید .اطمینان حاصل کنید که سازمان شما برای وقفه قابل توجه خدمات، حمله یا دیگر حادثه امنیتی جدی، آمادگی کافی را دارد.

❖ **به حوادث امنیتی اطلاعات پاسخ دهید**

مدیریت خوب برای کاهش تأثیر حوادث امنیتی و بهبود سریع آن بسیار حیاتی است .پاسخ حادثه باید یک قسمت اصلی از چارچوب امنیتی کلی شما باشد.

❖ **در هنگام وقوع حادثه روند صحیحی را دنبال کنید**

وقتی حادثه‌ای اتفاق می افتد، برای کاهش هرگونه تأثیر سریع اقدام کنید و به سازمان خود کمک کنید تا در اسرع وقت بهبود یابد. بعداً ممکن است لازم باشد اعتماد به نفس شرکا یا مشتریانی را که تحت یک حادثه آسیب دیده‌اند بازگردانید. تحقیق و پاسخ دادن :ابتدا جزئیات حادثه را جمع آوری کرده و میزان تأثیر را ارزیابی کنید .اقدامات اولیه لازم برای کاهش آسیب را انجام دهید.

برقراری ارتباط و تشدید :اطمینان حاصل کنید که حوادث امنیتی را برای اقدام طرفهای تحت تأثیر قرار داده‌اید .در صورت لزوم، به هر مقام مربوطه اطلاع دهید .همچنین ممکن است لازم باشد بعضی از افراد را فعالانه هشدار دهید تا از آسیب دیدگی در پایین دست جلوگیری کنند.

بازیابی و یادگیری: در صورت امکان اطلاعات از دست رفته را بازیابی کرده و عملکردهای تجاری خود را بازگردانید .اطمینان حاصل کنید که سازمان شما از این حادثه درس می‌گیرد تا بتوانید اقدامات امنیتی خود را در آینده بهبود ببخشید.

❖ **امنیت خود را به روز نگه دارید**

اطمینان حاصل کنید که امنیت اطلاعات شما برای هدف مناسب است: - نظارت بر رویدادهای امنیتی و پاسخگویی به آنها - به روز نگه داشتن تهدیدات در معرض خطر و آسیب پذیری ها - حفظ دسترسی مناسب به اطلاعات شما.

❖ **اقدامات امنیتی خود را مرور کنید**

برای اطمینان از مناسب بودن اهداف امنیتی خود، مرتباً بررسی کنید

تغییراتی را در نحوه استفاده و سازماندهی اطلاعات خود و هرگونه تغییر مورد نیاز در قانون را شناسایی کنید .برای اطلاع از پیشرفت‌ها از این اطلاعات استفاده کنید.

❖ **بررسی‌های دوره‌ای انجام دهید و از انطباق اطمینان حاصل کنید**

اقدامات امنیتی خود را مرتباً کنترل، بازبینی و حسابرسی کنید تا بدانید سیاست‌های امنیتی اطلاعات شما در چه مرحله‌ای اجرا و دنبال می‌شوند.

❖ **تغییرات مورد نیاز در امنیت اطلاعات خود را شناسایی کنید**

تغییر یک امر مسلم است .شما باید مشخص کنید که چه تغییراتی در محیط شما ممکن است بر امنیت اطلاعات شما تأثیر بگذارد و آماده باشید تا چرخه حیات امنیت اطلاعات خود را دوباره راه اندازی کنید.

برای اطلاع از تغییرات و پیشرفت‌ها، این سؤالات را در نظر بگیرید.

- آیا شما از اطلاعات به روش‌های جدید استفاده می‌کنید؟
- آیا شما یک تأمین کننده، ارائه دهنده یا شریک جدید برای رفع نیاز خاص خود می‌آورید؟

- آیا در حال برنامه ریزی برای بهبود خدمات امنیتی داخلی یا خارجی هستید؟
- آیا تهدیدات امنیتی یا آسیب پذیری های جدید را شناسایی کرده‌اید؟

❖ **اطلاعات را به صورت ایمن بازنشسته کنید**

وقتی دیگر به اطلاعات و سیستم‌های پشتیبانی کننده ICT شما نیازی نیست، باید بایگانی شوند، از بین بروند، دوباره مورد استفاده قرار بگیرند یا به طور ایمن از بین بروند NZISM .مشاوره و کنترل در مورد مدیریت اطلاعات و سیستم‌هایی را که به پایان چرخه عمر خود رسیده‌اند، ارائه می‌دهد.

این سؤالات را در نظر بگیرید:

- وقتی دیگر نیازی به علامت گذاری محافظتی نیست، چگونه اطلاعات و تجهیزات خود را طبقه بندی می‌کنید؟
- چگونه می‌توانید اطلاعات حساس و تجهیزات مربوطه را دور بیندازید؟

اطمینان حاصل کنید که قوانین مربوطه، NZISMو استانداردهای بهترین روش را در نظر گرفته‌اید.

۵-۳- ایجاد فرهنگ امنیتی

هر کس در سازمان شما باید بخشی از فرهنگ امنیتی شما باشد، در غیر این صورت فرایندها و ابزارهای امنیتی شما مbe ثر نخواهد بود. فقط یک پیوست ایمیل مخرب طول می‌کشد تا به طور بالقوه کل سازمان شما را به خطر بیندازد .شما باید اطمینان حاصل کنید که افراد و شرکای خود:

- خطرات امنیتی را درک کنید
- سیاست‌های امنیت اطلاعات خود را درک کنید
- رفتارهای امنیتی صحیح را اتخاذ کنید.

برای سوق دادن همه افراد، ارائه آموزش آگاهی از امنیت و پشتیبانی مداوم از اهمیت بالایی برخوردار است. مدیر ارشد امنیت اطلاعات (CISO) یا سایر مدیران ارشد مسئول امنیت اطلاعات سازمان شما، مطابق با سیاست کلی محافظتی است.

۵-۴- چارچوبی را برای مدیریت امنیت اطلاعات اتخاذ کنید

سازمان شما باید چارچوبی برای هدایت و هماهنگی مدیریت امنیت اطلاعات شما ایجاد کند.

چارچوب شما باید:

- متناسب با سطح خطر امنیتی در محیط اطلاعاتی شما باشد
- با نیازهای تجاری و تعهدات قانونی خود سازگار باشید
- با هر چارچوب دیگر حاکم بر امنیت سازمان خود ادغام شوید.

چارچوب شما همچنین باید شامل چگونگی اطمینان شما از سازمان شما باشد:

- سیاست‌ها و فرایندهای امنیتی را می‌فهمد و دنبال می‌کند
- نسبت به تغییر در سیستم‌ها، خطرات یا استانداردها هشدار داده می‌شود
- اطلاعات محافظت شده را به درستی علامت گذاری می‌کند، دسترسی پیدا می‌کند و از آنها طبقه بندی می‌کند

- دسترسی به اطلاعات را مدیریت و کنترل می‌کند.

نمونه‌هایی از بهترین چارچوب‌های تمرین عبارتند از:

- ISO / IEC 27001: 2013فناوری اطلاعات - تکنیک های امنیتی - سیستم های مدیریت امنیت اطلاعات - الزامات
- چارچوب امنیت سایبری موسسه ملی استاندارد و فناوری ایالات متحده (NIST)

۵-۵- سیستم طبقه بندی امنیتی کشور نیوزیلند

سیستم طبقه بندی دولت نیوزیلند از طریق یک سری اقدامات امنیتی از اطلاعات رسمی محافظت می‌کند .این اقدامات پس از اعمال، برای هر کسی که به اطلاعات رسمی دسترسی داشته باشد اعمال می‌شود.

۵-۱-۲- محافظت از اطلاعات رسمی در برابر دسترسی غیر مجاز و افشای تصادفی

سیستم طبقه بندی امنیتی دولت نیوزیلند از طریق یک سری اقدامات امنیتی از اطلاعات رسمی محافظت می‌کند .این اقدامات پس از اعمال، برای هر کسی که به اطلاعات رسمی دسترسی داشته باشد اعمال می‌شود. سیستم طبقه بندی برای محافظت از اطلاعات رسمی در برابر افشای اطلاعات یا دسترسی‌هایی که برای شهروندان نیوزیلند، دولت نیوزیلند یا سازمانهای دولتی مضر است، ساخته شده است.

❖ **امنیت اطلاعات خود را طراحی کنید**

در اوایل مراحل برنامه ریزی، انتخاب و طراحی، امنیت اطلاعات را در نظر بگیرید .تدابیر امنیتی را طراحی کنید که خطرات سازمان شما را تهدید می‌کند و با اشتهای شما سازگار است .اقدامات امنیتی شما باید مطابق با موارد زیر باشد: • سیستم طبقه بندی امنیتی دولت نیوزیلند • کتابچه راهنمای امنیت اطلاعات نیوزلند • هرگونه تعهدات حریم خصوصی، قانونی و نظارتی که تحت آن فعالیت می‌کنید .یک چارچوب مناسب مدیریت امنیت اطلاعات متناسب با خطرات خود اتخاذ کنید.

آژانس شما باید از سیستم طبقه بندی استفاده کند تا:

- مشخص کنید آژانس شما برای محافظت از کدام دارایی‌های اطلاعاتی نیاز دارد
- سیاست‌ها و پروتکل‌های مربوط به مدیریت اطلاعات رسمی و استفاده از علائم محافظ را پیاده سازی کنید.

هیئت دولت در دسامبر سال ۲۰۰۰ با سیستم طبقه بندی امنیتی موافقت کرد.[CAB (00) M42 / 4G (4)]

❖ **قانون همچنین از اطلاعات رسمی محافظت می‌کند**

سازمان شما باید هرگونه الزامات قانونی را برای محافظت از اطلاعات رسمی تحت قوانین مربوطه مانند موارد زیر در نظر بگیرد:

- قانون سوابق عمومی ۲۰۰۵
- حریم خصوصی قانون ۲۰۲۰
- قانون اطلاعات رسمی ۱۹۸۲.

اگر الزامات قانونی بیشتر از سیستم طبقه بندی به اقدامات امنیتی نیاز دارد، اقدامات قانونی را اعمال کنید.

❖ **قانون اطلاعات رسمی ۱۹۸۲**

اطلاعات رسمی قانون ۱۹۸۲ اساس قانونی برای انتشار اطلاعات دولت فراهم می‌کند بخشهای ۶، ۷ و ۹ قانون انواع اسناد دولتی را توصیف می‌کند که ممکن است معاف شوند یا مشروط از افشای مجاز معاف هستند.

❖ **اطلاعات رسمی چیست؟**

اطلاعات رسمی هر اطلاعاتی است که توسط دولت نیوزیلند و سازمان‌های آن نگهداری می‌شود.

دو نوع اطلاعات رسمی وجود دارد:

- اطلاعاتی که نیازی به افزایش امنیت ندارند
- اطلاعاتی که برای محافظت در برابر افشای غیرمجاز به اقدامات امنیتی بیشتر نیاز دارد.

اطلاعات رسمی می‌تواند شامل اطلاعات بخش عمومی باشد که برای دسترسی عمومی یا گردش عمومی تحریم شده‌اند، مانند انتشارات یا وب سایت‌ها

❖ **محدود کردن دسترسی به اطلاعات رسمی**

اقدامات امنیتی برای محافظت از اطلاعات رسمی شامل موارد زیر است:

- اقدامات رویه‌ای که افرادی را که می‌توانند از اطلاعات رسمی مانند سیاستها و فرایندها استفاده، مدیریت، انتقال و دسترسی به آنها را محدود کنند، محدود می‌کند
- اقدامات فیزیکی که دسترسی به مناطقی را که اطلاعات رسمی در آنها ذخیره یا استفاده می‌شود مانند موانع فیزیکی یا گاوصندوق‌ها کنترل می‌کند

اقدامات فنی که به محافظت از اطلاعات رسمی، مانند دیوارهای آتش و رمزگذاری کمک می‌کند.

❖ **دسترسی به افراد دارای "نیاز به دانستن" را محدود کنید**

برای کاهش خطر افشای غیرمجاز، فقط افرادی که نیاز به دانش اثبات شده‌ای دارند باید دسترسی به اطلاعات رسمی داده شود، صرف نظر از اینکه این موضوع تابع سیستم طبقه بندی است یا خیر. شما نباید به افراد اجازه دسترسی به اطلاعات رسمی را بدهید زیرا دانستن آنها برای آنها مناسب است یا به دلیل وضعیت، موقعیت، درجه یا سطح دسترسی مجاز آنها.

برای جزئیات بیشتر در مورد نیازهای امنیتی پرسنل، به پروتکل مدیریت امنیت پرسنل بروید.

❖ استفاده از علائم محافظ

نشانه‌های محافظتی بر روی اطلاعات و تجهیزات قرار داده می‌شود تا سطح حفاظت مورد نیاز آنها را نشان دهد .سطح حفاظت بر اساس ارزیابی خطر آسیب یا تعصبی است که می‌تواند در نتیجه به خطر افتادن محتوای خاص باشد. پس از شناسایی اطلاعاتی که نیاز به محافظت یا استفاده ویژه دارد (یا هر دو)، باید یک علامت محافظ به آن اختصاص دهید.

مارک محافظ نشان می‌دهد:

- که اطلاعات از نظر ماهیت حساس شناخته شده‌اند
- سطح حفاظتی که اطلاعات باید هنگام تولید، استفاده، ذخیره، انتقال، انتقال و دفع داشته باشند.

الزامات استفاده از علائم محافظ همچنین در مورد اطلاعاتی که در سیستم‌های فناوری اطلاعات و ارتباطات (ICT) نگهداری می‌شوند نیز اعمال می‌شود.

❖ **انواع علائم محافظ**

سه نوع علامت گذاری محافظ وجود دارد:

- ·طبقه بندی های امنیتی
- ·تأیید و علامت های محفظه ای.

هنگامی که این علامت گذاری‌ها بر روی اطلاعات رسمی اعمال می‌شود، از این اطلاعات به عنوان "محافظ علامت گذاری شده" یاد می‌شود. الزامات استفاده از اطلاعات و تجهیزات دارای علامت محافظ ، جزئیات و راهنمایی در مورد نحوه صحیح استفاده از علائم محافظ را ارائه می‌دهد. با این حال ، قبل از اینکه هرگونه اطلاعات و تجهیزات را علامت گذاری کنید ، مطمئن شوید که طبقه بندی‌های امنیتی را به درستی درک کرده و آنها را تعیین کرده‌اید.

۵-۱-۳- مروری بر طبقه بندی‌های امنیتی

یک طبقه بندی امنیتی مشخص می‌کند که مردم چگونه باید از اطلاعات و تجهیزات مورد استفاده خود محافظت کنند.

طبقه بندی‌های امنیتی را می‌توان به دو نوع اطلاعات تقسیم کرد:

- اطلاعات سیاست و حریم خصوصی
- اطلاعات امنیت ملی
- اطلاعات سیاست و حریم خصوصی

طبقه بندی برای موادی که باید به دلیل منافع عمومی یا حریم شخصی محافظت شوند عبارتند از:

- با اطمینان
- حساس.

طبقه بندی های امنیتی برای اطلاعات سیاست و حریم خصوصی دارای جزئیات بیشتری است.

❖ **اطلاعات امنیت ملی**

طبقه بندی برای موادی که باید به دلیل امنیت ملی محافظت شوند عبارتند از:

- محصور
- محرمانه
- راز
- فوق سری.

طبقه بندی های امنیتی اطلاعات امنیت ملی دارای جزئیات بیشتری است.

❖ **اطلاعات طبقه بندی نشده**

اطلاعات رسمی که به طبقه بندی امنیتی نیاز ندارند، اطلاعات "طبقه بندی نشده" نامیده می‌شوند .بیشتر اطلاعات رسمی متناسب با این دسته است.

UNCLASSIFIEDیک طبقه بندی امنیتی نیست، اما به عنوان یک علامت محافظ استفاده می‌شود زیرا نشان می‌دهد که تأثیر افشای غیر مجاز یا سو استفاده از آن ارزیابی شده است. سازمان شما باید خط مشی در مورد چگونگی علامت گذاری، محافظت و رسیدگی به اطلاعاتی که نیاز به حفاظت بیشتر دارند اما واجد شرایط طبقه بندی امنیتی نیستند داشته باشد.

۵-۱-۴- طبقه بندی امنیتی برای اطلاعات سیاست و حریم خصوصی

این بخش طبقه بندی امنیتی IN CONFIDENCE و SENSITIVE را پوشش می‌دهد.

❖ **با اطمینان**

هنگامی که احتمالاً سازش در اطلاعات وجود دارد، از طبقه بندی IN CONFIDENCE استفاده کنید.

- پیشگیری از حفظ قانون و نظم
- مانع عملکرد مؤثر دولت می‌شود
- بر حریم خصوصی شهروندان نیوزلند تأثیر منفی می‌گذارد .

به عنوان مثال، هنگامی که به خطر انداختن اطلاعات می‌تواند پیش داوری کند:

- اطلاعات تجاری شهروندان
- تعهدات اعتماد به نفس
- اقدامات برای محافظت از سلامتی و ایمنی مردم
- منافع اقتصادی قابل توجه نیوزیلند
- اقداماتی که موجب جلوگیری یا کاهش خسارات مادی افراد می‌شود.

یا وقتی مصالحه اطلاعاتی می‌تواند:

- کنوانسیون‌های قانون اساسی را نقض کنید
- مانع انجام مؤثر امور عمومی می‌شود
- نقض امتیاز حقوقی حرفه‌ای
- مانع فعالیتهای تجاری دولت شود
- منجر به افشای یا استفاده از اطلاعات رسمی برای سود یا مزیت نامناسب می‌شود.

❖ **حساس**

هنگامی که به خطر افتادن اطلاعات به منافع نیوزلند آسیب می‌رساند یا امنیت شهروندان آن را به خطر می‌اندازد، از طبقه بندی امنیتی حساس استفاده کنید.

به عنوان مثال، جایی که سازش می‌تواند:

- امنیت هر شخصی را به خطر بیندازد

- با افشای زودرس تصمیمات تغییر یا ادامه سیاست‌های اقتصادی یا مالی دولت در رابطه با:
  - نرخ ارز یا کنترل معاملات ارزی خارج از کشور
  - مقررات بانکی یا اعتباری
  - مالیات
  - ثبات، کنترل و تنظیم قیمت کالاها و خدمات، اجاره و سایر هزینه‌ها و نرخ دستمزد، حقوق و سایر درآمدها
  - وام گرفتن پول توسط دولت نیوزیلند
  - انعقاد قراردادهای تجاری خارج از کشور
- مانع مذاکرات دولت (از جمله مذاکرات تجاری و صنعتی) شود.

۵-۱-۵- طبقه بندی‌های امنیتی برای اطلاعات امنیت ملی

این بخش طبقه بندی امنیتی محدود شده، محرمانه، راز و راز را پوشش می‌دهد.

- **محصور**

هنگامی که به خطر افتادن اطلاعات ممکن است تأثیر منفی بر منافع ملی بگذارد، از طبقه بندی امنیتی محدود شده استفاده کنید.

به عنوان مثال، جایی که سازش می‌تواند:

- بر روابط دیپلماتیک تأثیر منفی می‌گذارد
- مانع اثربخشی عملیاتی یا امنیت نیوزیلند یا نیروهای دوست می‌شود
- مانع امنیت نیروهای نیوزیلند یا نیروهای دوست است
- بر ثبات داخلی یا رفاه اقتصادی نیوزیلند یا کشورهای دوست تأثیر منفی می‌گذارد.

❖ **محرمانه**

هنگامی که به خطر انداختن اطلاعات آسیب قابل توجهی به منافع ملی می زند، از طبقه بندی امنیتی محرمانه استفاده کنید.

به عنوان مثال، جایی که سازش می‌تواند:

- روابط دیپلماتیک را به شدت آسیب می زند و باعث اعتراض رسمی یا تحریم‌های دیگر می‌شود
- به اثر بخشی عملیاتی نیروهای نیوزلند یا نیروهای دوست آسیب برساند
- به امنیت نیروهای نیوزیلند یا نیروهای دوست آسیب برساند
- به اثربخشی عملیات امنیتی یا اطلاعاتی ارزشمند آسیب برساند
- آسیب به ثبات داخلی نیوزیلند یا کشورهای دوست
- زیرساخت‌های قابل توجه ملی را مختل کند.

❖ **راز**

هنگامی که به خطر انداختن اطلاعات آسیب جدی به منافع ملی وارد می‌کند، از طبقه بندی امنیتی SECRET استفاده کنید.

به عنوان مثال، جایی که سازش می‌تواند:

- تنش بین المللی را بالا ببرید
- آسیب جدی به روابط با دولت‌های دوست
- آسیب جدی به امنیت نیروهای نیوزیلند یا نیروهای دوست
- آسیب جدی به کارآیی عملیاتی نیروهای نیوزیلند یا نیروهای دوست
- آسیب جدی به اثربخشی عملیات امنیتی یا اطلاعاتی ارزشمند می زند
- آسیب جدی به ثبات داخلی نیوزیلند یا کشورهای دوست می زند
- زیرساخت‌های قابل توجه ملی را خاموش یا قابل ملاحظه‌ای مختل کند.

❖ **فوق سری**

از طبقه بندی امنیتی استفاده کنید وقتی که به خطر افتادن اطلاعات صدمات زیادی به منافع ملی وارد کند

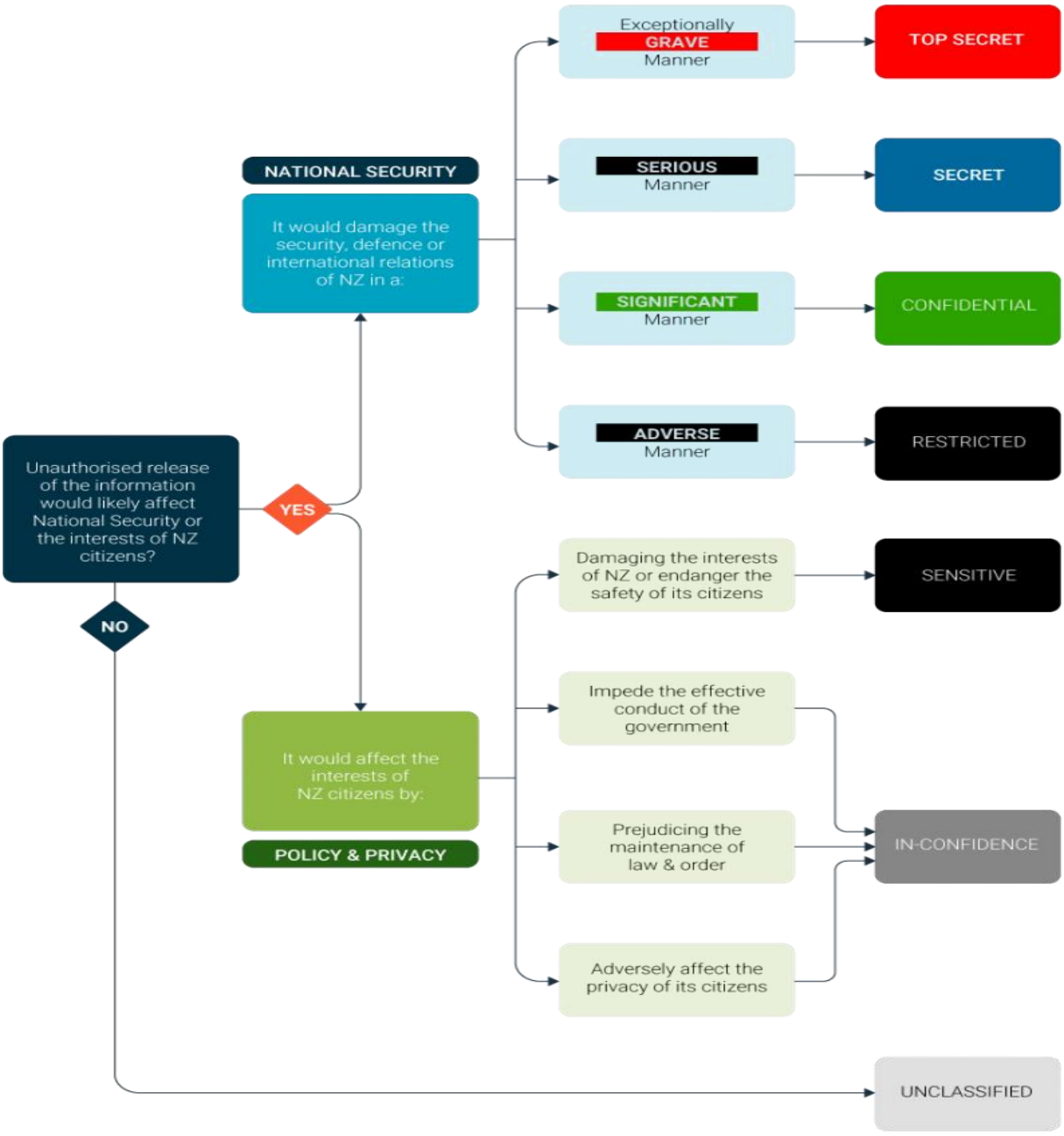
به عنوان مثال، جایی که سازش می‌تواند:

- ثبات داخلی نیوزیلند یا کشورهای دوست را تهدید کند
- منجر به از دست دادن گسترده زندگی می‌شود
- آسیب‌های استثنایی به امنیت نیوزیلند یا متحدان وارد کند
- باعث خسارت استثنایی به کارآیی عملیاتی نیروهای نیوزلند یا نیروهای دوست شود
- باعث خسارت استثنایی به اثربخشی مستمر عملیات امنیتی یا اطلاعاتی بسیار ارزشمند شود
- موجب صدمه استثنایی به روابط با سایر دولت‌ها می‌شود
- باعث آسیب شدید طولانی مدت به زیرساخت‌های قابل توجه ملی شود .

۵-۱-۶- شناسایی اطلاعات امنیت ملی

برای شناسایی اطلاعات امنیت ملی، از نمودار جریان کمک کننده طبقه بندی استفاده کنید.

نمودار جریان یاور طبقه بندی



❖ **تعریف "اطلاعات امنیت ملی"**

اطلاعات امنیت ملی به عنوان هرگونه اطلاعات یا منبع رسمی (شامل تجهیزات) تعریف می‌شود که اطلاعات مربوط به نیوزلند را ضبط می‌کند یا با آن مرتبط است:

- محافظت در برابر جاسوسی، خرابکاری، خشونت با انگیزه سیاسی، ارتقا of خشونت جمعی، حمله به سیستم دفاعی نیوزلند، اقدامات دخالت خارجی
- حفاظت از تمامیت ارضی و مرزی در برابر تهدیدات جدی
- برنامه‌ها و عملیات دفاعی
- روابط بین الملل (روابط سیاسی و اقتصادی قابل توجه با سازمانهای بین المللی و دولتهای خارجی)

- عملیات اجرای قانون (در مواردی که سازش می‌تواند راهبردهای ملی پیشگیری از جرم یا تحقیقات خاص را مختل کند یا بی فایده کند، یا بر ایمنی شخصی تأثیر منفی بگذارد)
- منافع ملی (مربوط به امور اقتصادی، علمی یا فناوری که برای ثبات و یکپارچگی نیوزلند حیاتی است).

❖ **آیا همه اطلاعات امنیت ملی نیاز به علامت محافظ دارند؟**

اطلاعات امنیت ملی فقط در صورتی باید محافظت شود که سازش یا سو استفاده از آن باعث آسیب به امنیت ملی، دولت نیوزیلند، نهادهای تجاری یا افراد عمومی شود.

۵-۱-۷- طبقه بندی‌های امنیتی اسناد کابینه

این بخش اسناد کابینه، مانند دستور کار هیئت وزیران و کمیته کابینه، مقالات، صورتجلسه ها و یادداشت‌ها را شامل می‌شود.

اسنادی که کابینه برای تدوین سیاست‌ها و تصمیم گیری‌ها استفاده می‌کند، نیاز به اقدامات حفاظتی ویژه‌ای دارند.

اسناد کابینه برخلاف سایر اطلاعات رسمی متعلق به دولتهایی است که آنها را ایجاد می‌کنند .آن‌ها یکپارچه در فرآیند تصمیم گیری دولت‌ها هستند و سوابق این تصمیمات را تشکیل می‌دهند.

هرگونه افشای غیرمجاز به صراحت و صراحت بحث در اتاق کابینه لطمه می زند و روند دولت خوب را مختل می‌کند.

❖ **مارک‌های محافظ برای مقالات کابینه**

حداقل علامت محافظ برای مقالات کابینه در اطمینان است .در صورت لزوم باید از طبقه بندی‌های امنیتی بالاتر استفاده شود.

برای اطمینان از اینکه سطح مقاله از سطح حفاظتی مناسبی برخوردار است، آژانس مبدأ (یا دفتر وزیر) موظف است طبقه بندی امنیتی را برای ارائه هیئت وزیران اعمال کند.

اگر آژانس شما یک مقاله کابینه را بدون طبقه بندی امنیتی یا با طبقه بندی نامناسب ارائه دهد، دفتر هیئت دولت با مشورت با دفتر وزیر مربوطه، طبقه بندی امنیتی صحیح را تعیین می‌کند.

❖ **علامت گذاری برای مقالات کابینه**

هنگامی که آژانس شما نیاز به شناسایی الزامات مراقبت ویژه برای مقالات کابینه دارد، باید یک علامت گذاری تأیید را اعمال کنید.

مارک‌های تأیید شده برای کاغذهای کابینه شامل موارد زیر است:

- بودجه: اقدامات پیشنهادی یا واقعی برای بودجه قبل از اعلام آنها
- بازرگانی: فرآیندهای تجاری، مذاکرات یا امور حساس
- کارکنان: اشاره به نامها یا افراد قابل شناسایی
- نیاز به رسیدگی ویژه: الزامات خاص رسیدگی اعمال می‌شود.

❖ **از کنترل ویژه‌ای که مورد نیاز است کم استفاده کنید**

اطلاعات بسیار کمی نیاز به علامت گذاری تأیید نیاز به رسیدگی ویژه‌ای دارد و باید از آنها کم استفاده شود.

این مارک تأیید مخصوص مقاله‌های هیئت دولت است .اگر مواد موجود در مقاله از نظر ماهیت بسیار حساس ارزیابی شده و نیاز به حفاظت بیشتری داشته باشد، ممکن است با طبقه بندی امنیتی SENSITIVE استفاده شود.

مشاوره بیشتر در مورد طبقه بندی و دست زدن به مواد کابینه

- وزارت نخست وزیر و کابینه (DPMC)
- جابجایی ایمن مواد کابینه

۵-۱-۸- طبقه بندی‌های امنیتی برای اطلاعات دولت‌های خارجی

این بخش اعمال طبقه بندی‌های امنیتی برای اطلاعات دولت‌های خارجی است.

سازمان‌های دولتی نیوزیلند باید به هر گونه مقررات مربوط به امنیت مردم، اطلاعات و دارایی‌های مندرج در توافق نامه‌ها و توافق نامه‌های چند جانبه یا دو جانبه که نیوزلند یا سازمان عضو آن است، پایبند باشند.

❖ حمایت متقابل تحت توافق نامه‌های امنیتی دوجانبه

توافق نامه‌های امنیتی دو جانبه می‌تواند شامل حفاظت متقابل برای تبادل اطلاعات دارای علامت محافظ باشد .در چنین مواردی، علامت گذاری طبقه بندی امنیتی معادل نیوزیلند را اعمال کنید .اطمینان حاصل کنید که حفاظت معادل، اما نه کمتر از آنچه مورد نیاز دولت ارائه دهنده اطلاعات است، است.

❖ انتشار اطلاعات از دولت‌های خارجی

قبل از انتشار اطلاعات از دولت‌های خارجی باید اجازه بگیرید .شما به تأیید کتبی آنها نیاز دارید.

❖ علامت گذاری اطلاعات در صورت عدم وجود توافق نامه‌های امنیتی دو جانبه

برای کمک به NZSIS جهت استفاده از علامت گذاری صحیح امنیتی در اطلاعات دارای علامت محافظتی که از کشور دیگری دریافت می‌کنید، مشورت کنید - کشوری که نیوزیلند با آن توافق نامه امنیتی دوجانبه ندارد.

۵-۱-۹- تأیید و مارک‌های محفظه‌ای

این بخش علائم مورد استفاده در کنار طبقه بندی‌های امنیتی را نشان می‌دهد تا نشان دهد اطلاعات دارای امنیت اضافی هستند.

❖ مارک‌های تأیید

علائم تأیید به مردم هشدار می‌دهد که اطلاعات دارای شرایط خاصی هستند.

علائم تأیید ممکن است نشان دهنده موارد زیر باشد:

- ماهیت خاص اطلاعات
- حساسیت‌های موقتی
- محدودیت در دسترس بودن

- چگونه گیرندگان باید اطلاعات را مدیریت یا افشا کنند.

❖ **انواع تأییدها و اهداف آنها**

مواد قابل حساب

این علامت گذاری نشان می‌دهد که اطلاعات به موارد زیر نیاز دارد:

- کنترل دقیق بر دسترسی و حرکت
- حسابرسی منظم برای اطمینان از حضانت ایمن آن (برای تعیین اینکه هر چند وقت یکبار حسابرسی کنید، از ارزیابی ریسک استفاده کنید).

آنچه مواد سازگار را تشکیل می‌دهد از نمایندگی به نمایندگی دیگر متفاوت خواهد بود. **توجه:** اطلاعات به طور پیش فرض از مواد ACCOUNTABLE است

❖ **قرارها**

این علامت گذاری ممکن است قبل از اعلام قرارهای واقعی یا احتمالی یا در مرحله بررسی روند توصیه و تأیید استفاده شود.

❖ **بودجه**

این علامت گذاری ممکن است برای اقدامات پیشنهادی یا واقعی بودجه قبل از اعلام آنها استفاده شود.

❖ **کابینت**

این علامت گذاری ممکن است برای موادی که به کمیته‌های هیئت دولت یا هیئت وزیران ارائه می‌شود و یا نیاز به تصمیم گیری دارد، استفاده شود.

❖ **تجاری**

این علامت گذاری ممکن است برای فرایندهای تجاری، مذاکرات یا امور حساس تجاری مورد استفاده قرار گیرد.

❖ **[بخش] فقط استفاده کنید**

این مارک می‌تواند برای موادی استفاده شود که فقط برای استفاده در بخش (های) مشخص شده باشد.

برای آزادی بارگیری شده است

این علامت گذاری ممکن است قبل از زمان مشخصی که در آن اطلاعیه یا آدرس در آن اعلام می‌شود، روی مواد استفاده شود یا اطلاعات منتشر شود.

❖ **ارزشگذارانه**

این علامت گذاری ممکن است برای مطالبی در مورد ارزیابی‌های رقابتی مانند سوابق مصاحبه و ارزیابی‌های مناقصه استفاده شود.

❖ **افتخارات**

این علامت گذاری ممکن است برای مطالبی در مورد اعطای افتخار واقعی یا بالقوه استفاده شود .ممکن است استفاده شود:

❖ **قبل از اعلام جایزه**

در مرحله بررسی یک توصیه یا فرآیند تأیید

هنگامی که شما در حال بررسی سیاست‌های افتخارات مربوط به اعمال حق سلطنتی هستید.

❖ **امتیاز حقوقی**

این علامت گذاری ممکن است برای موادی که دارای امتیاز قانونی هستند استفاده شود.

❖ **پزشکی**

این مارک می‌تواند برای مواد مربوط به موارد زیر استفاده شود:

- گزارشات پزشکی
- سوابق پزشکی و سایر مطالب مرتبط با آنها.

❖ **فقط چشمهای جدید نیوزیلند(NZEO)**

این علامت گذاری نشان می‌دهد که دسترسی به اطلاعات برای شهروندان نیوزیلندی با مجوز امنیتی مناسب بر اساس نیاز محدود شده است. برای اطلاعات رسمی همراه با تأیید مارک NZEO و طبقه بندی امنیتی در "اعتماد"، "حساس" یا "محدود:"

اگر یک رئیس آژانس فکر کند که به اتباع خارجی باید اطلاعاتی با عنوان NZEO داده شود، رئیس آژانس باید با آژانس مبدأ مشورت کند تا ببیند آیا هنوز علامت گذاری تأییدیه لازم است یا اینکه آیا برای آزاد سازی امکان اصلاح وجود دارد یا خیر .ممکن است بتوان علامت تأیید را حذف کرد یا با حذف علامت تأیید بخشی از اطلاعات را آزاد کرد.

❖ **برای اطلاعات رسمی همراه با تأیید مارک NZEO و طبقه بندی امنیتی محرمانه، راز یا راز بالا:**

اتباع خارجی مجاز به دسترسی نیستند، حتی اگر دارای مجوز امنیتی مناسب نیوزلند باشند .با این حال، در شرایط محدود، آژانس‌ها ممکن است اجازه دهند اطلاعات اتمام یافته NZEO توسط اتباع خارجی که به طور مناسب پاک شده‌اند، در صورت نیاز تجاری ضروری، مشاهده شود .در تمام چنین شرایطی، مدیرکل سرویس اطلاعاتی امنیتی نیوزلند باید مجوز این دسترسی را صادر کند.

❖ **کارکنان**

این علامت گذاری ممکن است برای موادی که شامل ارجاع به کارکنان نام برده یا قابل شناسایی است، استفاده شود. همچنین می‌تواند توسط کارکنان برای سپردن رازهای شخصی به مدیریت استفاده شود.

❖ **خط مشی**

این علامت گذاری ممکن است برای مطالب مربوط به پیشنهادهای سیاست جدید یا تغییر یافته دولت قبل از انتشار استفاده شود.

❖ **در مورد بازبینی شود**

این علامت گذاری ممکن است هنگامی استفاده شود که طبقه بندی در زمان تعیین شده بررسی شود.

❖ **آزاد شدن در(REL)**

این علامت گذاری مشخص کننده اطلاعاتی است که فقط برای کشورهای خارجی مشخص شده یا شهروندان آن کشورها نشان داده شده است یا قابل انتشار است. به عنوان مثال، RELEASABLE TO // GBR، NZیاGBR // REL ، NZبه این معنی است که اطلاعات ممکن است فقط به شهروندان و دولت‌های انگلستان و نیوزیلند منتقل شود. قرار دادن کشورها به ترتیب حروف الفبا و در درجه اول کشور مبدأ معمول است .به عنوان مثال، RELEASABLE TO // NZ، CAN، GBRنشان می‌دهد که کشور مبدأ نیوزیلند است و سند را می‌توان با شهروندان و دولت‌های کانادا و انگلستان به اشتراک گذاشت. برای نشان دادن نام کشورها و زیرمجموعه‌های آنها باید از کدهای کشور سه حرفی مناسب از کدهای ISO 3166-1 - SAI-Globalاستفاده کنید به بخش ۱: کد کشورها مراجعه کنید.

❖ **با استفاده از مارک‌های تأیید**

شما فقط در صورت نیاز واضح به مراقبت‌های ویژه باید از علامت‌های تأیید استفاده کنید .به یاد داشته باشید که نشانه‌های تأیید به خودی خود طبقه بندی امنیتی نیستند - نباید بدون طبقه بندی امنیتی ظاهر شوند.

❖ **محدود کردن دسترسی به افراد مجاز**

قبل از اینکه به اطلاعات با علامت تأیید اجازه دسترسی دهید، بررسی کنید که فرد از سطح امنیتی مناسب برخوردار باشد. آن‌ها باید دارای مجوز امنیتی باشند که در همان سطح یا بالاتر از طبقه بندی امنیتی اطلاعات باشد .به افرادی که از ترخیص صحیح برخوردار نیستند، نباید اجازه دسترسی داده شود. قبل از دستیابی به اطلاعات، باید اطلاعاتی در مورد اهمیت اطلاعات در اختیار افراد مجاز قرار دهند.

❖ **انتشار یا تغییر اطلاعات با مارک‌های تأیید از آژانس دیگری**

اگر می‌خواهید اطلاعاتی را که دارای علامت تأیید است از آژانس دیگری منتشر یا منتقل کنید، باید ابتدا مراحل مناسب را با آن آژانس توافق کنید .این ممکن است منجر به برچسب گذاری مجدد اطلاعات شود.

همچنین برای حذف علامت گذاری تأیید به توافق آژانس مبدأ نیاز دارید .اگر آژانس مبدأ با حذف تأییدیه موافقت نکرد، اطلاعات نباید منتشر شود. با این حال، الزام موافقت آژانس مبدأ برای انتشار مواد نباید تحت هیچ شرایطی یک استثنا در سیاست باشد.

❖ **علامت گذاری اسناد کابینه**

برای طبقه بندی امنیت اسناد کابینه بروید

❖ **مارک‌های محفظه‌ای**

علامت گذاری محفظه‌ای کلمه‌ای است که نشان می‌دهد اطلاعات در یک محفظه خاص برای دانستن وجود دارد .این کلمه می‌تواند یک رمز کد یا "Sensitive Compartmented Information (SCI)" باشد. معمولاً لازم است اقدامات احتیاطی امنیتی بیش از مواردی که به طور معمول توسط طبقه بندی امنیتی نشان داده می‌شود، انجام شود تا از اطلاعات مارک بندی جدا شده محافظت شود. آژانس دارنده اطلاعات مشخص می‌کند که اقدامات احتیاطی اضافی چیست .در ابتدا به افراد نیاز به دسترسی به اطلاعات توجیهی ویژه داده می‌شود. الزامات رسیدگی به اطلاعات و تجهیزات دارای علامت محافظ ، اطلاعات بیشتری می‌دهد.

۵-۱-۱۰- دستورالعمل‌های مارک‌های محافظ

این بخش به برخی از سؤالات رایج در مورد علائم محافظ پاسخ می‌دهد.

❖ چگونه اطلاعاتی را که نیاز به مارک محافظ دارند شناسایی کنیم

برای ارزیابی اینکه عواقب احتمالی اطلاعات در معرض خطر، افشای بدون مجوز یا سوmis استفاده قرار دارد، از سطوح تأثیر تجاری (BIL) استفاده کنید. اگر ارزیابی شما نشان می‌دهد که سازش یا سو استفاده از اطلاعات نتایج نامطلوبی به همراه دارد، باید از آن اطلاعات در راستای شدت آسیب احتمالی محافظت بیشتری کنید .باید از نظر محافظ مشخص شود.

❖ درباره استفاده از سطوح تأثیر تجاری بیشتر بیاموزید

سایر اطلاعات رسمی که نیاز به افزایش حفاظت دارند (اما تعریف اطلاعات امنیت ملی را برآورده نمی‌کنند) اغلب مربوط به موارد زیر است:

- مشاغل دولتی یا آژانس‌ها در مواردی که سازش می‌تواند بر توانایی دولت در تصمیم گیری یا فعالیت، اعتماد عمومی به دولت یا ثبات بازارهای اقتصادی تأثیر بگذارد
- منافع تجاری که در آن مصالحه می‌تواند بر روند رقابت تأثیر بگذارد و فرصتی برای مزیت غیرمنصفانه فراهم کند
- اطلاعات شخصی که تحت قانون حریم خصوصی ۲۰۲۰، قانون سوابق عمومی یا سایر قوانین لازم است از آن محافظت شود.

همه اطلاعات در مورد این موارد نیازی به علامت محافظتی ندارند .اطلاعات فقط باید به صورت محافظتی علامت گذاری شوند که سازش باعث آسیب می‌شود.

طبقه بندی بیش از حد اطلاعات می‌تواند اثرات مضر داشته باشد.

❖ زمان استفاده از علائم محافظ

هنگام ایجاد اطلاعات، مبتکر باید ارزیابی ریسک انجام دهد .اگر عواقب نامطلوب ممکن است رخ دهد، یا آژانس از نظر قانونی ملزم به محافظت از اطلاعات است، باید به آن علامت گذاری محافظ داده شود.

علائم محافظتی که توسط سازمانها یا اشخاص خارجی پیشنهاد شده است، نباید بطور خودکار توسط سازمانهای دولتی نیوزلند پذیرفته شود، مگر اینکه توافق قبلی وجود داشته باشد.

اطلاعاتی که مستقیماً از منابع دارای علامت محافظ به دست می‌آیند، باید حداقل دارای بالاترین طبقه بندی امنیتی از هر یک از طبقه بندی‌های منبع باشند.

❖ چه کسی باید علائم محافظ را اعمال کند؟

- شخص یا آژانس مسئول تهیه اطلاعات، علامت گذاری محافظ آن را تعیین می‌کند.
- به این شخص یا آژانس "مبتکر" گفته می‌شود.
- اگر اطلاعاتی در خارج از دولت نیوزیلند ایجاد شده باشد، شخصی که در سازمان دولتی فعالیت می‌کند اطلاعات را تعیین می‌کند یا خیر.

❖ **چه کسی می‌تواند علائم محافظ را تغییر دهد؟**

فقط آژانس نمایندگی محافظ اصلی (آژانس مبدأ) می‌تواند آن را تغییر دهد .همه آژانس‌ها باید به این قانون احترام بگذارند. اگر فکر می‌کنید مارک محافظتی مناسب نیست، آن را با شخصی که اطلاعات را علامت گذاری کرده است (مبدع) یا آژانس مبدأ قرار دهید.

❖ **چه زمانی از علائم محافظ استفاده نکنید**

طبق قانون اطلاعات رسمی ۱۹۸۲ ، اطلاعات رسمی نباید از نظر محافظتی علامت گذاری شود:

- تخلفات قانونی، ناکارآمدی یا خطای اداری را پنهان کنید
- از خجالت کشیدن برای یک فرد، سازمان، آژانس یا دولت جلوگیری کنید
- مهار رقابت
- جلوگیری از تأخیر یا تأخیر در انتشار اطلاعاتی که نیازی به محافظت از منافع عمومی ندارد.

❖ **مراقب باشید که اطلاعات رسمی را بیش از حد طبقه بندی نکنید**

اطلاعات رسمی فقط باید از نظر محافظتی علامت گذاری شود که نتیجه مصالحه هزینه افزایش حمایت را تأمین می‌کند .اطلاعات دولت نیوزلند با علامت محافظ باید در حداقل باشد. مهم است که اطلاعات رسمی که نیازی به محافظت ندارند، بدون طبقه بندی باقی بمانند

طبقه بندی بیش از حد اطلاعات می‌تواند آسیب جدی وارد کند .در اینجا چند نمونه از آسیب‌ها آورده شده است

- دسترسی عمومی به اطلاعات دولت بی مورد محدود می‌شود.
- ترتیبات اداری غیر ضروری تنظیم شده است که برای عمر سند باقی می‌ماند (از جمله ترتیبات مخزن اطلاعاتی که به بایگانی نیوزیلند منتقل می‌شود)، که هزینه غیرضروری را به آژانس تحمیل می‌کند
- حجم اطلاعات دارای علامت محافظ برای محافظت کافی از آژانس بسیار زیاد می‌شود.
- سیستم طبقه بندی امنیتی دولت نیوزیلند و اقدامات امنیتی مرتبط با آن بی اعتبار می‌شوند.

این اثرات مضر ممکن است منجر به کاهش ارزش یا عدم توجه به علائم محافظتی شود.

به همین دلایل، دولت نیوزیلند انتظار دارد آژانس‌ها فقط در صورت نیاز واضح و قابل توجیه، اطلاعات را به صورت محافظتی علامت گذاری کنند. برای به حداقل رساندن حجم اطلاعات با علامت محافظ، آژانس‌ها باید مدت زمان علامت گذاری محافظ را محدود کرده و مراحل بازبینی را تنظیم کنند.

❖ **چگونه می‌توان علامت‌های محافظ را تأیید کرد**

مارک‌های محافظ باعث گران شدن اطلاعات برای ایجاد، مدیریت، ذخیره و انتقال آن‌ها می‌شود .آژانس شما باید روشی برای تأیید علائم محافظتی داشته باشد، خصوصاً وقتی چنین علامتی برای آژانس شما طبیعی یا استاندارد نباشد.

❖ اگر نمایندگی از بین برود یا ادغام شود چه باید کرد

اگر آژانس از بین برود یا ادغام شود، آژانس با مسئولیت آژانس سابق، آژانس مبدأ محسوب می‌شود.

محل تماس باید رئیس ارشد امنیت (CSO) آژانس جدید باشد.

❖ چه اتفاقی می افتد که اطلاعات به Archives نیوزیلند می‌رود

هنگامی که سوابق علامت گذاری شده محافظتی به بایگانی نیوزیلند منتقل می‌شوند، آن‌ها علائم محافظتی خود را حفظ می‌کنند و مطابق با آن علائم ذخیره و نگهداری می‌شوند. با این حال، بایگانی‌های نیوزلند ظرفیت محدودی برای ذخیره اطلاعات دارای علامت محافظ دارند، بنابراین ابتدا با آنها مشورت کنید .اگر آن‌ها نمی‌توانند اطلاعات شما را در اختیار شما قرار دهند، به دنبال مرخصی برای انتقال سوابق دارای علامت محافظ مطابق با قانون سوابق عمومی ۲۰۰۵ باشید.

اگر آژانس شما در حال انتقال سوابق دارای محرمانه یا بالاتر است، در مورد طبقه بندی علامت محافظ به سطح مناسب‌تر، با نیوزیلند مشورت کنید. هنگامی که یک رکورد تحت قانون سوابق عمومی ۲۰۰۵ به عنوان یک رکورد دسترسی آزاد علامت گذاری شده باشد، هرگونه علامت گذاری محافظ برای هر منظور دیگر متوقف می‌شود.

❖ نحوه تنظیم مدت زمان علامت گذاری محافظ

هنگامی که برای اولین بار علامت گذاری محافظ را روی اطلاعات اعمال می‌کنید، سعی کنید تاریخ یا رویدادی را تعیین کنید که آنها را از طبقه بندی خارج کنید .تاریخ یا رویداد را براساس ارزیابی حساسیت اطلاعات قرار دهید.

به عنوان مثال، اسناد بودجه قبل از انتشار بودجه به حفاظت بالایی نیاز دارند، اما بعد از آن نه. برخی از اطلاعات ممکن است به محافظت بیشتر احتیاج داشته باشند زیرا تحت بیانیه‌ای تحت بیانیه سیاست‌های عمومی خاص قرار گرفته و پس از آن به اطلاعات عمومی تبدیل می‌شود. با رسیدن به تاریخ یا رویداد، اطلاعات باید به طور خودکار به سطح کنترل بیشتری مربوط شوند.

اسناد کابینه در چنین ترتیبات گنجانده نشده است .برای اطلاعات بیشتر به طبقه بندی امنیتی اسناد کابینه مراجعه کنید .

❖ چه زمانی علامت‌های محافظ خود را مرور کنید

آژانس شما باید علامت گذاری محافظ اطلاعات را مرتباً بررسی کند به عنوان مثال، پس از اتمام یک پروژه یا دنباله‌ای از رویدادها، یا هنگامی که پرونده‌ای از آن خارج یا برای استفاده بازگردانده می‌شود.

تمام گیرندگان اطلاعات باید با مبدع تماس بگیرند تا در مورد هرگونه مارک محافظتی که به نظر آنها نادرست است بحث کنند.

❖ نحوه مدیریت انتشار اطلاعات رسمی برای عموم

کارمندان دولت نیوزلند باید فارغ از هرگونه مارک محافظتی که ممکن است داشته یا نداشته باشند، مجوز آژانس را برای انتشار هرگونه اطلاعات برای مردم داشته باشند. مجوز ممکن است توسط رئیس آژانس یا شخصی که از طرف رئیس آژانس تفویض اختیار شده باشد، صادر شود. حتی اگر اطلاعاتی برای انتشار یا انتشار عمومی در نظر گرفته شده باشد، ممکن است یک معیار

کنترل مانند مارک تأیید قبل از انتشار داشته باشد .به عنوان مثال، اوراق بودجه. در این حالت، نقطه‌ای که اطلاعات در دسترس عموم قرار می‌گیرد باید مشخص شود .هنگامی که این اطلاعات دیگر به اقدامات کنترل اصلی متوقف نمی‌شوند، آژانس شما باید اقدامات حفاظتی متناسب با نوع اطلاعات مندرج در سند را در نظر بگیرد.

کلیه اطلاعات شخصی نگهداری شده، حتی اگر در دسترس عموم باشد، باید مطابق با قانون حفظ حریم خصوصی ، اصول حفظ حریم خصوصی اطلاعات باشد.

❖ **سیاستی برای رسیدگی به درخواست‌ها برای اطلاعات رسمی داشته باشید**

آژانس‌های نمایندگی شما باید خط مشی در نظر گرفته شده برای رسیدگی به هر درخواست اطلاعات رسمی، که ممکن است تحت قانون اطلاعات رسمی ۱۹۸۲ (OIA) منتشر شود. درک قوانین و اجرای سیاست‌های ویژه سازمانOIA ، احتمال نقض امنیت اطلاعات رسمی را از طریق افشای ناخواسته یا تصادفی کاهش می‌دهد.

❖ **چرا داشتن یک سیاست طبقه بندی امنیتی مهم است؟**

آژانس شما باید اطلاعات رسمی را که نیاز به محافظت بیشتر دارند، شناسایی کند و روشهای محافظتی را برای اطلاعات حساس و دارای محافظت فراهم کند. عدم انجام این کار خطری غیرقابل قبول برای امنیت محافظتی دولت نیوزلند ایجاد می‌کند و همچنین می‌تواند به اشتراک گذاری اطلاعات و توافق نامه‌های مشورتی بین آژانس‌ها را به خطر بیندازد .این ترتیبات برای عملکرد کارآمد دولت ضروری است.

۶-۵- الزامات رسیدگی به اطلاعات و تجهیزات دارای علامت محافظ

الزامات مدیریت بخشی از امنیت اطلاعات در دولت نیوزیلند است و به آژانس شما کمک می‌کند تا الزامات امنیتی محافظ را اجرا کند. مارک‌های محافظ فقط برای اسناد کاغذی نیستند - همچنین برای اطلاعات الکترونیکی، رسانه‌های دیجیتال، اطلاعاتی که به صورت شفاهی تحویل داده می‌شوند و تجهیزاتی که اطلاعات دارای علامت محافظ در آنها نگهداری یا ذخیره می‌شود، هستند. برای کمک به شناسایی اینکه کدام اطلاعات و تجهیزات به علائم محافظ نیاز دارند، به سیستم طبقه بندی امنیتی دولت نیوزیلند مراجعه کنید.

۵-۱-۱۱- استفاده از علائم محافظ بر روی اطلاعات رسمی

علائم محافظ به حفظ امنیت اطلاعات رسمی کمک می‌کند .آن‌ها یک یادآوری بصری از اقدامات امنیتی است که در مورد اطلاعات یا تجهیزات اعمال می‌شود.

❖ **چه کسی باید اطلاعات را علامت گذاری کند و چه زمانی**

شخصی که اطلاعات را ایجاد می‌کند "مبتکر" است.

مبتکر وظیفه تعیین علامت محافظ هنگام ایجاد اطلاعات را دارد.

❖ **بررسی کنید که علامت گذاری در کل چرخه عمر درست باشد**

اگر سطح حفاظت در حین تهیه پیش نویس تغییر کند، مبتکر باید علامت گذاری محافظ را تنظیم کند. هنگامی که پیش نویس نهایی است، مبتکر باید تأیید کند که علامت محافظ در سطح مناسب است تا اطلاعات را ایمن نگه دارد.

❖ **نشانه‌های محافظ را کجا قرار دهید**

علائم محافظ در بالا و پایین هر صفحه از یک سند قرار دارد .سند به معنای هر نوع اطلاعات ضبط شده، مانند گزارش‌ها، نامه‌ها، کتاب‌ها، ایمیل، صورتجلسه ها، تفاهم نامه‌ها، فیلم‌ها، نمودارها، نوارها، تصاویر و رسانه‌های دیجیتال است. هنگام ثبت اسناد چاپ شده، علائم محافظتی آنها باید به وضوح دیده شود .همین قانون در مورد رسانه‌های الکترونیکی و نوری قابل جابجایی مانندUSB ، CD-ROM، میکروفیلم‌ها، عکس‌ها و هارد دیسک‌های قابل جابجایی اعمال می‌شود.

اطلاعات مرتبط: مدیریت و علامت گذاری پرونده‌های فیزیکی

❖ علامت گذاری کتاب، جزوه و گزارش

اسناد دارای جلد، مانند کتاب‌ها، جزوه‌ها و گزارش‌ها، باید علامت محافظ را در این موارد نشان دهند:

- هر صفحه
- روکش جلو و عقب
- صفحه عنوان
- الزام آور (در صورت امکان).

هرگونه اتصال یا بستن صفحات نباید نشانه‌های محافظ را پنهان کند.

❖ پرداختن به اطلاعات شفاهی

اگر اطلاعاتی که دارای علامت محافظتی است به صورت شفاهی (مثلاً از طریق مباحث طبقه بندی شده) تحویل داده شود، باید به گیرنده (ها) گفته شود که قبل از انتقال اطلاعات، اطلاعات به محافظت نیاز دارند.

❖ علامت گذاری پاراگراف‌ها

بعضی اوقات ممکن است نیاز به علامت گذاری پاراگراف‌ها باشد زیرا نیازهای امنیتی متفاوت یا بالاتری دارند .به عنوان مثال، یک پاراگراف در یک سند ممکن است حاوی اطلاعات محرمانه باشد .به علامت گذاری پاراگراف "شاخص‌های درجه بندی پاراگراف" گفته می‌شود. آژانس شما باید تدوین خط مشی مربوط به علامت گذاری محافظ پاراگراف‌ها را در اسنادی که به طبقه بندی امنیتی نیاز دارند، در نظر بگیرد.

❖ استفاده از شاخص‌های درجه بندی پاراگراف

نشانگرهای درجه بندی پاراگراف را در ابتدای هر پاراگراف قرار دهید .آن‌ها را با استفاده از حروف اول طبقه بندی امنیتی به طور کامل بنویسید یا آنها را مختصر کنید .به عنوان مثال، (S) برای SECRET یا (IC) برای .CONFIDENCE جدول ۱ اختصارات استانداردی را که می‌توانید استفاده کنید نشان می‌دهد.

❖ شاخص‌های درجه بندی پاراگراف باید همان رنگ متن موجود در سند باشد.

اگر از شاخص‌های درجه بندی پاراگراف استفاده می‌کنید، باید تمام پاراگراف‌های موجود در سند را نیز علامت گذاری کنید، به طوری که هیچ کس در مورد اینکه کدام علامت‌ها به چه متن اعمال می‌شوند گیج شود. برای بندهایی که علامت محافظ ندارند، از UNCLASSIFIED استفاده کنید .مثال ۱ نحوه انجام این کار را به شما نشان می‌دهد.

جدول ۱: طبقه بندی‌های اختصاری امنیتی

طبقه بندی نشده	(U)
با اطمینان	(مدار مجتمع)
حساس	(سن)
محصور	(R)
محرمانه	(C)
راز	(S)
فوق سری	(TS)

مثال ۱: استفاده از شاخص‌های درجه بندی پاراگراف

در این مثال "سری" در طبقه‌بندی امنیت این بند یا استفاده از کلمه S در آغاز بند نمایش داده شده است.

سری

اول آوریل ۲۰۱۴
آقای جان اسمیت
افسر ارشد عملیات اجرائی
اداره اسناد طبقه‌بندی شده
ولینگتن ۶۰۱۱

(U) موضوع: مثال

۱. (u) بند۱ در برگیرنده اطلاعات "غیر طبقه‌بندی شده" است و می‌توان آن را با علامت u در داخل پرانتز در آغاز بند نشان داد

– اگر تمام بندهای فرعی این متن دارای طبق‌بندی یکسان و مشابه‌هم باشند که در ابتدای بند درج گردیده، سپس نیاز نیست تماما بندهای فرعی را علامت‌گذاری نمایید.

(s) در حال، در صورتی که بخشیده هایی از متن دارای طبق‌بندی مشابه آدرس در ابتدای بند نیستند، لذا تمام بندهای اصلی و فرعی را باید به‌طور مجزا و جداگانه علامتگذاری کرد.

سری

❖ استفاده از یک علامت محافظ کلی

پس از استفاده از شاخص‌های درجه بندی پاراگراف، باید علامت گذاری محافظ کلی سند را تعیین کنید .علامت گذاری کلی باید حداقل برابر با بالاترین سطح طبقه بندی از هر پاراگراف در سند باشد.

❖ علامت گذاری برای طبقه بندی‌های امنیتی

طبقه بندی امنیتی باید به صورت ضخیم و در پایتخت مشخص شده‌اند .آن‌ها باید در همان اندازه به عنوان متن یا حداقل بالا ورق mm ۳ (هر کدام که بزرگتر) باشد.

❖ رنگ برنامه نویسی طبقه بندی امنیتی

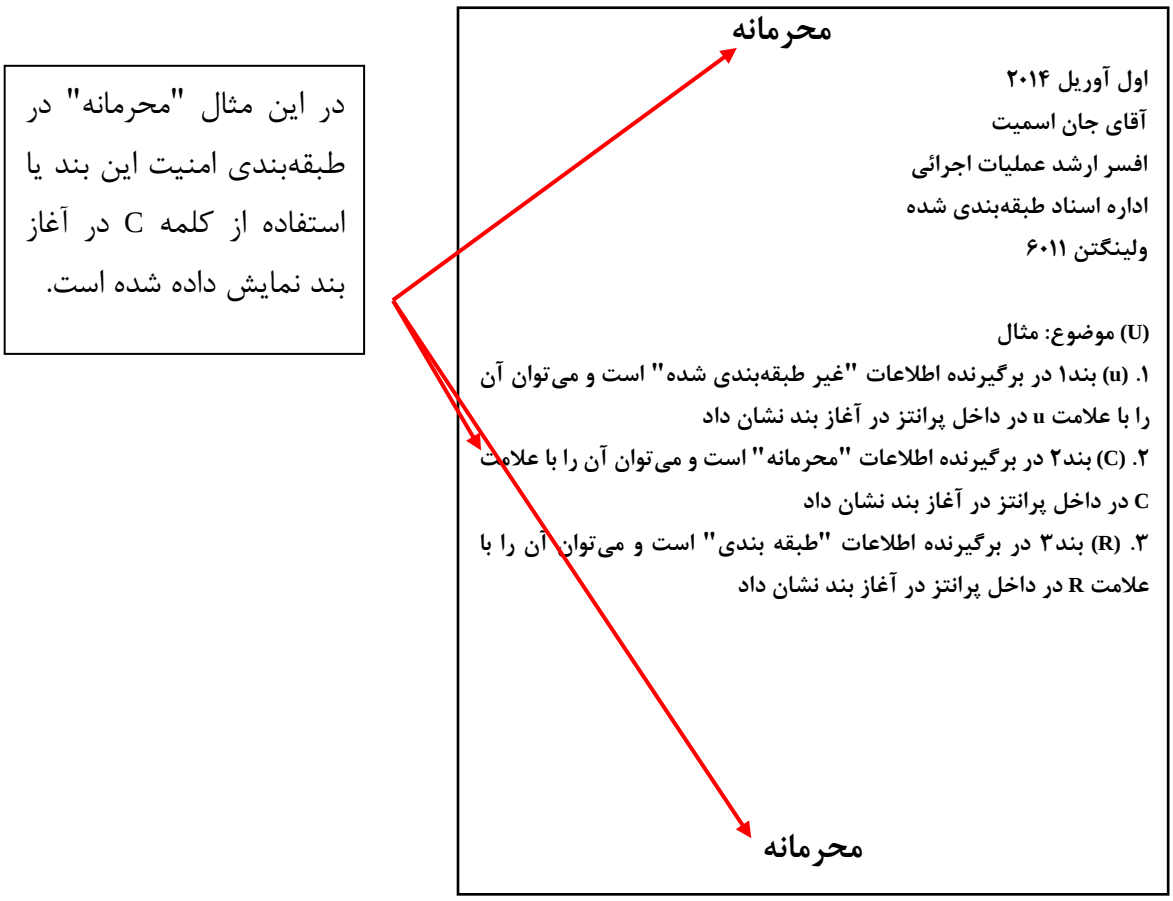
رنگ طبقه بندی برنامه نویسی باعث می‌شود امنیت آسان‌تر برای شناسایی و طبقه بندی تضمین می‌کند بالاتر ایستادگی کردن.

طبقه بندی امنیتی رنگ کد شرح زیر است:

- TOP SECRET - قرمز
- راز - آبی
- محرمانه – سبز
- محدود ، حساس و در اعتماد به نفس - سیاه و سفید

بالاترین طبقه بندی امنیتی باید به وضوح در بالای مرکز و پایین هر صفحه در یک خط مشخص شده به عنوان مثال نشان داده شده است ۲. در صورت لزوم، طبقه بندی امنیتی را می‌توان در مرکز انباشته صفحه متناسب با اطراف یک سربرگ.

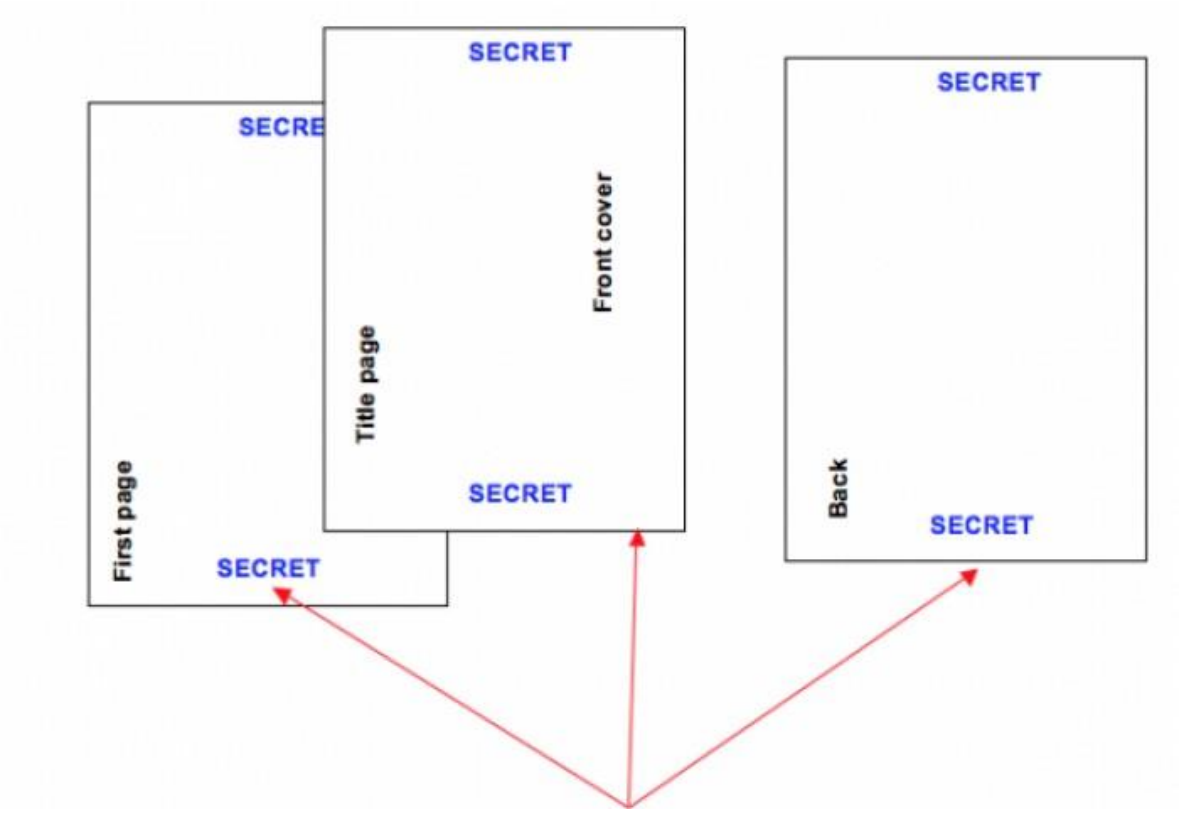
مثال ۲: استفاده از یک طبقه بندی امنیتی مارک



اسناد با درپوش، و یا در پوشه، باید طبقه بندی امنیتی در نشان می‌دهد:

- روکش جلو و عقب
- صفحه عنوان
- همه صفحات دیگر در سند.
- هر اتصالات یا بست باید محافظ مارک پنهان نمی‌کند.

مثال ۳: استفاده از نشانه گذاری‌های محافظ به اسناد با بیش از یک صفحه



در این مثال، سند در برگیرنده بیش از یک صفحه است بنابراین، تمام علامت‌گذاری، در بالای تمام صفحات و در پایین آلف روی پوشش بیرونی درج می‌گردد و روی تمام صفحات داخل سند و روی بیرون پوشش پشت سند درج می‌گردد.

استفاده از نشانه گذاری‌های تأیید

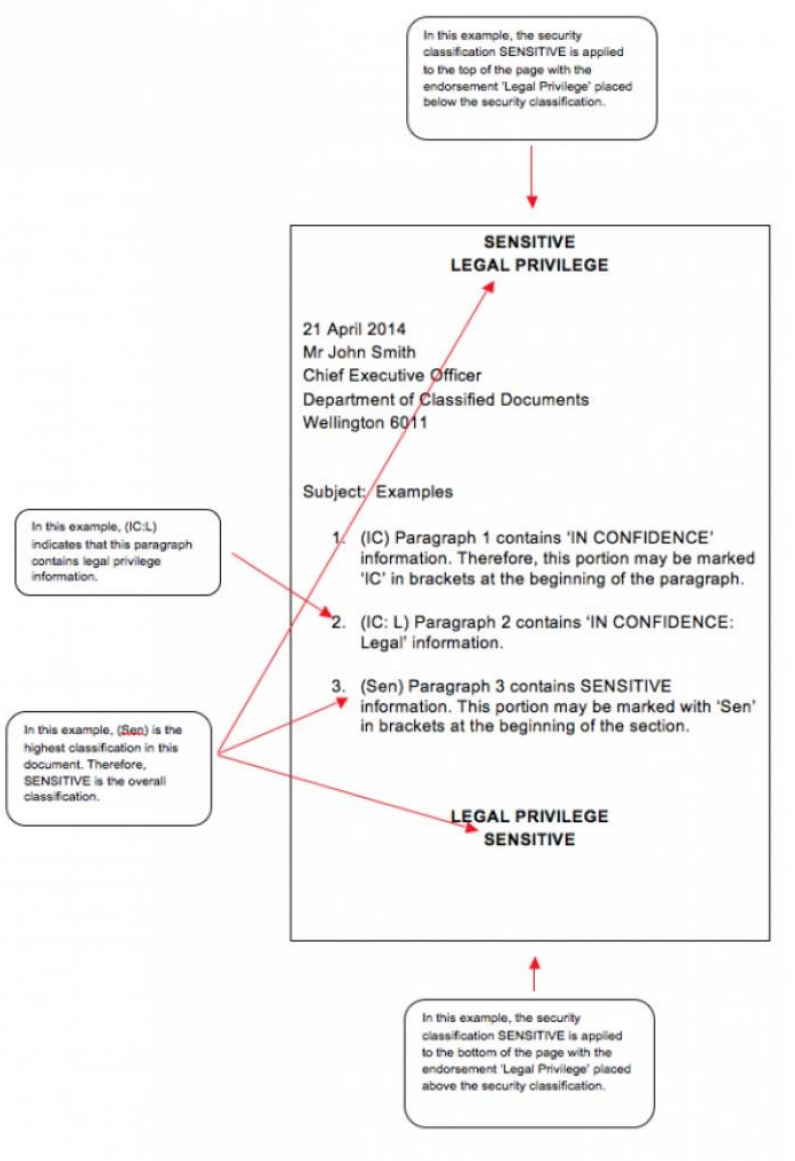
شما باید نشانه گذاری حمایت بدون طبقه بندی امنیتی استفاده نمی‌کند.

وقتی سندی به علامت گذاری تأیید نیاز دارد:

- طبقه بندی امنیتی را در بالا و پایین صفحه قرار دهید
- علامت تأیید را در زیر طبقه بندی امنیتی بالا و بالاتر از طبقه بندی امنیتی پایین قرار دهید.

همانطور که در مثال ۴ نشان داده شده است، یک علامت تأیید باید همیشه در اندازه، قالب و رنگ طبقه بندی امنیتی باشد.

مثال ۴: اعمال علامت گذاری تائید



❖ استفاده از مارک‌های محفظه‌ای

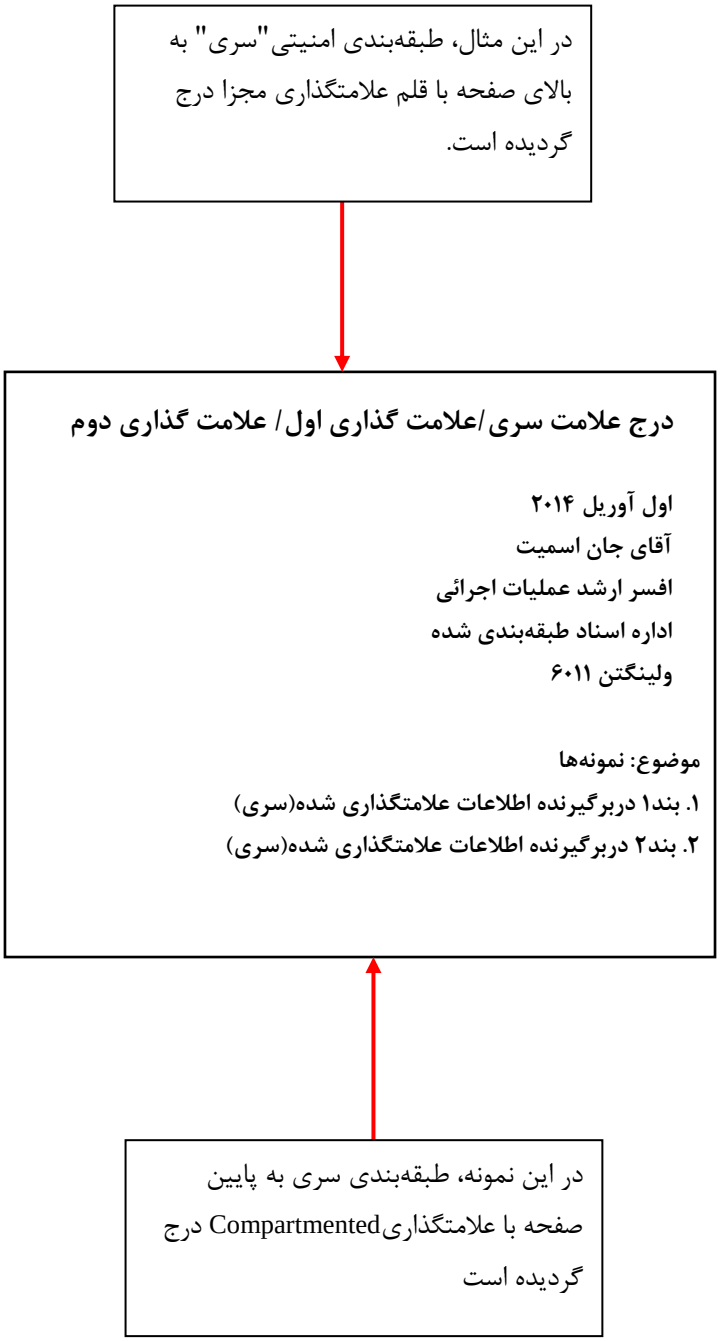
علائم منشعب شده باید از یک طبقه بندی امنیتی پیروی کنند .آن‌ها را در اطلاعاتی که طبقه بندی امنیتی ندارند اعمال نکنید.

علائم محفظه‌ای باید در همان اندازه، قالب و رنگ طبقه بندی امنیتی باشند.

علامت‌های جداگانه را در هر صفحه قرار دهید، و مستقیماً بعد از علامت گذاری برای طبقه بندی امنیتی .برای جدا کردن علامت گذاری‌ها از دو بریدگی استفاده کنید.

هنگامی که چندین نشانگر محفظه دارید، برای جدا کردن آنها از یک اسلش استفاده کنید .

مثال ۵: استفاده از مارک‌های محفظه‌ای

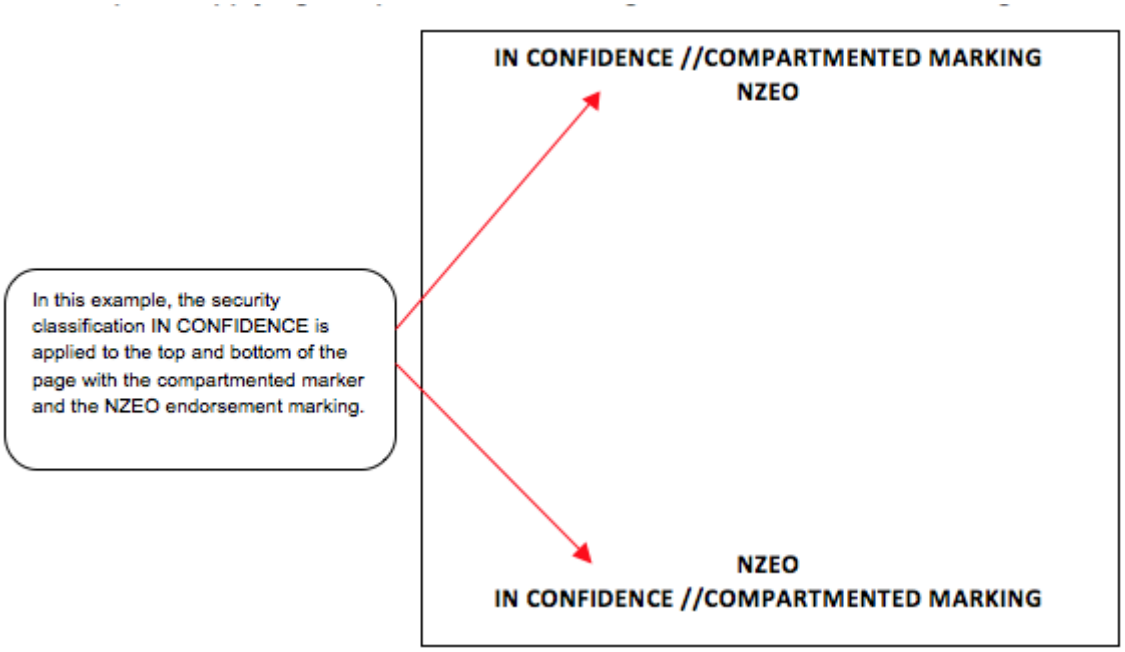


❖ **علامت‌های محفظه‌ای به همراه علامت تأیید**

اگر سند شما نیز به علامت گذاری تأیید نیاز دارد، آن را مستقیماً بعد از علامت گذاری جداگانه روی هر صفحه قرار دهید.

همانطور که در مثال ۶ نشان داده شده است، برای جدا کردن علامت‌ها از یک برش دوتایی استفاده کنید.

مثال ۶: استفاده از مارک‌های محفظه‌ای با نشان‌های تأیید



❖ **علامت گذاری عنوان‌ها**

هر زمان ممکن است، علائم محافظتی را روی عناوینی مانند پرونده‌ها، اسناد، کتاب‌ها و گزارش‌ها قرار ندهید .می‌توان آنها را در سیستم‌های مدیریتی مشاهده کرد که از نظر محافظتی مشخص نشده‌اند و این می‌تواند اطلاعات را در معرض خطر قرار دهد.

اگر علامت گذاری عنوان ضروری است، مبتکر باید از یک مرجع جداگانه طبقه بندی نشده استفاده کند .این علامت می‌تواند در پشت عنوان در براکت ها ظاهر شود.

❖ **علامت گذاری گرافیک چاپی**

برای گرافیک‌هایی مانند نقشه‌ها و نقشه‌ها:

- علامت‌های محافظ نزدیک مقیاس نقشه یا اعداد رسم را چاپ یا مهر کنید
- علامت‌های محافظ را در مرکز بالا و پایین گرافیک چاپ کنید.

اگر گرافیک تا شده است، مطمئن شوید که مارک پس از تا شدن قابل مشاهده است.

❖ **علامت گذاری پیوست‌ها، پیوست‌ها، پیوست‌ها و پوشش اسناد**

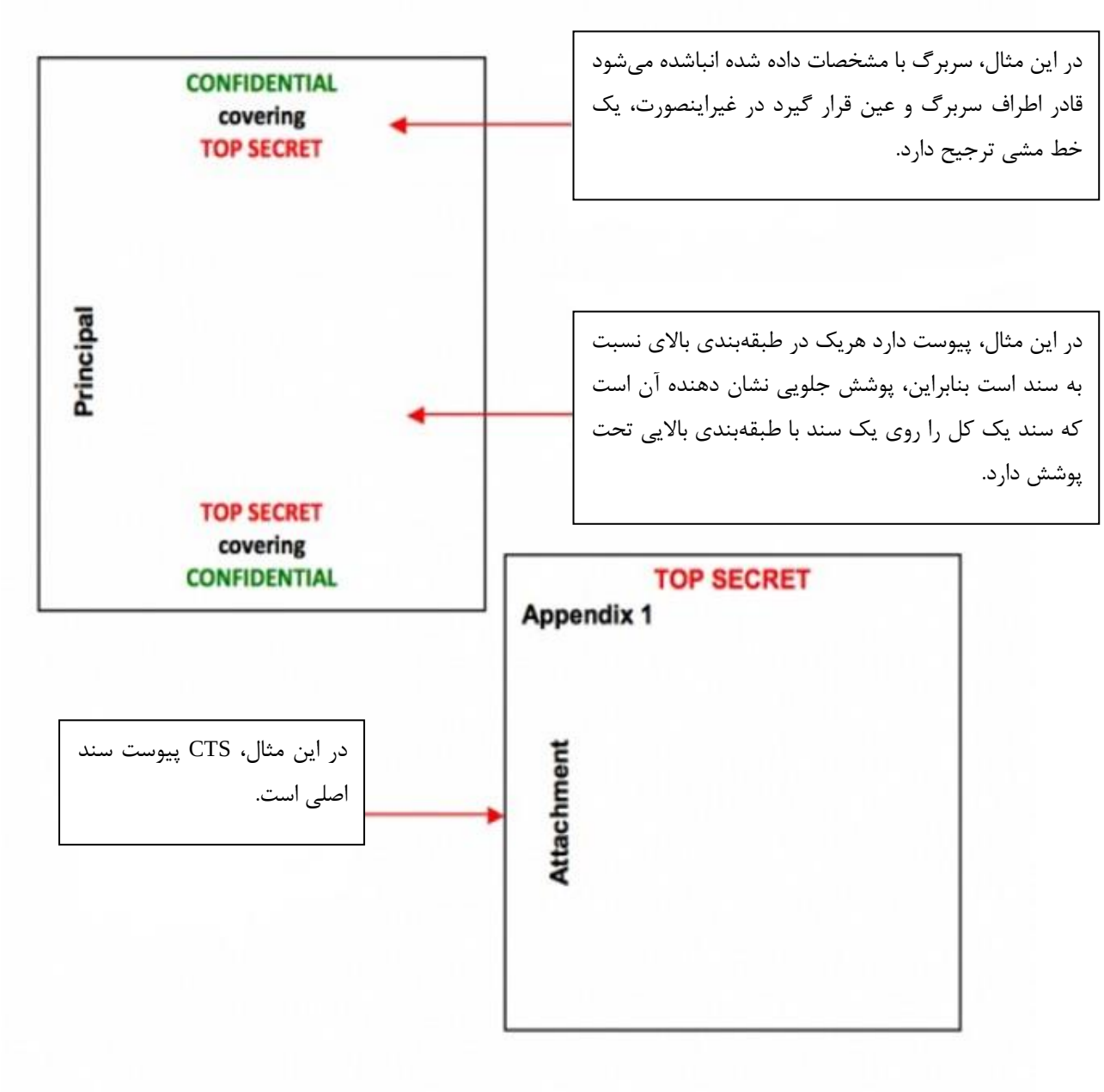
در بعضی موارد، ضمائم یا پیوست‌های یک سند حتی اگر بقیه سند طبقه بندی نشده باشد، به علامت‌های محافظ نیاز دارند.

گاهی اوقات، یک ضمیمه یا پیوست ممکن است به یک مارک محافظ متفاوت از سند اصلی که به آن پیوست نیاز داشته باشد.

اگر ضمیمه، پیوست یا پیوست دارای علامت محافظتی بالاتر از سند اصلی باشد، جلد سند باید نشان دهد که سند به طور کلی از طبقه بندی امنیتی بالاتری برخوردار است .مثال ۷ نحوه علامت گذاری صحیح را در این سناریو به شما نشان می‌دهد.

اگر ضمیمه، پیوست یا پیوست در همان سطح علامت محافظ سند اصلی یا پایین باشد، نیازی نیست که آن را روی جلد نشان دهید.

مثال ۷: استفاده از علائم محافظ به ضمائم و ضمائم



❖ **علامت گذاری تصاویر**

عکس‌ها و فیلم‌ها، و پاکت‌های ذخیره سازی یا ظروف آنها باید در صورت لزوم دارای نشانه‌های محافظتی واضح باشند.

علائم محافظ باید:

- در دو طرف ظروف و قرقره‌ها

- حداقل برای پنج ثانیه در عنوان و سکانس‌های انتهایی تصاویر رول، فیلم سینمایی و نوار ویدیویی پیش بینی شده است.

شما باید نگاتیوهای عکاسی را نیز علامت گذاری کنید، به این ترتیب علامت محافظ در تمام نسخه‌های تهیه شده از آن نگاتیو تولید می‌شود .

❖ علامت گذاری ارائه‌ها

ارائه‌ها و ارائه‌های رسمی با ارائه‌های طبقه بندی امنیتی نیاز به علائم محافظتی مناسب دارند.

هر اسلاید یا صفحه را مانند یک سند کاغذی مانند یک صفحه جداگانه در نظر بگیرید .علامت گذاری محافظ باید به صورت شفاهی برای مخاطب بیان شود .

❖ علامت گذاری صدا

برای ضبط‌های صوتی، سطح علامت گذاری محافظ باید به وضوح در ابتدا و انتهای هر ضبط مشخص شود .نوار یا رسانه‌های دیگر و محفظه آن باید به طور واضحی با علامت محافظ مناسب برچسب گذاری شوند.

❖ علامت گذاری ایمیل‌ها

ایمیل‌ها باید با یک علامت محافظ مناسب و مطابق با سیستم طبقه بندی علامت گذاری شوند .علامت گذاری ایمیل‌ها تضمین می‌کند که:

- اقدامات امنیتی مناسب برای اطلاعات اعمال می‌شود
- به جلوگیری از انتشار تصادفی اطلاعات در دامنه عمومی کمک می‌کند.

برای اعمال سیاست و کنترل در ایمیل‌ها، به بخش راهنمای امنیت اطلاعات نیوزلند Email Security - (NZSIM) بروید.

❖ علامت گذاری میکروفرم ها

برخی از آژانس‌ها هنوز می‌توانند از میکروفرم ها مانند کارت‌های دیافراگم، میکرو فیش و میکروفیلم استفاده کنند که حاوی اطلاعات مشخص شده با محافظ است .در این صورت، این ماده باید علامت گذاری محافظ مناسب را در مرکز بالا و پایین هر قاب نشان دهد. ظروف و پاکت‌ها باید دارای علامت محافظ مناسب از بالاترین ریز فرم محافظتی باشند.

علامت گذاری محافظ باید بدون فرافکنی روی کارتها و میکروفن قابل مشاهده باشد .میکرو فیلم باید در ابتدا و انتهای هر رول به طور برجسته مشخص شود.

❖ علامت گذاری رسانه ذخیره سازی الکترونیکی

برای خط مشی مارک گذاری رسانه ذخیره سازی الکترونیکی، به بخشهای زیر NZSIM بروید:

- 12.3طبقه بندی و برچسب زدن محصولات
- 13.2مدیریت رسانه.

❖ **تجهیزات علامت گذاری**

- آژانس شما باید رویه‌های خاصی را برای مارک گذاری تجهیزات ایجاد کند.
- علائم محافظ باید کاملاً واضح باشد و به راحتی پاک نشود.
- برای جزئیات بیشتر، به NZSIM - 12.3طبقه بندی و برچسب زدن محصولات بروید.

۵-۱-۱۲- کنترل و مدیریت اطلاعات رسمی با مارک‌های محافظ

اطلاعات رسمی با علائم محافظتی باید کنترل شده و به درستی کنترل شوند تا ایمن نباشند.

برای اطمینان از انطباق آژانس خود با امنیت محافظتی (PSR) برای امنیت اطلاعات، این شرایط را دنبال کنید.

این شرایط برای موارد زیر اعمال می‌شود:

- کلیه اطلاعات رسمی (با یا بدون طبقه بندی امنیتی)
- مدیریت اطلاعات یا ذخیره اطلاعات خود را به اشخاص ثالث مانند ارائه دهندگان خدمات ابری برون سپاری کنید یا از آنها خارج کنید.

❖ **مطابقت با الزامات اطلاعات طبقه بندی شده**

سطح حفاظت از اطلاعات و تجهیزات دارای محافظت مشخص مطابق با طبقه بندی‌های امنیتی آنها افزایش می‌یابد .هرچه طبقه بندی امنیتی بالاتر باشد، نیاز به حفاظت بیشتر خواهد بود.

شرایط زیر به شما کمک می‌کند تا از اطلاعات رسمی مطابق با طبقه بندی امنیتی مربوطه محافظت کنید.

- کنترل و رسیدگی به اسناد و مطالب حساس یا محدود شده
- کنترل و رسیدگی به اسناد و مطالب محرمانه
- اسناد و مطالب اسرارآمیز را کنترل و کنترل کنید
- کنترل و رسیدگی به اسناد و مطالبTOP SECRET

❖ **ایجاد سیستم ثبت نام**

آژانس شما باید سیستمی برای کنترل و مدیریت اطلاعات رسمی و دارای علامت محافظ داشته باشد.

برای هر سند یا پرونده، سیستم ثبت نام شما نیاز به جزئیات دارد:

- وقتی ایجاد شد
- جایی که ذخیره می‌شود
- چه زمانی نابود خواهد شد

برای ثبت رسانه، شرایط موجود در کتابچه راهنمای امنیت اطلاعات نیوزلند 13.2.14 - (NZSIM) ثبت رسانه را دنبال کنید.

❖ **حفظ ثبت اسناد طبقه بندی شده**

شما باید یک ثبت اسناد طبقه بندی شده (CDR) را برای همه TOP SECRET و ACATANIAL MATERIAL تولیدی یا دریافت شده در آژانس خود حفظ کنید. CDR باید شامل جزئیات اسناد دریافتی و کلیه نسخه‌های حفظ شده باشد.

ثبت نام برای اطلاعات SECRET روش خوبی است. در صورت لزوم برای کاهش خطر، می‌توانید از CDR برای اسنادی با طبقه بندی کمتر استفاده کنید. با مراقبت‌های لازم، CDR شما به ندرت نیاز به علامت گذاری محافظتی دارد .در صورت لزوم، CDR خود را بر اساس امتیازات خود علامت گذاری کنید - نه بر اساس علائم محافظ اسنادی که ثبت می‌کند مگر اینکه عنوان سندی در CDR شما از نظر محافظتی مشخص شده باشد، که باید نادر باشد. اگر حجم مکاتبات آن را توجیه می‌کند، از ثبت‌های جداگانه برای هر طبقه بندی امنیتی و مکاتبات داخل و خارج استفاده کنید.

❖ **ممیزیHardcopies**

آژانس شما باید سیستمی برای ممیزی اطلاعات نسخه چاپی ایجاد کند که دارای علائم محافظتی باشد .الزامات حسابرسی سیستم‌ها و تجهیزات ICT در NZISM تعریف شده است.

❖ **استفاده از فرآیند رسید برای افزایش امنیت**

فرآیند دریافت را برای زمان تحویل اطلاعات یا تجهیزات دارای مارک محافظتی به آژانس خود در نظر بگیرید .مزایا شامل توانایی:

- تأیید ارائه اطلاعات را ارائه دهید
- ردیابی حرکت اطلاعات محافظت شده
- اطمینان حاصل کنید که گیرنده مسئولیت محافظت از اطلاعات را بر عهده می‌گیرد.

هر نوع سازوکار دریافت مناسب است، به شرطی که سند را از طریق شماره مرجع یا عنوان مشخص کند.

یک شماره مرجع اغلب آسانتر از عنوان است، زیرا عنوان یک سند ممکن است محتوای یک سند با علامت محافظ را توصیف کند یا در موارد محدود حاوی کلمه‌ای مانند "محرمانه" یا "محرمانه" باشد .یک دوره را روی رسید مشخص کنید (به عنوان مثال، ۷ روز) که در آن گیرنده باید رسید را امضا کرده و برگرداند .تأیید کنید که همه بازپرداخت رسیدهای مورد انتظار را ظرف یک ماه از تاریخ سررسید دریافت کرده‌اید.

❖ **اطلاعات بررسی نقطه‌ای با علامت "بسیار محرمانه" و "مواد قابل پاسخگویی"**

در فواصل نامنظم، نمونه‌ای کوچک از TOP SECRET و MATERIAL ACCOUNTABLE را بررسی کنید تا اطمینان حاصل شود که از آن حساب شده و به درستی نگهداری و ذخیره شده است .مدیر مسئول اطلاعات باید مسئولیت انجام یا تنظیم چک‌های نقطه‌ای را به عهده بگیرد .آژانس شما همچنین باید ۵ درصد از مواد TOP SECRET و ACCOUNTABLE در هر ماه بررسی نقطه‌ای کند. تمام (۱۰۰ درصد) پرونده‌های TOP SECRET و MATERIAL ACCOUNTABLE شما باید در هر دو سال بررسی شوند.

❖ **ضبط چک‌های نقطه‌ای**

سابقه چک‌های نقطه‌ای خود را حفظ کنید .روش خوبی است که در فواصل نامنظم از سایر پرونده‌های دارای علامت محافظ، یک بررسی نقطه‌ای مشابه انجام دهید.

❖ گزارش اختلافات

مدیر باید هرگونه مغایرت را به مدیر ارشد امنیت(CSO) ، رئیس ارشد امنیت اطلاعات (CISO) یا سایر مراجع مناسب برای تحقیق گزارش دهد .مثال‌هایی از مقامات دیگر که ممکن است مناسب باشند، کمیساریای حریم خصوصی، دادگستری، مرکز ملی امنیت سایبری (NCSC) یا Cert NZ هستند.برای اطلاعات بیشتر در مورد مدیریت رویدادهای امنیت اطلاعات ، به پروتکل مدیریت برای امنیت اطلاعات بروید.

❖ مدیریت و علامت گذاری پرونده‌های فیزیکی

حداقل یک پرونده باید دارای علامت محافظ برابر با بالاترین طبقه بندی امنیتی اطلاعات درون آن باشد .اطمینان حاصل کنید که ارزش و حساسیت اطلاعات درون یک پرونده را به طور کلی در نظر گرفته‌اید .اگر هنگام جمع شدن اطلاعات (تلفیق)، خطرات امنیتی افزایش یابد، ممکن است پرونده به طبقه بندی و علامت گذاری امنیتی بالاتری نیاز داشته باشد.

❖ افزودن اطلاعات به پرونده

وقتی اطلاعات جدیدی به پرونده اضافه می‌شود، کاربر پرونده باید اطمینان حاصل کند که علامت گذاری محافظ هنوز مناسب است .اگر اطلاعاتی اضافه شود که دارای طبقه بندی امنیتی بالاتری نسبت به خود پرونده باشد، کاربر پرونده باید قبل از پیوست سند جدید، پرونده را دوباره طبقه بندی کند.

❖ ثبت اسناد TOP SECRET وSECRET

اسناد TOP SECRET و SECRET را در یک پرونده مناسب قرار دهید یا بلافاصله آن را پوشش دهید .

سپس محل حداقل سند TOP SECRET باید در CDR ثبت شود.

❖ ثبت اطلاعات کمتر ازSECRET

اگر می‌خواهید اطلاعات مشخص شده در سطوح کمتر از SECRET را بایگانی کنید، آن‌ها را در اسرع وقت پس از ایجاد یا دریافت، در یک پرونده مناسب قرار دهید.

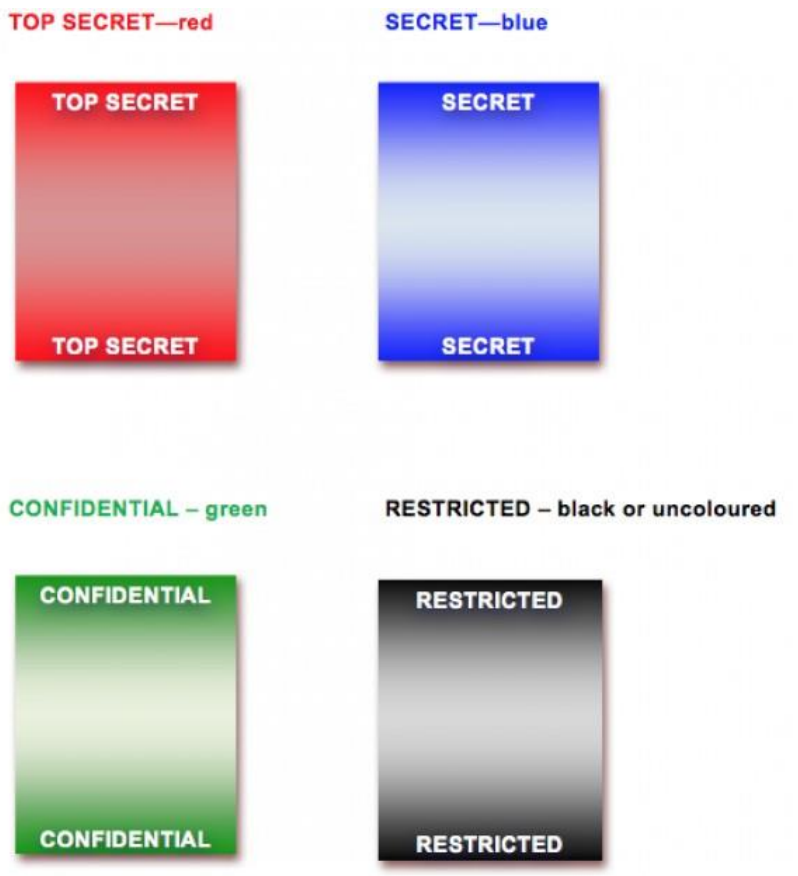
❖ با استفاده از منابع پرونده و شماره گذاری

آژانس شما باید از یک پرونده مرجع و شماره برگ برای پرونده‌های دارای علامت محافظ استفاده کند، بنابراین شما می‌توانید اطلاعاتی را که در پرونده وجود دارد ثبت کنید .همچنین رعایت مراحل معمول بایگانی، مانند ثبت تاریخ و نام شخصی که پرونده را در اختیار دارد، روش خوبی تلقی می‌شود.

❖ با استفاده از رنگ‌های استاندارد برای مشاهده علامت گذاری فایل آسان است

علائم محافظ روی پرونده‌ها باید واضح و روشن باشد و از سایر علائم قابل تشخیص باشد .در صورت امکان، از رنگهای استاندارد برای جلد پرونده در پرونده‌های دارای علامت محافظ استفاده کنید) .بعضی از نمایندگی‌ها ممکن است شرایط دیگری داشته باشند که مانع استفاده از رنگ‌های استاندارد می‌شود(.

شکل ۱: رنگ‌های استاندارد برای جلد پرونده



❖ **مدیریت ترتیبات برون سپاری و برون سپاری ICT**

اگر در نظر دارید کارکردها، خدمات یا توانایی‌های خود را به اشخاص ثالث در داخل یا خارج از نیوزیلند اختصاص دهید، مطمئن شوید که ارزش، طبقه بندی و خطرات اطلاعاتی را که تأمین کنندگان و پیمانکاران فرعی آنها به آنها دسترسی خواهند داشت، درک کرده‌اید .

آژانس شما باید از دستورالعمل‌ها و سیاست‌های برون سپاری و برون سپاری تعریف شده در زیر پیروی کند.

❖ **انجام تنظیمات :ICT کاری که می‌توانید انجام دهید و نمی‌توانید انجام دهید**

نمایندگی شما می‌تواند به موارد زیر وارد شود:

- ترتیبات برون سپاری و برون سپاری برای ذخیره یا پردازش اطلاعات مشخص شده در، یا در زیر، با محدود شده است
- ترتیبات برون سپاری در نیوزیلند برای ذخیره یا پردازش اطلاعات مشخص شده در محرمانه، راز یا TOP SECRET فقط با تأیید قبلی اداره امنیت ارتباطات دولت.(GCSB)

آژانس شما نباید برای ذخیره یا پردازش اطلاعات مشخص شده به عنوان "محرمانه"، "راز" یا "راز برتر" ترتیبات برون مرزی را انجام دهد.

❖ **در نظر گرفتن یا برنامه ریزی خدمات ابری**

اگر آژانس شما در حال استفاده از خدمات ابری است، باید برای مشاوره با رئیس دیجیتال دولت (GCDO) تماس بگیرید .ابتدا محتوای آنلاین آنها را بررسی کنید :استفاده از Cloud Services

اگر آژانس شما قصد استفاده از سرویس ابری را دارد، باید:

- ارزیابی رسمی خطر را انجام دهید
- راهنمایی در رایانش ابری را دنبال کنید: ملاحظات امنیت اطلاعات و حریم خصوصی.

در مرحله بعدی، شما باید از ارزیابی ریسک و راهنمایی برای شناسایی کنترلهایی که برای مدیریت خطرات مرتبط با استفاده از سرویس (اطلاعات و خطرات رازداری) نیاز دارید، استفاده کنید.

❖ **خدمات برون سپاری برای ذخیره و پردازش اطلاعات رسمی**

قبل از اینکه آژانس خدمات شما را برای ذخیره و پردازش اطلاعات رسمی به یک ارائه دهنده دریایی یا برون مرزی واگذار کند، مراحل مختلفی باید انجام دهید.

این مراحل درمورد ترتیبات انجام خدمات برون سپاری به موارد زیر اعمال می‌شود:

- ارائه دهنده خدمات دریایی که اطلاعات مشخص شده در یا محدود شده در RESTRICTED را ذخیره یا پردازش می‌کند (به استثنای اطلاعات عمومی بدون علائم محافظ)
- ارائه دهنده خشکی که اطلاعات مشخص شده در بالا RESTRICTED را ذخیره یا پردازش می‌کند.

آژانس شما باید:

- ارزیابی ریسک رسمی را برای شناسایی کنترلهای لازم برای مدیریت مناسب امنیت اطلاعات و خطرات حریم خصوصی مرتبط با استفاده از سرویس انجام دهید
- رسماً خطر باقی مانده مربوط به استفاده از سرویسی را که اطلاعات دارای علامت محافظ را پردازش می‌کند، بپذیرید
- تصمیم خود را به GCDO اطلاع دهید و به او شواهدی بدهید که ارزیابی رسمی خطر را انجام داده‌اید و از راهنمایی‌های وی پیروی کرده‌اید
- سیستم‌های مورد استفاده پیمانکار را حداقل به همان حداقل استاندارد سیستم‌های خود اعتبار دهید
- اطمینان حاصل کنید که ارائه دهنده خدمات ابری کنترل‌های مشخص شده در کتابچه راهنمای امنیت اطلاعات نیوزلند را برای هر سیستم میزبانی، پردازش یا ذخیره داده‌ها و سیستم‌های آژانس شما اعمال می‌کند
- از خدمات ابری عمومی یا ترکیبی برای میزبانی، پردازش یا ذخیره مواد با مارک تأیید فقط نیوزلند (NZEO) استفاده نکنید.

❖ **اطلاعات طبقه بندی نشده که در دسترس عموم است**

آژانس شما می‌تواند برای ذخیره یا پردازش اطلاعاتی که به صورت عمومی در دسترس است و هیچ گونه علامت محافظتی ندارد، ترتیبات برون سپاری و برون سپاری را انجام دهد .با این حال، شما باید رسماً خطرات امنیتی مرتبط را ارزیابی کرده و کنترل‌های لازم برای مدیریت آنها را شناسایی کنید.

همچنین باید اطمینان حاصل کنید که ارائه دهندگان اطلاعات، مطابق با پروتکل مدیریت امنیت اطلاعات را اداره، ذخیره، انتقال، حمل و دفع می کنند.

❖ **تأیید کنترل‌های امنیتی: صدور گواهینامه یا اعتبارسنجی خدمات**

قبل از اینکه آژانس خدمات شما را برای استفاده تأیید یا تأیید کند، باید تأیید کنید که کنترلهای امنیتی لازم برای مدیریت خطرات مربوط به امنیت و حریم خصوصی اجرا شده و مثر هستند. برای اطلاعات بیشتر به بخش "اعتبار سنجی" چرخه عمر امنیت اطلاعات مراجعه کنید.

❖ **ذخیره اطلاعات رسمی و دارای علامت محافظ با خیال راحت**

اطلاعات رسمی و دارای علامت محافظ را مطابق با مناطق امنیتی ذخیره کنید.

۵-۱-۱۳- بازتولید اطلاعات دارای علامت محافظ

هنگام تولید مجدد، از اطلاعات صحیح برای محافظت از اطلاعات رسمی با مارک‌های محافظ استفاده کنید.

این شرایط برای کلیه اطلاعات رسمی (با یا بدون طبقه بندی امنیتی) اعمال می‌شود

برای اطمینان از انطباق آژانس با الزامات امنیتی محافظتی برای امنیت اطلاعات، این شرایط را دنبال کنید.

❖ **تولید مثل اسناد**

برای کمک به کنترل اطلاعات دارای علامت محافظ، تعداد نسخه‌ها را به حداقل برسانید .فقط در صورت لزوم اطلاعات دارای علامت محافظ را تولید کنید.

اگر نسخه‌های اضافی یا خراب دارید که طبق قانون Public Records Act 2005 نگهداری آنها لازم نیست ، باید فوراً آنها را از بین ببرید .برای کسب اطلاعات بیشتر به تخریب رسانه‌ها و اسناد ICT بروید.

❖ **گرفتن مجوز برای کپی کردن**

برای تهیه کپی از اطلاعات دارای علامت محافظ با شماره کپی، باید از مبدأ یا آژانس مبدأ (شخص یا آژانس ایجاد کننده اطلاعات) اجازه بگیرید .با این حال، بهتر است از مبتکر بخواهید نسخه‌های اضافی مورد نیاز شما یا نمایندگی خود را تهیه کند .

اگر مبتکر اجازه ساخت کپی را داد، به آنها بگویید که چند نسخه را برای توزیع مجاز دارید .سپس مبتکر به شما خواهد گفت که کدام شماره کپی را باید در نسخه‌های خود علامت گذاری کنید.

آژانس شما ممکن است بخواهد فرآیند مشابهی را برای سایر اطلاعات رسمی و دارای علامت محافظ دنبال کند.

توجه :اگر آژانس شما از یک رجیستری طبقه بندی شده استفاده کند، روند دریافت مجوز برای کپی کردن اجباری است.

❖ **مدیریت "مطالب قابل پاسخگویی"**

پس از انتشار، مواد ACCOUNTABLE نباید به هر شکلی کپی یا تکثیر شود.

اگر نمایندگی شما به نسخه‌های بیشتری نیاز دارد، باید آنها را از مبتکر درخواست کنید.

شما همچنین برای استخراج اطلاعات از ACCOUNTABLE MATER به اجازه مبتکر نیاز دارید .

تمام اطلاعات TOP SECRET به طور پیش فرض باید ACCOUNTABLE MATERIAL باشد.

❖ **ردیابی "مطالب قابل پاسخگویی"**

در مواد جلویی باید شماره کپی داشته باشید، بنابراین آژانس شما می‌تواند سوابق دقیق را کنترل و توزیع را کنترل کند.

وقتی سندی با علامت محافظ "پاسخگو" می‌شود، شخصی که مسئولیت آن سند را دارد باید در فواصل زمانی مشخص، به طور معمول هر شش ماه، حق حضانت آن را بررسی و تأیید کند.

❖ **استفاده از دستگاه‌های فتوکپی، دستگاه‌های نمابر و دستگاه‌های مشابه**

دستگاه‌هایی که برای کپی و انتقال اسناد با علامت محافظ استفاده می‌شوند دارای خطرات هستند که باید آنها را درک کرده و مدیریت کنید.

دستگاه‌های فتوکپی، دستگاه‌های نمابر و دستگاه‌های مشابه، معروف به دستگاه‌های چند منظوره:(MFD)

- تصاویری از اسناد کپی شده را که می‌توانند منتقل شوند حفظ کنند
- به سیستم‌های ICT متصل شوند که سطح حفاظتی لازم را ندارند.

برای مشاوره در مورد دستگاه‌های ضدعفونی کننده، با اداره امنیت ارتباطات دولت (GCSB) مشورت کنید.

❖ **دستگاه‌هایی که نمی‌توانید از آنها برای کپی و انتقال استفاده کنید**

اگر دستگاهی به سیستم ICT شما متصل است و سندی دارای علامت محافظتی بالاتر از سیستم ICT شما است، نمی‌توانید از دستگاه برای کپی یا انتقال آن سند استفاده کنید.

همچنین نمی‌توانید یک سند محافظت شده را با استفاده از دستگاه متصل به شبکه عمومی یا دستگاه فکس کپی یا انتقال دهید (مگر اینکه این اطلاعات مطابق با کتابچه راهنمای امنیت اطلاعات نیوزلند 11 - (NZISM) سیستم ارتباطی و دستگاه باشد).

❖ **هنگام کپی و انتقال اطلاعات محافظت شده، خطرات را کاهش دهید**

برای کاهش خطرات اقدامات زیر را انجام دهید.

- دستگاه‌های تأیید شده را در محلی قرار دهید که بتوانید همه فعالیت‌های کپی و انتقال را مشاهده کنید .
- اطمینان حاصل کنید که یک فرد تعیین شده تا پایان تمام فعالیت‌ها در نزدیکی دستگاه باقی بماند.
- به محض پایان فعالیت، اسناد را از دستگاه خارج کنید .

۵-۱-۱۴- حذف مواد محافظت شده از محل زندگی خود

درک کنید که چگونه اطلاعات رسمی را با استفاده از علائم محافظتی که از محل زندگی خود دور می‌کنید محافظت می‌کنید.

این شرایط برای کلیه اطلاعات رسمی (با یا بدون طبقه بندی امنیتی) اعمال می‌شود

برای اطمینان از انطباق آژانس با الزامات امنیتی محافظتی برای امنیت اطلاعات، این شرایط را دنبال کنید.

❖ **قرار دادن سیاست‌ها و فرایندها**

اگر آژانس شما می‌خواهد اطلاعات دارای علامت محافظ را از محل کار شما بردارد (حذف کند)، باید اطمینان حاصل کنید که از آن محافظت می‌شود، خط مشی‌ها و فرآیندهایی را در نظر بگیرید .ممکن است بخواهید اطلاعات محافظت شده را برای جلسه یا محل کار خود به آژانس یا محل کار دیگری ببرید.

با این حال، اطلاعات محافظت شده فقط باید از محل زندگی شما حذف شود:

- یک نیاز قطعی وجود دارد
- سطح صحیح حفاظت را می‌توان در مسیر و در مقصد حفظ کرد

.

❖ **خط مشی اطلاعات "بسیار محرمانه"**

شما نباید اطلاعات TOP SECRET را برای کار کوتاه مدت در خانه بدون تأیید سرویس اطلاعات امنیتی نیوزیلند (NZSIS) و آژانس مبدأ (اگر آژانس شما نیست) حذف کنید.

❖ **حذف اطلاعات محافظت شده در نیوزلند**

قبل از اینکه هر کسی در آژانس شما اطلاعات دارای علامت محافظ را از مناطق کاری امن یا مجاز بگیرد، باید تأیید داشته باشد.

❖ **مجاز کردن موارد حذف**

آژانس شما تصمیم می‌گیرد چه کسی می‌تواند مجازات حذف شود .با این حال، مدیر یا شخص معادل آن مسئول تأیید اطلاعات است.

مصوب باید:

- از وجود نیاز واقعی راضی باشید
- مختصراً به شخصی که اطلاعات مربوط به خطرات موجود را از بین می‌برد، خلاصه کنید
- از وجود تمهیدات کافی برای نگهداری ایمن اطلاعات، راضی باشید
- آماده پذیرش مسئولیت ایمنی در نگهداری اطلاعات باشید.

اطمینان حاصل کنید که همه موارد حذف شده را در سطوح TOP SECRET و SECRET ثبت کرده‌اید.

❖ **حمل اطلاعات دارای علامت محافظ به صورت ایمن - کیف و کیف**

NZSISدارای کیف و کیف‌های مناسب برای حمل اطلاعات دارای علامت محافظ مناسب است .لطفاً برای اطلاعات بیشتر با تیم PSR تماس بگیرید، زیرا لیست محصولات تأیید شده طبقه بندی شده است.

هنگامی که اطلاعات دارای علامت محافظ در یک کیف یا کیف تأیید شده به خارج از نمایندگی شما منتقل می‌شود، باید آن را در یک پاکت مات در کیف قرار دهید .

کیف یا کیف باید باشد:

- همیشه قفل شده
- تحت حمایت شخصی متولی نگهداری می‌شود.

برای جلوگیری از کپی شدن کلیدها یا دستکاری قفل‌ها:

- کلیدها را در قفل رها نکنید
- کیف یا کیف را قفل کنید، حتی اگر خالی باشد.

❖ **محافظت از رسانه‌های الکترونیکی**

شما باید از رسانه‌های الکترونیکی مانند لپ تاپ، CDو USB که برای پردازش اطلاعات با علامت محافظ به همان درجه مواد مبتنی بر کاغذ استفاده می‌شوند، محافظت کنید.

سطح حفاظت باید معادل بالاترین سطح اطلاعات دارای علامت محافظتی باشد که تاکنون در رسانه‌ها قرار داده نشده است تا زمانی که آن را سالم سازی کنید .

❖ **دور از اداره یا خارج از سایت کار کردن**

برای هماهنگی‌های منظم و طولانی مدت برای افرادی که خارج از دفتر کار می‌کنند:

- رعایت الزامات امنیتی در محل کار دور از دفتر
- مراجعه به - NZISM خارج از سایت.

گاهی اوقات ممکن است نیاز داشته باشید تا اطلاعات را به یک دفتر منطقه‌ای یا شعبه منتقل کنید نه اینکه اجازه دهید آن را به مکانی ببرید که نمی‌توانید امنیت آن را تضمین کنید .به عنوان مثال، ممکن است در برخی موارد نگهداری اطلاعات محافظت شده در اتاق هتل از امنیت کافی برخوردار نباشد.

❖ **گرفتن اطلاعات محافظت شده در خارج از نیوزیلند**

وقتی آژانس شما قصد دارد اطلاعات دارای مارک محافظتی را در خارج از کشور بگیرد، مراقبت ویژه‌ای داشته باشید .این می‌تواند در معرض خطرات بسیار بیشتری قرار گیرد، بنابراین اقدامات امنیتی بیشتری لازم است.

قبل از اینکه به هر یک از افراد خود اجازه انتقال یا کنترل اطلاعات دارای علامت محافظ در خارج از نیوزیلند را بدهید، مناطق امنیتی را بخوانید.

❖ **بررسی با وزارت امور خارجه و تجارت**

خدمات بین المللی پیک دستی ایمن دیپلماتیک به نمایندگی از دولت نیوزیلند توسط وزارت امور خارجه و تجارت (MFAT) تحت مواد ۲۷ و ۴۰ کنوانسیون روابط دیپلماتیک وین (۱۹۶۱) برای حمل و نقل امن مواد رسمی طبقه بندی شده اداره می‌شود محرمانه یا بالاتر شبکه پیک دیپلماتیکMFAT ، تحویل ایمن و روتین محموله‌های طبقه بندی شده در سراسر جهان را تسهیل می‌کند .این وسیله ترجیحی برای انتقال تمام اطلاعات طبقه بندی شده به خارج از نیوزیلند است MFAT .می‌تواند جزئیات بیشتری را به هر آژانس که مایل به استفاده از خدمات پیک دستی ایمن دیپلماتیک هستند، ارائه دهد.

اگر استفاده از سرویس پیک دستی ایمن دیپلماتیک عملی نیست، رئیس ارشد امنیتی شما باید با MFAT تماس بگیرد تا در مورد گزینه‌های دیگر بحث کند .

۵-۱-۱۵- انتقال یا انتقال اطلاعات دارای علامت محافظ

بدانید که چگونه اطلاعات محافظت شده را هنگام انتقال یا انتقال یا دریافت آن ایمن نگه دارید.

این شرایط برای کلیه اطلاعات رسمی (با یا بدون طبقه بندی امنیتی) اعمال می‌شود

برای اطمینان از انطباق آژانس با الزامات امنیتی محافظتی برای امنیت اطلاعات، این شرایط را دنبال کنید.

❖ **اقدامات امنیتی و سیاست انتقال اطلاعات محافظت شده**

اقدامات امنیتی لازم برای محافظت از اطلاعات دارای علامت محافظ در هنگام انتقال فیزیکی به موارد زیر بستگی دارد:

- علائم محافظ
- از کجا و به کجا می‌رود
- روش استفاده شده

گیرنده مورد نظر باید قبل از انتقال اطلاعات، "نیاز به دانستن" و سطح امنیتی لازم را داشته باشد.

آژانس شما باید سیاستی مبتنی بر حداقل اقدامات و همچنین سیاستی برای اطلاعات و مطالب بیش از حد بزرگ برای اصل "مانع مضاعف" تدوین کند .

❖ **آماده سازی اطلاعات دارای علامت محافظ برای انتقال**

برای محافظت از اطلاعات مشخص شده هنگام حمل و نقل، باید از اقدامات امنیتی استفاده کنید.

اقدامات می‌تواند شامل موارد زیر باشد:

- با استفاده از کیف‌های مورد تأییدNZSIS ، کیف، مهر، کیسه یا کیف حمل و نقل
- با استفاده از روش‌های خاص پاکت گذاری
- انتقال اطلاعات با دست بین افراد با مجوز امنیتی مناسب یا پیام رسان‌های مجاز.

از روش‌های امنیتی می‌توان با هم استفاده کرد تا امنیت بیشتری ایجاد شود .برای مثال:

- با استفاده از یک پاکت داخلی و خارجی - دو پوششی
- ترکیب یک مانع داخلی با یک مانع بیرونی - روش "دو مانع."

از هر ترکیبی که استفاده کنید، سد داخلی باید کاملاً آشکار باشد و سد بیرونی باید ماهیت اطلاعات منتقل شده را پنهان کند.

❖ **آدرس دهی صحیح اطلاعات**

اطلاعات علامت گذاری شده محافظ را به موقعیت خاص، قرار ملاقات یا فردی که مشخص شده است، آدرس دهید .

اطمینان حاصل کنید که مخاطب و گزینه جایگزین از سطح امنیتی لازم برخوردار هستند .

نام، نامگذاری و آدرس خیابان کامل گیرنده مورد نظر را مشخص کنید .

اطلاعات دارای علامت محافظ را به صندوق پستی ارسال نکنید.

برای اطلاعاتTOP SECRET ، باید فرد یا قرار ملاقات دیگری را ارائه دهید .همچنین باید این کار را برای اطلاعات دارای علامت محافظ طبقه بندی شده در بالا راز انجام دهید.

❖ **انتقال اطلاعات در داخل دفتر کار خود**

می‌توانید اطلاعات علامت گذاری شده محافظت شده را در محیط اداری مجزا و بدون هیچ گونه پوششی، مانند پاکت نامه، انتقال دهید:

اطلاعات مستقیماً بین کارکنانی که سطح دسترسی مناسب برای دسترسی به آنها را دارند و نیاز به اطلاعات منتقل می‌شوند

هیچ فرصتی برای افراد غیر مجاز برای مشاهده اطلاعات وجود ندارد.

اگر این خطر وجود داشته باشد که یک شخص غیر مجاز بتواند اطلاعات را مشاهده کند، باید این اطلاعات را پوشش داد.

❖ **دو لفافه**

برای انتقال ایمن اسناد محافظ دار به خارج از آژانس خود باید از یک مانع مضاعف استفاده کنید.

هنگام انتقال اطلاعات دارای علامت محافظ و مواد قابل استفاده، برای محافظت از اصل نیاز به دانستن از دو پوششی استفاده می‌شود. دو پوششی شواهدی از دستکاری را ارائه می‌دهد .همانطور که از نامش پیداست، دو پاکت شامل قرار دادن اطلاعات دارای علامت محافظ در دو پاکت مهر و موم شده است. آژانس شما هنگام تحویل دستی یا استفاده از پیک مورد تأییدNZSIS ، باید برای کلیه اطلاعات طبقه بندی شده به عنوان "محرمانه"، "راز" و "راز برتر" آژانس شما استفاده کند.

برای اطلاعات طبقه بندی شده به عنوان "با اطمینان"، "حساس" یا "محدود"، بنا به صلاحدید خود از پوششی مضاعف استفاده کنید .برای اطلاع از تصمیمات، از برنامه مدیریت خطر امنیتی خود استفاده کنید.

اطلاعات یا مطالب حساس و محدود باید هنگام ارسال از طریق پست یا پیک تجاری، دارای دو بسته باشد.

❖ **از جمله رسیدها**

از پاکت دوبل باید همراه با رسیدهایی استفاده شود که:

- با اسناد محافظت شده محصور شده است
- تاریخ و زمان اعزام و نام افسر اعزام را مشخص کنید
- یک شماره شناسایی منحصر به فرد داشته باشید.

❖ **درست پاکت بیرونی گرفتن**

از پاکت بیرونی به روشی مشابه پاکت نامه‌های عادی استفاده کنید .از پاکت داخلی محافظت می‌کند.

پاکت بیرونی نباید:

- علائم محافظ سند را نمایش دهید
- از مهر و موم‌های مشهود استفاده کنید.

❖ **پاکت بیرونی باید نمایش داده شود:**

- آدرس فیزیکی گیرنده
- یک شماره مرجع مجزا (اگر پاکت نامه‌ها به صورت جداگانه شماره گذاری نشوند، این ممکن است شماره رسید باشد)
- نام و امضای افسر اعزام کننده

- تاریخ ارسال.

❖ **درست گرفتن پاکت داخلی**

از پاکت داخلی برای اثبات دستکاری استفاده می‌شود.

پاکت داخلی باید:

- علائم محافظتی را در بالا و پایین و جلو و عقب پاکت نشان دهید
- با مهر و موم معتبر دستکاری شده توسط NZSIS مهر و موم شده به گونه‌ای که ورود مخفیانه به پاکت مقابله شود.

❖ **با استفاده از روش‌های دیگر پاکت نامه**

برخی از پاکتهای یکبار مصرف توسط NZSIS برای استفاده تأیید شده‌اند:

- به عنوان یک پاکت داخلی
- به عنوان یک پاکت خارجی هنگامی که برای محصور کردن چندین پاکت داخلی استفاده می‌شود که تحویل اولیه به یک رجیستری یا موارد مشابه انجام می‌شود.

از کیف‌های چند منظوره نیز ممکن است در برخی شرایط استفاده شود .برای کسب اطلاعات بیشتر با تیم محافظت از امنیت مورد نیاز تماس بگیرید، زیرا لیست محصولات تأیید شده طبقه بندی شده است.

❖ **روش‌های انتقال اطلاعات محافظت شده**

آژانس شما باید روش انتقال را برای دستیابی به بهترین شکل در انتقال ایمن اطلاعات محافظت شده انتخاب کند.

❖ **با استفاده از روش 'دست امن'**

روش "دست ایمن" هنگامی است که اطلاعات با علائم محافظ در اختیار مأمور مجاز یا جانشینی افسران مجاز، که مسئول حمل و نگهداری آن هستند، به مخاطب ارسال می‌شود.

در هر تحویل، یک رسید بدست می‌آید که حداقل نشان می‌دهد:

- شماره شناسایی بسته
- زمان و تاریخ تحویل
- نام و امضای گیرنده.

هدف از ارسال مقاله با استفاده از دست ایمن ایجاد ردیابی حسابرسی است که به فرستنده اجازه می‌دهد تائیدیه را دریافت کند که مخاطب اطلاعات را دریافت کرده است.

برای ارسال اطلاعات با استفاده از روش ایمن:

- آن را در یک سد مضاعف محصور کنید (آن را دو پاکت کنید)

- به آن یک شماره شناسایی منحصر به فرد بدهید (معمولاً شماره رسید)
- یک رسید دو بخشی را با اطلاعات در پاکت داخلی قرار دهید - مخاطب یک قسمت را نگه می‌دارد و آن را امضا می‌کند و سپس قسمت دیگر را به فرستنده برمی گرداند
- اطمینان حاصل کنید که نوعی سیستم ثبت یا رسید با بسته همراه است، به طوری که هر تحویل مستند است
- اطلاعات را در یک کیف یا کیسه نامه تأیید شده حمل کنید
- اطمینان حاصل کنید که اطلاعات بدون مراقبت باقی نمی‌مانند، مگر در مواردی که در محفظه بار هواپیما قرار می‌گیرند .

❖ **استفاده از پیک‌های تجاری یا خدمات پستی**

آژانس شما می‌تواند از طریق پست یا پیک تجاری در نیوزلند مطالبی را طبقه بندی و محدود کند که از آنها محدود شده است.

موارد طبقه بندی شده SENSITIVE یا محدود شده باید دارای دو بسته باشد.

هنگامی که هیچ پیام رسان مجاز یا سرویس پیک سفارشی وجود ندارد، آژانس شما می‌تواند اجازه دهد مواد طبقه بندی شده به عنوان "محرمانه" توسط پیک تجاری مورد نیاز امضا یا پست ثبت شده در نیوزیلند حمل شود .این روش می‌تواند مورد استفاده قرار گیرد:

- تحویل با دست ایمن در عرض ۱۵ دقیقه انجام نمی‌شود (با پای پیاده یا وسیله نقلیه)
- آژانس‌های ارسال کننده و گیرنده توافق نامه‌ای در مورد استفاده از پیک‌های تجاری برای حمل مواد محرمانه دارند
- تمهیداتی اندیشیده شده است تا اطمینان حاصل شود آژانس پذیرنده قادر به پذیرش اطلاعات در زمان تحویل پیش بینی شده است.

فقط پیک‌های تجاری که توسط NZSIS تأیید شده‌اند باید برای حمل مواد SECRET استفاده شوند .سازمان امنیت ملی شما می‌تواند جزئیات مورد نیاز و روند تأیید را از NZSIS درخواست کند.

❖ **دستورالعمل‌های عمومی**

رسیدها :کلیه اطلاعات محرمانه یا محرمانه ارسال شده از طریق پیک تجاری یا آژانس پستی باید همراه با رسید باشد .رسید باید توسط آژانس پذیرنده امضا شود و به آژانس ارسال کننده برگردانده شود.

بسته بندی :برای حمل از طریق پیک تجاری، کیسه پیک در حالت مات می‌تواند به عنوان پاکت بیرونی باشد .پاکت‌ها و لفاف‌ها باید مقاوم باشند تا در برابر فرسودگی و پارگی مقاومت کنند.

ارسال و تحویل :اطلاعاتی را که با علامت محافظ مشخص شده‌اند، مراقب نباشید تا در حال تحویل گرفتن توسط پیک باشید.

قبل از تعطیلات آخر هفته یا تعطیلات رسمی، اطلاعات دارای علامت محافظ را ارسال نکنید، مگر اینکه مخاطب بتواند روز بعد آن را دریافت کند و به طور مناسب از آن محافظت کند. اسناد تحویل خود را بررسی کنید تا اطمینان حاصل کنید که اقلام در بازه‌های زمانی پیش بینی شده وارد می‌شوند اگر تاخیری بی دلیل وجود داشته باشد و یا نشانه‌ای از دستکاری وجود داشته باشد، باید هم سازمانهای جامعه مدنی اعزامی و دریافت کننده به آنها اطلاع داده شود.

❖ **وقتی نمی‌توانید از پیک یا آژانس پست استفاده کنید**

TOP SECRETمواد و مواد دارای مارک بندی جداگانه نباید توسط پیک تجاری یا آژانس پست حمل شود . الزامات خاص رسیدگی که به اطلاعات حامل مارک‌های تأیید اعمال می‌شود نیز ممکن است از استفاده از پیک تجاری جلوگیری کند.

اطلاعاتی که با علامت تأیید فقط چشم نیوزیلند (NZEO) مشخص شده‌اند باید با توجه به سطح طبقه بندی امنیتی آن منتقل شوند.

الزامات سایر مارک‌های تأیید توسط سازمان کنترل تعیین می‌شود .

❖ برخورد با مواد حجیم

به طور کلی، وقتی اندازه و وزن مواد به معنای جابجایی آن با استفاده از روش ایمن دستی یا پیک‌های تجاری نیست، باید اقدامات احتیاطی ویژه‌ای را انجام دهید تا اطمینان حاصل کنید که مواد در حین عبور، به خطر نیفتد، از بین نرود و آسیب نبیند.

از CSO خود راهنمایی بگیرید .ممکن است CSO شما از NZSIS مشاوره بگیرد.

❖ برخورد با مواد طبقه بندی نشده با ریسک بالا

اگر نیاز دارید مواد ارزشمندی مانند کارهای هنری یا پول را به آژانس دیگری منتقل کنید، می‌توانید از خدمات پیک تجاری استفاده کنید. با این حال، ابتدا مراقب باشید که خدمات پیک را ارزیابی کنید .اطمینان حاصل کنید که قانونی، قابل اعتماد است و می‌تواند سطح حفاظت مناسبی را برای خطرات شناسایی شده شما ایجاد کند. شما همچنین باید هر نوع قانونگذاری را که در مورد مواد شما اعمال می‌شود، برآورده کنید. در صورت امکان، از جلب توجه به ماهیت خاص مواد جابجا شده خودداری کنید .

اقدامات امنیتی اضافی ممکن است در برخی شرایط لازم باشد .مراحل مانند:

- آب بندی مواد
- پاکسازی امنیتی کارکنان خدمات پیک
- ترتیب اسکورت امنیتی یا پلیس.
- انتقال داده‌های الکترونیکی

داده‌های دارای علامت محافظتی که به صورت الکترونیکی وارد، صادر یا منتقل می‌شوند، باید مطابق با .NZISM - 20مدیریت داده ها محافظت شوند.

❖ دریافت نسخه‌های چاپی

قبل از اینکه به هر کسی در آژانس خود اجازه دهید نسخه‌های چاپ شده اطلاعات دارای علامت محافظ را دریافت کند، اطمینان حاصل کنید که آنها از مسئولیت‌های خود آگاه هستند و در صورت لزوم، از تصویب امنیتی مناسب برخوردار هستند.

اسناد دارای علامت محافظ فقط باید توسط مخاطب یا مخاطب جایگزین باز شود .با این حال، رئیس نمایندگی شما ممکن است به شخص یا منطقه مشخصی اجازه دهد که همه نامه‌ها را باز کند و اطلاعات مربوط به آن یا عملکردهای مدیریت امنیت را انجام دهد.

هنگامی که باز شدن آن به غیر از مخاطب مورد نظر متهم شد، معمولاً فقط باز کردن پاکت بیرونی را انجام دهید .پاکت داخلی فقط باید در حضور مخاطب باز شود.

گیرنده بسته‌ای که حاوی اسنادی با علامت محافظ است باید تأیید کند که:

- اطلاعات با استفاده از روش مناسب منتقل می‌شد
- مهر و موم و بسته بندی هنوز سالم است.

هرگونه شکستگی، علائم دستکاری، یا روشهای انتقال نامناسب را به CSO خود و CSO آژانس ارسال کننده گزارش دهید .اگر بسته توسط پیک مورد تأیید NZSIS تحویل داده شده است، باید NZSIS را راهنمایی کنید. گیرنده باید بررسی کند که محتویات و یکپارچگی آنها حفظ شده است .به عنوان مثال، صفحات و فهرست مطالب را بررسی کرده و هر رسید همراه با اطلاعات را امضا کرده و برگردانید. اگر آژانس شما برای اسناد دارای علامت محافظ ثبت نام می‌کند، مطمئن شوید که اطلاعات ثبت شده است.

۵-۱-۱۶- تخریب اطلاعات دارای علامت محافظ به طور ایمن

- برای از بین بردن رسانه‌های ICT و اسناد دارای علائم محافظ، از روش‌های مصوب استفاده کنید.
- این شرایط برای کلیه اطلاعات رسمی (با یا بدون طبقه بندی امنیتی) اعمال می‌شود
- برای اطمینان از انطباق آژانس با الزامات امنیتی محافظتی برای امنیت اطلاعات، این شرایط را دنبال کنید.

❖ **دریافت مشاوره و تنظیم خط مشی**

افسر ارشد امنیتی (CSO) شما می‌تواند در مورد روشهای تأیید شده برای تخریب معمول یا اضطراری اطلاعات دارای علامت محافظ، از NZSIS مشاوره بگیرد. آژانس شما باید سیاستی برای از بین بردن اطلاعات رسمی بدون علائم محافظ داشته باشد - سیاستی مطابق با برنامه مدیریت ریسک امنیتی شما.

شما نباید از خدمات یا سیستم‌های زباله یا بازیافت برای دفع اطلاعات محافظت شده استفاده کنید، مگر اینکه قبلاً از طریق فرآیند تخریب مورد تأیید NZSIS مانند خرد کردن انجام شده باشد. زباله‌ها، خواه در یک زباله یا محل دیگری برای جمع آوری قرار گیرند، یا مستقیماً به یک سرویس دفع زباله منتقل شوند، بسیار آسیب پذیر هستند.

❖ **دفع سوابق رسمی**

سوابق رسمی را مطابق با قانون سوابق عمومی ۲۰۰۵ دفع کنید این معمولاً تحت مفاد مرجع دفع صادر شده توسط بایگانی نیوزیلند است.

- برای کسب اطلاعات بیشتر با بایگانی نیوزیلند تماس بگیرید

❖ **روش‌های تخریب**

در زیر روش‌های معمول تخریب اطلاعات دارای علامت محافظ وجود دارد.

- **Pulping**– تبدیل جرم به اندازه معین که توسط صفحه قابل جابجایی تعیین می‌شود
- **سوختن**– سوختن مطابق با محدودیت‌های مربوط به حفاظت از محیط زیست
- **ضخیم سازی**– استفاده از آسیاب‌های چکش با چکش‌های فولادی دوار برای ایجاد مواد روی مواد

- **از هم پاشیدگی**- استفاده از تیغه‌ها برای برش و کاهش تدریجی ذرات زباله به اندازه معین که توسط صفحه قابل جدا شدن تعیین می‌شود
- **خرد کردن**- استفاده از دستگاه‌های خرد کن نواری و خرد کن‌های متقاطع .فقط خرد کنهای متقاطع برای اطلاعات دارای علامت محافظ مورد تأیید NZSIS هستند. برای مشاوره در مورد تجهیزات برای از بین بردن اطلاعات محافظت شده، با اطمینان به اطلاعات و دارایی های بازنشستگی بروید

❖ **با استفاده از روش خرد کردن**

هنگامی که روش تخریب خرد می‌شود، باید از طبقه بندی صحیح خرد کن برای طبقه بندی امنیتی اطلاعات استفاده کنید .

و دستگاه خرد کن باید توسط NZSIS تأیید شود.

- اطلاعات - TOP SECRET دستگاه خرد کن متقاطع درجه ۵
- اطلاعات با مارک‌های محفظه‌ای - خرد کن متقاطع درجه ۵
- محرمانه یا محرمانه - خردکن متقاطع درجه ۴
- اطلاعات حداکثر و محدود شده توسط - خردکن متقاطع درجه ۳
- از بین بردن میکرو فیش و سایر مواد عکاسی
- میکرو فیش محافظ و سایر مواد عکاسی باید با استفاده از تجهیزات یا فرایندهای مورد تأیید NZSIS از بین بروند .

❖ **قرارداد تخریب مواد چاپی**

تصمیم گیری در مورد انعقاد تخریب مواد محافظت شده را بر اساس مدیریت صحیح ریسک قرار دهید.

در اینجا چند فاکتور برای بررسی وجود دارد.

- چگونه شرکت اطلاعات را حمل می‌کند؟
- مراحل آنها چیست؟
- ظروف آنها چقدر ایمن هستند؟
- امکانات آنها چقدر ایمن است؟
- آن‌ها از چه تجهیزاتی استفاده می‌کنند؟
- نتیجه روند تخریب آنها چیست؟ (به عنوان مثال، اندازه ذرات حاصل از مواد تخریب شده.)

به یاد داشته باشید که کیسه‌ها و سطل‌های زباله طبقه بندی شده ظروف امنیتی نیستند .بنابراین، آن‌ها باید قبل از جمع آوری محافظت مناسب داشته باشند .کیسه‌های زباله و سطل زباله طبقه بندی شده باید با توجه به بالاترین سطح اطلاعات دارای علامت محافظتی که در آنها وجود دارد، ذخیره شوند.

❖ **گرفتن تأیید برای استفاده از پیمانکار**

قبل از اینکه آژانس شما قراردادی برای از بین بردن اطلاعات مبتنی بر کاغذ منعقد کند که محرمانه یا بالاتر باشد، باید تأیید NZSIS را داشته باشید .آن‌ها باید اطمینان حاصل کنند که پیمانکار می‌تواند از اطلاعات در تمام مراحل تخریب محافظت کند.

آژانس شما باید فرایندهایی را که شما و پیمانکار برای حفظ سطح امنیتی مناسب در طول وانت، حمل و تخریب زباله استفاده می‌کنید، تعیین کند.

فرآیندهای مناسب شامل موارد زیر است:

- زباله‌ها نباید در هر زمان بدون مراقبت رها شوند
- وسایل نقلیه و محل‌های ذخیره باید به طور مناسب ایمن شوند
- تخریب باید بلافاصله پس از رسیدن مواد به محل انجام شود
- نمایندگان آژانس با سطح صحیح از نظر امنیتی باید ضایعات را اسکورت کرده و شاهد نابودی آن باشند

کارکنان شرکت تخریب باید دارای امنیت امنیتی در بالاترین سطح اطلاعات دارای علامت محافظتی باشند که در حال انتقال و تخریب هستند.

اطلاعاتی که با TOP SECRET و MATERIAL ACCOUNTABLE علامت گذاری شده‌اند باید در محوطه آژانس تخریب شوند و فقط هنگامی که آژانس مبدأ اطلاع داده شود .مبتکران همچنین ممکن است شرایط خاصی را برای از بین بردن برخی از اطلاعات دارای علامت محافظتی که ممکن است از انهدام تخریب جلوگیری کند، اعمال کنند.

❖ از بین بردن رسانه‌ها و تجهیزاتICT

رسانه‌ها و تجهیزات ICT باید مطابق با این دو بخش NZISM نابود شوند:

- 12.6بهداشت و دفع محصولات
- 13حذف و دفع مدیریت رسانه.

❖ قرارداد تخریب رسانه‌ها و تجهیزاتICT

برای اطلاعات در مورد سالم سازی و تخریب رسانه‌ها و تجهیزات الکترونیکی، به بخش‌های زیر NZISM بروید:

- 12.6بهداشت و دفع محصولات
- 13حذف و دفع مدیریت رسانه.

❖ حمل وسایل حساس برای تخریب

برای اطلاعات در مورد حمل و نقل ایمن اطلاعات حساس یا دارایی برای تخریب، به این موارد بروید:

- حمل و نقل ایمن وسایل حساس

فصل ۶

گزارش گیری

۶- مدل بلوغ قابلیت

الزامات اجباری

❖ **توانایی خود را ارزیابی کنید**

از یک فرآیند ارزیابی مبتنی بر شواهد سالانه برای اطمینان از مناسب بودن توانایی امنیتی سازمان خود استفاده کنید .در صورت درخواست، گزارش اطمینان را از طریق تیم محافظت از امنیت مورد نیاز به دولت ارائه دهید .سیاست‌ها و برنامه‌های خود را هر ۲ سال یا در صورت لزوم تغییر در تهدید یا محیط کار، زودتر مرور کنید.

مدل بلوغ قابلیت (CMM) به سازمان شما کمک می‌کند تا توانایی فعلی شما را در تعدادی از ابعاد امنیتی محافظتی ارزیابی کند، سطوح توانایی متناسب با خطرات امنیتی که با آن روبرو هستید را شناسایی کرده و برخی از روشهای بالابردن قابلیت را شناسایی کند. راهنمای انطباق امنیت حفاظتی یک لیست چک ساده برای کمک به رهبران امنیتی سازمان شما برای بررسی توانایی امنیتی سازمان شما فراهم می‌کند .این امر براساس الزامات اجباری الزامات امنیتی محافظتی و همچنین بهترین روش انجام می‌شود.

۶-۱- گزارش اطمینانPSR

رهنمودهایی که روند ارزیابی خودکار سالانه و گزارش اطمینان را توضیح می‌دهند.

❖ **توانایی خود را ارزیابی کنید**

از یک فرآیند ارزیابی مبتنی بر شواهد سالانه برای اطمینان از مناسب بودن توانایی امنیتی سازمان خود استفاده کنید .در صورت درخواست، گزارش اطمینان را از طریق تیم محافظت از امنیت مورد نیاز به دولت ارائه دهید .سیاست‌ها و برنامه‌های خود را هر ۲ سال یا در صورت لزوم تغییر در تهدید یا محیط کار، زودتر مرور کنید.

❖ **هدف**

از این راهنما برای دستیابی به یک رویکرد سازگار برای ارزیابی قابلیت امنیتی محافظت و انطباق در سازمانها استفاده کنید .این کمک به:

- مناطق تمرکز را شناسایی کرده و از طریق اقدامات تخفیف و آموزش به آنها رسیدگی کنید
- ارزیابی اثربخشی اقدامات امنیتی محافظتی آنها
- سیاست‌ها و رویه‌های امنیتی محافظتی آنها را بهبود ببخشید

❖ **این اطلاعات برای چه کسانی است**

این اطلاعات در درجه اول برای مدیران ارشد، افسران ارشد امنیتی(CSO) ، افسران ارشد امنیت اطلاعات (CISO) و سایر پرسنل مدیریت امنیت آژانس است .همچنین این یک مرجع مفید برای ارائه دهندگان خدمات مدیریت امنیت محافظ قراردادی است.

❖ **الزامات قانونی**

در مواردی که الزامات قانونی بالاتر از کنترلی است که در این الزامات مشخص شده است، الزامات قانونی مقدم است و باید اعمال شود.

❖ **استانداردهای مربوطه**

استانداردهای مربوط به این الزامات عبارتند از:

- ISO 31000: 2018 - مدیریت ریسک - دستورالعمل‌ها
- HB 167: 2006 مدیریت ریسک امنیتی

۲-۶- مزایای گزارشگری

رعایت الزامات اجباری به آژانس‌ها کمک می‌کند تا بتوانند مدیریت امنیتی محافظتیeffective ثر و متناسب با انتظارات دولت نیوزلند داشته باشند.

انطباق با PSR مزایایی را برای دولت، اوراق بهادار و آژانس‌ها فراهم می‌کند.

❖ **مزایای دولت نیوزیلند**

مزایای دولت شامل موارد زیر است:

- ارائه مکانیزمی برای اطمینان از دولت که امنیت محافظتی سالم و مسئولانه در سراسر دولت اتفاق می افتد
- امکان شناسایی هرگونه مسئله امنیتی جدی یا سیستمی محافظتی در سراسر دولت، که می‌تواند از طریق تغییر سیاست‌ها و برنامه‌های آموزشی رفع شود
- دولت را قادر می‌سازد تا امنیت محافظتی بهتر را شناسایی و اجرا کند
- امکان ایجاد، در صورت لزوم، برقراری ارتباط با وزیران در زمینه رعایت موارد قابل توجه در نمونه کارها
- ارتقا همکاری درون پرتفوی بین آژانس‌ها برای رسیدگی به موضوعات گسترده پرتفوی.

اطلاعات ارائه شده برای اطلاع رسانی گزارش وضعیت امنیتی محافظتی کل دولت استفاده خواهد شد.

❖ **مزایای سازمان شما**

مزایا عبارتند از:

- توانایی شناسایی مناطق دارای قابلیت امنیتی کم محافظت و رسیدگی به موقع به هر موضوعی
- دانش به دست آمده توسط یک آژانس می‌تواند برای کلیه آژانسهای مربوطه ضبط و صادر شود و باعث بهبود کارایی و اثربخشی اقدامات امنیتی محافظتی شود
- اطمینان در مورد امنیت اطلاعات و ترتیبات تقسیم دارایی.

۳-۶- مسئولیت‌ها و مسئولیت‌ها

❖ **آژانس‌ها**

- برای انجام تعهدات امنیتی محافظتی و ارزیابی میزان رعایت آنها با PSR پاسخگو هستند

- باید مسئولیت‌هایی را برای مدیریت امنیت محافظتی در سازمان خود به کارکنان آموزش دیده و با صلاحیت مناسب اختصاص دهند
- باید اطلاعات و مساعدت لازم را جهت ارتقا انطباق و مشاوره در مورد عواقب عدم رعایت آن به کارمندان از جمله پیمانکاران ارائه دهد
- در صورت درخواست، باید در مورد سطح امنیت امنیتی خود و موارد امنیتی قابل توجه یا سیستمیک از جمله اقدامات اصلاحی برای کاهش مشکلات گزارش دهند
- برای تهیه سابقه‌ای که می‌توانند برای ارزیابی انطباق آنها با الزامات اجباری PSR استفاده کنند، باید مستثنیات سیاست را ثبت کنند
- در صورت لزوم، باید عملکردها و سازوکارهای امنیتی محافظتی موجود را بر اساس ارزیابی ریسک آنها تقویت کند.

❖ **کارمندان**

کارمندان باید:

- به عنوان شرط پذیرش شغل در یک سازمان، موافقت خود را با رعایت سیاستهای امنیتی محافظتی آن سازمان اعلام کنید
- از عواقب عدم رعایت سیاست‌های سازمان و الزامات اجباری PSR آگاه باشید.

❖ **سران آژانس**

روسای آژانس باید مسئول این موارد باشند:

- اطمینان از مطابقت نمایندگی آنها با PSR و دارای سطح مناسب توانایی امنیتی محافظتی
- گزارش در مورد تأثیر سیاست‌ها و رویه‌های امنیتی حفاظتی آژانس در انطباق با الزامات اجباری.

❖ **کارمندان مسئول مدیریت امنیت محافظتی**

کارکنانی که مسئولیت مدیریت امنیت محافظتی را بر عهده دارند، از جمله CSO ها و CISO ها، باید:

- به طور مؤثر امنیت آژانس خود را مدیریت کنند، از جمله اعمال اقدامات امنیتی محافظتی مناسب بر اساس مشخصات آنها
- به ویژه در مواردی که یک رویکرد متمرکز برای مدیریت انطباق وجود دارد، با پرسنل مربوطه مربوط به امنیت، حاکمیت و انطباق ارتباط برقرار کنید
- کمک به سازمان و هماهنگی ارزیابی ریسک، ممیزی داخلی و بررسی انطباق
- در مورد الزامات انطباق مربوط به نمایندگی آنها مشاوره دهید
- موارد استثنا را ثبت و مدیریت کنید
- شناسایی و ترتیب دادن به ارائه آموزش مناسب مورد نیاز برای بهبود یا اطمینان از قابلیت حفاظتی مناسب
- گزارش استثنای انطباق آژانس را در برابر الزامات اجباری PSR تهیه کنید، یا در مواردی که نقش تضمین و گزارش انطباق در سایر نقاط آژانس انجام شده است، گزارش را ارائه دهید

۴-۶- گزارش قابلیت امنیتی و انطباق محافظ

برخی از سازمان‌ها باید از خارج و به صورت مکتوب، در مورد توانایی امنیتی محافظتی و انطباق با الزامات اجباری PSR گزارش دهند.

گزارش خارجی تأیید می‌کند که:

- آن‌ها ارزیابی را بر اساس الزامات اجباری انجام داده‌اند
- انطباق برای هر مورد اجباری به طور مؤثر مدیریت می‌شود
- هرگونه خطر غیرقابل قبول مربوط به این الزامات اجباری به طور مناسب رفتار شده است
- آن‌ها برنامه‌ای برای دستیابی و حفظ سطح مناسب یا توانایی امنیتی محافظتی بر اساس مشخصات ریسک خود دارند
- تعهدات انطباق آنها انجام شده است.

❖ **گزارش کتبی از رئیس آژانس باید:**

- حاوی اعلامیه انطباق با الزامات اجباری است
- در مواردی که مطابقت ندارد، مواردی را که مطابقت ندارد مطابقت دهید، مشخص کنید:

  - جزئیات اقدامات انجام شده برای کاهش خطرات شناسایی شده
  - مناطق عدم انطباق که نیاز به اقدامات بیشتری دارند
  - اقدامات پیشنهادی آینده برای رفع عدم انطباق
  - خطرات باقیمانده

آژانس‌ها همچنین باید هرگونه عدم رعایت الزامات خاص PSR را به آژانس‌های مربوطه که در زیر ذکر شده است، توصیه کنند.

مدیر کل دفتر امنیت ارتباطات دولت (GCSB) در امور مربوط به مطالب محرمانه و بالاتر و کتابچه راهنمای امنیت اطلاعات دولت نیوزلند.

- مدیر ارشد اطلاعات دولت (GCIO) برای امور مربوط به خطر فناوری اطلاعات و ارتباطات.(ICT)
- مدیر کل امنیت اطلاعات سرویس امنیتی نیوزلند (NZSIS) در امور مربوط به امنیت ملی.
- روسای هر آژانس که افراد، اطلاعات یا دارایی‌های آنها ممکن است تحت تأثیر توانایی و / یا عدم انطباق آژانس قرار بگیرند، درصورتی که در هنگام شناسایی عدم انطباق قبلاً توصیه نشده باشد. آژانس‌ها باید در زمان وقوع هر حادثه‌ای، GCSB، NZSISیا آژانس‌های تحت تأثیر را به طور مناسب مشاوره دهند.
- همچنین به گزارش حوادث و انجام تحقیقات امنیتی مراجعه کنید

Security laws in New Zealand