ریاست جمهوری
مرکز فناوری اطلاعات

## راهنمای پیاده‌سازی

# سیستم مدیریت امنیت اطلاعات

**گردآوری و تدوین: محمود خالقی**

**دبیرخانه شورای عالی امنیت فضای تبادل اطلاعات کشور**

# فهرست مطالب


| عنوان | صفحه |
|---|---|
| **پیشگفتار** | **۱** |
| **مقدمه** | **۳** |
| **فصل اول - سیستم مدیریت امنیت اطلاعات (ISMS)** | **۵** |
| ۱-۱- مقدمه | ۵ |
| ۱-۲- استانداردهای مدیریت امنیت اطلاعات | ۵ |
| ۱-۲-۱- استاندارد BS7799 | ۶ |
| ۱-۲-۲- استاندارد ISO/IEC 17799 | ۱۳ |
| ۱-۲-۳- گزارش فنی ISO/IEC TR 13335 | ۱۳ |
| ۱-۳- نتیجه‌گیری | ۲۷ |
| ۱-۳-۱- مرجع پیاده‌سازی سیستم مدیریت امنیت اطلاعات | ۲۷ |
| ۱-۳-۲- اقدامات موردنیاز به منظور پیاده‌سازی سیستم مدیریت امنیت اطلاعات | ۲۸ |
| **فصل دوم- چارچوب پیشنهادی برای تدوین اهداف، راهبردها و سیاست‌های امنیتی** | **۳۰** |
| ۲-۱- مقدمه | ۳۰ |
| ۲-۲- اهداف امنیت شبکه | ۳۰ |
| ۲-۲-۱- سرمایه‌های مرتبط با شبکه | ۳۱ |
| ۲-۲-۲- اهداف امنیت شبکه | ۳۱ |
| ۲-۳- راهبردهای تامین امنیت شبکه | ۳۳ |
| ۲-۳-۱- راهبردهای کوتاه مدت | ۳۳ |
| ۲-۳-۲- راهبردهای میان مدت | ۳۴ |
| ۲-۴- تشکیلات تامین امنیت شبکه | ۳۵ |
| ۲-۴-۱- اجزاء و ساختار تشکیلات | ۳۵ |
| ۲-۴-۲- شرح وظایف تشکیلات | ۳۷ |
| ۲-۵- سیاست‌های امنیتی شبکه | ۴۲ |
| ۲-۵-۱- سیاست‌های امنیتی سرویس‌های شبکه | ۴۲ |
| ۲-۵-۲- سیاست‌های امنیتی سخت‌افزارها | ۵۶ |
| ۲-۵-۳- سیاست‌های امنیتی نرم‌افزارها | ۶۸ |

۲-۵-۴- سیاست‌های امنیتی اطلاعات ۷۶
۲-۵-۵- سیاست‌های امنیتی ارتباطات شبکه ۸۱
۲-۵-۶- سیاست‌های امنیتی کاربران شبکه ۸۵
۲-۵-۷- سیاست‌های امنیتی محافظت فیزیکی ۹۱

**فصل سوم- چارچوب پیشنهادی برای طرح ارزیابی مخاطرات امنیتی شبکه ۹۵**
۳-۱- مقدمه ۹۵
۳-۲- مخاطرات امنیتی معماری شبکه ۹۷
۳-۲-۱- ساختار شبکه ۹۷
۳-۲-۲- ساختار آدرس‌دهی و مسیریابی شبکه ۹۹
۳-۲-۳- ساختار دسترسی به شبکه ۱۰۰
۳-۳- مخاطرات امنیتی تجهیزات شبکه ۱۰۳
۳-۴- مخاطرات امنیتی مدیریت و نگهداری شبکه ۱۰۴
۳-۴-۱- تشکیلات و روش‌های مدیریت و نگهداری ۱۰۴
۳-۴-۲- ابزارها و مکانیزم‌های مدیریت ۱۰۶
۳-۵- مخاطرات امنیتی سرویس‌های شبکه ۱۰۷
۳-۶- مخاطرات تشکیلات و روش‌های امنیت شبکه ۱۰۹

**فصل چهارم- چارچوب پیشنهادی برای طرح امنیت شبکه ۱۱۲**
۴-۱- مقدمه ۱۱۲
۴-۲- اهداف و روش‌های تامین امنیت در طرح امنیت شبکه ۱۱۳
۴-۲-۱- ساختار شبکه ۱۱۳
۴-۲-۲- اهداف طرح امنیت شبکه ۱۱۴
۴-۲-۳- روش‌های تامین امنیت در طرح امنیت شبکه ۱۱۵
۴-۳- معماری، ساختار و مشخصات سیستم امنیتی شبکه ۱۱۸
۴-۳-۱- معماری امنیت شبکه ۱۱۹
۴-۳-۲- ساختار شماتیک طرح امنیت شبکه ۱۲۳
۴-۳-۳- مشخصات فنی ابزارهای امنیت شبکه ۱۲۳
۴-۳-۴- جریان اطلاعات در طرح امنیت شبکه ۱۴۰
۴-۴- تخمین هزینه و اجرای طرح امنیت شبکه ۱۴۵
۴-۴-۱- لیست و تخمین هزینه طرح امنیت شبکه ۱۴۵
۴-۴-۲- اجرای طرح امنیت شبکه ۱۴۵

**فصل پنجم- چارچوب پیشنهادی برای طرح پشتیبانی حوادث شبکه** ۱۴۶
۵-۱- مقدمه ۱۴۶
۵-۱-۱- اهداف و ابعاد ۱۴۷
۵-۱-۲- مخاطبین ۱۴۷
۵-۱-۳- ساختار طرح ۱۴۸
۵-۲- ساختار تیم پشتیبانی حوادث ۱۴۸
۵-۲-۱- دسته‌بندی حوادث ۱۴۸
۵-۲-۲- پاسخ به حوادث ۱۴۸
۵-۲-۳- سیاست‌ها و روال‌های پشتیبانی حوادث ۱۴۹
۵-۲-۴- ساختار تیم پشتیبانی حوادث ۱۴۹
۵-۲-۵- سرویس‌های تیم پشتیبانی حوادث ۱۵۰
۵-۲-۶- توصیه‌ها ۱۵۰
۵-۳- متدولوژی پشتیبانی حوادث ۱۵۱
۵-۳-۱- آماده‌سازی ۱۵۲
۵-۳-۲- تشخیص و تحلیل حوادث ۱۵۳
۵-۳-۳- محدودسازی، ترمیم و ریشه‌کنی ۱۵۶
۵-۳-۴- فعالیت‌های بعد از ترمیم ۱۵۸
۵-۳-۵- تدوین چک‌لیست پشتیبانی حوادث ۱۶۰
۵-۳-۶- توصیه‌ها ۱۶۰
۵-۴- الگوی پشتیبانی حوادث ۱۶۰

**فصل ششم- چارچوب پیشنهادی برای برنامه آگاهی‌رسانی، تربیت نیروی انسانی و آموزش امنیت شبکه** ۱۶۲
۶-۱- مقدمه ۱۶۲
۶-۱-۱- اهداف ۱۶۲
۶-۱-۲- مخاطبین ۱۶۳
۶-۱-۳- ابعاد ۱۶۴
۶-۱-۴- سیاست ۱۶۴
۶-۱-۵- وظایف و مسئولیت‌ها ۱۶۵
۶-۲- آگاهی‌رسانی، تربیت نیروی انسانی و آموزش امنیت ۱۶۵
۶-۲-۱- آگاهی‌رسانی امنیتی ۱۶۶
۶-۲-۲- تربیت نیروی انسانی ۱۶۷
۶-۲-۳- آموزش امنیت ۱۶۷

۶-۲-۴- مقایسه ۱۶۷
۶-۳- متدولوژی آگاهی‌رسانی، تربیت نیروی انسانی و آموزش امنیت ۱۶۹
۶-۳-۱- طراحی ۱۷۰
۶-۳-۲- توسعه ۱۷۴
۶-۳-۳- پیاده‌سازی ۱۷۵
۶-۳-۴- پشتیبانی ۱۷۶

**مراجع ۱۷۹**
**عبارات اختصاری ۱۸۱**
**واژه‌نامه فارسی به انگلیسی ۱۸۲**

# پیشگفتار

بدون شک گسترش و توسعه روزافزون دو فناوری ارتباطات و اطلاعات و همگرا شدن آن‌ها، ظهور اینترنت و چندرسانه‌ها دلیل توفیقاتی است که بشر امروز، شاهد آن است و موجب نامگذاری عصر حاضر به عصر اطلاعات گردیده ولی قطعاً اگر بحث به اشتراک گذاشتن اطلاعات مطرح نبود هرگز کاربرد این فناوری‌ها عمومیت نمی‌یافت و امروز شاهد اتصال رایانه خانه‌های روستاییان دور افتاده آفریقا به اینترنت نبودیم. انبوه اطلاعات موجود در شبکه‌های عمومی خصوصاً اینترنت، موجب گشته تا آحاد مختلف مردم در گوشه و کنار دنیا راغب به عضویت در این شبکه‌ها گردند. این امکان عظیم در کنار توسعه‌های مرتبط با فناوری‌های گوناگون، منجر به شکل‌گیری جامعه نوینی شد که امروز از آن با نام **جامعه اطلاعاتی** یاد می شود.

تفاوت این عصر با سایر اعصار را بایستی در سرعت تغییرات فناوری‌ها، رشد سریع و چشم‌گیر علوم و همه این‌ها را باید مدیون دسترسی وسیع و همگانی به اطلاعات دانست. دسترسی گسترده همگان به اطلاعات، موجب شکوفایی استعدادهای نهفته گردیده و در سایه شکوفایی استعدادهاست که موفقیت‌های بشری شکل می گیرد و هر روز محصول جدیدی معرفی می شود و هر دم از این باغ بری می رسد.

هیچ کشوری جز در سایه بلوغ فکری مردم خود به توسعه پایدار و همه جانبه دست نخواهد یافت و بلوغ فکری تنها از طریق افزایش اطلاعات حاصل می‌گردد. نقش فناوری اطلاعات و ارتباطات در توسعه کشورها به عنوان ابزاری برای اشتراک اطلاعات و دسترسی همگانی به انبوه اطلاعات جهانی برکسی پوشیده نیست و بر عقلای جامعه است تا در توسعه و گسترش آن از هیچ کوششی دریغ نورزند.

کوتاه‌ترین راه برای دستیابی به توسعه و کاربرد فناوری ارتباطات واطلاعات، رفع موانع پیش روی آن است. ورود به این عرضه، بدون رویکردی نظام‌مند و تدوین معماری فناوری ارتباطات و اطلاعات و برنامه‌های مدون مبتنی بر معماری، می‌تواند کشور را با چالش‌هایی مواجه سازد که خروج از آن‌ها مشکل و گاه ناممکن خواهد بود. در کنار چالش‌های فرهنگی و اجتماعی – که جای دارد در مجالی دیگر بطور جامع مورد بحث قرارگیرد– بزرگ‌ترین چالش را می‌توان مرتبط با امنیت فضایی دانست که این فناوری‌ها ایجاد می‌کنند و ما از آن با نام **امنیت فضای تبادل اطلاعات** یاد کرده‌ایم.

امنیت فضای تبادل اطلاعات کشور به عوامل متعددی وابسته است و اقدامات مختلفی در سطح ملی و بخشی نیاز دارد که پرداختن به آن‌ها موضوع سند راهبردی امنیت فضای تبادل اطلاعات کشور است ولی به موازات ایجاد زیرساخت‌های امنیتی در سطح ملی – از قبیل نظام تایید هویت الکترونیکی(CA_PKI)، نظام تشخیص مخاطرات و مقابله با تهدیدات و ... – ایجاد **سیستم مدیریت امنیت اطلاعات** در دستگاه‌های دولتی و شرکت‌های خصوصی امری لازم و ضروری است. این مهم با بخش‌نامه معاون اول محترم رییس جمهور به کلیه دستگاه‌ها در حال شکل‌گیری است.

ایجاد و توسعه سیستم مدیریت امنیت اطلاعات در کنار توسعه و گسترش کاربرد فناوری اطلاعات در شرکت‌های خصوصی، وزارتخانه‌های مختلف، سازمان‌ها، موسسات و نهادهای انقلابی موجب خواهد شد کشور با آمادگی بیشتری وارد جامعه اطلاعاتی شود. رویکردی نظام‌مند در این حوزه نیز ضرورت استفاده از استانداردها را مورد تاکید قرار می‌دهد.

استانداردی که برای این منظور انتخاب شده است، استانداردی انگلیسی تحت عنوان BS7799 است. اولین نسخه این استاندارد در سال ۱۹۹۵ میلادی معرفی و در سال ۲۰۰۰ میلادی موسسه‌ی بین‌المللی استاندارد (ISO) بخش اول آن را تحت استاندارد ISO/IEC17799 ارایه کرد. نسخه ۲۰۰۰ این استاندارد به همت دبیرخانه شورای‌عالی انفورماتیک ترجمه، تدوین و به تصویب موسسه استاندارد کشورمان رسید. البته اطلاعات بسیار مهمی در بخش دوم استاندارد وجود دارد که استاندارد ISO از آن بی‌بهره است.

استاندارد BS7799 از جامعیت مناسبی برخوردار است و از معرفی بخش‌های مختلف سازمان مورد نیاز و جایگاه آن در ساختار تشکیلاتی، اقدامات مورد نیاز در سطوح فیزیکی تا ابعاد فنی و تخصصی آن را پیشنهاد نموده است.

این مجموعه سعی کرده است با استفاده از این استاندارد و مطالعه استانداردهای گوناگون دیگر در زمینه سیستم مدیریت امنیت اطلاعات، گزارش‌های فنی با عنوان TR 13335 ، راهنماها و دستورالعمل‌های مختلف، روش پیاده سازی استاندارد انتخابی را معرفی نماید.

در انتها بر خود لازم می دانم از زحمات کلیه دوستان و همکارانی که در بررسی و ویرایش این مجموعه مسئولیتی به عهده داشته‌اند خصوصاً تلاش‌های جناب آقای مهندس خالقی در مطالعه تهیه و تنظیم مجموعه حاضر، تشکر و قدردانی نمایم.

مجتبی جعفری
رئیس مرکز فناوری اطلاعات ریاست جمهوری
و دبیر شورای عالی امنیت فضای تبادل اطلاعات کشور

# مقدمه

حرکت سریع کشورها به سوی جامعه اطلاعاتی، موجب رشد وسیع سیستم‌ها و سرویس‌های اطلاعاتی شده است. در این شرایط، بخش وسیعی از خدمات در همین بستر ارائه شده و ارائه‌دهندگان و دریافت‌کنندگان خدمات را ناگزیر از پیوستن به این جامعه نموده است.

اطلاعات، گنجینه‌ای که تا چندی قبل در کمدها و پستوهای سازمان‌ها نگهداری می‌شد، از چند سال قبل و با توسعه شبکه‌های محلی درون سازمانی، به شبکه داخلی سازمان‌ها راه یافت. در آن زمان، اطلاعات محدود کاربران شبکه و اعمال کنترل‌های مدیریتی، محافظت‌های فیزیکی و محدود نمودن تعداد افرادی که به سرویس‌ها و بویژه سرویس‌های حساس دسترسی داشتند، موجب می‌شد تا مشکل خاصی بروز نکند. اما اینک با اتصال شبکه‌های سازمانی به شبکه جهانی، همان گنجینه حساس در معرض دید و استفاده طیف وسیعی از مخاطبین در سراسر جهان قرار گرفته است. مخاطبینی که مجهز به انواع اطلاعات و ابزارهای اطلاعاتی می‌باشند. البته تهدید فقط از سوی مخاطبین خارج از سازمان نیست. بررسی‌های انجام شده نشان می‌دهد که امروزه عمده تهدیدهای موجود علیه اطلاعات و سیستم‌های اطلاعاتی سازمان‌ها، منشاء داخلی داشته و خواسته یا ناخواسته توسط پرسنل سازمان ایجاد می‌شود.

در این شرایط، تامین امنیت همان گنجینه گران‌مایه یعنی اطلاعات، بدون شک یکی از ضروریات هر سازمانی است. حاصل تجربه و اقدامات انجام شده در طول یک دهه گذشته در جهان، رویکردی است تحت عنوان سیستم مدیریت امنیت اطلاعات.

بر اساس این رویکرد که در فصل اول، تشریح و استانداردهای مدیریتی و فنی آن ارائه شده است، سازمان‌ها به منظور تامین امنیت اطلاعات خود، باید مجموعه‌ای از اقدامات پیش‌گیرانه و تدافعی را بصورت مداوم و در چرخه‌ای تحت عنوان چرخه امنیت انجام دهند.

در فصل دوم، ضمن تشریح اولین گام از چرخه امنیت، یعنی تعیین سیاست‌های امنیت اطلاعات سازمان، چارچوب پیشنهادی برای تدوین اهداف، راهبردها و سیاست‌های امنیتی برگرفته شده از استانداردهای فوق، ارائه شده است.

در فصل سوم، نحوه ارزیابی امنیتی شبکه سازمان و تدوین طرح ارزیابی امنیتی، بر اساس استانداردهای فوق و مستندات ارائه شده توسط موسسه استاندارد و فن‌آوری ملی امریکا، آمده است.

فصل چهارم، ساختار و نحوه تدوین طرح امنیت شبکه سازمان را تشریح می‌کند. در فصل پنجم، ساختار پیشنهادی برای طرح پشتیبانی حوادث امنیتی، بر اساس متدولوژی ارائه شده توسط موسسه استاندارد و فن‌آوری ملی امریکا، تشریح شده است و فصل ششم، نحوه تدوین و اجرای برنامه آگاهی‌رسانی، تربیت نیروی انسانی و آموزش امنیت سازمان را ارائه نموده است.

**محمود خالقی**
**پاییز ۱۳۸۳**

# ۱

# سیستم مدیریت امنیت اطلاعات (ISMS)

## ۱-۱- مقدمه

با ارائه اولین استاندارد مدیریت امنیت اطلاعات در سال ۱۹۹۵، نگرش سیستماتیک به مقوله امنیت اطلاعات شکل گرفت. بر اساس این نگرش، تامین امنیت اطلاعات در یک مجموعه سازمانی، دفعتا مقدور نمی‌باشد و لازم است این امر بصورت مداوم و در یک چرخه ایمن‌سازی شامل مراحل طراحی، پیاده‌سازی، ارزیابی و اصلاح، انجام گیرد. برای این منظور لازم است هر سازمان بر اساس یک متدولوژی مشخص، ضمن تهیه طرح‌ها و برنامه‌های امنیتی موردنیاز، تشکیلات لازم جهت ایجاد و تداوم امنیت اطلاعات خود را نیز ایجاد نماید.

در این فصل، ابتدا مروری بر استاندارد مدیریتی BS7799 موسسه استاندارد انگلیس، استاندارد مدیریتی ISO/IEC 17799 و گزارش فنی ISO/IEC TR 13335 موسسه بین‌المللی استاندارد ارائه شده و در خاتمه بعنوان نتیجه‌گیری، لیست طرح‌ها و برنامه‌های امنیتی و ساختار تشکیلات امنیت فن‌آوری اطلاعات موردنیاز هر سازمان، ارائه شده است. مطالب این فصل، مروری بر مطالب ارائه شده در مراجع ۱ تا ۹ می‌باشد.

## ۱-۲- استانداردهای مدیریت امنیت اطلاعات

در حال حاضر، مجموعه‌ای از استانداردهای مدیریتی و فنی امنیت اطلاعات و ارتباطات، ارائه شده‌اند که استاندارد مدیریتی BS7799 موسسه استاندارد

انگلیس، استاندارد مدیریتی ISO/IEC 17799 و گزارش فنی ISO/IEC TR 13335 موسسه بین‌المللی استاندارد، از برجسته‌ترین استانداردها و راهنماهای فنی محسوب می‌گردند. در این استانداردها، نکات زیر مورد توجه قرار گرفته شده است:

- تعیین مراحل ایمن‌سازی و نحوه شکل‌گیری چرخه امنیت
- جزئیات مراحل ایمن‌سازی و تکنیکهای فنی مورد استفاده در هر مرحله
- لیست و محتوای طرح‌ها و برنامه‌های امنیت اطلاعات موردنیاز سازمان
- ضرورت و جزئیات ایجاد تشکیلات سیاستگذاری، اجرائی و فنی تامین امنیت
- کنترل‌های امنیتی موردنیاز برای هر یک از سیستم‌های اطلاعاتی و ارتباطی

### ۱-۲-۱- استاندارد BS7799

استاندراد BS7799 اولین استاندارد مدیریت امنیت اطلاعات است که توسط موسسه استاندارد انگلیس ارائه شده است. نسخه اول این استاندارد (BS7799:1) در سال ۱۹۹۵ و در یک بخش منتشر شد و نسخه دوم آن (BS7799:2) که در سال ۱۹۹۹ ارائه شد، علاوه بر تغییر نسبت به نسخه اول، در دو بخش مستقل ارائه گردید. همچنین آخرین نسخه این استاندارد، (BS7799:2002) در سال ۲۰۰۲ و همانند نسخه دوم، در دو بخش منتشر گردید.

این استاندارد در حال حاضر بصورت فراگیر در سطح جهان مورد استفاده قرار می‌گیرد و بر اساس آمار منتشر شده در سایت گروه کاربران بین‌المللی سیستم مدیریت امنیت اطلاعات (ISMS IUG) تا انتهای اکتبر سال ۲۰۰۴، مجموعا تعداد ۹۱۵ سازمان در سطح جهان، موفق به اجرای ISMS بر اساس این استاندارد و اخذ تائیدیه از مراکز صدور گواهی مبتنی بر این استاندارد شده‌اند. این در حالی است که بر اساس آمار همین سایت، تا انتهای جولای ۲۰۰۴، تعداد سازمان‌های فوق مجموعا ۸۰۸ مورد و در انتهای اکتبر ۲۰۰۳، ۳۸۸ مورد بوده است.

**بخش اول استاندارد BS7799:2 1999:**

در بخش اول این استاندارد، که تحت عنوان "آئین‌نامه کار مدیریت امنیت اطلاعات" ارائه شده است، مجموعه کنترل‌های امنیتی موردنیاز سیستم‌های اطلاعاتی و ارتباطی هر سازمان، در قالب ده دسته‌بندی کلی شامل موارد زیر، ارائه شده است:

۱- تدوین سیاست امنیتی سازمان

در این بخش، ضرورت تدوین و اعلام سیاست امنیت اطلاعات سازمان و مشخصات موردنیاز برای چنین سیاستی ارائه شده است.

۲- تشکیلات امنیت

در این بخش، نکاتی در خصوص موضوعات زیرساخت امنیت اطلاعات در سازمان، امنیت دسترسی شخص ثالث و واگذاری فعالیت‌ها به خارج از سازمان ارائه شده است.

در موضوع زیرساخت امنیت اطلاعات سازمان، نکاتی در خصوص ضرورت تشکیل مجمع مدیریت امنیت اطلاعات، تعیین هماهنگ‌کننده امنیت اطلاعات، مسئولیت‌ها و اختیارات مرتبطین با امنیت اطلاعات و همکاری اجزاء درگیر در تامین امنیت اطلاعات سازمان با یکدیگر، ارائه شده است. در خصوص امنیت دسترسی شخص ثالث، شناسائی ریسک دسترسی شخص ثالث از طریق تعیین انواع دسترسی‌ها، اهداف دسترسی‌ها، پرسنل قراردادی و نیازهای امنیتی که باید در قراردادهای شخص ثالث مورد توجه قرار گیرند، ارائه شده است.در خصوص واگذاری فعالیت‌ها به خارج از سازمان نیز ملاحظاتی که باید در قراردادها مورد توجه قرار گیرند، ارائه شده است.

۳- طبقه‌بندی سرمایه‌ها و تعیین کنترل‌های لازم

در این بخش، مواردی در خصوص ضرورت شناسائی و تهیه لیست از کلیه سرمایه‌های سازمان و ضرورت و نحوه طبقه‌بندی اطلاعات سازمان، ارائه شده است.

٤- امنیت پرسنلی

در این بخش، نکاتی در خصوص موضوعات امنیت در تعریف کار پرسنل، آموزش کاربران و پاسخ‌گویی به حوادث امنیتی و ضعف عملکرد، ارائه شده است.

در خصوص امنیت در تعریف کار پرسنل، نکاتی در خصوص ملاحظات امنیتی در مسئولیت‌های کاری پرسنل، آزمایش پرسنل قبل از بکارگیری، محرمانگی پیمان، دوره انتصاب و شرایط پرسنل ارائه شده است.

در خصوص آموزش کاربران، ضرورت ارائه آموزش به کلیه کاربران در زمینه امنیت اطلاعات اشاره شده است.

در خصوص پاسخ‌گویی به حوادث امنیتی و ضعف عملکرد، نکاتی در خصوص گزارش نمودن حوادث، ضعف‌ها و عملکرد اشتباه نرم‌افزارها، درس گرفتن از حوادث و وجود روندهای انضباطی برای پرسنل ارائه شده است.

٥- امنیت فیزیکی و پیرامونی

در این بخش، نکاتی در خصوص موضوعات محیطهای امن، امنیت تجهیزات و کنترل‌های عمومی ، ارائه شده است.

در خصوص محیط‌های امن، نکاتی در خصوص امنیتی فیزیکی، کنترل مدخل‌های فیزیکی، ایمن‌سازی دفاتر، اطاق‌ها و وسایل، ملاحظات کار در محیط امن و ضرورت ایزوله نمودن محیطهای تحویل و بارگیری از محیطهای اطلاعاتی سازمان ارائه شده است.

در خصوص امنیت تجهیزات، نکاتی در خصوص قراردادن تجهیزات در سایت و ایمن‌سازی سایت، منابع تغذیه، امنیت کابل‌کشی، نگهداری تجهیزات و امنیت تجهیزات با قابلیت کاربرد مجدد ارائه شده است.

در خصوص کنترل‌های عمومی، مواردی از قبیل سیاست میز خالی، سیاست صفحه نمایش خالی و تغییر خصوصیات سیستم‌ها ارائه شده است.

٦- مدیریت ارتباطات و بهره‌برداری

در این بخش، نکاتی در خصوص موضوعات رویه‌ها و مسئولیت‌های بهره‌برداری، طراحی و پذیرش سیستم، محافظت در برابر نرم‌افزارهای مخرب، عملیات روزمره پشتیبانی، امنیت در مدیریت شبکه، امنیت در پشتیبانی رسانه‌ها، مبادله اطلاعات و نرم‌افزارها، ارائه شده است.

در خصوص رویه‌ها و مسئولیت‌های بهره‌برداری، نکاتی در خصوص ضرورت مستندسازی عملکرد، کنترل موثر تغییرات، رویه‌های مدیریت حوادث، تفکیک ماموریت‌ها، جداسازی امکانات توسعه، تست و بهره‌برداری سیستم‌ها و مدیریت امکانات خارج از سازمان ارائه شده است.

در خصوص امنیت در پشتیبانی رسانه‌ها، نکاتی در خصوص مدیریت رسانه‌های متحرک کامپیوتر، در اختیار قرار دادن رسانه‌ها و رویه‌های پشتیبانی حوادث ارائه شده است.

در خصوص مبادله اطلاعات و نرم‌افزارها، نکاتی در خصوص پیمان مبادله اطلاعات و نرم‌افزار، امنیت رسانه در انتقال، امنیت تجارت الکترونیک، امنیت پست الکترونیک، امنیت سیستم‌های اتوماسیون اداری و سیستم‌های در دسترس عموم ارائه شده است.

۷- کنترل دسترسی

در این بخش، نکاتی در خصوص موضوعات نیازهای تجاری برای کنترل دسترسی، مدیریت دسترسی کاربران، مسئولیت کاربران، کنترل دسترسی شبکه، کنترل دسترسی در سیستم عامل، کنترل دسترسی نرم‌افزارهای کاربردی، نظارت بر استفاده و دستیابی سیستم و پردازش متحرک و کار از راه دور، ارائه شده است.

در خصوص مسئولیت کاربران، نکاتی در خصوص ثبت کاربران، مدیریت اختیارات، مدیریت رمز عبور و مروز دسترسی‌های واقعی کاربران ارائه شده است.

در خصوص کنترل دسترسی شبکه، نکاتی در خصوص تصدیق هویت کاربر و ایستگاه، کنترل اتصالات و مسیریابی شبکه، امنیت در سرویس‌های شبکه ارائه شده است.

۸- توسعه و پشتیبانی سیستم‌ها

در این بخش، نکاتی در خصوص موضوعات نیازهای امنیتی سیستم‌ها، امنیت در سیستم‌های کاربردی، کنترل‌های مبتنی بر رمزنگاری، امنیت در فایل‌های سیستم و امنیت در فرآیند توسعه و پشتیبانی، ارائه شده است.

در خصوص امنیت در سیستم‌های کاربردی، نکاتی در خصوص اعتبار سنجی اطلاعات ورودی و خروجی و کنترل پروسه داخلی سیستم، ارائه شده است.

در خصوص امنیت در فرآیند توسعه و پشتیبانی، نکاتی در خصوص رویه‌های کنترل تغییرات، مرور فنی تغییرات و محدودسازی تغییرات ارائه شده است.

۹- مدیریت تداوم فعالیت

در این بخش، نکاتی در خصوص موضوعات فرآیند مدیریت تداوم فعالیت، آنالیز تداوم فعالیت، تدوین و پیاده‌سازی برنامه‌های تداوم فعالیت، گروه کاری تداوم فعالیت و آزمایش، نگهداری و ارزیابی برنامه‌های تداوم فعالیت، ارائه شده است.

۱۰- سازگاری

در این بخش، نکاتی در خصوص موضوعات سازگاری با قانون، مرور سیاست حفاظتی و سازگاری فنی و ملاحظات بازرسی و کنترل سیستم، ارائه شده است.

**بخش دوم استاندارد BS7799:2 1999:**

در این بخش از استاندارد که تحت عنوان "ویژگی‌های سیستم مدیریت امنیت اطلاعات" ارائه شده است، ضمن تاکید بر ضرورت ایجاد سیستم مدیریت امنیت اطلاعات ، نیازهای سیستم مدیریت امنیت اطلاعات و کنترل‌های همه‌جانبه که برای تامین امنیت اطلاعات، مورد نیاز می‌باشند، ارائه شده است.

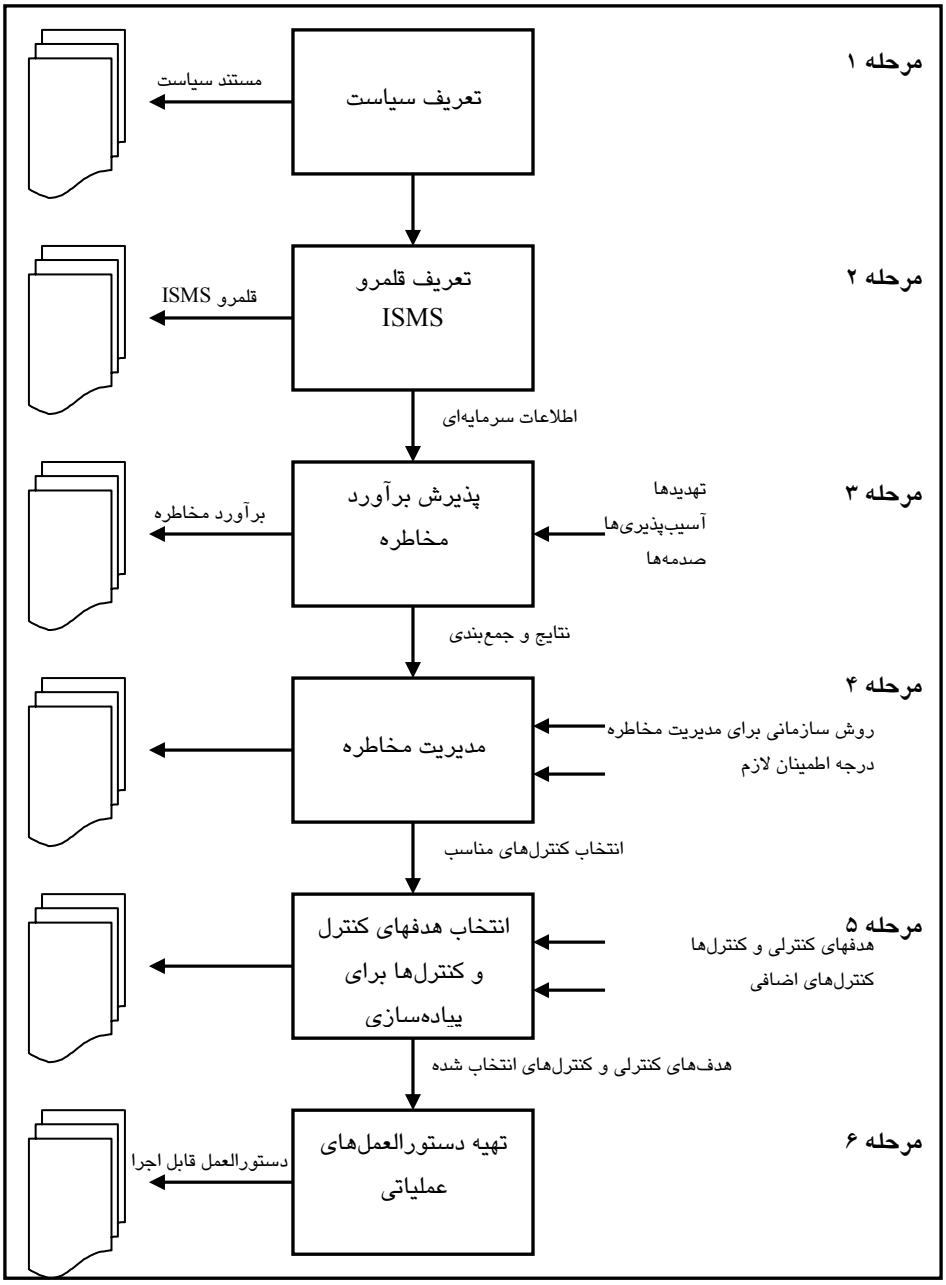
۱- نیازهای سیستم مدیریت امنیت اطلاعات

در این قسمت تاکید شده که هر سازمان، باید سیستم مدیریت امنیت اطلاعات خود را مستند، تعریف، ایجاد و نگهداری نماید. در چارچوب مدیریتی ارائه شده در این بخش از استاندارد، که در شکل (۱-۱) ارائه شده است، لازم است مراحل شش‌گانه زیر برای مدیریت امنیت اطلاعات در نظر گرفته شده باشند:

- تعریف سیاست امنیت اطلاعات
- تعریف قلمرو سیستم مدیریت امنیت اطلاعات و مرزبندی آن، متناسب با نوع و نیازهای سازمان
- انجام و پذیرش برآورد مخاطرات، متناسب با نوع و نیازهای سازمان
- پیش‌بینی زمینه‌ها و نوع مخاطرات، بر اساس سیاست‌های امنیتی
- انتخاب هدف‌های کنترل و کنترل‌های مناسب که قابل توجیه باشند، از لیست کنترل‌های همه‌جانبه
- تدوین دستوالعمل‌های عملیاتی

۲- کنترل‌های همه‌جانبه

در این قسمت، لیست کلیه کنترل‌های ارائه شده در بخش اول این استاندارد، هدف از اعمال این کنترل و توضیح مختصری پیرامون آن، ارائه شده است.




شکل (۱-۱) : ایجاد چارچوب مدیریت امنیت اطلاعات [۹]

### ۱-۲-۲- استاندارد ISO/IEC 17799

در سال ۲۰۰۰ ، بخش اول استاندارد BS7799:2 بدون هیچگونه تغییری توسط موسسهٔ بین المللی استاندارد بعنوان استاندارد ISO/IEC 17799 منتشر شد.

### ۱-۲-۳- گزارش فنی ISO/IEC TR 13335

این گزارش فنی در قالب ۵ بخش مستقل در فواصل سالهای ۱۹۹۶ تا ۲۰۰۱ توسط موسسهٔ بین المللی استاندارد منتشر شده است . اگر چه این گزارش فنی به عنوان استاندارد ISO منتشر نشد و عنوان Technical Report بر آن نهاده شد، لیکن تنها مستندات فنی معتبری است که جزئیات و تکنیکهای مورد نیاز مراحل ایمن سازی اطلاعات و ارتباطات را تشریح نموده و کنترل‌های موردنیاز برای محافظت فیزیکی و لاجیکی برای سیستم‌های فن‌آوری اطلاعات را با دقت تشریح نموده است. این گزارش فنی، مکمل استانداردهای مدیریتی BS7799 و ISO/IEC 17799 محسوب شده و در پیاده‌سازی سیستم مدیریت امنیت اطلاعات، کاربرد زیادی دارد. در این قسمت، مروری بر بخش‌های مختلف این گزارش فنی، ارائه شده است.

### بخش اول ISO/IEC TR 13335:

بخش اول گزارش فنی شماره ISO/IEC TR 13335 در سال ۱۹۹۶ تحت عنوان "مفاهیم و مدل ها برای امنیت فن آوری اطلاعات" منتشر شد. در این بخش، پس از بیان تعاریف و ساختارهای اولیه، در قسمتی تحت عنوان "مفاهیم مدیریت امنیت فن‌آوری اطلاعات"، اهداف، راهبردها و سیاست‌های امنیت فن‌آوری اطلاعات، تشریح شده است. در ادامه و تحت عنوان "عناصر امنیت"، به مفاهیمی از قبیل سرمایه، تهدید، آسیب پذیری، ریسک، ضربه، حفاظ، ریسک باقیمانده و فشار، پرداخته شده و تعریف و مصادیق آنها در فن آوری اطلاعات ارائه شده است. در ادامه و تحت عنوان "فرآیند مدیریت امنیت فن‌آوری اطلاعات"، به

ضرورت و جایگاه مدیریت پیکربندی، مدیریت تغییرات، مدیریت مخاطره، آنالیز مخاطره، پاسخ‌گویی، آگاهی‌رسانی امنیتی، نظارت و طرح‌های پشتیبانی حوادث و ترمیم خرابی در این فرآیند تشریح شده است. در خاتمه، روابط بین عناصر امنیت و جایگاه آنها در فرآیند مدیریت ریسک ارائه شده است.

**بخش دوم ISO/IEC TR 13335:**

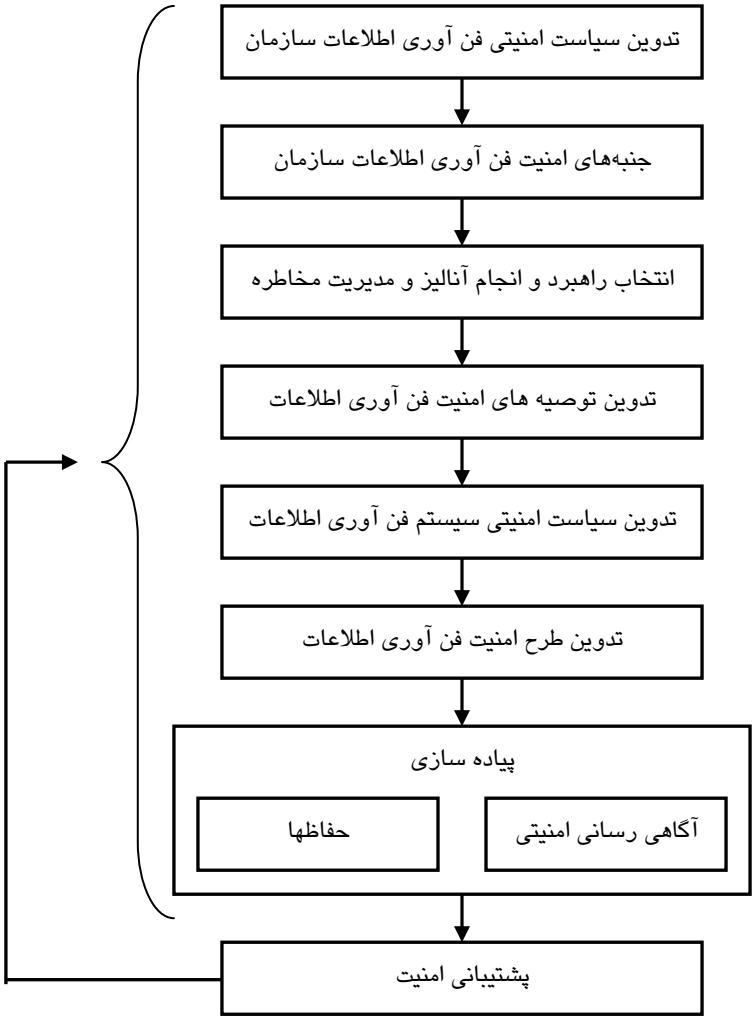
بخش دوم گزارش فنی شماره ISO/IEC TR 13335 در سال ۱۹۹۷ تحت عنوان "مدیریت و طراحی امنیت فن آوری اطلاعات" منتشر شد. در این بخش، پس از بیان تعاریف و ساختارهای اولیه، مواردی به شرح زیر ارائه شده است:

۱- مدیریت امنیت فن آوری اطلاعات

ابتدا مراحل فرآیند طراحی و مدیریت امنیت فن آوری اطلاعات، مطابق شکل (۱-۲) ارائه شده و در ادامه هر یک از این مراحل تشریح شده است.

۲- سیاست امنیتی سازمان

سیاست امنیتی فن آوری اطلاعات سازمان تشریح شده و ارتباط آن با سیاست های بالادستی سازمان، شامل سیاست فروش سازمان، سیاست امنیتی سازمان و سیاست فن آوری اطلاعات سازمان و سیاست های پایین دستی از قبیل سیاست امنیتی فن آوری اطلاعات ادارات سازمان و سیاست امنیتی سیستم های فن آوری اطلاعات، نشان داده شده است..




شکل (۱-۲) : فرآیند طراحی و مدیریت امنیت فن آوری اطلاعات [۵]

۳- تشکیلات سازمانی امنیت فن آوری اطلاعات

ساختار تشکیلات امنیت فن آوری اطلاعات سازمان ارائـه شـده و وظـایف و مسئولیت های هر یک از اجزاء این تشکیلات تشریح شده است.

۴- گزینه‌های قابل انتخاب برای راهبرد آنالیز ریسک سازمان

گزینه‌های قابل انتخاب بعنوان راهبرد آنالیز ریسک سازمان، شامل روش پایه، روش غیررسمی، روش تفصیلی و روش ترکیبی به همراه مزایا و معایب هر یک، تشریح شده است.

۵- توصیه‌های امنیت فن‌آوری اطلاعات

متناسب با روش انتخابی برای آنالیز ریسک سازمان، لازم است تعدادی توصیه امنیتی با هدف کاهش ریسک سیستم‌های اطلاعاتی، تهیه و ارائه گردد. در این قسمت، لیست و توضیحات این توصیه‌ها ارائه شده است.

۶- سیاست امنیتی سیستم‌های فن‌آوری اطلاعات

ضمن تشریح مشخصات سیاست امنیتی سیستم‌های فن‌آوری اطلاعات، نحوه استخراج این سیاست از سیاست امنیتی فن‌آوری اطلاعات سازمان و سیاست امنیتی فن‌آوری اطلاعات اداره مربوطه ارائه شده است.

۷- طرح امنیت فن‌آوری اطلاعات

مشخصات طرح امنیت فن‌آوری اطلاعات در این قسمت شده است.

۸- پیاده‌سازی حفاظها

مدیر امنیت فن‌آوری اطلاعات سازمان بعنوان مسئول اجرای طرح امنیت فن‌آوری اطلاعات سازمان معرفی شده و مراحل اجرای طرح نیز بیان شده است.

۹- آگاهی‌رسانی امنیتی

ضرورت تدوین برنامه آگاهی‌رسانی امنیتی برای کلیه کاربران سازمان تشریح شده، ارتباط این برنامه با سیاست امنیتی فن‌آوری اطلاعات سازمان

و طرح امنیت سیستم‌های فن‌آوری اطلاعـات، بیـان و حـداقل محورهـایی کـه برنامه آگاهی‌رسانی امنیتی سازمان باید پوشش دهد، ارائه شده است.

۱۰-پشتیبانی امنیتی

به منظور تامین تداوم امنیت فن‌آوری اطلاعات سازمان، لازم است تشـکیلات امنیت فن‌آوری اطلاعات سازمان، عملیات پشتیبانی از حفاظهای پیـاده‌سـازی شده در مرحله اجرای طرح امنیت را بر عهده گیرد. در این قسمت از گـزارش فنی، ضمن معرفی "نگهداری از سیستم امنیتی"، "بررسـی سـازگاری امنیتـی"، "نظارت"، "پشتیبانی حـوادث" و "مـدیریت تغییـرات" بعنـوان اجـزاء پشـتیبانی امنیتی معرفی و تشریح شده‌اند.

از مجموعه مباحث مطرح شده در قسمت "تشکیلات سازمانی امنیـت فـن‌آوری اطلاعات" و قسمت "پشتیبانی امنیتی" از بخـش دوم گـزارش فنـی ISO/IEC TR 13335، اینگونه برداشت می‌شود که تشکیلات امنیت فن‌آوری اطلاعات سازمان، باید شامل اجزاء زیر باشد:

۱- مجمع امنیت فن‌آوری اطلاعات سازمان
۲- مدیر امنیت فن‌آوری اطلاعات سازمان
۳- مدیران امنیت فن‌آوری اطلاعات ادارات
۴- مدیران امنیت سیستم‌های فن‌آوری اطلاعات
۵- تیم پشتیبانی امنیت فن‌آوری اطلاعات سازمان، شامل:
- نگهداری از سیستم امنیتی
- بررسی سازگاری امنیتی
- نظارت
- پشتیبانی حوادث
- مدیریت تغییرات

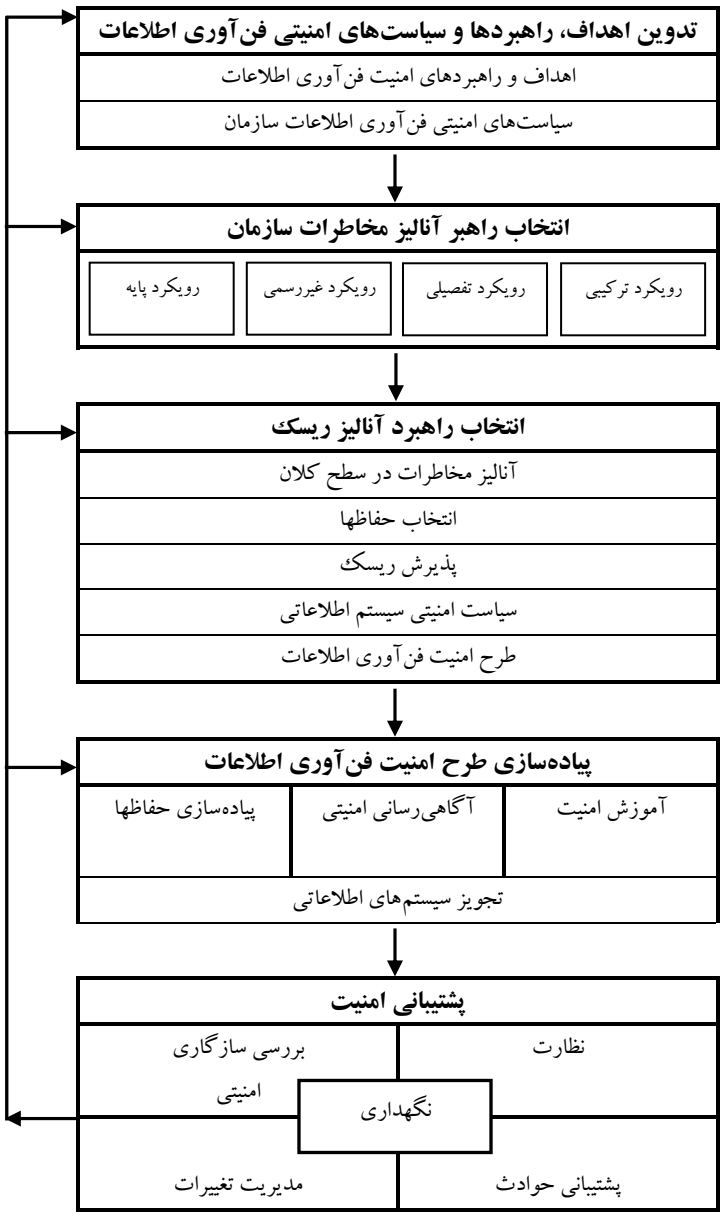
**بخش سوم ISO/IEC TR 13335:**

بخش سوم گزارش فنی شماره ISO/IEC TR 13335 در سال ۱۹۹۸ تحت عنوان "تکنیک‌هایی برای مدیریت امنیت فن‌آوری اطلاعات" منتشر شد. در این بخش، پس از بیان تعاریف و ساختارهای اولیه، مواردی به شرح زیر ارائه شده است:

۱- تکنیک‌هایی برای مدیریت امنیت فن‌آوری اطلاعات

محتوای این قسمت از گزارش فنی، فرآیند مدیریت امنیت فن‌آوری اطلاعات را مطابق شکل (۱-۳)، معرفی نموده است. بر اساس محتوای این قسمت از بخش سوم گزارش فنی ISO/IEC TR 13335، چرخه امنیت، شامل مراحلی به شرح زیر می‌باشد:

- تدوین اهداف،راهبردها و سیاست‌های امنیتی فن‌آوری اطلاعات سازمان
- انتخاب راهبرد آنالیز مخاطرات سازمان
- طراحی امنیت فن‌آوری اطلاعات، شامل:
  - انجام آنالیز مخاطرات بر اساس راهبر انتخاب شده
  - انتخاب حفاظها
  - پذیرش ریسک
  - تدوین سیاست امنیتی سیستم‌های فن‌آوری اطلاعات
  - ارائه طرح امنیت فن‌آوری اطلاعات
- پیاده‌سازی طرح امنیت فن‌آوری اطلاعات، شامل:
  - پیاده‌سازی حفاظها
  - آگاهی‌رسانی امنیتی
  - آموزش امنیت فن‌آوری اطلاعات
- پشتیبانی امنیتی، شامل:
  - نگهداری از سیستم امنیتی
  - بررسی سازگاری امنیتی
  - نظارت
  - پشتیبانی حوادث
  - مدیریت تغییرات




شکل (۱-۳) : مدیریت امنیت فن آوری اطلاعات [۶]

۲- اهداف، راهبردها و سیاست‌های امنیتی فن‌آوری اطلاعات

محتوای این قسمت از گزارش فنی، ضمن تبیین ضرورت و جایگاه اهداف، راهبردها و سیاست‌های امنیتی فن‌آوری اطلاعات سازمان، محورهای اصلی که باید پوشش داده شوند، تشریح شده است.

۳- انتخاب راهبرد آنالیز مخاطرات امنیتی

محتوای این قسمت از گزارش فنی، رویکردهای قابل انتخاب بعنوان راهبرد آنالیز مخاطرات امنیتی سازمان، شامل رویکرد پایه، غیررسمی، تفصیلی و ترکیبی، را تشریح نموده است.

۴- رویکرد ترکیبی

محتوای این قسمت از گزارش فنی، "رویکرد ترکیبی" را بعنوان پیچیده‌ترین رویکرد قابل انتخاب در آنالیز مخاطرات سازمان، را تشریح نموده است. در این رویکرد، ابتدا آنالیز مخاطرات در سطح کلان انجام می‌گیرد. در خاتمه این مرحله، باید مشخص شود که برای آنالیز مخاطرات هر یک از سیستم‌های اطلاعاتی موجود در سازمان، کدام یک از رویکردهای پایه یا تفصیلی مناسب‌تر است. در ادامه بر اساس رویکرد مناسب، برای هر یک از سیستم‌های اطلاعاتی، تحلیل مخاطره انجام خواهد شد.

در ادامه و پس از خاتمه تحلیل مخاطرات امنیتی، حفاظهای موردنیاز برای هر یک از سیستم‌های اطلاعاتی سازمان، تعیین خواهد شد.

با توجه به اینکه ایجاد امنیت مطلق امکان‌پذیر نمی‌باشد، پس از تعیین حفاظهای هر یک از سیستم‌های اطلاعاتی، میزان ریسک باقیمانده برای سیستم، مشخص خواهد شد. برای این‌که بتوان طرح امنیت را بر اساس حفاظهای تعیین شده ارائه نمود، میزان ریسک باقیمانده باید بر اساس سیاست‌های حاکم بر سازمان، در حیطه ریسک قابل پذیرش قرار داشته باشد.

در ادامه، باید سیاست امنیتی سیستم‌های اطلاعاتی سازمان، تدوین و در خاتمه، طرح امنیت فن‌آوری اطلاعات سازمان، ارائه گردد.

۵- پیاده سازی طرح امنیت فن‌آوری اطلاعات

به منظور پیاده‌سازی طرح امنیت فن‌آوری اطلاعات سازمان، لازم است موارد ذیل، به موازات پی‌گیری شوند:

- پیاده‌سازی حفاظها
- آگاهی‌رسانی امنیتی
- آموزش امنیت فن‌آوری اطلاعات

لذا در این قسمت از گزارش فنی، به تشریح نحوه پیاده‌سازی هر یک از موارد فوق، پرداخته شده است.

۶- پشتیبانی امنیت

به منظور پشتیبانی امنیت فن‌آوری اطلاعات سازمان، لازم است عملیات زیر، انجام گیرند:

- نگهداری از سیستم امنیتی
- بررسی سازگاری امنیتی
- نظارت
- پشتیبانی حوادث
- مدیریت تغییرات

لذا در این قسمت از گزارش فنی، به تشریح جزئیات هر یک از موارد فوق، پرداخته شده است.

در خاتمه بخش سوم گزارش فنی ISO/IEC TR 13335، ضمیمه‌های زیر، ارائه شده است:

ضمیمه (۱): لیست محورهای سیاست امنیتی فن‌آوری اطلاعات سازمان

ضمیمه (۲): راهنمای تعیین ارزش سرمایه‌های اطلاعاتی سازمان
ضمیمه (۳): لیست انواع تهدیدهای ممکن در حوزه فن‌آوری اطلاعات
ضمیمه (۴): نمونه‌هایی از آسیب‌پذیری‌های مشترک در حوزه زیرساخت شبکه، سخت‌افزارها، نرم‌افزارها، ارتباطات، مستندات، پرسنل و حوزه عمومی
ضمیمه (۵): انواع روش‌های آنالیز مخاطره

**بخش چهارم ISO/IEC TR 13335:**

بخش چهارم گزارش فنی شماره ISO/IEC TR 13335 در سال ۲۰۰۰ تحت عنوان "انتخاب حفاظها" منتشر شد. در این بخش، پس از بیان تعاریف و ساختارهای اولیه، مواردی به شرح زیر ارائه شده است:

۱- مقدمه‌ای بر انتخاب حفاظ و مفهوم امنیت پایه
محتوای این قسمت از گزارش فنی، ضمن تشریح روش‌های کلی انتخاب حفظها، رویکردهای مختلف انتخاب حفاظ را بیان نموده است.

۲- ارزیابی‌های مقدماتی
محتوای این قسمت از گزارش فنی، اقدامات و ارزیابی‌هایی که قبل از انتخاب حفاظ باید انجام گیرد را مشخص نموده است. بر اساس محتوای ارائه شده، شناسایی نوع سیستم اطلاعاتی موردنظر، شناسایی شرایط فیزیکی و پیرامونی و ارزیابی حفاظهای موجود یا طراحی شده برای سیستم اطلاعاتی موردنظر، از جمله مواردی هستند که باید در این مرحله مورد بررسی و ارزیابی قرار گیرند.

۳- حفاظها
محتوای این قسمت از گزارش فنی، به معرفی حفاظهایی می‌پردازد که برای تامین امنیت، می‌توانند مورد استفاده قرار گیرند. برای این منظور، ابتدا

حفاظها را به دو دسته "حفاظهای فیزیکی و سازمانی" و "حفاظهای خاص سیستم‌های اطلاعاتی" تقسیم نموده و در ادامه، برای هر یک از محورهای فوق، موارد زیر را ارائه نموده است:

- حفاظهای فیزیکی و سازمانی

در این مبحث، نقش سیاست امنیتی فن‌آوری اطلاعات سازمان، سیاست امنیتی سیستم‌های اطلاعاتی، مدیریت امنیت فن‌آوری اطلاعات، تدوین مسئولیت‌ها، تشکیلات امنیت فن‌آوری اطلاعات سازمان، شناسایی و ارزش‌گزاری سرمایه‌ها، بررسی سازگاری امنیتی، پشتیبانی حوادث، آگاهی‌رسانی و آموزش امنیت، مدیریت پیکربندی و تغییرات، مستندسازی، نگهداری، نظارت، ارزیابی و تست امنیتی و طرح تداوم فعالیت، بعنوان حفاظهای سازمانی و نقش محافظت فیزیکی از اجسام و محیطها در مقابل دسترسی فیزیکی، محافظت در مقابل آتش، آب، حوادث طبیعی، دزدی و برق، جریان سالم هوا و کابل‌کشی بعنوان حفاظهای فیزیکی تشریح شده و در ادامه، مراجع موجود در خصوص هر یک از حفظهای فوق، ارائه شده است.

- حفاظهای خاص سیستم‌های اطلاعاتی

در این مبحث، نقش شناسایی و تشخیص هویت، دسترسی کنترل لاجیکی و بازرسی، محافظت در مقابل کدهای مخرب، مدیریت شبکه و رمزنگاری، بعنوان حفاظهای خاص سیستم‌های اطلاعاتی تشریح شده و در ادامه، مراجع موجود در خصوص هر یک از حفظهای فوق، ارائه شده است.

۴- رویکرد پایه: انتخاب حفاظ بر اساس نوع سیستم اطلاعاتی

محتوای این قسمت از گزارش فنی، ابتدا حفاظهای عمومی قابل استفاده برای سیستم‌های اطلاعاتی و در ادامه، حفاظهای خاص سیستم‌های اطلاعاتی را به تفکیک برای ایستگاه‌های کاری مستقل، ایستگاه‌های کاری متصل به شبکه و سرویس‌دهنده‌های شبکه، ارائه داده است.

۵- انتخاب حفاظ بر اساس تهدیدها و نگرانی‌های موجود
محتوای این قسمت از گزارش فنی، ابتدا به ارزیابی نگرانی‌های امنیتی پرداخته و این موضوع را شامل ارزیابی صدمات وارده بر محرمانگی، تمامیت، دسترس‌پذیری، پاسخ‌گویی، قابلیت تشخیص هویت و قابلیت اعتماد دانسته و ابعاد هر یک از موارد را تشریح و در ادامه، حفاظهای قابل استفاده برای تامین هر یک از فاکتورهای امنیتی فوق را ارائه نموده است.

**بخش پنجم ISO/IEC TR 13335:**

بخش پنجم گزارش فنی شماره ISO/IEC TR 13335 در سال ۲۰۰۱ تحت عنوان "رهنمود مدیریتی در امنیت شبکه" منتشر شد. در این بخش، پس از بیان تعاریف و ساختارهای اولیه، مواردی به شرح زیر ارائه شده است:

۱- نیازمندی‌های بازبینی سیاست امنیتی فن‌آوری اطلاعات سازمان
به منظور تامین امنیت شبکه، لازم است ابتدا سیاست امنیتی فن‌آوری اطلاعات موجود، بررسی شود. محتوای این قسمت از گزارش فنی، ابتدا موضوع بازبینی سیاست امنیتی فن‌آوری اطلاعات سازمان را تشریح و در ادامه، فراهم نمودن نیازمندی‌های لازم برای اجرایی نمودن سیاست‌ها را مطرح نموده است.

۲- بازبینی ساختار و کاربردهای شبکه
به منظور تامین امنیت شبکه، همچنین لازم است ساختار شبکه و کاربردهای ارائه شده یا طراحی شده برای ارائه روی شبکه، ارزیابی شوند. محتوای این قسمت از گزارش فنی، انواع شبکه‌ها، پروتکل‌های ارتباطی و اجرای کاربردها

روی شبکه را ارائه داده و مواردی که باید بررسی شوند را مطرح نموده است.

۳- بازبینی انواع اتصالات شبکه

اقدام دیگری که لازم است به منظور تامین امنیت شبکه انجام گیرد، بررسی اتصالات شبکه در داخل و یا به خارج از سازمان می‌باشد. محتوای این قسمت از گزارش فنی، لیستی از اتصالات ممکن در شبکه ارائه داده و در ادامه، موضوعات قابل بررسی در ارتباط با اتصالات شبکه را ارائه نموده است.

۴- ارزیابی ویژگی‌های شبکه و ارتباط مطمئن

خصوصی یا عمومی بودن شبکه، نوع اطلاعاتی که در شبکه مبادله می‌شود، مثلا دیتا، صوت، تصویر و یا ترکیبی، مواردی هستند که بر اساس محتوای این قسمت از گزارش فنی، باید بررسی شوند. همچنین در خصوص ارتباط مطمئن، در این قسمت از گزارش فنی، ۳ سطح اطمینان کم، متوسط و زیاد تعریف شده و بیان شده که هر یک از اطلاعات قابل مبادله روی شبکه، لازم است متناسب با نوع و ویژگی‌هایشان، در یکی از این سطوح قرار گیرند.

۵- تعیین میزان ریسک امنیتی

به منظور تعیین میزان ریسک شبکه، لازم است میزان صدمات وارده بر محرمانگی اطلاعات، تمامیت اطلاعات، دسترس‌پذیری اطلاعات و سرویس های شبکه، عدم انکار تعهدات، پاسخ‌گویی در خصوص عملیات انجام شده، قابلیت تشخیص هویت اطلاعات و قابلیت اعتماد اطلاعات را بدست آوریم. در این قسمت از گزارش فنی، نحوه تعیین این پارامترها و تعیین میزان ریسک امنیتی شبکه؛، ارائه شده است.

۶- شناسایی حفاظهای قابل استفاده

در این قسمت از گزارش فنی، حفاظهای قابل استفاده برای تامین امنیت شبکه، به شکل زیر دسته بندی شده اند:

- مدیریت امن سرویس
  - تعریف مسئولیت های افراد مرتبط با سرویس
  - مستندسازی سیاست امنیتی سیستم
  - مستندسازی رویه های عملیاتی امنیت
  - بررسی سازگاری امنیتی به منظور تشخیص پشتیبانی امنیت در سطح موردنیاز
  - مستندسازی شرایط امنیتی کاربران، سرویس ها و اتصال های شبکه
  - وجود ساختار پشتیبانی حوادث
  - مستندسازی طرح تداوم عملکرد و ترمیم خرابی
- شناسایی و تشخیص هویت
  - تامین امنیت دسترسی از راه دور
  - بهینه سازی تشخیص هویت
  - استفاده از Single Sign-On امن
- بازرسی
- تشخیص تهاجم
- محافظت در مقابل کدهای مخرب
- مدیریت امن شبکه
- گذرگاه های ارتباطی امن
- تامین محرمانگی اطلاعات در حال مبادله در شبکه
- تامین تمامیت اطلاعات در حال مبادله در شبکه

- مکانیزم های عدم انکار
- استفاده از شبکه های خصوصی مجازی
- تداوم فعالیت و ترمیم خرابی
- مستندسازی و بازبینی گزینه های ساختار امنیت

## ۱-۳- نتیجه گیری

با توجه به محتوای استانداردهای BS7799، ISO/IEC 17799 و گزارش فنی ISO/IEC TR 13335، نقاط اشتراک زیاد بین محتوای آن‌ها و تفاوت های ظاهری اندکی که بین محتوای استانداردها و گزارش فنی مشاهده می شود، پاسخ به سوالات زیر، می‌تواند راه‌گشا باشد:

۱- در نهایت، پیاده سازی سیستم مدیریت امنیت اطلاعات در یک سازمان، باید بر اساس کدام استاندارد یا گزارش فنی انجام گیرد؟

۲- به منظور پیاده سازی سیستم مدیریت امنیت اطلاعات در یک سازمان، چه اقداماتی باید انجام گیرد؟

### ۱-۳-۱- مرجع پیاده‌سازی سیستم مدیریت امنیت اطلاعات

محتوای استانداردهای BS7799، ISO/IEC 17799 و گزارش فنی ISO/IEC TR 13335 ، نشان می‌دهد که تمامی این استانداردها و گزارش‌های فنی، در کلیات مشترک می‌باشند و تنها گزارش فنی 13335، با نگاهی فنی به پیاده‌سازی سیستم مدیریت امنیت اطلاعات پرداخته و جزئیات بیشتری را مطرح نموده است. لیکن با توجه به اینکه این گزارش فنی، اعتبار استاندارد را ندارد و تائیدیه‌های بین‌المللی برای آن ارائه نمی‌گردد، لذا به منظور پیاده‌سازی موفق سیستم مدیریت امنیت اطلاعات در سازمان‌ها، لازم است استاندارد BS7799 به عنوان مرجع اصلی مورد استفاده قرار گیرد و گزارش فنی ISO/IEC TR 13335 به عنوان

راهنمای فنی در مواردی که کلیات آن در استاندارد مذکور ارائه شده است، مورد استفاده قرار گیرد.

### ۱-۳-۲- اقدامات موردنیاز به منظور پیاده‌سازی سیستم مدیریت امنیت اطلاعات

اقدامات لازم به منظور پیاده‌سازی سیستم مدیریت امنیت اطلاعات، بر اساس استاندارد BS7799 و گزارش فنی ISO/IEC TR 13335، عبارتند از:

۱- تهیه و اجرای طرح‌ها و برنامه‌های امنیت فن‌آوری اطلاعات سازمان

۲- ایجاد تشکیلات امنیت فن‌آوری اطلاعات سازمان، به منظور پشتیبانی موثر امنیت فن‌آوری اطلاعات، بر اساس طرح‌ها و برنامه‌های ارائه شده

### طرح‌ها و برنامه‌های امنیتی مورد نیاز

بر اساس مراجع فوق، هر سازمان باید مجموعه مستندات مدیریت امنیت فن‌آوری اطلاعات خود را تدوین و اجرا نماید. این مستندات شامل مجموعه‌ای از طرح‌ها و برنامه‌های امنیت فن‌آوری اطلاعات به شرح زیر می‌باشند:

- اهداف، راهبردها و سیاست‌های امنیتی فن‌آوری اطلاعات سازمان
- طرح ارزیابی مخاطرات امنیتی فن‌آوری اطلاعات سازمان
- طرح امنیت فن‌آوری اطلاعات سازمان
- طرح پشتیبانی حوادث امنیتی فن‌آوری اطلاعات سازمان
- طرح تداوم عملکرد و ترمیم خرابی‌های فن‌آوری اطلاعات سازمان
- برنامهٔ آگاهی رسانی، تربیت نیروی انسانی و آموزش امنیت فن‌آوری اطلاعات سازمان

در ۵ فصل بعدی این کتاب، به ترتیب چارچوب پیشنهادی برای تدوین طرح ارزیابی مخاطرات، سیاست‌های امنیتی، طرح امنیت، طرح پشتیبانی حوادث و برنامه آگاهی‌رسانی، تربیت نیروی انسانی و آموزش امنیت سازمان ارائه شده است.

**تشکیلات تامین امنیت فن‌آوری اطلاعات سازمان**

بر اساس مراجع فوق، هر سازمان باید تشکیلات امنیت فن‌آوری اطلاعات خود را ایجاد نماید. اجزاء این تشکیلات عبارتند از:

- واحد راهبری و سیاست‌گذاری

تعیین اهداف، راهبردها و سیاست‌های امنیتی سازمان، توسط واحدی با عنوان "کمیته راهبری امنیت فن‌آوری اطلاعات سازمان" انجام خواهد شد.

- واحد اجرائی

مسئولیت اجرای امنیت فن‌آوری اطلاعات سازمان، بر عهده مدیر امنیت فن‌آوری اطلاعات سازمان می‌باشد.

- واحد پشتیبانی فنی

مسئولیت فنی پیاده‌سازی و پشتیبانی امنیت فن‌آوری اطلاعات سازمان، بر عهده یک تیم فنی متخصص امنیت فن‌آوری اطلاعات می‌باشد.

اجزاء فوق، اجزاء پیش‌بینی شده در استانداردهای مدیریت امنیت می‌باشند که لازم است در داخل سازمان تشکیل شوند. اطلاعات بیشتر در خصوص ساختار و شرح وظایف اجزاء فوق، در بخش تشکیلات تامین امنیت شبکه از فصل دوم، ارائه شده است.

# ۲

# چارچوب پیشنهادی برای تدوین اهداف، راهبردها و سیاست‌های امنیتی

## ۲-۱- مقدمه

اولین گام به سوی تامین امنیت شبکه هر سازمان، تعیین، تدوین و اعلام سیاست‌های امنیت شبکه سازمان می‌باشد. مدیر امنیت شبکه سازمان، مسئول تهیه و ارائه این سیاست‌ها به کمیته راهبری امنیت شبکه سازمان می‌باشد. سیاست‌های پیشنهادی پس از تصویب، به شیوه‌ای مناسب، به اطلاع کلیه مخاطبین این سیاست‌ها رسانده می‌شود.

برای تعیین سیاست‌های امنیتی، باید ابتدا اهداف نهائی و احیانا اهداف مقطعی امنیت را تعیین نمود و در ادامه، راهبردهای مناسبی که سازمان با رویکرد به آنها بتواند به اهداف موردنظر دست یابد را مشخص نمود.

## ۲-۲- اهداف امنیت شبکه

به منظور تعیین اهداف امنیت، باید ابتدا سرمایه‌های مرتبط با اطلاعات و ارتباطات سازمان، شناسائی شده و سپس اهداف تامین امنیت برای هر یک از این سرمایه‌ها، مشخص شود.

### ۲-۲-۱-سرمایه‌های مرتبط با شبکه

سرمایه‌های مرتبط با شبکه سازمان، عبارتند از:

- **سخت‌افزارها**: شامل ایستگاههای کاری، سرویس‌دهنده‌ها، خطوط ارتباطی، تجهیزات شبکه، تجهیزات انتقال داده، لینک‌های ارتباطی، اینترفیس‌ها و سیستم‌های ارتباطی.
- **نرم‌افزارها**: شامل سیستم‌عامل‌ها، نرم‌افزارهای کاربردی عمومی، نرم‌افزارهای کاربردی اختصاصی، نرم‌افزارهای مدیریت شبکه و ابزارهای نرم‌افزاری.
- **اطلاعات**: شامل اسناد و اطلاعات ذخیره شده در شبکه، اسناد و اطلاعات پشتیبان و اسناد و اطلاعات در حال انتقال در شبکه.
- **ارتباطات**: شامل ارتباطات داخلی سازمان و ارتباطات شبکه سازمان با سایر شبکه‌های موجود، از قبیل شبکه دولت، شبکه سایر سازمان‌ها و شبکه اینترنت.
- **کاربران**: شامل مدیران، کارشناسان فنی و کاربران عادی ادارات، مدیر و کارشناسان فنی تیم مدیریت شبکه، کارشناسان فنی و مدیر امنیت شبکه، پیمانکاران مرتبط با شبکه و سایر کاربرانی که به نحوی، اطلاعاتی از شبکه سازمان داشته و یا با آن در ارتباط می‌باشند.

### ۲-۲-۲-اهداف امنیت شبکه

موارد مطرح به عنوان اهداف کوتاه‌مدت و میان‌مدت امنیت، به شرح زیر، می‌باشند:

۱- اهداف کوتاه مدت امنیت شبکه :

- جلوگیری از حملات و دسترسی‌های غیرمجاز، علیه سرمایه‌های شبکه
- مهار خسارت‌های ناشی از ناامنی موجود در شبکه

- کاهش رخنه‌پذیری‌های سرمایه‌های شبکه

۲- اهداف میان مدت امنیت شبکه :

- تامین صحت عملکرد، قابلیت دسترسی و محافظت فیزیکی برای سخت‌افزارها، متناسب با حساسیت آنها.
- تامین صحت عملکرد و قابلیت دسترسی برای نرم‌افزارها، متناسب با حساسیت آنها.
- تامین محرمانگی، صحت و قابلیت دسترسی برای اطلاعات، متناسب با طبقه‌بندی اطلاعات از حیث محرمانگی.
- تامین محرمانگی، صحت و قابلیت دسترسی برای ارتباطات، متناسب با طبقه‌بندی اطلاعات از حیث محرمانگی و حساسیت ارتباطات.
- تامین قابلیت تشخیص هویت، حدود اختیارات و پاسخ‌گویی، حریم خصوصی و آگاهی‌رسانی امنیتی برای کاربران شبکه، متناسب با طبقه‌بندی اطلاعات قابل دسترس و نوع کاربران.

| سرمایه‌ها / اهداف | شبکه | | | | کاربران شبکه |
|---|---|---|---|---|---|
| | سخت‌افزارها | نرم‌افزارها | اطلاعات | ارتباطات | |
| محرمانگی (Confidentiality) | | | | | |
| صحت (Integrity) | | | | | |
| قابلیت دسترسی (Availability) | | | | | |
| محافظت فیزیکی (Physical Protection) | | | | | |
| تشخیص هویت (Authenticity) | | | | | |
| حدود اختیارات (Authority) | | | | | |
| پاسخ‌گویی (Accountability) | | | | | |
| حریم خصوصی (Privacy) | | | | | |
| آگاهی‌رسانی امنیتی (Security Awareness) | | | | | |

جدول (۲-۱ ): اهداف تامین امنیت سرمایه‌های شبکه

## ۲-۳- راهبردهای تامین امنیت شبکه

راهبردهای امنیت شبکه، بیانگر رویکرد سازمان به منظور دست‌یابی به اهداف امنیت شبکه تعیین شده برای سازمان می‌باشد.

### ۲-۳-۱-راهبردهای کوتاه‌مدت

به منظور تامین امنیت شبکه در کوتاه مدت، راهبردهای زیر مناسب می‌باشند:

**شناسائی و رفع ضعف‌های امنیتی شبکه**

به منظور ایجاد امنیت اولیه برای شبکه سازمان، لازم است بررسی دقیقی در خصوص شبکه و وضعیت امنیت این شبکه، انجام گرفته، ضعف‌های موجود شناسائی و اولویت‌بندی شده و برنامه‌ریزی لازم جهت رفع آنها انجام گیرد. در این مرحله، جهت رفع ضعف‌های موجود، حدالمقدور باید از امکانات در دسترس استفاده شود و از درگیر شدن در پروسه‌های زمان‌بر از قبیل خرید تجهیزات اجتناب نمود.

**آگاهی‌رسانی به کاربران**

به منظور تامین بخشی از امنیت اولیه برای شبکه سازمان، لازم است آشنائی کاربران با مباحث امنیت شبکه و اطلاع از شیوه‌های نفوذ از داخل و خارج از شبکه سازمان به سرمایه‌های این شبکه و مسئولیت کاربران در خصوص تامین امنیت این شبکه، مورد توجه قرار گیرد.

**کنترل ارتباطات شبکه سازمان با سایر شبکه‌ها**

به منظور تامین بخشی از امنیت اولیه برای شبکه سازمان، لازم است کلیه گذرگاه‌های اتصال شبکه سازمان به شبکه اینترنت، شبکه دولت و سایر شبکه‌ها، به امکانات کنترل دسترسی و کنترل ارتباطات مجهز شوند.

### ۲-۳-۲-راهبردهای میان‌مدت

به منظور تامین امنیت شبکه سازمان، در میان مدت، راهبردهای زیر مناسب می‌باشند:

**تهیه طرح‌ها و برنامه‌های امنیت شبکه**

به‌منظور تامین امنیت شبکه سازمان در میان مدت، لازم است طرحها و برنامه‌های امنیتی از قبیل موارد ذیل، تهیه و ارائه شوند:

- اهداف، راهبردها و سیاست‌های امنیتی شبکه سازمان
- طرح ارزیابی مخاطرات امنیتی شبکه سازمان
- طرح امنیت شبکه سازمان
- طرح پشتیبانی حوادث امنیتی شبکه سازمان
- طرح تداوم عملکرد و ترمیم خرابی‌های شبکه سازمان
- برنامهٔ آگاهی رسانی، تربیت نیروی انسانی و آموزش امنیت شبکه سازمان

**ایجاد و آماده‌سازی تشکیلات تامین امنیت شبکه**

برای این منظور، لازم است اقدامات زیر انجام گیرد:

- ساختار و شرح وظایف تشکیلات موردنیاز به‌منظور تامین تداوم امنیت شبکه، در سطوح مختلف، طراحی و تدوین شود.
- اقدامات لازم به منظور ایجاد تشکیلات، انجام گیرد. از جمله این اقدامات، می‌توان به گنجانیدن تشکیلات امنیت در چارت سازمانی سازمان و تامین پرسنل موردنیاز برای این تشکیلات اشاره نمود.
- آموزشهای لازم جهت آماده‌سازی تشکیلات فوق به منظور پذیرش مسئولیت تامین تداوم امنیت شبکه، انجام گیرد.

**اجرای طرح‌ها و برنامه‌های امنیت شبکه**

کلیه طرح‌ها و برنامه‌های امنیت شبکه سازمان، باید اجرا شوند. در خاتمه اجرای این طرح‌ها و برنامه‌ها، امنیت در سطح مطلوب برقرار شده و تمهیدات لازم به منظور پشتیبانی امنیت نیز اندیشیده شده است.

**پشتیبانی امنیت شبکه**

پس از نصب و راه‌اندازی تجهیزات امنیت شبکه سازمان، پشتیبانی امنیت شبکه سازمان، بر اساس طرح پشتیبانی حوادث و طرح تداوم فعالیت سازمان، به عهده تشکیلات تامین امنیت سازمان گذاشته خواهد شد.

## ۲-۴- تشکیلات تامین امنیت شبکه

هر سازمان باید تشکیلات امنیت شبکه خود را ایجاد نماید. اجزاء ، ساختار و شرح وظایف این تشکیلات عبارتند از:

### ۲-۴-۱- اجزاء و ساختار تشکیلات

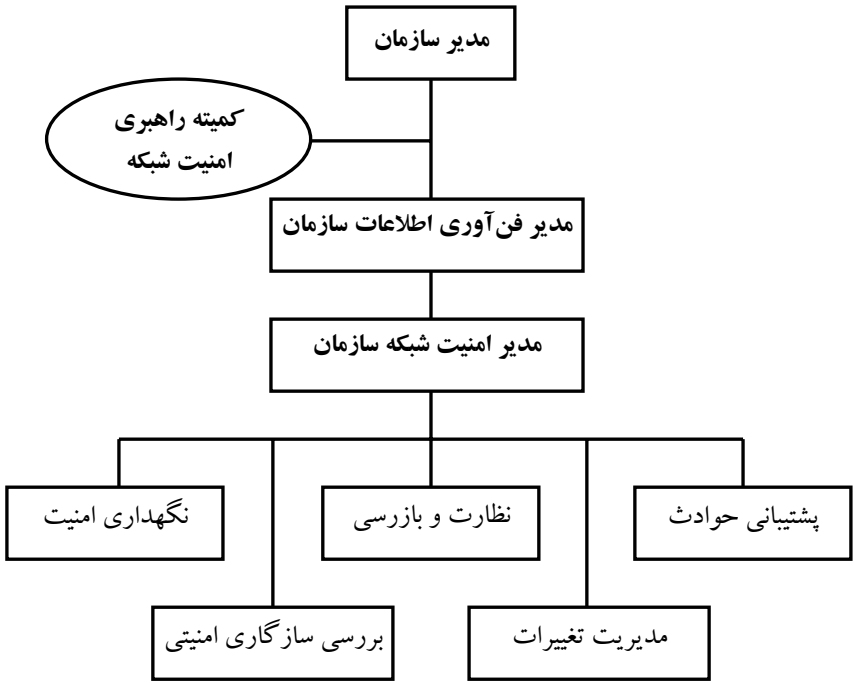
تشکیلات امنیت شبکه، متشکل از سه جزء اصلی به شرح زیر می باشد:

- در سطح راهبری و سیاست‌گذاری: کمیته راهبری امنیت شبکه
- در سطح مدیریت اجرائی: مدیر امنیت شبکه
- در سطح فنی: واحد پشتیبانی امنیت شبکه

علاوه بر موارد فوق، واحدهای دیگری از جمله "مشاوره و طراحی" و "نظارت بر اجرای طرح‌ها و برنامه‌های امنیتی" نیز لازم است. لیکن این واحدها الزاما در داخل سازمان و چارت سازمانی، تشکیل نخواهند شد.

**ساختار تشکیلات امنیت شبکه:**

ساختار تشکیلات امنیت شبکه سازمان، مطابق آنچه در شکل (۲-۲) نشان داده شده می‌باشد.




شکل (۲-۱): ساختار تشکیلات امنیت شبکه سازمان

**اعضاء تشکیلات امنیت شبکه :**

- کمیته راهبری امنیت شبکه:

اعضاء مناسب جهت حضور در کمیته راهبری امنیت شبکه سازمان، عبارتند از:

- مدیر سازمان ( رئیس کمیته )

- نماینده ویژه مدیر سازمان
- مدیر حراست سازمان
- مدیر فن آوری اطلاعات سازمان
- مدیر امنیت شبکه سازمان (دبیر کمیته )

- مدیر امنیت شبکه سازمان

مدیریت واحد پشتیبانی امنیت شبکه را به عهده دارد و توسط مدیر فن‌آوری اطلاعات سازمان تعیین می‌شود.

- تیم‌های پشتیبانی امنیت شبکه سازمان

تیم‌های کارشناسی که زیر نظر مدیر امنیت شبکه سازمان فعالیت نموده و توسط وی تعیین می‌شوند.

### ۲-۴-۲- شرح وظایف تشکیلات

**کمیته راهبری :**

- بررسی، تغییر و تصویب سیاست‌های امنیتی شبکه
- پیگیری اجرای سیاست‌های امنیتی از مدیر امنیت شبکه
- تائید طرح‌های و برنامه‌های امنیت شبکه
- بررسی ضرورت تغییر سیاست‌های امنیتی شبکه
- بررسی، تغییر و تصویب تغییرات سیاست‌های امنیتی شبکه

**مدیر امنیت شبکه :**

- تهیه پیش نویس سیاست‌های امنیتی شبکه و ارائه به کمیته راهبری
- نظارت بر اجرای کامل سیاست‌های امنیتی

- تهیه طرح‌ها و برنامه‌های امنیت شبکه
- مدیریت واحد پشتیبانی امنیت شبکه
- تشخیص ضرورت و پیشنهاد بازنگری و اصلاح سیاست‌های امنیتی شبکه
- تهیه پیش نویس تغییرات سیاست‌های امنیتی شبکه

**واحد پشتیبانی امنیت** :

- شرح وظایف پشتیبانی حوادث امنیتی شبکه:
  - تشخیص و مقابله با تهاجم
    - ✓ مرور روزانه Log تجهیزات شبکه و امنیت شبکه
    - ✓ مرور ترددهای انجام شده به سایت
    - ✓ مرور روزانه گزارش سیستم‌های تشخیص تهاجم
    - ✓ انجام اقدامات لازم به‌منظور کنترل دامنه تهاجم
    - ✓ ترمیم خرابی‌های ناشی از تهاجم
    - ✓ مستندسازی و ارائه گزارش تهاجم
    - ✓ اعمال تغییرات لازم در سیستم امنیت شبکه
    - ✓ آگاهی‌رسانی به کاربران شبکه

  - تشخیص و مقابله با ویروس

    - ✓ بررسی، انتخاب، تست نرم افزار ضدویروس مناسب به صورت دوره‌ای
    - ✓ نصب نرم‌افزار ضدویروس روی ایستگاههای کاری و سرویس‌دهنده‌های شبکه
    - ✓ تهیه راهنمای نصب و Update نمودن نرم‌افزار ضدویروس
    - ✓ مرور روزانه Log و گزارشات نرم‌افزارهای ضد ویروس
    - ✓ مطالعه و بررسی ویروس‌های جدید و روش‌های مقابله با آن
    - ✓ ارائه روش‌های مقابله با ویروس

- ✓ انجام اقدامات پیشگیرانه به‌منظور کنترل دامنه تاثیر ویروس
- ✓ ترمیم خرابی‌های ناشی از ویروس
- ✓ مستندسازی و ارائه گزارشهای آماری از ویروس‌ها، مقابله با آنها و خرابی‌های ناشی از ویروس‌ها در شبکه سازمان
- ✓ فراهم نمودن امکان Update نمودن نرم‌افزار ضد ویروس، بصورت دوره‌ای
- ✓ آگاهی‌رسانی به کاربران شبکه در خصوص ویروس‌های جدید و روش‌های مقابله با آنها

- ➢ تشخیص و پشتیبانی حوادث فیزیکی

- ✓ انتخاب ابزارهای مناسب جهت محافظت فیزیکی از تجهیزات و سرمایه‌های شبکه در مقابل حوادث فیزیکی و دسترسی‌های غیرمجاز
- ✓ مرور روزانه رویدادنامه‌های دسترسی فیزیکی به سرمایه‌های شبکه، بویژه در سایت
- ✓ سرکشی دوره‌ای به سایت، تجهیزات مستقر در طبقات ساختمان‌ها و مسیر عبور کابل‌ها به منظور اطمینان از تامین امنیت فیزیکی
- ✓ مطالعه و بررسی حوادث فیزیکی و روش‌های مقابله با آن
- ✓ انجام اقدامات لازم به‌منظور کنترل دامنه حوادث فیزیکی
- ✓ ترمیم خرابی‌های ناشی از حوادث فیزیکی
- ✓ مستندسازی و ارائه گزارشهای آماری از حوادث فیزیکی، مقابله با این حوادث و خرابی‌های ناشی از آنها
- ✓ ارائه پیشنهاد در خصوص تغییر تجهیزات و روش‌های تامین امنیت فیزیکی
- ✓ ارائه اطلاعات لازم جهت آگاهی رسانی به کاربران

- شرح وظایف نظارت و بازرسی امنیتی شبکه
  - مانیتورینگ ترافیک شبکه ( در حیطه مانیتورینگ مجاز )
  - بازرسی دوره ای از ایستگاههای کاری، سرویس‌دهنده‌ها، تجهیزات شبکه و سایر سخت‌افزارهای موجود شبکه، به منظور اطمینان از رعایت سیاست‌های امنیتی
  - بازرسی دوره ای از سخت‌افزارهای خریداری شده و تطبیق پروسه "سفارش، خرید، تست، نصب و پیکربندی سخت‌افزارهای شبکه سازمان" با سیاست‌های امنیتی
  - بازرسی دوره ای از نرم‌افزارهای موجود شبکه به منظور اطمینان از رعایت سیاست‌های امنیتی
  - بازرسی دوره ای از نرم‌افزارهای خریداری شده و تطبیق پروسه "سفارش، خرید، تست، نصب و پیکربندی نرم‌افزارهای شبکه سازمان" با سیاست‌های امنیتی
  - بازرسی دوره ای از نحوه اتصال شبکه سازمان بر اساس سیاست‌های امنیتی
  - بازرسی دوره ای از اطلاعات شبکه سازمان به منظور اطمینان از رعایت سیاست‌های امنیتی
  - بازرسی دوره ای از کاربران شبکه سازمان به منظور اطمینان از آگاهی کاربران از حقوق و مسئولیت‌های خود و رعایت سیاست‌های امنیتی
  - بازرسی دوره ای از روند تهیه اطلاعات پشتیبان
  - بازرسی دوره ای از روند پشتیبانی حوادث
  - بازرسی دوره ای از روند نگهداری سیستم امنیتی شبکه
  - بازرسی دوره ای از روند مدیریت تغییرات در شبکه
  - بازرسی دوره ای از روند آگاهی‌رسانی امنیتی به کاربران شبکه
  - بازرسی دوره ای از روند آموزش پرسنل واحد پشتیبانی امنیت شبکه

- بازرسی دوره ای از روند واگذاری فعالیت‌ها به پیمانکاران خارج از سازمان

- شرح وظایف مدیریت تغییرات
- بررسی درخواست خرید، ایجاد یا تغییر سخت‌افزارها، نرم‌افزارها، لینک‌های ارتباطی، سیستم‌عامل‌ها و سرویس‌های شبکه از دیدگاه امنیت شبکه، آسیب‌پذیری‌های سیستم یا سرویس مورد نظر، مشکلات امنیتی ناشی از بکارگیری آن بر سایر بخش‌های شبکه و نهایتا تصمیم‌گیری در خصوص تائید یا رد درخواست
- بررسی آسیب‌پذیری‌های سخت‌افزارها، نرم‌افزارهای کاربردی، سیستم عامل‌ها، خطوط ارتباطی و سرویس‌های شبکه و امنیت شبکه
- بررسی موارد مربوط به جابجایی کاربران شبکه و پرسنل تشکیلات امنیت شبکه به‌منظور تغییر در دسترسی و حدود اختیارات آنها
- بررسی نیازمندی‌های امنیتی و روش‌های ایمن‌سازی سیستم عامل‌ها، سرویس‌دهنده‌های شبکه، خطوط ارتباطی، نرم‌افزارها، تجهیزات شبکه و امنیت شبکه جدید که بکارگیری آنها در شبکه، مورد تائید قرار گرفته است

- شرح وظایف نگهداری امنیت شبکه
- بررسی وضعیت عملکرد سیستم امنیتی شبکه
- ارائه گزارشات روزانه در خصوص عملکرد سیستم امنیتی شبکه
- ارائه گزارشات آماری از وضعیت سیستم امنیتی شبکه
- رفع اشکالات تشخیص داده شده در عملکرد سیستم امنیتی شبکه

## ۲-۵- سیاست‌های امنیتی شبکه

در این بخش، مواردی که لازم است در سیاست‌های امنیتی شبکه سازمان آورده شوند، ارائه شده است.

### ۲-۵-۱- سیاست‌های امنیتی سرویس‌های شبکه

#### ۲-۵-۱-۱- سیاست امنیتی سرویس دسترسی به شبکه داخلی

در سیاست‌های امنیتی سرویس دسترسی به شبکه داخلی سازمان، لازم است سیاست سازمان در خصوص موارد ذیل مشخص گردد:

**دسترسی کاربران به شبکه داخلی**:

- تعیین افراد مجاز به دسترسی به شبکه داخلی سازمان، از داخل و خارج از سازمان
- بیان ضرورت تدوین آئین‌نامه یا دستورالعمل استفاده کاربران از سرویس دسترسی به شبکه داخلی، شامل لیست و محدودیت‌های افراد
- بیان ضرورت اعلام تغییرات لیست و محدودیت‌های افراد مجاز به واحد پشتیبانی امنیت شبکه
- منع تلاش کاربران در دسترسی غیرمجاز به سایر سرویس‌ها و سرمایه‌های شبکه داخلی سازمان
- منع تلاش کاربران در دسترسی غیرمجاز به سایر شبکه‌های متصل به شبکه داخلی سازمان
- تاکید بر استفاده صحیح کاربران از شبکه داخلی در راستای انجام امور اداری محوله
- تاکید بر اعمال کنترل‌های امنیتی موردنیاز جهت دسترسی کاربران به شبکه داخلی و تعیین مسئول اعمال کنترل‌های امنیتی

- بیان ضرورت تعیین و اعلام مقررات تنبیهی در خصوص دسترسی غیرمجاز کاربران

**محدودیت‌های ایجاد ترافیک در شبکه داخلی** :

- تعیین و اعلام نوع و حجم ترافیک قابل قبول برای هر یک از سرویس‌های شبکه داخلی سازمان، به تفکیک برای ساعات اداری و غیر اداری
- تعیین و اعلام محدودیت‌های ایجاد ترافیک توسط کاربران، بویژه در موارد ذیل:
  - انتقال آگاهانه یا ناآگاهانه ویروس‌های کامپیوتری، اسب‌های تروا و سایر کدهای مخرب
  - تلاش به منظور ممانعت از ارائه سرویس توسط هر یک از سرمایه‌های شبکه داخلی
  - تلاش به منظور دسترسی غیرمجاز به اطلاعات شبکه داخلی
  - تلاش به منظور ایجاد ترافیک با آدرس غیرمعتبر یا آدرس متعلق به سایر کاربران شبکه
  - تلاش به منظور مانیتورینگ اطلاعات در حال مبادله در شبکه داخلی
  - مبادله فایل با حجم زیاد، در ساعات اداری
  - مبادله فایل‌های تصویری، ویدئو و موارد مشابه، در ساعات اداری

### ۲-۵-۱-۲- سیاست امنیتی سرویس دسترسی به شبکه اینترنت

در سیاست‌های امنیتی سرویس دسترسی به شبکه اینترنت سازمان، لازم است سیاست سازمان در خصوص موارد ذیل مشخص گردد:

**دسترسی کاربران به شبکه اینترنت:**

- تعیین افراد مجاز به دسترسی به شبکه اینترنت، از داخل و خارج از سازمان

- بیان ضرورت تدوین آئین‌نامه یا دستورالعمل استفاده کاربران از سرویس، شامل لیست و محدودیت‌های افراد
- بیان ضرورت اعلام تغییرات لیست و محدودیت‌های افراد مجاز به واحد پشتیبانی امنیت شبکه
- منع تلاش کاربران در دسترسی غیرمجاز به سایر سرویس‌ها و سرمایه‌های شبکه دسترسی به اینترنت
- تاکید بر استفاده صحیح کاربران از شبکه اینترنت در راستای انجام امور اداری محوله
- تاکید بر اعمال کنترل‌های امنیتی موردنیاز جهت دسترسی کاربران به شبکه اینترنت و تعیین مسئول اعمال کنترل‌های امنیتی
- ضرورت تعیین و اعلام مقررات تنبیهی در خصوص دسترسی غیرمجاز کاربران

**محدودیت‌های ایجاد ترافیک در شبکه دسترسی به اینترنت** :

- تعیین و اعلام نوع و حجم ترافیک قابل قبول برای هر یک از سرویس‌های شبکه اینترنت، به تفکیک برای ساعات اداری و غیر اداری
- تعیین و اعلام محدودیت‌های ایجاد ترافیک توسط کاربران، بویژه در موارد ذیل:
  - انتقال آگاهانه یا ناآگاهانه ویروس‌های کامپیوتری، اسب‌های تروا و سایر کدهای مخرب
  - تلاش به منظور ممانعت از ارائه سرویس توسط هر یک از سرمایه‌های شبکه دسترسی به اینترنت سازمان
  - تلاش به منظور دسترسی غیرمجاز به اطلاعات شبکه دسترسی به اینترنت سازمان

- تلاش به منظور ایجاد ترافیک با آدرس غیرمعتبر یا آدرس متعلق به سایر کاربران شبکه
- تلاش به منظور مانیتورینگ اطلاعات در حال مبادله در شبکه دسترسی به اینترنت سازمان
- مبادله فایل با حجم زیاد، در ساعات اداری
- مبادله فایل‌های تصویری، ویدئو و موارد مشابه، در ساعات اداری

### ۲-۵-۱-۳- سیاست امنیتی سرویس Video Conference

در سیاست‌های امنیتی سرویس کنفرانس ویدیوئی، لازم است سیاست سازمان در خصوص موارد ذیل مشخص گردد:

- تعیین افراد مجاز به دسترسی به این سرویس، از داخل و خارج از سازمان
- بیان ضرورت تدوین آئین‌نامه یا دستورالعمل استفاده کاربران از این سرویس
- ضرورت اعلام تغییرات لیست و محدودیت‌های افراد مجاز به واحد پشتیبانی امنیت شبکه
- تعیین طبقه‌بندی اطلاعات سرویس
- تعیین مرجع تشخیص و مسئول اقدام در خصوص مانیتورینگ سرویس
- تعیین و اعلام مسئولیت استفاده‌کنندگان از سرویس، در خصوص محتوای صحبت‌ها و اطلاعات مورد مبادله
- تاکید بر استفاده صحیح کاربران از سرویس در راستای انجام امور اداری محوله
- منع تلاش کاربران سرویس در دسترسی غیرمجاز به سایر منابع
- تاکید بر اعمال کنترل‌های امنیتی موردنیاز جهت دسترسی کاربران به این سرویس و تعیین مسئول اعمال کنترل‌های امنیتی

- بیان ضرورت تعیین و اعلام مقررات تنبیهی در خصوص عدم رعایت سیاست‌ها
- تعیین حداقل مشخصات امنیتی که نرم‌افزار سرویس، باید داشته باشد

### ۲-۵-۱-۴- سیاست امنیتی سرویس Voice over IP

در سیاست‌های امنیتی این سرویس، لازم است سیاست سازمان در خصوص موارد ذیل مشخص گردد:

- تعیین افراد مجاز به دسترسی به این سرویس، از داخل و خارج از سازمان
- ضرورت تدوین آئین‌نامه یا دستورالعمل استفاده کاربران از این سرویس
- ضرورت اعلام تغییرات لیست و محدودیت‌های افراد مجاز به واحد پشتیبانی امنیت شبکه
- تعیین طبقه‌بندی اطلاعات سرویس
- تعیین مرجع تشخیص و مسئول اقدام در خصوص مانیتورینگ سرویس
- تعیین و اعلام مسئولیت استفاده کنندگان از سرویس، در خصوص محتوای صحبت‌ها و اطلاعات مورد مبادله
- تاکید بر استفاده صحیح کاربران از سرویس در راستای انجام امور اداری محوله
- تلاش کاربران سرویس در دسترسی غیرمجاز به سایر منابع
- تاکید بر اعمال کنترل‌های امنیتی موردنیاز و تعیین مسئول اعمال کنترل‌های امنیتی
- بیان ضرورت تعیین و اعلام مقررات تنبیهی در صورت عدم رعایت سیاست‌ها
- تعیین مشخصات امنیتی که نرم‌افزار سرویس، باید داشته باشد

### ۲-۵-۱-۵- سیاست امنیتی سرویس Web Casting

در سیاست‌های امنیتی این سرویس، لازم است سیاست سازمان در خصوص موارد ذیل مشخص گردد:

- تعیین افراد مجاز به دسترسی به این سرویس، از داخل و خارج از سازمان
- بیان ضرورت تدوین آئین‌نامه یا دستورالعمل استفاده کاربران از این سرویس
- بیان ضرورت اعلام تغییرات لیست و محدودیت‌های افراد مجاز به واحد پشتیبانی امنیت شبکه
- تعیین طبقه‌بندی اطلاعات سرویس
- تعیین مرجع تشخیص و مسئول اقدام در خصوص مانیتورینگ سرویس
- تعیین و اعلام مسئولیت استفاده کنندگان از سرویس، در خصوص محتوای اطلاعات مورد مبادله
- تاکید بر استفاده صحیح کاربران از سرویس در راستای انجام امور اداری محوله
- منع تلاش کاربران سرویس در دسترسی غیرمجاز به سایر منابع
- تاکید بر اعمال کنترل‌های امنیتی موردنیاز و تعیین مسئول اعمال کنترل‌های امنیتی
- بیان ضرورت تعیین و اعلام مقررات تنبیهی در صورت عدم رعایت سیاست‌ها

### ۲-۵-۱-۶- سیاست امنیتی سرویس Web

در سیاست‌های امنیتی این سرویس، لازم است سیاست سازمان در خصوص موارد ذیل مشخص گردد:

- تعیین افراد مجاز به دسترسی به این سرویس، از داخل و خارج از سازمان
- بیان ضرورت تدوین آئین‌نامه یا دستورالعمل استفاده کاربران از این سرویس

- بیان ضرورت اعلام تغییرات لیست و محدودیت‌های افراد مجاز به واحد پشتیبانی امنیت شبکه
- تعیین طبقه‌بندی اطلاعات سرویس
- تعیین مرجع تشخیص و مسئول اقدام در خصوص مانیتورینگ سرویس
- تعیین و اعلام مسئولیت استفاده کنندگان از سرویس، در خصوص محتوای اطلاعات مورد مبادله
- تاکید بر استفاده صحیح کاربران از سرویس در راستای انجام امور اداری محوله
- منع تلاش کاربران سرویس در دسترسی غیرمجاز به سایر منابع

تاکید بر اعمال کنترل‌های امنیتی موردنیاز جهت دسترسی کاربران به این سرویس، بویژه در خصوص موارد ذیل و تعیین مسئول اعمال کنترل‌های امنیتی

- ثبت اطلاعات دسترسی‌های انجام شده
- جلوگیری از حملات ممانعت از سرویس، علیه این سرویس
- جلوگیری از نفوذ کاربران به سرویس
- جلوگیری از مشاهده، حذف یا تغییر اطلاعات محتوای سرویس، توسط کاربران غیرمجاز شبکه داخلی و شبکه دولت

- بیان ضرورت تعیین و اعلام مقررات تنبیهی در صورت عدم رعایت سیاست‌ها

### ۲-۵-۱-۷- سیاست امنیتی سرویس Web Hosting

در سیاست‌های امنیتی این سرویس، لازم است سیاست سازمان در خصوص موارد ذیل مشخص گردد:

- تعیین افراد یا واحدهای مجاز به استفاده از این سرویس و نحوه دسترسی کاربران از داخل و خارج از سازمان به سایت‌های ایجاد شده

- بیان ضرورت تدوین آئین‌نامه یا دستورالعمل استفاده افراد یا واحدهای سازمان از این سرویس
- تعیین طبقه‌بندی اطلاعات سرویس
- تعیین مرجع تشخیص و مسئول اقدام در خصوص مانیتورینگ سرویس
- تعیین و اعلام مسئولیت استفاده کنندگان از سرویس، در خصوص محتوای اطلاعات سایت‌ها
- تاکید بر استفاده صحیح استفاده کنندگان از سرویس در راستای انجام وظایف سازمانی
- منع تلاش کاربران سرویس در دسترسی غیرمجاز به سایر منابع
- تاکید بر اعمال کنترل‌های امنیتی موردنیاز جهت دسترسی کاربران به این سرویس، بویژه در خصوص موارد ذیل و تعیین مسئول اعمال کنترل‌های امنیتی
  - ثبت اطلاعات دسترسی‌های انجام شده
  - جلوگیری از حملات ممانعت از سرویس، علیه این سرویس
  - جلوگیری از نفوذ کاربران به سرویس
  - جلوگیری از مشاهده، حذف یا تغییر اطلاعات محتوای سرویس، توسط کاربران غیرمجاز شبکه داخلی و شبکه دولت
- بیان ضرورت تعیین و اعلام مقررات تنبیهی در صورت عدم رعایت سیاست‌ها

### ۲-۵-۱-۸- سیاست امنیتی سرویس Email داخلی

در سیاست‌های امنیتی این سرویس، لازم است سیاست سازمان در خصوص موارد ذیل مشخص گردد:

- تعیین افراد مجاز به داشتن Account

- تعیین امکان دسترسی به این سرویس، برای خواندن نامه‌های الکترونیکی توسط صاحب Account از داخل و خارج از سازمان
- تعیین امکان دسترسی به این سرویس، برای ارسال نامه‌های الکترونیکی به Mail Box از داخل و خارج از سازمان
- بیان ضرورت تدوین آئین‌نامه یا دستورالعمل استفاده کاربران از این سرویس
- بیان ضرورت اعلام تغییرات لیست و محدودیت‌های افراد مجاز به واحد پشتیبانی امنیت شبکه
- تعیین طبقه‌بندی اطلاعات سرویس
- تعیین حیطه حریم خصوصی اشخاص در سرویس و بویژه در مورد:
  - محتوای اطلاعات نامه‌ها
  - آدرس E-Mail مخاطبین
- تعیین مرجع تشخیص و مسئول اقدام در خصوص مانیتورینگ سرویس
- تعیین و اعلام مسئولیت استفاده کنندگان از سرویس، در خصوص محتوای اطلاعات مورد مبادله
- تاکید بر استفاده صحیح کاربران از سرویس در راستای انجام امور اداری محوله یا امور شخصی
- منع تلاش کاربران سرویس در دسترسی غیرمجاز به سایر منابع
- تاکید بر اعمال کنترل‌های امنیتی موردنیاز و تعیین مسئول اعمال کنترل‌های امنیتی
- بیان ضرورت تعیین و اعلام مقررات تنبیهی در خصوص دسترسی غیرمجاز کاربران در خصوص:
  - سعی در دستیابی به اطلاعات Account کاربران
  - استفاده از Account سایر کاربران
  - ارسال E-Mailهای غیرواقعی یا E-Mailهای با محتوای نامناسب

### ۲-۵-۱-۹- سیاست امنیتی سرویس Terminal Service

در سیاست‌های امنیتی این سرویس، لازم است سیاست سازمان در خصوص موارد ذیل مشخص گردد:

- تعیین افراد یا واحدهای مجاز به ارائه سرویس
- تعیین افراد مجاز به دسترسی به سرویس
- بیان ضرورت تدوین آئین‌نامه یا دستورالعمل ایجاد و استفاده کاربران از این سرویس
- بیان ضرورت اعلام تغییرات لیست و محدودیت‌های افراد مجاز به واحد پشتیبانی امنیت شبکه
- تعیین طبقه‌بندی اطلاعات سرویس
- تعیین مرجع تشخیص و مسئول اقدام در خصوص مانیتورینگ سرویس
- تعیین و اعلام مسئولیت استفاده کنندگان از سرویس، در خصوص محتوای اطلاعات مورد مبادله
- تاکید بر استفاده صحیح کاربران از سرویس در راستای انجام امور اداری محوله
- منع تلاش کاربران سرویس در دسترسی غیرمجاز به سایر منابع
- تاکید بر اعمال کنترل‌های امنیتی موردنیاز و تعیین مسئول اعمال کنترل‌های امنیتی
- بیان ضرورت تعیین و اعلام مقررات تنبیهی در خصوص ارائه غیرمجاز سرویس و دسترسی غیرمجاز کاربران

**۲-۵-۱-۱۰- سیاست امنیتی سرویس Wireless**

در سیاست‌های امنیتی این سرویس، لازم است سیاست سازمان در خصوص موارد ذیل مشخص گردد:

- تعیین افراد مجاز به استفاده از تجهیزات Wireless، از داخل و خارج از سازمان
- بیان ضرورت تدوین آئین‌نامه یا دستورالعمل استفاده کاربران از این سرویس
- بیان ضرورت اعلام تغییرات لیست و محدودیت‌های افراد مجاز به واحد پشتیبانی امنیت شبکه
- تعیین طبقه‌بندی اطلاعات قابل مبادله از طریق تجهیزات Wireless
- تعیین و اعلام مسئولیت استفاده کنندگان از سرویس، بویژه در خصوص محتوای اطلاعات مورد مبادله
- تاکید بر اعمال کنترل‌های امنیتی قابل پشتیبانی توسط تجهیزات Wireless، بویژه در خصوص:
  - محرمانگی اطلاعات
  - صحت اطلاعات
  - تصدیق اصالت سیستم‌های فرستنده و گیرنده
- تاکید بر اعمال کنترل‌های امنیتی اضافی قابل اعمال برای ارتباطات Wireless ، متناسب با محرمانگی اطلاعات و تعیین مسئول اعمال کنترل‌های امنیتی
- بیان ضرورت تعیین و اعلام مقررات تنبیهی در خصوص استفاده غیرمجاز از تجهیزات Wireless

### ۲-۵-۱-۱۱- سیاست امنیتی سرویس Remote Access

در سیاست‌های امنیتی این سرویس، لازم است سیاست سازمان در خصوص موارد ذیل مشخص گردد:

- تعیین افراد و واحدهای مجاز به ارائه سرویس، جهت دسترسی کاربران از داخل و خارج از سازمان
- تعیین افراد مجاز به دسترسی به این سرویس، از داخل و خارج از سازمان
- بیان ضرورت تدوین آئین‌نامه یا دستورالعمل ارائه و استفاده کاربران از این سرویس
- بیان ضرورت اعلام تغییرات لیست و محدودیت‌های افراد مجاز به واحد پشتیبانی امنیت شبکه
- تعیین محدودیت مبادله اطلاعات طبقه‌بندی شده در این سرویس
- تعیین مرجع تشخیص و مسئول اقدام در خصوص مانیتورینگ سرویس
- تعیین و اعلام مسئولیت استفاده کنندگان از سرویس، در خصوص محتوای اطلاعات مورد مبادله
- تاکید بر استفاده صحیح کاربران از سرویس در راستای انجام امور اداری محوله
- منع تلاش کاربران سرویس در دسترسی غیرمجاز به سایر منابع
- تاکید بر اعمال کنترل‌های امنیتی موردنیاز و تعیین مسئول اعمال کنترل‌های امنیتی
- بیان ضرورت تعیین و اعلام مقررات تنبیهی در صورت تخطی از سیاست‌ها
- تعیین حداقل کنترل‌های امنیتی که تجهیزات و نرم‌افزار سرویس، باید پشتیبانی نمایند، بویژه در خصوص:
  - محرمانگی اطلاعات
  - صحت اطلاعات
  - تشخیص هویت کاربران و سیستم‌ها

- حدود اختیارات کاربران راه دور
- ثبت کلیات ارتباطهای برقرار شده

**۲-۵-۱-۱۲- سیاست امنیتی سرویس File Sharing, Access and Transfer**

در سیاست‌های امنیتی این سرویس، لازم است سیاست سازمان در خصوص موارد ذیل مشخص گردد:

- تعیین افراد و ادارات مجاز به ارائه سرویس، متناسب با محرمانگی اطلاعات
- تعیین افراد مجاز به دسترسی به این سرویس، از داخل و خارج از سازمان
- بیان ضرورت تدوین آئین‌نامه یا دستورالعمل استفاده کاربران از این سرویس
- بیان ضرورت اعلام تغییرات لیست و محدودیت‌های افراد مجاز به واحد پشتیبانی امنیت شبکه
- تعیین طبقه‌بندی اطلاعات مجاز به ارائه در سرویس
- تعیین مرجع تشخیص و مسئول اقدام در خصوص مانیتورینگ سرویس
- تعیین و اعلام مسئولیت ارائه دهندگان و استفاده کنندگان از سرویس، در خصوص محتوای اطلاعات مورد مبادله
- تاکید بر استفاده صحیح کاربران از سرویس در راستای انجام امور اداری محوله
- منع تلاش کاربران سرویس در دسترسی غیرمجاز به سایر منابع
- تاکید بر اعمال کنترل‌های امنیتی موردنیاز و تعیین مسئول اعمال کنترل‌های امنیتی
- بیان ضرورت تعیین و اعلام مقررات تنبیهی در خصوص تخطی از سیاست‌های امنیتی

### ۲-۵-۱-۱۳- سیاست امنیتی سرویس Central Data Storage

در سیاست‌های امنیتی این سرویس، لازم است سیاست سازمان در خصوص موارد ذیل مشخص گردد:

- تعیین افراد و ادارات مجاز به ارائه این سرویس
- تعیین افراد مجاز به دسترسی به این سرویس، از داخل و خارج از سازمان
- بیان ضرورت تدوین آئین‌نامه یا دستورالعمل ارائه و استفاده کاربران از این سرویس
- بیان ضرورت اعلام تغییرات لیست و محدودیت‌های افراد و ادارات مجاز به واحد پشتیبانی امنیت شبکه
- تعیین طبقه‌بندی اطلاعات قابل ارائه در سرویس
- تعیین حریم خصوصی افراد یا ادارات در سرویس
- تعیین مرجع تشخیص و مسئول اقدام در خصوص مانیتورینگ سرویس
- تعیین و اعلام مسئولیت ارائه دهندگان و استفاده کنندگان از سرویس، در خصوص محتوای اطلاعات مورد مبادله
- تاکید بر استفاده صحیح کاربران از سرویس در راستای انجام امور اداری محوله
- منع تلاش کاربران سرویس در دسترسی غیرمجاز به سایر منابع
- تاکید بر اعمال کنترل‌های امنیتی موردنیاز و تعیین مسئول اعمال کنترل‌های امنیتی
- بیان ضرورت تعیین و اعلام مقررات تنبیهی در خصوص تخطی از سیاست‌های امنیتی

### ۲-۵-۱-۱۴- سیاست امنیتی سرویس Printer Sharing

در سیاست‌های امنیتی این سرویس، لازم است سیاست سازمان در خصوص موارد ذیل مشخص گردد:

- تعیین موارد مجاز استفاده از سرویس
- بیان ضرورت تدوین آئین‌نامه یا دستورالعمل ارائه و استفاده کاربران از این سرویس
- تعیین طبقه‌بندی اطلاعات قابل مبادله در سرویس
- تعیین و اعلام مسئولیت ارائه دهندگان و استفاده کنندگان از سرویس، در خصوص محتوای اطلاعات مورد مبادله
- تاکید بر استفاده صحیح کاربران از سرویس در راستای انجام امور اداری محوله
- تاکید بر اعمال کنترل‌های امنیتی موردنیاز و تعیین مسئول اعمال کنترل‌های امنیتی
- بیان ضرورت تعیین و اعلام مقررات تنبیهی در خصوص تخطی از سیاست‌های امنیتی

## ۲-۵-۲- سیاست‌های امنیتی سخت‌افزارها

### ۲-۵-۲-۱- اولویت‌بندی سخت‌افزارهای شبکه سازمان

در سیاست‌های امنیتی اولویت‌بندی سخت‌افزارها، لازم است سیاست سازمان در خصوص موارد ذیل مشخص گردد:

- دسته‌بندی سخت‌افزارهای شبکه سازمان و تعیین اولویت سخت‌افزارها از حیث حساسیت
- بیان ضرورت و نحوه استفاده از ماجول‌ها و سیستم‌های Redudndant در سخت‌افزارهای مختلف

### ۲-۵-۲-۲- سیاستهای امنیتی ایستگاه‌های کاری

در سیاست‌های امنیتی ایستگاه‌های کاری، لازم است سیاست سازمان در خصوص موارد ذیل مشخص گردد:

**تنظیمات ایستگاههای کاری:**

- بیان ضرورت بکارگیری رمزهای عبور مدیریتی و کاربر
- بیان ضرورت تدوین دستورالعمل مدیریت رمزهای عبور و تبعیت کاربران از آن
- بیان ضرورت یا عدم ضرورت اعمال محدودیت‌هایی در خصوص پورت‌های ارتباطی و درایوهای ایستگاه‌های کاری
- بیان ضرورت توجه به ترتیب اولویت درایوها در زمان Boot شدن ایستگاه
- تعیین محدودیت‌های نصب مودم روی ایستگاههای کاری متصل به شبکه داخلی و شبکه دسترسی به اینترنت سازمان
- تعیین نحوه تخصیص آدرس IP به ایستگاههای کاری شبکه سازمان، تدوین و اعلام دستورالعمل تخصیص، ثبت و تغییر آدرس IP ایستگاههای کاری
- شرایط تغییر کارت شبکه ایستگاه

**سیستم عامل ایستگاه:**

- تاکید بر انتخاب سیستم عامل امن برای ایستگاههای کاری
- بیان ضرورت تدوین دستورالعمل ایمن‌سازی سیستم عامل ایستگاههای کاری

**محافظت در مقابل ویروس:**

- بیان ضرورت نصب نرم‌افزار ضد ویروس یکپارچه در کلیه ایستگاههای کاری شبکه

- بیان ضرورت تصمیم‌گیری در خصوص نوع نرم‌افزار ضدویروس بصورت دوره‌ای توسط تیم پشتیبانی امنیت شبکه
- بیان ضرورت تهیه و در دسترس قرار دادن نرم‌افزار ضد ویروس و ارائه اطلاعات و آموزشهای لازم به کاربران
- بیان ضرورت Update نمودن نرم‌افزار ضد ویروس
- تعیین وظایف و مسئولیت‌های کاربر و تیم پشتیبانی حوادث در خصوص مقابله با ویروس

**نرم‌افزارهای مخرب:**

- بیان مجاز یا غیرمجاز بودن نصب نرم‌افزار Game، نرم‌افزار فاقد License و نرم‌افزار غیرضروری روی ایستگاههای کاری شبکه سازمان
- تعیین مسئول آسیب‌های احتمالی ناشی از نصب و بکارگیری نرم‌افزارهای فوق

**تهیه نسخه پشتیبان:**

- بیان ضرورت تهیه نسخه پشتیبان از اطلاعات ایستگاه و تعیین مسئول
- تاکید بر تامین امکانات تهیه و نگهداری نسخه پشتیبان اطلاعات

**ثبت و اعلام مشخصات ایستگاه کاری:**

- بیان ضرورت اعلام و ثبت آخرین مشخصات ایستگاه به واحد پشتیبانی امنیت شبکه
- بیان ضرورت تطبیق آخرین وضعیت موجود ایستگاه با وضعیت اعلام شده
- تعیین و اعلام مسئولیت کاربران ایستگاههای کاری در خصوص موارد فوق
- بیان ضرورت تعیین و اعلام مقررات تنبیهی در خصوص تخطی

**بازرسی دوره‌ای امنیت ایستگاههای کاری:**

- بیان ضرورت تطبیق مشخصات اعلام شده با مشخصات واقعی ایستگاه، بصورت دوره‌ای

### ۲-۵-۲-۳- سیاستهای امنیتی سرویس‌دهنده‌های شبکه

در سیاست‌های امنیتی سرویس‌دهنده‌های شبکه، لازم است سیاست سازمان در خصوص موارد ذیل مشخص گردد:

**تنظیمات سرویس‌دهنده:**

- بیان ضرورت بکارگیری رمزهای عبور مدیریتی و کاربر
- بیان ضرورت تدوین دستورالعمل مدیریت رمزهای عبور و تبعیت کاربران از آن
- بیان ضرورت اعمال محدودیت‌هایی در خصوص پورت‌های ارتباطی و درایوهای سرویس‌دهنده‌ها
- بیان ضرورت توجه به ترتیب اولویت درایوها در زمان Boot شدن سرویس‌دهنده‌ها
- محدودیت‌های نصب مودم روی سرویس‌دهنده‌های متصل به شبکه داخلی و شبکه دسترسی به اینترنت سازمان
- تعیین نحوه تخصیص آدرس IP به سرویس‌دهنده‌های شبکه سازمان و ضرورت تدوین و اعلام دستورالعمل تخصیص، ثبت و تغییر آدرس IP سرویس‌دهنده‌ها
- شرایط تغییر کارت شبکه سرویس‌دهنده‌ها

**سیستم عامل:**

- تاکید بر انتخاب سیستم عامل امن برای سرویس‌دهنده‌ها
- بیان ضرورت تدوین دستورالعمل ایمن‌سازی سیستم عامل سرویس‌دهنده‌ها

**محافظت در مقابل ویروس:**

- بیان ضرورت نصب نرم‌افزار ضد ویروس یکپارچه در کلیه سرویس‌دهنده‌های شبکه
- بیان ضرورت تصمیم‌گیری در خصوص نوع نرم‌افزار ضدویروس بصورت دوره‌ای توسط تیم پشتیبانی امنیت شبکه
- بیان ضرورت تهیه و در دسترسی کاربر قرار دادن نرم‌افزار ضد ویروس و ارائه اطلاعات و آموزشهای لازم به مدیران سرویس
- بیان ضرورت به روز نمودن نرم‌افزار ضد ویروس
- تعیین وظایف و مسئولیت‌های مدیران سرویس و تیم پشتیبانی حوادث در خصوص مقابله با ویروس

**نرم‌افزارهای مخرب:**

- بیان مجاز یا غیرمجاز بودن نصب نرم‌افزار Game، نرم‌افزار فاقد License و نرم‌افزار غیرضروری روی سرویس‌دهنده‌های شبکه سازمان
- تعیین مسئول آسیب‌های احتمالی ناشی از نصب و بکارگیری نرم‌افزارهای فوق

**تهیه نسخه پشتیبان:**

- بیان ضرورت تهیه نسخه پشتیبان از اطلاعات سرویس‌دهنده‌ها و تعیین مسئول آن
- تاکید بر تامین امکانات تهیه و نگهداری نسخه پشتیبان اطلاعات

**ثبت و اعلام مشخصات:**

- بیان ضرورت اعلام و ثبت آخرین مشخصات سرویس‌دهنده‌ها به واحد پشتیبانی امنیت شبکه
- بیان ضرورت تطبیق آخرین وضعیت موجود سرویس‌دهنده‌ها با وضعیت اعلام شده
- تعیین و اعلام مسئولیت کاربران سرویس‌دهنده‌ها در خصوص موارد فوق
- بیان ضرورت تعیین و اعلام مقررات تنبیهی در خصوص عدم اجرای سیاست‌های فوق

**بازرسی دوره‌ای امنیت ایستگاههای کاری:**

- بیان ضرورت تطبیق مشخصات اعلام شده با مشخصات واقعی سرویس‌دهنده‌ها بصورت دوره‌ای و تعیین مسئول انجام بازرسی

**۲-۵-۲-۴- سیاستهای امنیتی تجهیزات زیرساختار شبکه**

در سیاست‌های امنیتی تجهیزات زیرساختار شبکه، لازم است سیاست سازمان در خصوص موارد ذیل مشخص گردد:

**مدیریت تجهیزات:**

- تعیین امکان مدیریت از راه دور تجهیزات، پروتکل‌های مجاز و مکانیزم‌های امنیتی موردنیاز جهت مدیریت از راه دور تجهیزات
- تاکید بر مبادله اطلاعات پیکربندی با تجهیزات، بصورت امن
- تاکید بر نگهداری از یک نسخه از اطلاعات پیکربندی تجهیزات، در محل امن و قابل دسترس

**حذف اینترفیسها و سرویس‌های غیرضروری:**

- تاکید بر غیرفعال نمودن سرویس‌های بالقوه خطرناک و سرویس‌هائی که معمولا مورد استفاده قرار نمی‌گیرند
- تاکید بر غیرفعال نمودن اینترفیسهایی از تجهیزات که در حال حاضر مورد استفاده قرار نگرفته‌اند

**رویدادنگاری:**

- ثبت تنظیمات، دسترسی‌ها و مبادلات با جزئیات مناسب
- استفاده همزمان از روش‌های مختلف ثبت رویداد به‌منظور افزایش ایمنی در تجهیزات زیرساختار شبکه
- سنکرون بودن کلیه تجهیزات شبکه، به‌منظور استفاده مفید از رویدادنامه‌ها

**تصدیق هویت، تعیین حدود اختیارات و ثبت اقدامات کاربران:**

- تاکید بر استفاده از مکانیزم‌های مناسب تعیین هویت
- تاکید بر تعیین حدود اختیارات کاربران مدیریتی تجهیزات

**تشخیص و خنثی نمودن حملات:**

- تاکید بر تشخیص و خنثی نمودن حملات انجام شده علیه خود تجهیزات، بویژه حملات ممانعت از سرویس،با استفاده از کنترل‌های موجود روی تجهیزات
- تعیین نحوه برخورد با بسته‌هائی که از خارج از شبکه، به مقصد تجهیزات شبکه ارسال شده‌اند
- تعیین نحوه برخورد با بسته‌هائی که توسط ایستگاههای کاربران غیرمدیریتی داخل شبکه برای تجهیزات شبکه ارسال می‌شوند
- تعیین نحوه برخورد با حذف بسته‌هایی که آدرس جعل شده دارند

**سفت‌افزار تجهیزات شبکه:**

- تاکید بر بررسی و رفع دوره‌ای آسیب‌پذیری‌های سفت‌افزار تجهیزات شبکه
- تاکید بر ارتقاء دوره‌ای نسخه سفت‌افزار تجهیزات شبکه

**محافظت فیزیکی:**

- تاکید بر قرار دادن تجهیزات زیرساختار شبکه، تجهیزات گذرگاه‌های اتصال به شبکه دولت و شبکه اینترنت در داخل سایت و محافظت فیزیکی از آنها.

**شناسنامه تجهیزات شبکه:**

- تاکید بر ایجاد شناسنامه تجهیزات و یادداشت اطلاعات زیر در آن:
  - اینترفیسهای موجود و فعال
  - روش و پروتکل مدیریت
  - ایستگاههای مجاز برای مدیریت
  - نسخه سفت‌افزار
  - آخرین Patchهای نصب شده
  - آخرین تغییرات انجام شده روی پیکربندی
  - متن آخرین پیکربندی
  - آدرس هر یک از اینترفیسها
  - مشخصات VLAN های تعریف شده ( برای سوئیچ‌ها )

**بازرسی امنیتی تجهیزات شبکه:**

- تاکید بر بررسی دوره‌ای رعایت کلیه سیاست‌های فوق

### ۲-۵-۲-۵- سیاستهای امنیتی استفاده از کامپیوترهای Laptop

در سیاست‌های امنیتی کامپیوترهای Laptop، لازم است سیاست سازمان در خصوص موارد ذیل مشخص گردد:

- تاکید بر ایمن‌سازی کامپیوترهای Laptop متعلق به مدیران سازمان
- تعیین محدودیت‌های اتصال کامپیوترهای Laptop به شبکه داخلی و دسترسی به اینترنت
- تعیین محدودیت‌های قرار دادن اطلاعات روی کامپیوترهای Laptop
- تعیین سیستم عامل و نرم‌افزارهایی که باید روی کامپیوترهای Laptop نصب شوند
- تعیین ضرورت یا عدم ضرورت بررسی وضعیت کامپیوترهای Laptop متعلق به افراد خارج از سازمان، قبل از ورود به سازمان یا اتصال به شبکه سازمان
- بیان ضرورت تدوین دستورالعمل فنی و اجرایی ایمن‌سازی کامپیوترهای Laptop
- تعیین کنترل‌هائی که سیستم امنیتی شبکه سازمان باید روی Laptopها داشته باشد

### ۲-۵-۲-۶- سیاست‌های امنیتی استفاده از مودم

در سیاست‌های امنیتی استفاده از مودم، لازم است سیاست سازمان در خصوص موارد ذیل مشخص گردد:

**استفاده از مودم روی ایستگاههای کاری شبکه:**

- تعیین مجاز بودن یا نبودن نصب مودم روی ایستگاههای کاری شبکه داخلی
- تعیین مجاز بودن یا نبودن نصب مودم روی ایستگاههای کاری شبکه دسترسی به اینترنت سازمان

- تعیین مجاز بودن یا نبودن نصب مودم روی ایستگاههای مدیریتی و امنیتی شبکه
- تعیین مسئول تشخیص نصب مودم روی ایستگاههای شبکه

**استفاده از مودم روی سرویس‌دهنده‌های شبکه:**

- تعیین مجاز بودن یا نبودن نصب مودم روی سرویس‌دهنده‌های متصل به شبکه داخلی
- تعیین مجاز بودن یا نبودن نصب مودم روی سرویس‌دهنده‌های متصل به شبکه اینترنت سازمان

**استفاده از مودم روی کامپیوترهای مستقل ( Single ):**

- مجاز بودن یا نبودن نصب مودم روی کامپیوترهای مستقل از شبکه

**شرایط استفاده از مودم:**

- بیان ضرورت تدوین دستوالعمل استفاده صحیح از مودم

### ۲-۵-۲-۷- سیاست‌های امنیتی استفاده از تجهیزات بی‌سیم

در سیاست‌های امنیتی استفاده از تجهیزات بی‌سیم، لازم است سیاست سازمان در خصوص موارد ذیل مشخص گردد:

- تعیین محدودیت‌های استفاده از تجهیزات دسترسی بی‌سیم در شبکه داخلی و شبکه دسترسی به اینترنت سازمان
- تعیین مرجع تشخیص ضرورت استفاده از تجهیزات دسترسی بی‌سیم
- بیان ضرورت تدوین دستورالعمل و شرایط خرید تجهیزات دسترسی بی‌سیم و مجوزهای لازم

- بیان ضرورت تعیین و اعلام مقررات تنبیهی استفاده غیرمجاز از تجهیزات دسترسی بی‌سیم

**شرایط فنی بکارگیری تجهیزات بی‌سیم**:

- تعیین مشخصات فنی موردنیاز تجهیزات دسترسی بی‌سیم، جهت بکارگیری در شبکه داخلی و شبکه اینترنت سازمان ، بویژه در خصوص:
  - محرمانگی اطلاعات مورد مبادله
  - صحت اطلاعات مورد مبادله
  - تصدیق هویت فرستنده و گیرنده

### ۲-۵-۲-۸- سیاستهای امنیتی سفارش، خرید، تست، نصب و پیکربندی سخت‌افزار

در سیاست‌های امنیتی سفارش،خرید، تست، نصب و پیکربندی سخت‌افزارها، لازم است سیاست سازمان در خصوص موارد ذیل مشخص گردد:

**سفارش خرید سخت‌افزار**:

- بیان ضرورت توجه به آسیب‌پذیری‌های امنیتی سخت‌افزارها در زمان اعلام مشخصات
- بیان ضرورت اعلام مشخصات و قابلیت‌های امنیتی سخت‌افزارها در زمان اعلام مشخصات
- بیان ضرورت اعلام مشخصات و قابلیت‌های امنیتی مدیریت سخت‌افزارها در زمان اعلام مشخصات
- تعیین مسئول اعلام مشخصات امنیتی موردنیاز سخت‌افزارها
- تعیین دستورالعملها و مجوزهای موردنیاز
- بیان ضرورت توجه به پیش‌بینی سیستم‌ها و ماجولهای Redundant

- تعیین مسئول و ضرورت توجه به موارد امنیتی در خرید سخت‌افزارها

**خرید سخت‌افزار:**

- بیان ضررت عدم اعلام شرایط و محل بکارگیری سخت‌افزار در شبکه سازمان

**تست و تحویل سخت‌افزار:**

- بیان ضرورت انجام بررسی‌های فیزیکی قبل از نصب سخت‌افزارها
- تاکید بر تست سخت‌افزارها در شبکه جداگانه
- تعیین و اعلام تست‌های موردنیاز سخت‌افزارها

**پیکربندی سخت‌افزار:**

- تاکید بر عدم واگذاری تنظیم نهائی پیکربندی سخت‌افزارها به فروشنده
- بیان ضرورت تغییر کلیه رمزهای عبور پیش‌فرض یا تنظیم شده توسط شرکت فروشنده
- بیان ضرورت بستن کلیه پورتها و سرویس‌های غیرضروری، قبل از نصب در شبکه

**نصب سخت‌افزار:**

- تاکید بر ضرورت هماهنگی قبل از اتصال سخت‌افزارهائی که موجب قطع موقت سرویس‌های شبکه می‌شوند
- محدودیت‌های تغییر، حذف یا افزودن سخت‌افزارهائی که موجب قطع موقت سرویس‌های شبکه می‌شوند، بویژه در ساعات اداری

- محافظتهای فیزیکی خاص از سخت‌افزارهای حساس از قبیل تجهیزات شبکه و سرویس‌دهنده‌ها
- کنترل‌ها و حساسیت‌های برق تجهیزات لایه هسته، لایه توزیع، سرویس‌دهنده‌ها و تجهیزات گذرگاه‌های اتصال شبکه داخلی و اینترنت سازمان به سایر شبکه‌ها

**پشتیبانی سخت‌افزار:**

- تاکید بر ضرورت بررسی دوره‌ای
- تعیین مسئول بررسی‌های دوره‌ای

### ۲-۵-۳- سیاست‌های امنیتی نرم‌افزارها

#### ۲-۵-۳-۱- اولویت‌بندی نرم‌افزارهای شبکه

در سیاست‌های امنیتی اولویت‌بندی نرم‌افزارها، لازم است سیاست سازمان در خصوص موارد ذیل مشخص گردد:

- تعیین انواع نرم‌افزارهای شبکه سازمان و دسته‌بندی آنها از حیث حساسیت
- بیان ضرورت توجه به استفاده از نرم‌افزارهای امنیت شبکه تولید داخل
- بیان ضرورت توجه به استفاده از نرم‌افزارهای دارای تائیدیه‌های معتبر ارزیابی امنیتی یا ارزیابی اعتماد به عملکرد
- بیان ضرورت توجه به پیاده‌سازی ماجولهای امنیتی ویژه سازمان و افزودن آن به نرم‌افزارهای کاربردی که از این پس ایجاد خواهند شد
- بیان ضرورت توجه به استفاده از نرم‌افزارهای دارای license

**۲-۵-۳-۲- سیاست‌های امنیتی سیستم عامل‌های مورد استفاده در شبکه**

در سیاست‌های امنیتی سیستم‌عامل‌ها، لازم است سیاست سازمان در خصوص موارد ذیل مشخص گردد:

**سیستم عامل سرویس‌دهنده‌ها:**

- پیکربندی امن کلیه سیستم عامل‌های مورد استفاده در سرویس‌دهنده‌های شبکه
- تدوین و اعلام دستورالعمل‌های فنی در خصوص ایمن‌سازی سیستم عامل سرویس‌دهنده‌ها
- اطلاع‌رسانی واحد پشتیبانی امنیت شبکه در خصوص امنیت سیستم عامل سرویس‌دهنده‌ها، اعلام و نصب Patchها و نرم‌افزارهای ضد ویروس
- توجه به استفاده از سیستم‌عامل‌های امن یا سیستم‌عامل‌های Open Source از قبیل Open BSD، Free BSD و Linux
- استفاده از سیستم عامل‌های متفاوت به‌منظور جلوگیری از بروز مشکل از کار اندازی سرویس
- توجه به نصب فقط یک سیستم عامل روی هر یک از سرویس‌دهنده‌های شبکه
- تدوین روال تغییر سیستم عامل یا نصب مجدد آن
- پرهیز از قراردادن فایلهای اطلاعاتی متفرقه، نسخه پشتیبان اطلاعات همان سرویس‌دهنده و نسخه پشتیبان اطلاعات سایر سرویس‌ها روی سرویس‌دهنده‌ها
- ثبت دسترسی‌های کاربران شبکه سازمان یا سایر شبکه‌های متصل به آن، به نرم‌افزار سرویس یا سایر نرم‌افزارهای کاربردی موجود روی سرویس‌دهنده، سیستم عامل سرویس‌دهنده و اطلاعات سیستمی سیستم عامل و سیاست‌های امنیتی سیستم عامل

- بررسی دوره‌ای آسیب‌پذیری‌های سیستم عامل سرویس‌دهنده‌ها و نصب Patchهای مناسب

**سیستم عامل ایستگاههای کاری:**

- پیکربندی امن کلیه سیستم عامل‌های مورد استفاده در ایستگاهها
- تدوین و اعلام دستورالعمل‌های فنی در خصوص ایمن‌سازی سیستم عامل ایستگاهها
- اطلاع‌رسانی واحد پشتیبانی امنیت شبکه در خصوص امنیت سیستم عامل ایستگاهها، اعلام و نصب Patchها و نرم‌افزارهای ضد ویروس
- توجه به استفاده از سیستم‌عامل‌های امن یا سیستم‌عامل‌های Open Source از قبیل Open BSD، Free BSD و Linux
- تدوین روال تغییر سیستم عامل یا نصب مجدد آن
- پرهیز از قراردادن فایلهای اطلاعاتی متفرقه، نسخه پشتیبان اطلاعات و ... روی ایستگاه
- ثبت دسترسی‌های کاربران شبکه سازمان یا سایر شبکه‌های متصل به آن، به ایستگاه
- بررسی دوره‌ای آسیب‌پذیری‌های سیستم عامل ایستگاهها و نصب Patchهای مناسب

### ۲-۵-۳-۳- نیازمندی‌های امنیتی نرم‌افزارهای کاربردی شبکه

در سیاست‌های امنیتی نرم‌افزارهای کاربردی، لازم است سیاست سازمان در خصوص موارد ذیل مشخص گردد:

**نیازمندی‌های تامین محرمانگی اطلاعات:**

- الگوریتم‌های رمزنگاری متناسب با سطح طبقه‌بندی اطلاعات، در زمان ذخیره شدن اطلاعات در بانک اطلاعاتی، برای نسخه پشتیبان اطلاعات، برای مبادله اطلاعات در شبکه داخلی و مبادله اطلاعات در شبکه اینترنت

**نیازمندی‌های تامین صحت اطلاعات:**

- مکانیزم‌های متناسب با سطح طبقه‌بندی اطلاعات به منظور تامین صحت اطلاعات ذخیره شده، اطلاعات پشتیبان، اطلاعات در حال مبادله در شبکه داخلی و اطلاعات در حال مبادله در شبکه اینترنت

**نیازمندی‌های تعیین هویت کاربران:**

- مکانیزم تعیین هویت متناسب با سطح طبقه‌بندی اطلاعات به منظور شناسائی کاربران جهت دسترسی به اطلاعات نرم‌افزار

**نیازمندی‌های تعیین حدود اختیارات کاربران:**

- مکانیزم تعیین حدود اختیارات کاربران، متناسب با سطح طبقه‌بندی اطلاعات
- ضرورت توجه به تعیین حدود اختیارات کاربران، از نظر اقداماتی که کاربر در هر یک از قسمتهای نرم‌افزار، مجاز به انجام آنها می‌باشد، از قبیل مشاهده، ویرایش، حذف و تهیه پشتیبان

**نیازمندی‌های ثبت اقدامات انجام شده توسط کاربر:**

- ثبت اقدامات انجام شده توسط کاربر، بر اساس استانداردهای ثبت وقایع
- ثبت اقدامات کاربر با جزئیات مختلف و قابل انتخاب
- قابل انتخاب بودن جزئیات ثبت وقایع عملکرد کاربر در هر یک از قسمتهای نرم‌افزار
- قابل بازگشت بودن عملیات کاربر

**نیازمندی‌های تامین امنیت ارتباط:**

- مدیریت از راه دور نرم‌افزارهای مبتنی بر وب
- پشتیبانی نرم‌افزارهای مبتنی بر وب از پروتکل‌های امن ارتباطی

### ۲-۵-۳-۴- استانداردهای نرم‌افزارهای شبکه

در سیاست‌های امنیتی استانداردهای نرم‌افزارهای شبکه، لازم است سیاست سازمان در خصوص موارد ذیل مشخص گردد:

**استاندارد طراحی نرم‌افزار:**

- تعیین لیست و اولویت استانداردهای قابل پذیرش جهت طراحی نرم‌افزارهای کاربردی شبکه سازمان

**استاندارد پیاده‌سازی نرم‌افزار:**

- تعیین لیست و اولویت استانداردهای قابل پذیرش جهت پیاده‌سازی نرم‌افزارهای کاربردی شبکه سازمان

**استاندارد تست نرم‌افزار:**

- تعیین لیست و اولویت استانداردهای قابل پذیرش جهت تست کارآئی و امنیت نرم‌افزارهای کاربردی شبکه سازمان

**۲-۵-۳-۵- سیاست‌های امنیتی دسترسی کاربران به نرم‌افزارهای شبکه**

در سیاست‌های امنیتی دسترسی کاربران به نرم‌افزارهای شبکه، لازم است سیاست سازمان در خصوص موارد ذیل مشخص گردد:

**درخواست استفاده از سرویس:**

- بیان ضرورت تدوین آئین‌نامه و دستورالعمل دسترسی کاربران به نرم‌افزارهای شبکه

**ثبت اطلاعات کاربر:**

- ثبت اطلاعات مربوط به دسترسی کاربران به نرم‌افزارها و تشخیص تلاش‌های غیرمجاز آنان
- ثبت عملکرد کاربر جهت تامین قابلیت پی‌گیری

**حذف یا تقییر دسترسی کاربر:**

- اعلام جابجائی کاربران توسط ادارات

**۲-۵-۳-۶- سیاست‌های امنیتی سفارش، خرید، تست، نصب و پیکربندی نرم‌افزار**

در سیاست‌های امنیتی سفارش، خرید، تست، نصب و پیکربندی نرم‌افزارها، لازم است سیاست سازمان در خصوص موارد ذیل مشخص گردد:

**سفارش خرید نرم‌افزار:**

- توجه به آسیب‌پذیری‌های امنیتی نرم افزار در اعلام مشخصات
- توجه به نیازمندی‌های امنیتی موردنیاز برای نرم‌افزار، از قبیل مکانیزم‌های قابل قبول تصدیق هویت، روش تعیین حدود اختیارات و ثبت وقایع، بازگشت‌پذیری اقدامات کاربر، تامین محرمانگی اطلاعات در زمان ذخیره یا مبادله اطلاعات و سایر موارد، در زمان اعلام مشخصات نرم‌افزار
- توجه به پشتیبانی نرم‌افزار از پروتکل‌های امن مدیریت از راه دور
- توجه به امن بودن پایگاه داده در انتخاب نرم‌افزارهای اطلاعاتی
- دریافت تائید مشخصات امنیتی برای سفارش خرید نرم‌افزارهای حساس

**درخواست تغییر نرم‌افزار:**

- دریافت تائید امنیتی برای تغییر نرم‌افزارها

**خرید نرم‌افزار:**

- عدم انتقال اطلاعات بکارگیری نرم‌افزار به فروشنده

**تست و تحویل نرم‌افزار:**

- تست نرم‌افزار خریداری شده، قبل از نصب و اتصال به شبکه سازمان، در شبکه فرعی مستقل
- وارد ننمودن اطلاعات واقعی سازمان به نرم‌افزار، در مرحله تست

- رورت انجام تست عملکرد ( Functionality Test ) و تست آسیب‌پذیری‌های نرم‌افزار خریداری شده توسط نرم‌افزارهای Vulnerability Scanner و روش‌های دستی

**پیکربندی نرم‌افزار:**

- پیکربندی امن سیستم‌عامل سرویس‌دهنده یا ایستگاهی که نرم‌افزار روی آن نصب می‌شود، بر اساس دستورالعمل مشخص
- حذف و تغییر کلیه رمزهای عبور پیش‌فرض یا تنظیم شده توسط شرکت فروشنده یا پیاده‌ساز نرم‌افزار
- حذف مکانیزم‌های مدیریتی غیرضروری موجود روی نرم‌افزار، از قبیل اینترفیس مدیریت از طریق Web

**نصب نرم‌افزار:**

- هماهنگی با مسئولین، قبل از نصب نرم‌افزار تغییر یافته در شبکه سازمان
- نصب نرم‌افزار تغییر یافته در شبکه سازمان، خارج از ساعات اداری
- تهیه نسخه پشتیبان از اطلاعات و نسخه قبلی نرم‌افزار، قبل از نصب نرم‌افزار تغییر یافته در شبکه سازمان

**پشتیبانی نرم‌افزار:**

- بررسی و رفع آسیب‌پذیری‌های نرم‌افزارهای شبکه، بصورت دوره‌ای
- نگهداری از نسخه پشتیبان سورس کد کلیه نسخه‌های در حال استفاده نرم‌افزارهای توسعه یافته
- نگهداری از نسخه پشتیبان نرم‌افزارهای خریداری شده

### ۲-۵-۴- سیاست‌های امنیتی اطلاعات

#### ۲-۵-۴-۱- سند طبقه بندی اطلاعات رایانه‌ای

در سیاست‌های امنیتی طبقه‌بندی اطلاعات رایانه‌ای سازمان، لازم است سیاست سازمان در خصوص موارد ذیل مشخص گردد:

**سطوح طبقه بندی اطلاعات رایانه‌ای:**

- تعیین سطوح طبقه بندی مجاز برای اطلاعات شبکه سازمان
- تعیین سطوح طبقه بندی اطلاعاتی مع مجاز به قرار گرفتن در شبکه سازمان نمی‌باشند

**طبقه بندی اطلاعات رایانه‌ای:**

- تنظیم سند طبقه بندی اطلاعات، برای هر یک از سیستم های اطلاعاتی سازمان
- تعیین مسئول طبقه بندی اطلاعات
- تعیین مسئول تامین امنیت متناسب با سطح طبقه‌بندی اعلام شده برای اطلاعات
- اولویت‌بندی پارامترهای تعیین طبقه‌بندی اطلاعات

### ۲-۵-۴-۲- محدودیت‌های اطلاعات طبقه‌بندی شده شبکه

در محدودیت‌های اطلاعات طبقه‌بندی شده سازمان، لازم است سیاست سازمان در خصوص موارد ذیل مشخص گردد:

**محدودیت‌های ذخیره سازی اطلاعات:**

- تعیین محدودیت‌های محل قرار گرفتن اطلاعات روی ایستگاههای کاری، سرویس‌دهنده‌های شبکه داخلی و شبکه متصل به اینترنت سازمان، برای هر یک از اطلاعات طبقه‌بندی شده

**محدودیت‌های دسترسی به اطلاعات:**

- تعیین محدودیت‌های دسترسی به اطلاعات از طریق شبکه داخلی سازمان، شبکه WAN سازمان، شبکه دولت و شبکه اینترنت، برای هر یک از اطلاعات طبقه‌بندی شده

**محدودیت‌های مبادله، چاپ و کپی اطلاعات:**

- تعیین محدودیت‌های مبادله اطلاعات از طریق مودم و تجهیزات Wireless، امکان تهیه کپی اطلاعات روی دیسکت، CD، DVD و سایر رسانه‌ها، امکان چاپ اطلاعات روی چاپگرهای مشترک و امکان اشتراک اطلاعات در شبکه، برای هر یک از اطلاعات طبقه‌بندی شده

**محدودیت‌های نسخه پشتیبان اطلاعات:**

- تعیین محدودیت‌های نسخه پشتیبان اطلاعات، از قبیل رسانه یا سرویس‌دهنده مجاز برای ذخیره‌سازی، حداقل و حداکثر نسخ پشتیبان، مسئول تهیه و نگهداری از اطلاعات پشتیبان، برای هر یک از اطلاعات طبقه‌بندی شده

| محدودیتهای امنیتی اطلاعات | طبقه بندی | | |
|---|---|---|---|
| | طبقه‌بندی (۱) | طبقه‌بندی (۲) | طبقه‌بندی (۳) |
| **محل قرارگیری** | | | |
| امکان قرار گرفتن روی سرویس دهنده شبکه داخلی | | | |
| امکان قرار گرفتن روی ایستگاههای کاری شبکه داخلی | | | |
| امکان قرار گرفتن روی سرویس دهنده شبکه دسترسی به اینترنت | | | |
| امکان قرار گرفتن روی ایستگاههای کاری شبکه دسترسی به اینترنت | | | |
| امکان قرار گرفتن روی کامپیوترهای Laptop | | | |
| **دسترسی به اطلاعات** | | | |
| امکان دسترسی به اطلاعات، از طریق شبکه داخلی | | | |
| امکان دسترسی به اطلاعات، از طریق WAN سازمان | | | |
| امکان دسترسی به اطلاعات، از طریق شبکه دولت | | | |
| امکان دسترسی به اطلاعات، از طریق شبکه اینترنت | | | |
| **چاپ و انتقال اطلاعات** | | | |
| امکان مبادله از طریق مودم | | | |
| امکان مبادله اطلاعات از طریق تجهیزات Wireless | | | |
| امکان کپی شدن روی دیسکت، CD، DVD یا سایر رسانه‌ها | | | |
| امکان چاپ اطلاعات روی چاپگر مشترک | | | |
| امکان اشتراک اطلاعات، روی شبکه داخلی | | | |
| **نسخه پشتیبان** | | | |
| امکان تهیه پشتیبان روی دیسکت، CD یا DVD | | | |
| امکان قرار گرفتن روی سرویس دهنده پشتیبان | | | |
| حداقل تعداد نسخ پشتیبان | | | |
| حداکثر تعداد نسخ پشتیبان | | | |
| مسئول تهیه پشتیبان | | | |

| | | | |
|---|---|---|---|
| دوره زمانی تهیه پشتیبان | | | |
| محل نگهداری نسخه پشتیبان | | | |
| مسئول نگهداری نسخه پشتیبان | | | |
| رسانه ای که نسخه پشتیبان، روی آن تهیه شود | | | |
| محافظتهای خاص امنیتی موردنیاز نسخه پشتیبان | | | |

جدول (۲-۲): جدول محدودیت‌های اطلاعات طبقه‌بندی شده سازمان

**۲-۵-۴-۳- نیازمندی‌های امنیتی اطلاعات طبقه بندی شده شبکه**

در نیازمندی‌های امنیتی اطلاعات طبقه‌بندی شده سازمان، لازم است سیاست سازمان در خصوص موارد ذیل مشخص گردد:

**محرمانگی**:

- تعیین الگوریتم‌های مناسب و قابل قبول جهت تامین محرمانگی اطلاعات، در زمان ذخیره‌سازی، اطلاعات نسخه پشتیبان، مبادله در شبکه داخلی سازمان، شبکه WAN سازمان، شبکه دولت و شبکه اینترنت، برای هر یک از اطلاعات طبقه‌بندی شده شبکه سازمان

**صحت**:

- تعیین الگوریتم‌های مناسب و قابل قبول جهت تامین صحت اطلاعات، در زمان ذخیره‌سازی، اطلاعات نسخه پشتیبان، مبادله در شبکه داخلی سازمان، شبکه WAN سازمان، شبکه دولت و شبکه اینترنت، برای هر یک از اطلاعات طبقه‌بندی شده شبکه سازمان

**تشخیص هویت کاربران در دسترسی به اطلاعات**:

- تعیین مکانیزم‌های مناسب و قابل قبول به‌منظور تشخیص هویت کاربران جهت دسترسی به هر یک از اطلاعات طبقه‌بندی شده شبکه سازمان

**حدود اختیارات کاربران در دسترسی به اطلاعات:**

- تعیین مکانیزم‌های مناسب و قابل قبول به‌منظور تعیین حدود اختیارات کاربران جهت دسترسی به هر یک از اطلاعات طبقه‌بندی شده شبکه سازمان

**ثبت عملکرد کاربران در دسترسی به اطلاعات طبقه‌بندی شده:**

- تعیین موارد ثبت عملکرد کاربران در دسترسی به هر یک از اطلاعات طبقه‌بندی شده شبکه سازمان

| نیازمندی‌های امنیتی اطلاعات | طبقه بندی | | |
|---|---|---|---|
| | طبقه‌بندی (۱) | طبقه‌بندی (۲) | طبقه‌بندی (۳) |
| **الگوریتم‌های مناسب جهت تامین محرمانگی اطلاعات در زمان:** | | | |
| ذخیره شدن در بانک اطلاعاتی | | | |
| ذخیره شدن در نسخه پشتیبان | | | |
| مبادله در شبکه داخلی سازمان | | | |
| مبادله در شبکه WAN سازمان | | | |
| مبادله از طریق شبکه دولت | | | |
| مبادله از طریق شبکه اینترنت | | | |
| **الگوریتم‌های مناسب جهت تامین صحت اطلاعات در زمان:** | | | |
| ذخیره شدن در بانک اطلاعاتی | | | |
| ذخیره شدن در نسخه پشتیبان | | | |
| مبادله در شبکه داخلی سازمان | | | |
| مبادله در شبکه WAN سازمان | | | |
| مبادله از طریق شبکه دولت | | | |
| مبادله از طریق شبکه اینترنت | | | |
| **تشخیص هویت و تعیین حدود اختیارات** | | | |
| مکانیزم تشخیص هویت مناسب کاربران جهت دسترسی به اطلاعات | | | |
| مکانیزم تعیین حدود اختیارات کاربران | | | |

| ثبت عملکرد کاربر | | | |
|---|---|---|---|
| امکان ثبت مشاهده اطلاعات ؟ | | | |
| امکان ثبت ایجاد، ویرایش و حذف اطلاعات جدید؟ | | | |
| امکان ثبت انتقال اطلاعات ؟ | | | |
| امکان ثبت تهیه نسخه پشتیبان اطلاعات ؟ | | | |

جدول (۲-۳): جدول نیازمندی‌های امنیتی اطلاعات طبقه‌بندی شده سازمان

### ۲-۵-۵- سیاست‌های امنیتی ارتباطات شبکه

#### ۲-۵-۵-۱- ارتباطات مجاز شبکه

در سیاست‌های امنیتی ارتباطات مجاز شبکه سازمان، لازم است سیاست سازمان در خصوص موارد ذیل مشخص گردد:

**بخش‌های مختلف شبکه:**

- تعیین حوزه زیرساخت شبکه سازمان، که می‌تواند از دو بخش اصلی به شرح زیر، تشکیل شده باشد:
  - زیرساخت شبکه داخلی سازمان
  - زیرساخت شبکه دسترسی به اینترنت سازمان
- علاوه بر شبکه های فوق، شبکه های محلی داخلی ادارات در سازمان می‌توانند وجود داشته باشند که از نظر اهداف و ماهیت اطلاعات، متفاوت با زیرساختهای فوق باشند. تامین امنیت در این شبکه‌ها، توسط مالک شبکه و بر اساس سیاست‌های امنیتی مستقل، انجام خواهد شد.

**ارتباطات مجاز و غیرمجاز شبکه داخلی:**

- تعیین شبکه‌هائی که شبکه داخلی سازمان، مجاز به ارتباط مستقیم یا غیرمستقیم با آنها می‌باشد، از قبیل:

- شبکه دولت
- شبکه سایر سازمان‌ها

- تاکید بر استفاده از سیستم امنیتی شبکه مناسب، در محل اتصال شبکه داخلی سازمان، به سایر شبکه‌ها
- تاکید بر قرارگیری بخش‌هایی از شبکه داخلی سازمان که با شبکه دولت و شبکه سایر سازمان‌ها و شبکه WAN سازمان ارتباط مستقیم دارد، در نواحی امنیتی مستقل
- تاکید بر ارتباط با شبکه ادارات دولتی، از طریق شبکه دولت و در قالب سیاست‌های امنیتی این شبکه
- نیاز به اخذ مجوز، برای اتصال شبکه داخلی سازمان، به سایر شبکه‌ها
- تعیین مجاز یا غیرمجاز بودن ارتباط شبکه داخلی سازمان با شبکه های عمومی از قبیل شبکه اینترنت و تعیین مکانیزم‌های امنیتی موردنیاز در محل اتصال

**ارتباطات مجاز و غیرمجاز شبکه دسترسی به اینترنت:**

- محدودیت‌های شبکه دسترسی به اینترنت سازمان، در خصوص ارتباط با شبکه اینترنت
- محافظت‌های امنیتی موردنیاز از شبکه دسترسی به اینترنت سازمان، در اتصال با شبکه اینترنت
- تعیین مجاز یا غیرمجاز بودن ارتباط شبکه دسترسی به اینترنت سازمان با شبکه داخلی سازمان
- تعیین مجاز یا غیرمجاز بودن ارتباط شبکه دسترسی به اینترنت سازمان با شبکه دولت و سایر شبکه‌هایی که از سطحی از محرمانگی برخوردار می‌باشند

### ۲-۵-۵-۲- سیاست‌های امنیتی ارتباطات شبکه داخلی

در سیاست‌های امنیتی ارتباطات شبکه داخلی سازمان، لازم است سیاست سازمان در خصوص موارد ذیل مشخص گردد:

**بخشهای مختلف شبکه داخلی:**

- تعیین بخش‌های مختلف شبکه داخلی سازمان، با توجه به لزوم جداسازی و تشکیل نواحی امنیتی مستقل

**دسترسی های مجاز از هر یک از بخش‌های شبکه داخلی به سایر شبکه‌ها:**

- تعیین مجاز یا غیرمجاز بودن دسترسی کاربران هر یک از بخش‌های شبکه داخلی سازمان، به سایر بخش‌های این شبکه
- تعیین مجاز یا غیرمجاز بودن دسترسی کاربران هر یک از بخش‌های شبکه داخلی سازمان، به بخش خارجی این شبکه ( سایر شبکه‌های متصل )

**دسترسی های مجاز از سایر شبکه‌های متصل، به هر یک از بخش‌های شبکه داخلی:**

- تعیین مجاز یا غیرمجاز بودن دسترسی کاربران سایر شبکه‌های متصل، به هر یک از بخش‌های شبکه داخلی سازمان

**دسترسی های مدیریتی مجاز در شبکه داخلی:**

- تعیین ایستگاههای مجاز به دسترسی مدیریتی به تجهیزات و سرویس دهنده های شبکه داخلی سازمان

**امنیت ارتباطات در بخش‌های مختلف شبکه داخلی:**

- تاکید بر تامین امنیت ارتباطات مجاز بین کلیه بخش‌های شبکه داخلی سازمان، متناسب با طبقه بندی اطلاعات

- تاکید بر تامین امنیت ارتباطات مجاز بین بخش‌های شبکه داخلی سازمان با سایر شبکه‌های متصل
- تاکید بر تامین محرمانگی و صحت ارتباطات مدیریتی شبکه داخلی سازمان

**۲-۵-۵-۳- سیاست‌های امنیتی ارتباطات شبکه دسترسی به اینترنت**

در سیاست‌های امنیتی ارتباطات شبکه دسترسی به اینترنت سازمان، لازم است سیاست سازمان در خصوص موارد ذیل مشخص گردد:

**بخشهای مختلف شبکه دسترسی به اینترنت:**

- تعیین بخش‌های مختلف شبکه دسترسی به اینترنت سازمان، با توجه به لزوم جداسازی و تشکیل نواحی امنیتی مستقل، از قبیل:
  ۱- بخش خارجی
  ۲- بخش سرویس‌های عمومی (شامل سرویس دهنده های اینترنتی سازمان)
  ۳- بخش سرویس‌های مدیریتی (شامل سرویس دهنده های مدیریتی و امنیتی شبکه)
  ۴- شبکه دسترسی کاربران داخلی
  ۵- شبکه دسترسی کاربران راه دور

**دسترسی های مجاز کاربران داخلی و راه دور:**

- تعیین مجاز یا غیرمجاز بودن دسترسی کاربران داخلی و راه دور شبکه دسترسی به اینترنت سازمان، به سرویس دهنده های اینترنتی بخش سرویس‌های عمومی این شبکه

- تعیین مجاز یا غیرمجاز بودن دسترسی کاربران داخلی و راه دور شبکه دسترسی به اینترنت سازمان، به شبکه اینترنت
- تعیین مجاز یا غیرمجاز بودن ارتباط بین بخش کاربران داخلی و راه‌دور شبکه دسترسی به اینترنت سازمان

**دسترسی های مجاز کاربران شبکه اینترنت به شبکه دسترسی به اینترنت سازمان:**

- تعیین مجاز یا غیرمجاز بودن دسترسی کاربران شبکه اینترنت، به بخش‌های مختلف شبکه دسترسی به اینترنت سازمان

**دسترسی های مدیریتی مجاز در شبکه دسترسی به اینترنت:**

- تعیین ایستگاههای مجاز به دسترسی مدیریتی به تجهیزات و سرویس دهنده های شبکه دسترسی به اینترنت سازمان

**امنیت ارتباطات شبکه دسترسی به اینترنت:**

- تاکید بر تامین محرمانگی و صحت ارتباطات مدیریتی شبکه دسترسی به اینترنت سازمان

### ۲-۵-۶- سیاست‌های امنیتی کاربران شبکه

#### ۲-۵-۶-۱- کاربران شبکه سازمان

در سیاست‌های امنیتی کاربران شبکه سازمان، لازم است سیاست سازمان در خصوص موارد ذیل مشخص گردد:

**کاربران شبکه داخلی:**

- تعیین کاربران شبکه داخلی سازمان، که مخاطب سیاست‌های امنیتی می‌باشند:

- مدیران داخل سازمان
- کاربران عادی داخل سازمان
- کاربران مدیریتی شبکه ( مدیر و کارشناسان واحد مدیریت شبکه )
- کاربران امنیتی شبکه ( مدیر و کارشناسان واحد امنیت شبکه )
- کاربران شبکه دولت و سایر شبکه های متصل به شبکه داخلی سازمان
- پیمانکاران مرتبط با شبکه داخلی سازمان

**شرایط و محدودیتهای کاربران:**

- تعیین محدودیت‌های هر یک از کاربران، در خصوص کپی، چاپ و انتقال اطلاعات مجاز از شبکه، همچنین کپی نمودن اطلاعات به داخل ایستگاه کاری و اجراء نمودن نرم افزارها
- توجه به ویژگی‌های خاص کاربران مدیریتی و امنیتی شبکه، بواسطه برخورداری از دسترسی بالائی که به اطلاعات دارند
- دقت در انتخاب پیمانکاران مرتبط با شبکه و توجه به ارائه اطلاعات شبکه سازمان، در حد ضرورت و با نظارت واحد امنیت شبکه

### ۲-۵-۶-۲- سیاست‌های تعیین هویت و کنترل دسترسی کاربران

در سیاست‌های امنیتی تعیین هویت و کنترل دسترسی کاربران شبکه سازمان، لازم است سیاست سازمان در خصوص موارد ذیل مشخص گردد:

**تشخیص هویت کاربران:**

- ضرورت تشخیص هویت کاربران شبکه سازمان، در زمان برقراری ارتباط با شبکه و دسترسی به اطلاعات

- به‌کارگیری مکانیزم‌های تشخیص هویت کاربران در دسترسی به اطلاعات دارای طبقه‌بندی، متناسب با طبقه‌بندی اطلاعات

**حدود اختیارات کاربران:**

- تعیین و اعلام حدود اختیارات کاربران به خود کاربران و تیم امنیت شبکه
- تعیین مرجع تعیین و اعلام حدود اختیارات کاربران، به هر یک از سرویس‌های شبکه سازمان
- تاکید بر تدوین و اعلام دستورالعمل تعیین حدود اختیارات کاربران

**پاسخ‌گویی کاربران:**

- تعیین مسئولیت و پاسخ‌گویی کاربران شبکه، در قبال سیاست‌های امنیتی شبکه سازمان
- تعیین و اعلام مقررات تنبیهی عدم اجرای هر یک از سیاست‌های امنیتی شبکه سازمان، به کاربران

### ۲-۵-۶-۳- سیاست‌های حریم خصوصی کاربران

در سیاست‌های حریم خصوصی کاربران شبکه سازمان، لازم است سیاست سازمان در خصوص موارد ذیل مشخص گردد:

**حیطه حریم خصوصی کاربران:**

- تعیین اطلاعاتی که جزء حریم خصوصی کاربران تلقی خواهند شد، از قبیل:
  ۱- اطلاعات کلیه Accountهای کاربر
  ۲- محتوای نامه‌های الکترونیکی و آدرس مخاطب نامه ها
  ۳- آدرس سایتهای اینترنتی که کاربر به آنها مراجعه نموده
  ۴- محتوای اطلاعات مشاهده یا Download شده توسط کاربر

۵- محتوای فایلهای موجود روی ایستگاه کاری کاربر

**ضوابط حاکم بر حریم خصوصی کاربران:**

- تعیین شرایطی که هر یک از اطلاعات فوق، جزء حریم خصوصی کاربر قرار می‌گیرند
- تعیین شرایط بازرسی امنیتی شبکه، به‌نحوی که مغایرتی با حریم خصوصی کاربران نداشته باشد

**رعایت حریم خصوصی کاربران:**

- تعیین مواردی که لازم است، نظارت یا بازرسی با مجوز رسمی، برای مدت زمان محدود و مشخص و توسط فرد مشخص انجام گیرد
- تعیین ضوابط و مکانیزم‌های کنترلی مناسب، به‌منظور جلوگیری از تلاش کاربران و بویژه پرسنل واحدهای مدیریت شبکه و امنیت شبکه در خصوص تعرض به حریم خصوصی کاربران
- تعیین شرایط و ضرورت تدوین ضوابط نظارت بر ترافیک شبکه سازمان، بویژه مرجع تشخیص ضرورت نظارت و صادرکننده مجوز

**۲-۵-۶-۴- سیاست‌های آگاهی‌رسانی امنیتی به کاربران**

در سیاست‌های آگاهی‌رسانی امنیتی به کاربران شبکه سازمان، لازم است سیاست سازمان در خصوص موارد ذیل مشخص گردد:

- تاکید بر تدوین برنامه آگاهی‌رسانی، تربیت نیروی انسانی و آموزش امنیت شبکه سازمان و تعیین مسئول تهیه و اجرای برنامه
- تاکید بر اعلام حیطه حریم خصوصی کاربران، به ایشان

- تاکید بر اعلام وظایف، مسئولیت‌ها و مواردی که کاربران باید پاسخ‌گو باشند، به ایشان
- بیان ضرورت تدوین و اعلام مواردی که کاربران باید نسبت به آن حساسیت داشته باشند، از قبیل گزارش نمودن ضعف‌های امنیتی، حوادث امنیتی و صدمات ناشی از حوادث امنیتی
- اعلام دوره‌ای ( با تعیین دوره ) موارد فوق به کاربران
- برنامه‌ریزی و برگزاری دوره‌های آگاهی‌رسانی به کاربران، در قالب سمینار یا سایر موارد

### ۲-۵-۶-۵- سیاست‌های مدیریت رمز عبور

در سیاست‌های مدیریت رمز عبور، لازم است سیاست سازمان در خصوص موارد ذیل مشخص گردد:

- بیان ضرورت تدوین و اعلام دستورالعمل مدیریت رمز عبور کاربران شبکه سازمان، که حداقل باید حاوی مطالبی به شرح ذیل باشد:

**طول رمز عبور:**

- استفاده از رمز عبور در سیستم عامل ایستگاه‌های کاری و حداقل طول آن
- استفاده از رمز عبور در سیستم عامل سرویس‌دهنده‌ها و حداقل طول آن
- استفاده از رمز عبور در تجهیزات شبکه و حداقل طول آن

**ترکیب رمز عبور:**

- استفاده از ترکیب حروف کوچک، حروف بزرگ و اعداد در رمز عبور
- عدم استفاده از کلمات عمومی یا قابل حدس زدن توسط سایر افراد
- تغییر رمز عبور پیش‌فرض کلیه نرم‌افزارها و سخت‌افزارها

- عدم استفاده از رمزهای عبور یکسان در موارد مختلف

**تغییر رمز عبور**:

- ضرورت تغییر دوره‌ای رمز عبور کاربران و تعیین حداکثر مدت مجاز
- ضرورت تغییر دوره‌ای رمز عبور مدیریتی تجهیزات شبکه و سرویس‌دهنده‌ها و تعیین حداکثر مدت مجاز
- ضرورت تغییر دوره‌ای رمز عبور تجهیزات و نرم‌افزارهای امنیت شبکه و تعیین حداکثر مدت مجاز

**حذف رمز عبور**:

- حذف Accountهای غیرضروری
- استفاده از رمز عبور مستقل توسط هر کاربر، به‌منظور تامین قابلیت پی‌گیری
- حذف رمز عبور کاربرانی که قطع همکاری نموده یا منتقل شده‌اند و تعیین حداکثر زمان مجاز برای این امر

**محافظت از رمز عبور**:

- تعیین مسئول محافظت از رمز عبور
- ضرورت عدم یادداشت رمز عبور توسط استفاده‌کننده
- ضرورت عدم بیان رمز عبور یا الگوریتم ترکیب آن، به سایر افراد

**وارد نمودن رمز عبور**:

- عدم وارد نمودن رمز عبور در حضور دیگران
- عدم استفاده از امکان به خاطر سپردن رمز عبور، که برخی نرم‌افزارها ارائه می‌کنند

**آگاهی رسانی در خصوص رمز عبور:**

- ضرورت یادآوری مخاطرات امنیتی مربوط به رمز عبور، بصورت دوره‌ای به کاربران
- ضرورت اعلام نمونه‌هائی از سوء استفاده‌های انجام شده از رمز عبور کاربران، در صورت کشف در سازمان

**بازرسی امنیتی:**

- بازرسی امنیتی از رمزهای عبور، بویژه رمز عبور تجهیزات و سرویس‌دهنده‌های حساس شبکه

**۲-۵-۷- سیاست‌های امنیتی محافظت فیزیکی**

در سیاست‌های امنیت فیزیکی، لازم است سیاست سازمان در خصوص موارد ذیل مشخص گردد:

**محافظت از سایت:**

- تاکید بر تعیین و اعلام وظایف پرسنل سایت، به‌نحوی که مراجعه سایر کاربران به محل استقرار پرسنل سایت، کمترین میزان باشد
- تاکید بر تعیین و اعلام وظایف پرسنل سایت، به‌نحوی که مسئولیت مدیریت و پشتیبانی هر یک از سرویس‌دهنده‌های مستقر در سایت، فقط بر عهده یک فرد مشخص باشد
- تاکید بر تفکیک محل استقرار پرسنل سایت، از محل نصب تجهیزات و سرویس‌دهنده‌ها

- تاکید بر ثبت و کنترل تردد پرسنل سایت به محل استقرار تجهیزات و سرویس‌دهنده‌ها
- تاکید بر قرار گرفتن تجهیزات و سرویس‌دهنده‌ها در سایت، به‌نحوی که هر یک از سرویس‌دهنده‌ها و تجهیزات شبکه، فقط در دسترس مسئول سرویس یا تجهیزات مربوطه باشد
- تاکید بر ثبت کلیه مراجعات به محل سرویس‌دهنده‌ها و تجهیزات و اقدامات انجام شده
- تاکید بر در اختیار نبودن کابل ارتباطی و کابل برق در محل نصب سرویس‌دهنده‌ها و تجهیزات
- تاکید بر تعبیه سیستم‌های تشخیص و اطفاء حریق، تشخیص میزان رطوبت و کنترل دما برای سایت

**محافظت از سرویس‌دهنده‌های خارج از سایت:**

- محافظت فیزیکی از ایستگاههای سرویس‌دهنده، که در محل ادارات نگهداری می‌شوند، متناسب با حساسیت سرویس‌دهنده
- تعیین مسئول محافظت از سرویس‌دهنده‌های خارج از سایت

**محافظت از ایستگاههای کاری:**

- تعیین مسئول محافظت فیزیکی از ایستگاههای کاری

**محافظت از تجهیزات مستقر در طبقات ساختمان‌ها:**

- ضرورت محافظت فیزیکی از تجهیزات شبکه قرار گرفته در خارج از سایت
- عدم قرار دادن تجهیزات شبکه یا راک حاوی تجهیزات، در راهرو یا داخل اطاقهای عادی
- توجه به قابل رؤیت و در دسترس نبودن کابلهای ورودی و خروجی راکها

- توجه به انتخاب محل قرار دادن راک تجهیزات

**محافظت از خطوط ارتباطی شبکه:**

- توجه به مواردی از قبیل عدم نشت اطلاعات، عدم امکان ایجاد اتصال فیزیکی به لینک ارتباطی و قابلیت تشخیص سریع قطع خط ارتباطی، در انتخاب نوع خطوط ارتباطی بین ساختمان‌ها
- توجه به عدم امکان دسترسی فیزیکی افراد در انتخاب مسیر عبور خطوط ارتباطی بین ساختمان‌ها
- دور از دسترسی بودن مسیر عبور خطوط ارتباطی در داخل ساختمان‌ها
- عدم قرار دادن پریز (سوکت) اضافی شبکه، به صورتی که متصل به تجهیزات شبکه و آماده بهره‌برداری باشد
- شماره‌گذاری و علامت‌گذاری خطوط ارتباطی زیرساختار شبکه، کابلهای اتصال ایستگاههای کاری به تجهیزات دسترسی طبقات، کابلهای ارتباطی داخل سایت و سایر خطوط ارتباطی
- استفاده از هم‌بندی متفاوت در شبکه‌ها، بویژه شبکه‌های حاوی اطلاعات محرمانه

**محافظت از رسانه‌های حاوی اطلاعات:**

- توجه به در دسترس قرار ندادن رسانه‌های حاوی اطلاعات، روی میز کار یا در دسترس مراجعین
- توجه به عدم ثبت اطلاعات حساس بصورت موقت، روی CDهای معمولی (غیر قابل نوشتن مجدد)
- توجه به پاک نمودن اطلاعات روی دیسکت یا CDهای با قابلیت نوشتن مجدد، پس از اتمام فعالیت مربوطه

- حصول اطمینان از قرار نداشتن اطلاعات اضافی روی رسانه، قبل از تحویل نمودن آن به سایر افراد
- محافظت فیزیکی رسانه‌های حاوی اطلاعات و نرم‌افزارها، متناسب با محرمانگی اطلاعات موجود در آن
- خودداری از قرار دادن اطلاعات طبقه‌بندی شده روی رسانه‌ها، بجز در مورد نسخه پشتیبان

**بازرسی امنیتی از محافظت فیزیکی**:

- بازرسی دوره‌ای از محافظت فیزیکی و تعیین مسئول مربوطه

# ۳

# چارچوب پیشنهادی برای طرح ارزیابی مخاطرات امنیتی شبکه

## ۳-۱- مقدمه

تا چند سال اخیر، از یک‌سو اطلاعات فنی کاربران شبکه در حدی نبود که تهدیدی برای امنیت شبکه محسوب شوند و از سوی دیگر، با اعمال کنترل‌های مدیریتی ، محافظت‌های فیزیکی و محدود نمودن تعداد افرادی که به سرویس‌ها و بویژه سرویس‌های حساس دسترسی داشتند، مشکل خاص امنیتی در شبکه‌های سازمانی بروز نمی‌نمود. لیکن در حال حاضر، از یک‌سو فراهم شدن دسترسی به شبکه اینترنت موجب افزایش اطلاعات فنی کاربران شبکه‌ها شده است و ابزارهای مختلفی را در اختیار آنان قرار داده تا بتوانند به سادگی امنیت شبکه را به مخاطره بیاندازند و از سوی دیگر، اتصال شبکه‌های سازمانی به یکدیگر و به شبکه اینترنت، موجب افزایش تعداد افراد مرتبط با شبکه‌های سازمانی و در نتیجه افزایش احتمال مخاطرات امنیتی برای این شبکه‌ها را فراهم نموده است.

پس از تعیین سیاست‌های امنیتی شبکه سازمان، اولین گام، ارزیابی وضعیت امنیتی شبکه سازمان و تعیین ضعف‌های امنیتی موجود در بخش‌های مختلف این شبکه، از قبیل تجهیزات شبکه، ایستگاههای کاری، سرویس‌دهنده‌ها و معماری شبکه می‌باشد.

شبکه سازمان، می‌تواند از دو بخش اصلی تشکیل شده باشد. بخش اول شامل شبکه داخلی سازمان است که سرویس‌ها و خدمات خود را در اختیار کاربران

داخل سازمان و برای سازمان‌های متصل به شبکه دولت، احیانا در اختیار کاربران شبکه دولت قرار می‌دهد. همچنین امکان ارتباط کاربران سازمان به سرویس‌های شبکه دولت را فراهم می‌آورد. بخش دوم شبکه سازمان، بخش دسترسی به شبکه اینترنت است که از یک‌سو امکان دسترسی کاربران داخل سازمان به شبکه اینترنت را فراهم می‌آورد و از سوی دیگر، سرویس‌های مبتنی بر وب سازمان را در اختیار کاربران شبکه اینترنت قرار می‌دهد. با توجه به راهبرد اتخاذ شده توسط سازمان در خصوص اتصال یا عدم اتصال شبکه داخلی به شبکه اینترنت، دو بخش فوق می‌توانند متصل یا مستقل از یکدیگر باشند.

برای سازمان‌های دولتی، راهبردی که در چارچوب پیشنهادی برای اهداف، راهبردها و سیاست‌های امنیتی شبکه، در فصل دوم ارائه شد، جداسازی شبکه‌های فوق بود.

در این فصل، چارچوب موردنیاز در گزارش ارزیابی مخاطرات امنیتی شبکه که می‌بایست توسط مشاور امنیت شبکه سازمان تهیه و ارائه گردد، پیشنهاد شده است. **با عنایت به تفاوت‌های ماهیتی موجود بین شبکه داخلی سازمان و شبکه دسترسی به اینترنت سازمان، لازم است بررسی مخاطرات امنیتی برای هر یک از دو شبکه مذکور، بصورت جداگانه انجام گیرد**، لیکن به‌منظور جلوگیری از تکرار مطالب، محتوای این فصل، برای شبکه سازمان ارائه شده است که می‌تواند شبکه داخلی یا شبکه دسترسی به اینترنت باشد.

در ارزیابی مخاطرات امنیتی شبکه، به مواردی پرداخته می‌شود که بصورت بالقوه، امکان دسترسی غیرمجاز، نفوذ و حمله کاربران شبکه، به منابع ( سرمایه‌های) شبکه و منابع کاربران شبکه را فراهم می‌نمایند. در این فصل، مخاطرات امنیتی شبکه، در ۶ محور شامل "معماری شبکه"، "تجهیزات شبکه"، "سرویس‌دهنده‌های شبکه"، "ایستگاههای کاری"، "مدیریت و نگهداری شبکه" و "تشکیلات و روش‌های مدیریت امنیت شبکه"، بررسی خواهد شد.

## ۳-۲- مخاطرات امنیتی معماری شبکه

شبکه داخلی سازمان به‌منظور ارائه سرویس‌های داخلی به کاربران داخلی و احیانا کاربران شبکه دولت و همچنین فراهم نمودن امکان دسترسی به سرویس‌های شبکه دولت برای بخشی از کاربران داخلی ایجاد می‌شود.

شبکه اینترنت سازمان، از یک‌سو امکان دسترسی کاربران داخل سازمان به شبکه اینترنت را فراهم می‌آورد و از سوی دیگر، سرویس‌های مبتنی بر وب سازمان را در اختیار کاربران شبکه اینترنت قرار می‌دهد.

موارد فوق، اهداف تشکیل شبکه داخلی و شبکه دسترسی به اینترنت سازمان‌ها را تشکیل می‌دهند. اینک با توجه به اهداف فوق، در بررسی مخاطرات امنیتی معماری شبکه، ضعف‌هایی از معماری شبکه که بصورت بالقوه، امکان دسترسی غیرمجاز، نفوذ و حمله کاربران شبکه، به منابع ( سرمایه‌های) شبکه و منابع کاربران شبکه را فراهم می‌نمایند، بررسی خواهیم نمود. در این خصوص، مخاطرات امنیتی موجود در "ساختار شبکه"، "ساختار آدرس‌دهی و مسیریابی" و "ساختار دسترسی فیزیکی و منطقی به شبکه" مورد بررسی قرار خواهند گرفت.

### ۳-۲-۱-ساختار شبکه

به‌منظور بررسی وضعیت ساختار شبکه سازمان، لازم است نقشه شماتیک شبکه با اطلاعات زیر، تهیه و تحلیل شود:

۱- تجهیزات شبکه، نوع، مدل و آدرس IP
۲- نوع و ظرفیت خطوط ارتباطی
۳- ارتباطات شبکه با سایر شبکه‌ها در حیطه سازمان (اتصال به شبکه سایر ساختمان‌های سازمان)
۴- ارتباطات شبکه با سایر شبکه‌ها در خارج از حیطه سازمان (اتصال به شبکه دولت، شبکه سایر سازمان‌ها و شبکه اینترنت)
۵- سرویس‌دهنده‌های شبکه، سرویس و آدرس IP

۶- نحوه تامین برق برای تجهیزات و سرویس‌دهنده‌ها (برق، ژنراتور و UPS)
۷- سخت‌افزارها و نرم‌افزارهای امنیت شبکه سازمان ( شامل فایروال، سیستم تشخیص تهاجم، نرم‌افزار ضد ویروس، نرم‌افزار Vulnerability Scanner، سرویس‌دهنده AAA، سرویس‌دهنده Log، نرم‌افزار تحلیل Log و ... ) با تعیین نام، مدل و نسخه
۸- Data Flow دسترسی کاربران داخلی، کاربران شبکه دولت، کاربران اینترنت و کاربران سایر سازمان‌ها به سرویس‌ها و خدمات شبکه سازمان

**مخاطرات امنیتی محتمل در خصوص ساختار شبکه سازمان**، عبارتند از:
۱- عدم استفاده از سیستم‌های امنیت شبکه در محل اتصال شبکه سازمان به سایر شبکه‌ها
۲- پراکندگی اتصالات شبکه سازمان به سایر شبکه‌ها و عدم امکان کنترل دسترسی متمرکز بر گذرگاه‌های ارتباطی شبکه
۳- عدم استفاده از سیستم‌های امنیت شبکه در محل اتصال سرویس‌دهنده‌های شبکه
۴- پراکندگی سرویس‌دهنده‌ها به‌نحوی که امکان کنترل دسترسی به سرویس‌دهنده‌ها توسط سیستم امنیتی متمرکز وجود نداشته باشد
۵- ساختار نامناسب شبکه و استفاده نامناسب از تجهیزات شبکه، به‌نحوی که موجب انتشار بسته‌های حاوی اطلاعات، در بخش‌های غیرمرتبط شبکه شده و امکان مانیتورینگ غیرمجاز یا شنود اطلاعات را فراهم آورند
۶- سیم‌کشی نامنظم و ساختارنیافته شبکه، از یک‌سو می‌تواند موجب بروز اشتباه و ایجاد مشکلاتی برای شبکه شده و از سوی دیگر، در صورت بروز مشکل، موجب کندی عملیات پشتیبانی حوادث خواهد شد

### ۳-۲-۲-ساختار آدرس‌دهی و مسیریابی شبکه

به‌منظور بررسی ساختار آدرس‌دهی و مسیریابی شبکه سازمان، لازم است بررسی موارد زیر، انجام گیرد:

۱- محدوده آدرسهای IP مورد استفاده در شبکه
۲- نحوه انتساب آدرس IP به اجزاء شبکه
۳- محدوده آدرس IP، نحوه تخصیص آدرس، Subnet mask و آدرس Gateway تخصیص یافته به ایستگاههای کاری شبکه
۴- محدوده آدرس IP، نحوه تخصیص آدرس، Subnet mask و آدرس Gateway تخصیص یافته به تجهیزات شبکه
۵- محدوده آدرس IP، نحوه تخصیص آدرس، Subnet mask و آدرس Gateway تخصیص یافته به سرویس‌دهنده‌های شبکه
۶- لیست حوزه‌های کاری (Domain) و گروههای کاری (Work Group) تشکیل شده در شبکه و تعیین کنترل‌کننده هر حوزه
۷- آدرس‌های IP، ایستگاههای کاری و سرویس‌دهنده‌های قرار گرفته در هر حوزه
۸- سرویس‌های قابل دسترس برای کاربران هر حوزه
۹- سرویس‌دهنده اصلی و پشتیبان نام دامنه هر حوزه

**مخاطرات امنیتی محتمل در خصوص ساختار آدرس‌دهی و مسیریابی،** عبارتند از:

۱- ضعف در تشکیل زیرشبکه‌ها و استفاده از ویژگی‌های آنها
۲- عدم استفاده مناسب از قابلیت‌های تجهیزات شبکه، جهت تشکیل VLAN، محدودسازی دسترسی کاربران و ناحیه انتشار بسته‌ها
۳- عدم کنترل مناسب بر انتساب آدرس IP و قابل پی‌گیری نبودن مبداء ارتباطات

۴- فعال بودن سرویس‌های اضافی، بویژه مسیریابی و DNS روی تجهیزات و سرویس‌دهنده‌های شبکه

### ۳-۲-۳-ساختار دسترسی به شبکه

ساختار دسترسی به شبکه، از نظر فیزیکی و لاجیکی موردنظر می‌باشد.

### دسترسی فیزیکی به شبکه

به‌منظور بررسی وضعیت دسترسی فیزیکی به شبکه سازمان، لازم است موارد زیر، بررسی شوند:

۱- محافظت فیزیکی از تجهیزات و سرویس‌دهنده‌های مستقر در سایت شبکه سازمان
- کنترل دسترسی به‌منظور دسترسی فیزیکی افراد مجاز
- استفاده از راک مناسب به‌منظور دسترسی فیزیکی افراد مجاز
- در دسترس بودن پورتهای تجهیزات و سرویس‌دهنده‌ها جهت دسترسی عادی و مدیریتی

۲- محافظت فیزیکی از تجهیزات مستقر در طبقات ساختمان‌ها
- استفاده از راک مناسب به‌منظور دسترسی فیزیکی افراد مجاز
- در دسترس بودن پورتهای تجهیزات و سرویس‌دهنده‌ها جهت دسترسی عادی و مدیریتی

۳- محافظت فیزیکی از تجهیزات و سرویس‌دهنده‌های مستقر در ادارات مختلف
- استفاده از راک مناسب یا سایر تمهیدات محافظتی به‌منظور دسترسی فیزیکی افراد مجاز

- در دسترس بودن پورتهای تجهیزات و سرویس‌دهنده‌ها جهت دسترسی عادی و مدیریتی

۴- محافظت فیزیکی از خطوط ارتباطی شبکه، بویژه تجهیزات لایه هسته و توزیع شبکه

- استفاده از کانال امن در ارتباط بین ساختمان‌ها
- استفاده از خطوط ارتباطی مناسب از قبیل فیبر نوری که امکان دسترسی فیزیکی به آن میسر نباشد

**دسترسی لاجیکی به شبکه**

به‌منظور بررسی وضعیت دسترسی لاجیکی به شبکه سازمان، لازم است موارد زیر، بررسی شوند:

۱- امکان دسترسی غیرمجاز در سطح عادی یا مدیریتی به شبکه، در صورت:

- حضور در محل سازمان و در اختیار داشتن یک پورت از شبکه یا دسترسی غیرمجاز به خطوط ارتباطی شبکه
- حضور در محل سازمان و در اختیار داشتن Account معتبر کاربر عادی

۲- امکان دسترسی غیرمجاز در سطح عادی یا مدیریتی به شبکه، در صورت:

- داشتن دسترسی مجاز به شبکه دولت و مجاز نبودن به دسترسی به شبکه سازمان
- داشتن دسترسی مجاز به شبکه دولت و مجاز بودن به دسترسی به شبکه سازمان

۳- امکان دسترسی غیرمجاز در سطح عادی یا مدیریتی به شبکه، در صورت:

- دسترسی از طریق شبکه اینترنت و نداشتن Account در شبکه دسترسی به اینترنت سازمان

- دسترسی از طریق شبکه اینترنت و داشتن Account در شبکه دسترسی به اینترنت سازمان

۴- امکان دسترسی غیرمجاز از طریق Remote Access در سطح عادی یا مدیریتی به شبکه، در صورت:

- اطلاع از شماره تلفن Remote Access شبکه و نداشتن Account معتبر
- اطلاع از شماره تلفن و داشتن Account معتبر

۵- امکان انتقال ویروس، Worm یا سایر اطلاعات مخرب به داخل شبکه از طریق دسترسی‌های فوق

در موارد فوق، منظور از امکان دسترسی غیرمجاز، عبارت است از این‌که:

۱- به‌منظور کنترل دسترسی کاربران به منابع شبکه از مسیر موردنظر، از سیستم کنترل دسترسی و بویژه مکانیزم تشخیص هویت کاربر استفاده شده باشد

۲- عملکرد سیستم کنترل دسترسی مورد استفاده، ارزیابی شده و امکان نفوذ به آن ( جهت غیرفعال نمودن یا افزودن Account غیرمجاز) و دور زدن آن ( از طریق حملات سرریز بافر، Password Cracking و .. ) بررسی شده باشد

**مخاطرات امنیتی محتمل در خصوص ساختار دسترسی به شبکه**، عبارتند از:

۱- اتصال غیرضروری شبکه سازمان، به سایر شبکه‌ها

۲- عدم استفاده از مکانیزم‌های تشخیص هویت، کنترل دسترسی، ثبت وقایع، تشخیص نفوذ و تشخیص ویروس در محل اتصال:

- کاربران داخلی
- کاربران شبکه اینترنت

- کاربران شبکه دولت
- کاربران راه دور

۳- ضعف مکانیزم‌های بکارگرفته شده در خصوص تشخیص هویت، کنترل دسترسی، ثبت وقایع، تشخیص نفوذ و تشخیص ویروس و امکان غیرفعال نمودن یا دور زدن سیستم مربوطه

## ۳-۳- مخاطرات امنیتی تجهیزات شبکه

در بررسی مخاطرات امنیتی تجهیزات شبکه، ضعف‌هایی از تجهیزات شبکه که بصورت بالقوه، امکان دسترسی غیرمجاز، نفوذ و حمله کاربران شبکه، به خود سیستم را فراهم می‌نمایند، بررسی خواهند شد. در این میان، سوئیچ‌ها و مسیریاب‌های موجود در شبکه، از اهمیت ویژه‌ای برخوردار می‌باشند.

**مخاطرات امنیتی محتمل در خصوص مسیریاب‌ها و سوئیچ‌های** شبکه عبارتند از:

۱- عدم استفاده از آخرین نسخه پایدار نرم‌افزار
۲- عدم نصب بموقع Patchهای امنیتی و وجود آسیب‌پذیری با درجه ریسک زیاد
۳- فعال بودن امکان مدیریت از راه دور، از طریق پروتکل‌های SNMP، Telnet و HTTP
۴- فعال بودن پورت کنسول و امکان مدیریت از طریق این پورت
۵- فعال بودن سایر سرویس‌های غیرضروری از قبیل Finger
۶- فعال نبودن مکانیزم تصدیق هویت، تعیین اختیارات و ثبت عملکرد سیستم در دسترسی‌های مدیریتی
۷- فعال نبودن مکانیزم ثبت وقایع، بویژه جهت دسترسی‌های مدیریتی

۸- ضعف‌های امنیتی مکانیزم‌های ثبت وقایع
۹- فعال نبودن مکانیزم‌های تشخیص و مقابله با حملات ممانعت از سرویس
۱۰-عدم بررسی و نگهداری مناسب از پیکربندی سیستم
۱۱-پیکربندی سیستم با استفاده از پروتکل‌های ناامن
۱۲-عدم محافظت فیزیکی مناسب از سیستم، بویژه در خصوص دسترسی مدیریتی
۱۳-عدم تنظیم کلمه عبور در پیکربندی سیستم
۱۴-عدم تغییر کلمه عبور پیش‌فرض
۱۵-عدم استفاده از رمزنگاری در کلمه عبور
۱۶-انتخاب نام گویا برای سیستم
۱۷-فعال بودن پورت Aux
۱۸-عدم اعمال فیلترهای مناسب به‌منظور محافظت از سایر منابع شبکه در مقابل حملات
۱۹-عدم وجود روال و مسئول مشخص برای بازبینی و اصلاح پیکربندی سیستم

## ۳-۴- مخاطرات امنیتی مدیریت و نگهداری شبکه

در بررسی مخاطرات امنیتی مدیریت و نگهداری شبکه، ضعف‌های مربوط به تشکیلات و روش‌های مدیریت و ضعف‌های مربوط به سیستم‌ها و مکانیزم‌های مدیریت، که بصورت بالقوه، امکان ایجاد، تشدید و کندی در رفع حوادث امنیتی را موجب می‌شوند، بررسی خواهند شد.

### ۳-۴-۱- تشکیلات و روش‌های مدیریت و نگهداری شبکه

مخاطرات امنیتی محتمل در خصوص تشکیلات و روش‌های مدیریت شبکه عبارتند از:

۱- عدم وجود تشکیلات و تیم‌های منسجم مدیریت و نگهداری شبکه
۲- کافی نبودن تعداد پرسنل واحدهای مدیریت و نگهداری شبکه
۳- ساختار نامناسب و مشخص نبودن شرح وظایف پرسنل واحدهای مدیریت و نگهداری شبکه
۴- عدم وجود روال‌های اجرائی مناسب در خصوص مدیریت و نگهداری شبکه در زمینه:
- خرید، نصب، راه‌اندازی، تست و تحویل سخت‌افزارها
- خرید، نصب، راه‌اندازی، تست و تحویل نرم‌افزارها
- اعلام و اعمال تغییرات در شبکه
- تشخیص و اعلام حوادث
- پشتیبانی حوادث
- ترمیم خرابی‌ها
- نظارت بر وضعیت شبکه، ترافیک شبکه، عملکرد تجهیزات و سرویس‌دهنده‌های شبکه
- تهیه نسخه پشتیبان از اطلاعات حساس

۵- ناکافی بودن آموزش پرسنل مدیریت و نگهداری شبکه
۶- عدم وجود یا ضعف مستندات مناسب در خصوص اجزاء و سرویس‌های شبکه
۷- عدم وجود یا ضعف مستندات مدیریت و نگهداری شبکه، از قبیل آخرین تغییرات اعمال شده در پیکربندی سیستم‌ها
۸- عدم آگاهی به‌موقع کاربران، از تغییرات یا مشکلات موجود شبکه
۹- عدم آگاهی کاربران از مسئولیت‌های خود در زمینه مدیریت و نگهداری شبکه

**۳-۴-۲-ابزارها و مکانیزم‌های مدیریت شبکه**

**مخاطرات امنیتی محتمل در خصوص مکانیزم‌های مدیریت شبکه** عبارتند از:

۱- عدم دسته‌بندی صحیح کاربران در سیستم مدیریت شبکه

۲- عدم تعیین دقیق حدود اختیارات کاربران در سیستم مدیریت شبکه

۳- عدم اعمال کنترل دسترسی مناسب روی کاربران

۴- عدم اعمال کنترل‌های کافی روی اطلاعات مدیریتی شبکه

۵- عدم پیکربندی صحیح سرویس‌دهنده‌های مدیریتی شبکه

۶- عدم استفاده از سرویس‌دهنده‌های پشتیبان برای سرویس‌دهنده‌های مدیریتی شبکه، بویژه برای:

- سرویس‌دهنده کنترل دامنه
- سرویس‌دهنده DNS
- سرویس‌دهنده‌های امنیتی از قبیل تصدیق هویت و ثبت وقایع

۷- عدم رویدادنگاری مناسب، بویژه از اطلاعات مدیریتی شبکه

۸- عدم پشتیبان‌گیری مناسب و مداوم

۹- استفاده از مکانیزم‌های امنیتی ضعیف، بویژه در مدیریت شبکه

- استفاده از کلمات عبور با ترکیب ضعیف
- استفاده از سایر مکانیزم‌های آسیب‌پذیر تصدیق هویت

۱۰-عدم رعایت افزونگی، بویژه در سرویس‌دهنده‌ها و تجهیزات مدیریت شبکه

## ۳-۵- مخاطرات امنیتی سرویس‌های شبکه

در بررسی مخاطرات امنیتی سرویس‌دهنده‌های شبکه، ضعف‌هایی از سرویس‌دهنده‌ها که بصورت بالقوه، امکان دسترسی غیرمجاز، نفوذ و حمله کاربران شبکه، به خود سرویس‌دهنده، سایر منابع شبکه و منابع کاربران شبکه را فراهم می‌نمایند، بررسی خواهند شد.

برای این منظور، لازم است اطلاعاتی به شرح زیر، برای هر یک از سرویس‌دهنده‌های شبکه، جمع‌آوری و تحلیل شوند:

۱- نام سرویس‌دهنده
۲- آدرس‌های IP سرویس‌دهنده
۳- سرویس یا وظیفهٔ اصلی سرویس‌دهنده در شبکه
۴- نام و نسخه سیستم عامل به همراه Service Packها و Patchهای نصب شده
۵- نام و نسخه نرم‌افزار سرویس به همراه Patchهای نصب شده
۶- نام و نسخه نرم‌افزار ضد ویروس نصب شده
۷- وضعیت رویدادنگاری در سرویس‌دهنده
۸- وضعیت تصدیق اصالت در سرویس‌دهنده
۹- لیست سرویس‌های در حال اجرا بر روی سرویس‌دهنده
۱۰- لیست سایر نرم‌افزارها و سرویس‌های در حال اجراء روی سرویس‌دهنده
۱۱- نتایج پویش محلی سرویس‌دهنده با استفاده از یک نرم‌افزار پویش‌گر امنیتی
برای این منظور، لازم است نرم‌افزار پویش‌گر، روی سرویس‌دهنده و در حالی که نرم‌افزار سرویس در حال اجراء می‌باشد، اجراء گردد.
۱۲- نتایج پویش از راه دور با استفاده از یک نرم‌افزار پویش‌گر امنیتی
برای این منظور، لازم است نرم‌افزار پویش‌گر، روی یک ایستگاه متصل به شبکه سازمان و در حالی که نرم‌افزار سرویس در حال اجراء می‌باشد، اجراء گردد.

**مخاطرات امنیتی محتمل در خصوص سرویس‌دهندهای شبکه** عبارتند از:

۱- مخاطرات مربوط به سیستم عامل سرویس‌دهنده
- امنیت ارتباطات مدیریتی
- تصدیق اصالت کاربر
- حدود اختیارات و ثبت حسابرسی کاربر
- مکانیزم‌های محافظتی از سیستم عامل
- Patchهای امنیتی

۲- مخاطرات مربوط به نرم‌افزار سرویس
- امنیت ارتباطات سرویس
- امنیت ارتباطات مدیریتی
- تصدیق اصالت کاربر
- حدود اختیارات و ثبت حسابرسی کاربر
- مکانیزم‌های محافظتی از نرم‌افزار سرویس
- Patchهای امنیتی

۳- مخاطرات ناشی از عدم استفاده از ابزارهای امنیتی روی سرویس‌دهنده
- فایروال مبتنی بر ایستگاه
- محافظت در برابر ویروس
- تشخیص و مقابله یا پیشگیری از تهاجم، مبتنی بر ایستگاه
- فیلتر محتوا در مواردی از قبیل سرویس‌دهنده E-Mail

۴- مخاطرات ناشی از عدم رعایت افزونگی روی سرویس‌دهنده
- عدم استفاده از ماجولهای افزونه
- عدم استفاده از سرویس‌دهنده افزونه

## ۳-۶- مخاطرات تشکیلات و روش‌های امنیت شبکه

در بررسی مخاطرات امنیتی تشکیلات و روش‌های امنیت شبکه، تنها وجود تشکیلات، طرح‌ها، برنامه‌ها، روال‌های اجرائی و دستورالعمل‌های فنی تامین امنیت مورد بررسی قرار می‌گیرند و کیفیت عملکرد آنها موردنظر نمی‌باشد. در واقع کیفیت عملکرد کلیه روش‌های تامین امنیت، از طریق ارزیابی‌های قسمت‌های قبلی همین فصل، قابل ارزیابی می‌باشند و در این فصل، تنها عملیات ممیزی مدیریت امنیت، مورد نظر می‌باشد. لذا در صورتی که سازمان موفق به اخذ گواهی‌نامه بر اساس استاندارد BS7799 از یکی از موسسات صدور گواهی این استاندارد شده باشد، ضرورتی به بررسی‌های زیر نمی‌باشد.

برای این منظور، لازم است اطلاعاتی به شرح زیر، جمع‌آوری و تحلیل شوند:

**تشکیلات امنیت**

۱- آیا تشکیلات امنیت شبکه در سازمان وجود دارد؟

۲- آیا فرد یا افرادی، حتی به صورت غیر رسمی، مسئولیت تامین امنیت شبکه را بر عهده دارند؟

۳- آیا ساختار تشکیلاتی و شرح وظایف این تشکیلات، تعیین و تدوین شده است؟

۴- آیا روال‌های اجرائی مدون، مناسب و جامع برای پشتیبانی امنیت شبکه وجود دارد؟

۵- آیا دستورالعمل‌های فنی مدون، مناسب و جامع برای پشتیبانی امنیت شبکه وجود دارد؟

۶- آیا فرد یا واحد مشخصی، تدوین و به‌روز رسانی روال‌های اجرائی و دستورالعمل‌های فنی را بر عهده دارد؟

برای ساختار تشکیلات، شرح وظایف، روال‌های اجرائی و دستورالعمل‌های فنی، لازم است کلیه موارد ارائه شده در فصل دوم، مورد توجه قرار گیرند. برای مثال، دستورالعمل ایمن‌سازی در فصل دوم، برای سیستم‌عامل ایستگاه‌ها، سیستم‌عامل سرویس‌دهنده‌ها، تجهیزات شبکه و سایر موارد پیش‌بینی شده است، لذا در بررسی دستورالعمل‌های فنی، وجود و مناسب‌بودن دستوالعمل‌ها در کلیه موارد فوق، باید بررسی شوند.

**اهداف امنیت**

۱- آیا سرمایه‌های شبکه سازمان، شناسایی و ارزش‌گذاری شده‌اند؟
۲- آیا اهداف کوتاه‌مدت، میان‌مدت و بلندمدت امنیتی برای تامین امنیت شبکه سازمان، تعیین و مدون شده است؟
۳- آیا اهداف پیش‌بینی شده، با توجه به ماموریت‌های سازمان، کامل و جامع می‌باشند؟

**راهبردهای ایجاد و تداوم امنیت**

۱- آیا راهبردهای کوتاه‌مدت، میان‌مدت و بلندمدت سازمان جهت دستیابی به اهداف امنیت، تعیین و مدون شده است؟
۲- آیا راهبردهای پیش‌بینی شده، با توجه با ماموریت‌های سازمان، قادر به تامین اهداف امنیت پیش‌بینی شده می‌باشند؟

**سیاست‌های امنیتی**

۱- آیا سیاست‌های امنیتی شبکه سازمان، تعیین و مدون شده است؟
۲- آیا سیاست‌های امنیتی شبکه پیش‌بینی شده از جامعیت لازم، برخوردار می‌باشند؟

**تدوین طرح‌ها و برنامه‌های امنیتی شبکه**

۱- آیا طرح‌ها و برنامه‌های امنیتی موردنیاز سازمان که در قصمت نتیجه‌گیری فصل اول این کتاب به آنها اشاره شده است، تدوین شده‌اند؟

۲- آیا طرح‌ها و برنامه‌های امنیتی موجود، از جامعیت لازم برخوردار می‌باشند؟

**اجرای طرح‌ها و برنامه‌های امنیتی شبکه**

۱- آیا طرح‌ها و برنامه‌های امنیتی سازمان، اجرا شده‌اند؟

۲- آیا سیستم امنیت شبکه، نصب و راه‌اندازی شده است؟

۳- آیا سیستم امنیت شبکه، جامعیت لازم جهت تامین امنیت شبکه را دارد؟

**پشتیبانی امنیت شبکه**

۱- آیا طرح‌ها و برنامه‌های پشتیبانی امنیت شبکه، تدوین شده‌اند؟

۲- آیا طرح‌ها و برنامه‌های پشتیبانی امنیت شبکه، از جامعیت لازم برخوردار می‌باشند؟

۳- آیا پشتیبانی امنیت شبکه، بر اساس طرح‌ها و برنامه‌های فوق، انجام می‌گیرد؟

**ارزیابی امنیتی و رفع اشکالات**

۱- آیا وضعیت امنیت شبکه، به صورت دوره‌ای مورد ارزیابی قرار می‌گیرد؟

سوالات فوق، بسیار کلی می‌باشند و به منظور پاسخ‌گویی به آنها، یا باید هر یک از سوالات فوق را به تعداد زیادی سوالات جزئی‌تر تبدیل نماییم و یا باید هر یک از محورهایی که به عنوان محورهای پیشنهادی برای اهداف، راهبردها و سیاست‌های امنیتی شبکه در فصل دوم ارائه شدند را به صورت سوال مطرح نموده و پاسخ هر یک از آنها را بررسی نماییم.

# ۴

# چارچوب پیشنهادی برای طرح امنیت شبکه

## ۴-۱- مقدمه

پس از تدوین اهداف، راهبردها و سیاست‌های امنیتی شبکه سازمان و انجام بررسی مخاطرات امنیتی موجود در شبکه سازمان، می‌بایست طرح امنیتی شبکه سازمان، ارائه گردد. تدوین این طرح، باید به گونه‌ای انجام گیرد که منطبق بر سیاست‌های امنیتی شبکه بوده و اهداف تعیین شده برای امنیت شبکه سازمان را تامین نماید.

همان‌گونه که در فصل دوم و سوم نیز مطرح شد، شبکه سازمان، در کلی‌ترین حالت، می‌تواند از دو بخش اصلی تشکیل شود. بخش اول شامل شبکه داخلی سازمان است که سرویس‌ها و خدمات خود را در اختیار کاربران داخل سازمان و احیانا کاربران شبکه دولت قرار می‌دهد. همچنین امکان ارتباط کاربران سازمان به سرویس‌های شبکه دولت را فراهم می‌آورد. بخش دوم شبکه سازمان، بخش دسترسی به شبکه اینترنت است که از یک‌سو امکان دسترسی کاربران داخل سازمان به شبکه اینترنت را فراهم می‌آورد و از سوی دیگر، سرویس‌های مبتنی بر وب سازمان را در اختیار کاربران شبکه اینترنت قرار می‌دهد. با توجه به راهبرد اتخاذ شده توسط سازمان در خصوص اتصال یا عدم اتصال شبکه داخلی به شبکه اینترنت، دو بخش فوق می‌توانند متصل یا مستقل از یکدیگر باشند.

در این فصل، محورهای موردنیاز در طرح امنیتی شبکه که لازم است مشاور امنیت شبکه سازمان، تهیه و ارائه نماید، ارائه گردیده است. **با عنایت به تفاوت‌های ماهیتی موجود بین شبکه داخلی سازمان و شبکه دسترسی به اینترنت سازمان، در صورت جدا بودن این دو شبکه، لازم است طرح امنیت شبکه برای هر یک از دو شبکه مذکور، بصورت جداگانه ارائه گردد.** به‌منظور جلوگیری از تکرار مطالب، قالب پیشنهادی برای شبکه سازمان ( که می‌تواند شبکه داخلی یا شبکه دسترسی به اینترنت باشد)، ارائه شده است.

بر اساس چارچوب پیشنهادی در این فصل، در طرح امنیت شبکه لازم است ابتدا مروری بر اهداف امنیت شبکه سازمان و روش‌های تامین اهداف در طرح امنیت شبکه انجام گیرد و در ادامه، معماری امنیت شبکه، ساختار شماتیک طرح امنیت شبکه و مشخصات ابزارهای امنیتی بکار گرفته شده ارائه شوند. همچنین در ادامه، لازم است با ارائه جریان اطلاعات کلیه سرویس‌های شبکه، کفایت ابزارهای امنیتی ارائه شده در طرح، تضمین شود. در خاتمه نیز باید برآوردهای هزینه، پرسنل و مراحل اجرای طرح امنیت، ارائه گردد.

## ۴-۲- اهداف و روش های تامین امنیت در طرح امنیت شبکه

### ۴-۲-۱- ساختار شبکه

در این بخش، لازم است اجزاء شبکه موجود سازمان، ارائه شود. این ساختار باید حداقل شامل موارد زیر باشد:

۱- معماری شبکه شامل:

- ساختار شبکه
- ساختار آدرس‌دهی
- ساختار مسیریابی
- ساختار دسترسی به شبکه

۲- تجهیزات شبکه
۳- سرویس‌دهنده‌های شبکه
۴- مدیریت و نگهداری شبکه

در این بخش، همچنین تغییراتی که همزمان با افزودن سیستم امنیتی، لازم است در معماری، تجهیزات، سرویس‌دهنده‌ها و مدیریت شبکه انجام گیرد، تشریح خواهد شد. تغییرات مورد نظر، بر اساس پیشنهادات خروجی طرح ارزیابی مخاطرات امنیتی شبکه سازمان، بر اساس اولویت تعیین شده در طرح مذکور، اعمال خواهد شد. در بخش‌های بعد، سیستم امنیتی مناسب به ساختار اصلاح شده طرح، افزوده شده و طرح نهائی ترسیم خواهد شد.

### ۴-۲-۲- اهداف طرح امنیت شبکه

در این بخش، لازم است اهدافی که طرح امنیت شبکه سازمان، تامین خواهد نمود، تشریح شوند. نمونه‌هایی از اهداف قابل تامین توسط طرح امنیت شبکه، عبارتند از:

- تامین محرمانگی برای اطلاعات و ارتباطات مدیریتی شبکه، بویژه مدیریت امنیت شبکه.
- تامین صحت عملکرد [و قابلیت دسترسی] برای تجهیزات شبکه، سرویس‌دهنده‌ها و ایستگاههای کاری.
- تامین صحت عملکرد [و قابلیت دسترسی] برای سیستم عامل‌ها و نرم‌افزار سرویس‌های شبکه.
- تامین قابلیت تشخیص هویت برای کاربران مدیریتی، داخلی و Dialup.
- تامین کنترل دسترسی برای کاربران مدیریتی، داخلی، Dialup و کاربران سایر شبکه‌ها در دسترسی به تجهیزات و سرویس‌های شبکه.
- تامین پاسخ‌گویی برای کاربران مدیریتی، داخلی، Dialup و کاربران سایر شبکه‌ها از طریق ثبت دسترسی آنها به تجهیزات و سرویس‌های شبکه.

اهداف فوق، تنها شامل اهدافی است که طرح امنیت شبکه، باید تامین نماید. سایر اهداف امنیتی که در مستندات "اهداف، راهبردها و سیاست‌های امنیتی شبکه سازمان" مطرح می‌شوند، از طریق رعایت سیاست‌های امنیتی ارائه شده و سایر طرح‌های امنیت شبکه از قبیل "طرح پشتیبانی حوادث" و "طرح آگاهی‌رسانی، آموزش و تربیت نیروی انسانی" تامین خواهند شد. چارچوب پیشنهادی برای این طرح‌ها نیز در فصل پنجم و ششم ارائه شده است.

### ۴-۲-۳- روش‌های تامین امنیت در طرح امنیت شبکه

به‌منظور تامین هر یک از اهداف پیش‌بینی شده برای طرح امنیت شبکه سازمان، لازم است تمهیدات و روش‌هائی در طرح امنیت شبکه سازمان، پیش‌بینی شوند. در این بخش از طرح امنیت، لازم است این روش‌ها بیان شوند، لذا برخی از روش‌های پیشنهادی برای این منظور، در جدول زیر ارائه شده است .

| اهداف طرح امنیت | روش‌های تامین اهداف | تمهیدات موردنیاز در طرح امنیت شبکه |
|---|---|---|
| **محرمانگی** اطلاعات و ارتباطات مدیریتی | • ایمن‌سازی ارتباطات مدیریتی<br>• جداسازی ارتباطات مدیریتی، بویژه ارتباطات مدیریت امنیت شبکه | • استفاده از پروتکل‌های امن مدیریتی<br>• ایجاد زیرساختار مستقل برای مدیریت شبکه، بویژه مدیریت امنیت شبکه |
| **صحت عملکرد** تجهیزات شبکه | • پیکربندی امن تجهیزات | • ارائه دستورالعمل‌های پیکربندی امن تجهیزات |
| **صحت عملکرد** سرویس‌دهنده‌ها | • پیکربندی امن سیستم عامل سرویس‌دهنده<br>• پیکربندی امن نرم‌افزار سرویس | • ارائه دستورالعمل‌های پیکربندی امن سیستم عامل سرویس‌دهنده‌ها<br>• ارائه دستورالعمل‌های پیکربندی امن نرم‌افزار سرویس‌های شبکه |

| | | |
|---|---|---|
| | • تشخیص و مقابله با ویروس<br>• فیلتر نمودن نامه‌های الکترونیکی آلوده به ویروس<br>• تشخیص و جلوگیری از تهاجم مبتنی بر سرویس‌دهنده | • استفاده از نرم‌افزار آنتی‌ویروس مبتنی بر شبکه<br>• استفاده از نرم‌افزار آنتی‌ویروس مبتنی بر سرویس‌دهنده<br>• استفاده از نرم‌افزار Content Filter برای سرویس E-Mail<br>• ایجاد سرویس مدیریت Patch برای سیستم عامل‌ها و نرم‌افزارهای سرویس<br>• ایجاد سرویس Update برای نرم‌افزارهای آنتی‌ویروس |
| **صحت عملکرد** ایستگاههای کاری | • پیکربندی امن سیستم عامل ایستگاه کاری<br>• تشخیص و مقابله با ویروس<br>• فیلتر نمودن ارتباطهای منتهی به ایستگاه | • ارائه دستورالعمل‌های پیکربندی امن سیستم عامل ایستگاههای کاری<br>• استفاده از نرم‌افزار آنتی‌ویروس مبتنی بر Client<br>• ایجاد سرویس مدیریت Patch برای سیستم عامل ایستگاههای کاری<br>• ایجاد سرویس Update برای نرم‌افزار آنتی‌ویروس ایستگاههای کاری<br>• استفاده از فایروال‌های شخصی |
| **تشخیص هویت** کاربران مدیریتی | • Authentication کاربران مدیریت | • استفاده از AAA Server و مکانیزم‌های تشخیص هویت نرم‌افزارهای مدیریتی شبکه |
| **تشخیص هویت** کاربران محلی | • Authentication کاربران محلی | • استفاده از تصدیق هویت Domain Controller یا AAA Server مستقل |
| **تشخیص هویت** کاربران راه‌دور | • Authentication کاربران راه‌دور | • استفاده از قابلیت Remote Access Server یا AAA Server مستقل |
| **کنترل دسترسی** | • کنترل دسترسی در سطح | • استفاده از Firewall برای کنترل |

| | | |
|---|---|---|
| کاربران مدیریتی | سیستم‌ها و کاربردها<br>• کنترل دسترسی فیزیکی به ایستگاههای مدیریتی | دسترسی در سطح سیستم‌ها<br>• استفاده از مکانیزم‌های کنترل دسترسی در پیکربندی امن تجهیزات و سرویس‌دهنده‌ها |
| **کنترل دسترسی** کاربران محلی | • کنترل دسترسی با استفاده از Firewall<br>• تشخیص تهاجم مبتنی بر شبکه | • استفاده از Firewall<br>• استفاده از سیستم تشخیص تهاجم مبتنی بر شبکه ( N-IDS ) |
| **کنترل دسترسی** کاربران راه‌دور | • کنترل دسترسی با استفاده از Firewall<br>• تشخیص تهاجم مبتنی بر شبکه | • استفاده از Firewall<br>• استفاده از سیستم تشخیص تهاجم مبتنی بر شبکه ( N-IDS ) |
| **کنترل دسترسی** کاربران شبکه اینترنت | • کنترل دسترسی با استفاده از Firewall<br>• تشخیص و جلوگیری از تهاجم مبتنی بر شبکه | • استفاده از Firewall<br>• استفاده از سیستم تشخیص و جلوگیری از تهاجم مبتنی بر شبکه (N-IPS) |
| **پاسخ‌گویی** کاربران مدیریتی | • ثبت دسترسی‌های مدیریتی به تجهیزات و سرویس‌دهنده‌ها | • استفاده از Log Server<br>• استفاده از AAA Server<br>• استفاده از سیستمهای تشخیص تهاجم<br>• استفاده از نرم‌افزار تحلیل یکپارچه Log و تشخیص تهاجم Off Line<br>• استفاده از نرم‌افزار مانیتورینگ ترافیک |
| **پاسخ‌گویی** کاربران محلی | • ثبت دسترسی‌های انجام شده به تجهیزات و سرویس‌دهنده‌ها | • استفاده از Log Server<br>• استفاده از کنترل‌کنندهٔ حوزه<br>• استفاده از سیستمهای تشخیص تهاجم<br>• استفاده از نرم‌افزار تحلیل یکپارچه Log و تشخیص تهاجم Off Line<br>• استفاده از نرم‌افزار مانیتورینگ ترافیک |
| **پاسخ‌گویی** کاربران | • ثبت دسترسی‌های انجام | • استفاده از Log Server |

| | | |
|---|---|---|
| راه‌دور | شده به تجهیزات و سرویس‌دهنده‌ها | • استفاده از AAA Server<br>• استفاده از سیستمهای تشخیص تهاجم<br>• استفاده از نرم‌افزار تحلیل یکپارچه Log و تشخیص تهاجم Off Line<br>• استفاده از نرم‌افزار مانیتورینگ ترافیک |
| **پاسخ‌گویی** کاربران شبکه اینترنت | • ثبت دسترسی‌های انجام شده به تجهیزات و سرویس‌دهنده‌ها | • استفاده از Log Server<br>• استفاده از سیستمهای تشخیص تهاجم<br>• استفاده از نرم‌افزار تحلیل یکپارچه Log و تشخیص تهاجم Off Line<br>• استفاده از نرم‌افزار مانیتورینگ ترافیک |
| تأمین قابلیت دسترسی | • Load Balancing<br>• Redundancy | • Loadbalancing و Redundancy سرویس‌دهنده‌های حساس (Web، DNS و DC)<br>• Redundancy و تجهیزات یدکی در مورد اجزاء تجهیزات و سرویس‌دهنده‌ها |

جدول (۴-۱): روش‌های پیشنهادی برای تامین اهداف طرح امنیت شبکه

## ۴-۳- معماری، ساختار و مشخصات سیستم امنیتی شبکه

در این بخش، لازم است با توجه به ساختار شبکه سازمان و اهداف امنیتی پیش‌بینی شده برای آن، ابتدا معماری موردنیاز برای سیستم امنیتی شبکه فوق را تعیین نموده و سپس ساختار شماتیک اجزاء سیستم امنیتی پیش‌بینی شده برای این شبکه، ترسیم شود. در ادامه نیز لازم است پس از تشریح مشخصات فنی و قابلیت‌های هر یک از اجزاء سیستم امنیتی پیش‌بینی شده، جریان اطلاعات

دسترسی کاربران به هر یک از سرویس‌های شبکه، بررسی و کفایت ابزارها و مکانیزم‌های امنیتی پیش‌بینی شده برای شبکه، اثبات شوند.

### ۴-۳-۱- معماری امنیت شبکه

در این بخش، لازم است معماری پیش‌بینی شده برای امنیت شبکه سازمان، ارائه شود. نکته‌ای که باید در معماری امنیت شبکه مورد توجه قرار گیرد، این‌که تامین امنیت باید در سطوح مختلف انجام گیرد. به عنوان نمونه‌ای از معماری امنیت، جزئیات یک معماری چهار لایه‌ای برای امنیت در این بخش ارائه شده است. در این معماری، مطابق آنچه در شکل (۴-۱) نشان داده شده است، امنیت شبکه در ۴ سطح زیرساختار شبکه، ارتباطات، سیستم‌ها و کاربردها تامین خواهد شد.

| امنیت کاربردها |
| --- |
| امنیت سیستم‌ها |
| امنیت ارتباطات شبکه |
| امنیت زیرساختار شبکه |

شکل (۴-۱): معماری پیشنهادی برای تامین امنیت شبکه سازمان

۱- **امنیت زیرساختار شبکه:** مهم‌ترین عامل تامین کننده امنیت زیرساختار شبکه، پیکربندی امن تجهیزات شبکه و تجهیز آنها به قابلیت‌های دفاعی مناسب می‌باشد. به‌منظور پیکربندی امن تجهیزات، لازم است به پیوست طرح امنیت شبکه، دستورالعمل‌های پیکربندی امن تجهیزات شبکه، ارائه شوند و به‌منظور تجهیز به قابلیت‌های دفاعی، استفاده از قابلیت‌های فیلترینگ برای مسیریاب‌ها و قابلیت‌های VLAN و Port Security برای سوئیچ‌های شبکه، پیش‌بینی شوند.

۲- **امنیت ارتباطات شبکه:** تامین امنیت ارتباطات شبکه، به‌منظور تشخیص هویت و کنترل دسترسی کاربران و مانیتورینگ ارتباطات شبکه انجام می‌گیرد. برای این منظور، سیستم امنیت شبکه باید شامل اجزاء زیر باشد:

- Firewall
- Network Based Intrusion Detection & Prevention System
- Network Based Intrusion Detection System (N-IDS)
- Network Based AntiVirus Software
- Authentication Authorization & Accounting Server
- Log Server & Log Analyzer Software
- Monitoring Software

۳- **امنیت سیستم‌ها (سرویس‌دهنده‌ها و ایستگاهها) :** تامین امنیت سرویس‌دهنده‌های شبکه، به‌منظور تامین صحت عملکرد سرویس‌دهنده‌ها و کنترل و ثبت دسترسی کاربران انجام می‌گیرد. همچنین به‌منظور اطمینان از صحت عملکرد آنها، استفاده از نرم‌افزارهای Vulnerability Scanner، موردنیاز می‌باشد. تامین امنیت ایستگاههای کاری، به‌منظور صحت عملکرد ایستگاهها و کنترل دسترسی کاربران انجام می‌گیرد. برای این منظور، لازم است تمهیداتی به شرح زیر، در طرح امنیت پیش‌بینی شوند:

**سرویس‌دهنده‌ها**

- دستورالعمل‌های پیکربندی امن سیستم عامل سرویس‌دهنده‌ها
- Host Based Intrusion Detection System (H-IDS)
- Server Based AntiVirus Software
- Log Server & Log Analyzer Software
- Vulnerability Scanner

**ایستگاهها**

- دستورالعمل‌های پیکربندی امن سیستم عامل ایستگاهها
- Client Based AntiVirus Software (C-Av)
- Log Server & Log Analyzer Software
- Vulnerability Scanner

۴- **امنیت کاربردها (نرم‌افزار سرویس‌ها) :** تامین امنیت کاربردهای شبکه، به‌منظور تامین صحت عملکرد سرویس‌ها و کنترل و ثبت دسترسی کاربران به بخش‌های مختلف سرویس انجام می‌گیرد. همچنین به‌منظور اطمینان از صحت عملکرد آنها، استفاده از نرم‌افزارهای Vulnerability Scanner، موردنیاز می‌باشد. برای این منظور، لازم است تمهیداتی به شرح زیر، در طرح امنیت پیش‌بینی شوند:

- دستورالعمل‌های پیکربندی امن نرم‌افزار سرویس‌ها
- Host Based Intrusion Detection System (H-IDS)
- Server Based AntiVirus Software (S-Av)
- Log Server & Log Analyzer Software
- Vulnerability Scanner
- E-Mail Content Filter ( E-Mail Server )

با توجه به معماری پیشنهادی برای امنیت شبکه سازمان و اهداف موردنظر، نحوه توزیع سیستم امنیتی این شبکه باید به‌نحوی باشد که:

۱- یک **سیستم امنیتی چند لایه** را تشکیل دهد

۲- یک **سیستم امنیتی توزیع شده** را تشکیل دهد، به‌نحوی که کلیه بخش‌های شبکه، اعم از تجهیزات گذرگاه‌های ارتباط با سایر شبکه‌ها، گذرگاه اتصال کاربران Dialup، تجهیزات و ایستگاههای کاری کاربران محلی و سرویس‌دهنده‌های شبکه را در بر گیرد.

۳- **نواحی امنیتی شبکه** را تشکیل داده و دسترسی بین نواحی را کاملا کنترل نماید. نواحی قابل تشکیل، عبارتند از:
- ناحیه خارجی، شامل تجهیزات گذرگاه ارتباط با سایر شبکه‌ها
- ناحیه داخلی، شامل زیرساختار شبکه، تجهیزات دسترسی و ایستگاههای کاری کاربران محلی
- ناحیه دسترسی از راه دور، شامل تجهیزات ارتباط از راه دور و کاربران Dialup
- ناحیه سرویس‌های عمومی، شامل سرویس‌های ارائه شده توسط سازمان برای کاربران سایر شبکه‌ها
- ناحیه سرویس‌های غیرعمومی، شامل سرویس‌های ارائه شده توسط سازمان برای کاربران داخلی و احیانا کاربران Dialup

۴- **تامین زیرساخت مستقل برای مدیریت امنیت شبکه** را امکان‌پذیر نماید.

۵- **تجهیزاتی از مارک‌های مختلف** بکار گرفته شوند تا ضعف‌های امنیتی یکدیگر را پوشش داده و منجر به کاهش مخاطرات امنیتی شبکه شوند.

۶- در دفاع از شبکه، دیدگاه پیش‌گیرانه حاکم باشد، برای این منظور لازم است به‌جای استفاده از تجهیزات تشخیص تهاجم، تجهیزات پیشگیری از تهاجم مورد استفاده قرار گیرند.

### ۴-۳-۲- ساختار شماتیک طرح امنیت شبکه

با توجه به معماری ارائه شده برای سیستم امنیت شبکه سازمان و مشخصات کلیدی ارائه شده برای سیستم امنیتی، در این بخش ساختار شماتیک طرح امنیتی شبکه، ارائه خواهد شد.

در طرح شماتیک، لازم است مطالب زیر، ارائه شوند:

۱- نام، نوع، مدل و شرکت سازنده هر یک از تجهیزات، شامل تجهیزات شبکه و تجهیزات امنیت شبکه افزوده شده
۲- نحوه اتصال تجهیزات به یکدیگر
۳- نواحی امنیتی تشکیل شده توسط سیستم امنیتی شبکه
۴- نام و نسخه سیستم عامل، برای تجهیزات و سرویس‌دهنده‌ها
۵- نام و نسخه نرم‌افزار سرویس، برای سرویس‌دهنده‌ها
۶- مروری بر مشخصات کلیدی رعایت شده در سیستم امنیتی

### ۴-۳-۳- مشخصات فنی ابزارهای امنیت شبکه

#### ۴-۳-۳-۱- مشخصات فنی فایروال

در این بخش، ابتدا باید لیستی از فایروال‌های مورد استفاده در طرح، ارائه شده و در ادامه، حداقل مشخصات فنی موردنیاز برای هر یک از فایروال‌ها، ارائه شوند. برخی از مشخصاتی که لازم است در نیازمندی‌های فایروال به آنها اشاره شود، عبارتند از:

۱- سخت‌افزار و نرم‌افزار ویژه و امن، بعبارت دیگر، استفاده از فایروال سخت‌افزاری / نرم‌افزاری
۲- تعداد حداقل نواحی امنیتی قابل پشتیبانی توسط فایروال
۳- پشتیبانی از پورت مدیریت مستقل (در صورت نیاز)

۴- حداقل قابلیت گذردهی قابل پشتیبانی
۵- نوع فیلترینگ قابل پشتیبانی، مثلا Stateful inspection
۶- پشتیبانی از قابلیت Fail-Over
۷- امکان مدیریت امن بر اساس پروتکل‌هایی نظیر SSH، SSL و IPSec
۸- پشتیبانی از MIBهای متعارف SNMP
۹- امکان ثبت رویداد و فرمت‌های قابل پشتیبانی برای این منظور
۱۰- گواهی‌های معتبر موردنیاز از قبیل گواهی معیارهای مشترک یا گواهی ICSA
۱۱- پشتیبانی از VPN و حداقل تعداد VPNهای همزمان قابل پشتیبانی
۱۲- پشتیبانی از NAT (در صورت نیاز)

در ادامه، با توجه به مشخصات ارائه شده، بازاء هر فایروال موردنیاز، گزینه‌های مختلف فایروال‌های قابل انتخاب، مطرح و مقایسه شده و فایروال مناسب برای این منظور، انتخاب شود و در خاتمه، مشخصات فنی فایروال [های] انتخابی ارائه شود.

**۴-۳-۳-۲- مشخصات فنی سیستم ضدویروس:**

ابزارهای ضدویروس بسیار متنوع و فراوان می‌باشند. ضدویروس‌ها را می‌توان بر مبنای محل عملکرد آنها به سه دسته تقسیم کرد: ایستگاههای کاری، سرویس دهنده های مختلف و دروازه های ارتباطی.

با توجه به اینکه پست الکترونیکی یکی از راههای مهم انتقال اغلب ویروس‌ها و کرم‌ها می‌باشد، ضدویروس‌های خاصی برای این سرویس‌دهنده‌ها نیز ارائه می‌شود.

در انتخاب محصولات ضدویروس، انتخاب بین دو راهکار مفید که در تناقض با یکدیگر قرار دارند، تصمیم‌گیری را مشکل می‌کند: انتخاب محصولات متفاوت به‌منظور ایمنی بالاتر و انتخاب محصولات یک شرکت به‌منظور مدیریت مؤثرتر.

در این بخش، ابتدا باید لیستی از آنتی‌ویروس‌های مورد استفاده در طرح، ارائه شده و در ادامه، حداقل مشخصات فنی موردنیاز برای هر یک از آنتی‌ویروس‌ها، ارائه شوند.

برخی از مشخصاتی که لازم است در نیازمندی‌های آنتی‌ویروس‌های مبتنی بر ایستگاه و سرویس‌دهنده به آنها اشاره شود، عبارتند از:

۱- تعداد کاربران یا آدرس‌های قابل پشتیبانی

۲- انتخاب اولویت در خصوص "استفاده از محصولات مختلف، به‌منظور افزایش امنیت" یا "انتخاب محصولات یک شرکت، به‌منظور مدیریت موثرتر"

۳- اجزاء موردنیاز، شامل آنتی‌ویروس مبتنی بر ایستگاه، سرویس‌دهنده و شبکه

۴- قابلیت مدیریت متمرکز، امن و از راه دور کلیه اجزاء

۵- داشتن گواهی ICSA در موارد تشخیص و ترمیم : مؤسسهٔ ICSAیکی از معتبرترین مؤسسات صادر کنندهٔ گواهی برای محصولات امنیتی به حساب می‌آید. داشتن گواهی ICSA نشان‌دهندهٔ قدرت تشخیص و ترمیم تمام ویروس‌های خطرناک می‌باشد.

۶- داشتن گواهی سطح یک ودو ضدویروس و ضد اسب تراوای CHECK MARK از WEST COAST LABS : این مؤسسه نیز جزء معتبرترین مؤسسات ارزیابی‌کنندهٔ محصولات امنیتی می‌باشد که ضدویروس‌ها را بر اساس قدرت تشخیص و ترمیم ارزیابی می‌کند.

۷- امکان تشخیص ویروس روی پیام‌های پست الکترونیکی وارد شونده و خارج شونده

۸- امکان تشخیص ویروس روی فایل‌های فشرده شده

۹- امکان تشخیص و حذف Spaywareها، Dialerها ،trojanها، ابزارهای Hacking، ActiveX code و JavaApplet های مخرب

۱۰- امکان تشخیص ویروس روی فایل‌های ارسال شده توسط سیستم‌های پیغام‌رسانی فوری
۱۱- امکان تعریف قواعد فیلترینگ محتوا به‌منظور جلوگیری از آسیب ویروس‌ها و کرم‌هایی که هنوز الگوی تشخیص و ترمیم آنها فراهم نشده است
۱۲- امکان ترمیم خرابی‌ها بصورت متمرکز
۱۳- امکان فیلترینگSpam و فیلترینگ محتوا برای سرویس‌دهنده‌های پست الکترونیکی

همچنین برخی از مشخصاتی که لازم است در نیازمندی‌های آنتی‌ویروس‌های مبتنی بر شبکه (برای گذرگاه‌های ارتباطی شبکه) به آنها اشاره شود، عبارتند از:
۱- داشتن گواهی ICSA در زمینهٔ ابزار ضدویروس گذرگاه
۲- امکان جلوگیری از spam
۳- نظارت بر ترافیک SMTP، HTTP و FTP Over HTTP ورودی و خروجی برای جلوگیری از ورود ویروس‌ها و امکان فیلترینگ محتوا روی آنها
۴- امکان جلوگیری از کدهای Activex ، Java and VB Script ، و Java Appletهای مخرب
۵- امکان تعریف قواعد فیلترینگ محتوا به‌منظور جلوگیری از آسیب ویروس‌ها و کرم‌هایی که هنوز الگوی تشخیص و ترمیم آنها فراهم نشده است

در ادامه، با توجه به مشخصات ارائه شده، بازاء هر یک از اجزاء آنتی‌ویروس موردنیاز، گزینه‌های مختلف قابل انتخاب، مطرح و مقایسه شده و آنتی‌ویروس مناسب برای این منظور، انتخاب شود و در خاتمه، مشخصات فنی آنتی‌ویروس[های] انتخابی ارائه شود.

**۴-۳-۳-۳- مشخصات فنی سیستم تشخیص و مقابله با تهاجم مبتنی بر شبکه**

در ابتدا فایروال‌ها بعنوان اصلی‌ترین مکانیسم دفاعی به حساب می‌آمدند. بعدها اشتباهات در پیکربندی فایروال‌ها بدلیل پیچیدگی‌های خاص سرویس‌ها و بعضاً مبهم بودن سیاست‌ها، عدم توانایی فایروال‌ها در مقابله با برخی از تهدیدات بخصوص تهدیدات داخلی، و افزایش حملات از طریق پروتکل‌های مجاز، ضرورت وجود مکانیسم‌های دفاعی چند لایه را بیش از پیش مشخص نمود. طی سالیان بعد، سیستم‌های تشخیص تهاجم به‌عنوان یکی از اولین و مهمترین مؤلفه‌های ایجاد امنیت چندلایه‌ای معرفی شدند. IDSها بعنوان سیستم‌های هشدار می‌توانند خط دوم دفاع در برابر حملات را (بعد از فایروال‌ها بعنوان خط اول) تشکیل دهند.

مدتی از معرفی IDSها و بخصوص N-IDSها می‌گذرد. اولین محصول تجاری از این نوع توسط شرکت ISS ارائه شد که همواره بعنوان یکی پیشروترین شرکت‌ها در این زمینه به حساب می‌آمده است.

N-IDSها با بررسی بسته‌های عبوری سعی در کشف ترافیک غیرمجاز و غیرمتعارف براساس مقایسه با الگوهای حملات شناخته شده یا تحلیل پروتکل دارند. در صورت کشف ترافیک مشکوک چنین سیستمی می‌تواند تولید اخطار کند یا اینکه اتصال مربوطه را، معمولاً با استفاده از TCP Reset پایان دهد. بعضی از N-IDSها قابلیت تغییر دادن قوانین فایروال‌ها به‌منظور جلوگیری از حملات بعدی از طریق مهاجم شناخته شده را نیز دارند. چنین سیستم‌هایی معمولاً در حالت بی‌قاعده عمل می‌کنند. با توجه به این مسأله و با توجه به اینکه برای تشخیص حملات پیشرفته و حملاتی که به روش‌های مختلف سعی در دور زدن IDSها دارند، لازم است که N-IDSها اطلاعات نشست‌ها را نگه‌دارند و بصورت stateful عمل کنند، حجم پردازش و میزان حافظه مورد نیاز این سیستم‌ها بشدت افزایش خواهد یافت.

اگر چه چنین سیستم‌هایی بعضاً ادعای جلوگیری از تهاجم را نیز دارند اما در واقع این سیستم‌ها فقط امکان جلوگیری از ادامهٔ حمله‌ای که تشخیص داده شده

است را فراهم می‌کنند و در واقع امکان عکس‌العمل واکنشی را فراهم می‌آورند. بدین ترتیب قبل از اینکه واکنش مناسب صورت گیرد ممکن است حمله تأثیر خود را گذاشته باشد.

در این بخش، ابتدا باید لیستی از N-IDSهای مورد استفاده در طرح، ارائه شده و در ادامه، حداقل مشخصات فنی موردنیاز برای هر یک از N-IDSها، ارائه شوند.

برخی از مشخصاتی که لازم است در نیازمندی‌های سیستم تشخیص تهاجم مبتنی بر شبکه به آنها اشاره شود، عبارتند از:

۱- پشتیبانی از روش‌های پیشرفتهٔ تشخیص تهاجم شامل Stateful Pattern Maching، Protocol Decode، Heuristic Analysis، و Anomaly Analysis
۱- مقاومت در برابر روش‌های فریب IDS
۲- سخت‌افزار و نرم‌افزار ویژه و امن
۳- قابلیت تشخیص حملات برای کاربردهای HTTP، SMTP، FTP، POP3
۴- امکان تولید اخطار به روش‌های گوناگون شامل Mail، Pager، SNMP Trapو ثبت در پایگاه داده و فایل
۵- امکان پایان دادن به ارتباط مشکوک با استفاده از TCP Reset و ICMP Unreachable و تغییر در پیکربندی فایروال
۶- امکان مدیریت متمرکز و امن
۷- پشتیبانی از MIBهای متعارف SNMP
۸- امکان عمکرد بصورت سیستم پیش‌گیری از تهاجم

در ادامه، با توجه به مشخصات ارائه شده، بازاء هر یک از سیستم‌های تشخیص تهاجم مبتنی بر شبکه موردنیاز، گزینه‌های مختلف قابل انتخاب، مطرح و مقایسه شده و سیستم[های] مناسب برای این منظور، انتخاب شود و در خاتمه، مشخصات فنی سیستم[های] تشخیص تهاجم انتخابی ارائه شود.

### ۴-۳-۳-٤- مشخصات فنی دروازهٔ امنیتی

دروازهٔ امنیتی درواقع سیستمی است که می‌تواند ترکیبی از قابلیت‌های فایروال، سیستم بازدارندهٔ تهاجم (N-IPS) و ضدویروس‌های گذرگاهی را ارائه کند. با توجه به اینکه قابلیت‌های فایروالی و ضدویروسی در بخش‌های قبل عنوان شده‌اند در این بخش روی قابلیت‌های بازدارندگی از تهاجم یک دروازهٔ امنیتی تمرکز می‌شود.

سیستم‌های IPS سیستم‌های بازدارنده‌ای هستند که به‌منظور تشخیص بسته‌های خطرناک در داخل ترافیک معمولی (عملیاتی که فایروال‌های فعلی عملاً نمی‌توانند انجام دهند) و جلوگیری از رسیدن این بسته‌ها به مقصد و در نتیجه سد کردن تلاشهای نفوذی طراحی شده‌اند. چنین قابلیتی بسیار فراتر از قابلیت‌های معمول در IDSها است که می‌توانند بعد از رسیدن ترافیک خطرناک به قربانی اعلام هشدار کنند یا سعی در جلوگیری از ادامهٔ نفوذ کنند. در حال حاضر، گرایش اغلب تولیدکنندگان، به سمت تولید سیستم‌های IPS می‌باشد.

N-IPSها در واقع قابلیت‌های فایروال و IDSهای استاندارد را با یکدیگر در آمیخته‌اند و بعضاً Inline IDS یا Gateway IDS نیز نامیده می‌شوند. یک N-IPS واقعی شبیه یک فایروال بطور سری روی خط انتقال قرار می‌گیرد، بطوریکه تمام بسته‌ها باید از داخل آن عبور کنند. بنابراین همین که یک بسته مشکوک تشخیص داده شد و قبل از اینکه به رابط داخلی و شبکهٔ محافظت شده منتقل شود، می‌تواند حذف شود. همچنین نشست مربوط به آن بسته می‌تواند به‌نوعی با عنوان مشکوک علامت‌گذاری شود و در نتیجه تمام بسته‌های مربوط به آن نشست نیز می‌تواند با پردازش کوچکی حذف شود. همچنین بعضی از این سیستم‌ها قابلیت ارسال TCP Reset و ICMP Unreachable به میزبان مهاجم برای خاتمه دادن به این نشست‌ها را نیز دارند.

در این بخش، ابتدا باید لیستی از دروازه‌های امنیتی مورد استفاده در طرح، ارائه شده و در ادامه، حداقل مشخصات فنی موردنیاز برای هر یک از دروازه‌های امنیتی، ارائه شوند.

برخی از مشخصاتی که لازم است در نیازمندی‌های دروازه امنیتی به آنها اشاره شود، عبارتند از:

۱- کلیه نیازمندی‌های اعلام شده برای سیستم تشخیص تهاجم
۲- In-Line Operation: تنها در چنین حالتی می‌توان عملکرد بازدارنده واقعی داشت
۳- Reliability and Availability: چنین سیستمی عملاً می‌تواند یک single point of failure شبکه باشد بنابراین باید نرخ معیوب شدن آن بسیار پایین باشد. بعضی از محصولات برای رفع این مشکل امکان failover نیز فراهم می‌آورند
۴- امکان به‌روز نمودن سیستم بدون نیاز به راه‌اندازی مجدد
۵- Resilience: دارا بودن قابلیت fail-open و fail-close
۶- Low Latency: سرعت پردازش بسته‌ها در یک N-IPS باید به اندازه‌ای باشد که تأخیر کلی سیستم تا جای ممکن به دیگر وسایل لایه ۲ و ۳ شبکه نظیر سوئیچ نزدیک باشد و از تأخیر تجهیزات لایهٔ ٤ نظیر فایروال و Load balancer بیشتر نشود
۷- High Performance: سیستم مورد نظر باید کارآیی عنوان شده را با فعال بودن تمام الگوها نیز ارائه دهد و به تعداد الگوها وابسته نباشد
۸- Unquestionable detection accuracy: با توجه به اینکه تشخیص نادرست حمله در این سیستم‌ها می‌تواند سبب DoS شود، تشخیص‌های نادرست این سیستم‌ها باید تقریباً در حد صفر باشد
۹- Fine-grained granularity and control: انتخاب دقیق و جزئی ترافیکی که باید سد شود یا log شود باید ممکن باشد

۱۰- Advanced alert handling and forensic analysis capabilities:
امکانات گزارش‌گیری و مشاهده و دسته‌بندی رویدادنامه‌ها از ویژگی‌های ضروری است که راحتی و سودمندی استفاده از سیستم را نشان می‌دهد

در ادامه، با توجه به مشخصات ارائه شده، به ازاء هر یک از دروازه‌های امنیتی موردنیاز، گزینه‌های مختلف قابل انتخاب، مطرح و مقایسه شده و سیستم مناسب برای این منظور، انتخاب شود و در خاتمه، مشخصات فنی دروازه[های] امنیتی انتخابی ارائه شود

با توجه به آزمایشات علمی، دقیق و کاربردی که مؤسسهٔ NSS بر روی محصولات امنیتی بخصوص فایروال‌ها و سیستم‌های تشخیص و مقابله با تهاجم انجام می‌دهد، هم‌اکنون این مؤسسه بعنوان معتبرترین مؤسسه برای آزمایش این سیستم‌ها در محیط واقعی محسوب می‌شود و لذا توصیه سیستم‌ها توسط این موسسه، معیار مناسبی برای انتخاب دروازه‌های امنیتی است.

**۴-۳-۳-۵- مشخصات فنی سیستم تشخیص و مقابله با تهاجم مبتنی بر میزبان**

مکانیسم‌های HIDSها قابل تقسیم‌بندی به دو دسته می‌باشد که برخی از محصولات، ترکیبی از این روش‌ها را پیاده‌سازی می‌کنند.

- IDSهای سنتی با استفاده از برنامه‌هایی که روی میزبانها قرار می‌گیرند، عمل می‌کنند. این برنامه‌ها رویدادنامه‌های سیستم، فایل‌های بحرانی سیستم و دیگر منابع قابل بازرسی را به‌منظور کشف تغییرات غیرمجاز یا الگوهای فعالیت‌های مشکوک بررسی می‌کنند. در صورت کشف چنین فعالیت‌هایی اخطارها یا SNMP trapهای مناسب تولید می‌شوند.
- ارزیابی کنندگان جامعیت فایل وضعیت فایلهای سیستم و کاربرد یا رجیستری را از طریق ایجاد و بررسی hashهای مناسب بطور پی‌درپی

بررسی می‌کنند. این محصولات علاوه بر تولید اخطار می‌توانند از تغییر فایل‌ها و در نتیجه از اثرات حملات نیز جلوگیری کنند.

در این بخش، ابتدا باید لیستی از سیستم‌های تشخیص و مقابله با تهاجم مبتنی بر میزبان مورد استفاده در طرح، ارائه شده و در ادامه، حداقل مشخصات فنی موردنیاز برای هر یک از سیستم‌ها، ارائه شوند.

برخی از مشخصاتی که لازم است در نیازمندی‌های سیستم‌های تشخیص و مقابله با تهاجم مبتنی بر میزبان به آنها اشاره شود، عبارتند از:

۱- امکان مدیریت متمرکز و امن
۲- ارتباطات امن و رمز شده بین اجزاء سیستم
۳- امکان جلوگیری از تغییرات غیرمجاز و محافظت از منابع سیستم
۴- امکان تولید اخطار به روش‌های گوناگون شامل Mail، Pager، SNMP Trapو ثبت در پایگاه داده و فایل
۵- امکانات گزارش‌گیری و مشاهده و دسته‌بندی رویدادنامه‌ها
۶- پشتیبانی از MIBهای متعارف SNMP

در ادامه، با توجه به مشخصات ارائه شده، بازاء هر یک از انواع سیستم‌های تشخیص و مقابله با تهاجم مبتنی بر میزبان موردنیاز، گزینه‌های مختلف قابل انتخاب، مطرح و مقایسه شده و سیستم مناسب برای این منظور، انتخاب شود و در خاتمه، مشخصات فنی سیستم[های] انتخابی ارائه شود.

### ۴-۳-۳-۶- مشخصات فنی پویش‌گر امنیتی

یکی از مراحل اصلی در چرخهٔ امنیت، نظارت و بازرسی مستمر سیستم‌ها از منظر امنیت می‌باشد. پویش‌گرهای امنیتی ابزارهایی برای اتوماتیک نمودن این مرحله به حساب می‌آیند. پویش‌گرهای امنیتی را می‌توان به دو دستهٔ پویش‌گرهای Passive یا مبتنی بر میزبان و پویش‌گرهای Active یا مبتنی بر

شبکه تقسیم نمود. پویش‌گرهای Passive در واقع سیاست‌های امنیتی سیستم‌ها را با سیاست امنیتی مورد نظر مقایسه می‌کنند و اختلافات را گزارش می‌دهند، در حالیکه پویش‌گرهای Active شبیه یک نفوذگر عمل می‌کنند و سعی می‌کنند با بکارگیری روش‌های تشخیص آسیب‌پذیری‌های شناخته شده، ضعف‌های امنیتی سیستم در برابر حملات مختلف را شناسایی و اولویت‌بندی کنند. پویش‌گرهای امنیتی را می‌توان از نظر معماری به دو دسته متمرکز و توزیع‌شده نیز تقسیم نمود.

در این بخش، ابتدا باید لیستی از پویش‌گرهای امنیتی مورد استفاده در طرح، ارائه شده و در ادامه، حداقل مشخصات فنی موردنیاز برای هر یک از پویش‌گرها، ارائه شوند.

برخی از مشخصاتی که لازم است در نیازمندی‌های پویش‌گرهای امنیتی به آنها اشاره شود، عبارتند از:

۱- دارای قابلیت‌های پویش Passive و Active
۲- ارائهٔ راه حل‌های رفع ضعف‌ها بصورت جزئی
۳- ارائهٔ مکانیسم‌های اتوماتیک اصلاح ضعف‌ها تا حد امکان و قابلیت برگشت به حالت قبل از انجام اصلاحات
٤- پشتیبانی توسط یک تیم معتبر
٥- امکان تعریف پویش‌های جدید

در ادامه، با توجه به مشخصات ارائه شده، بازاء هر یک از پویش‌گرهای موردنیاز، گزینه‌های مختلف قابل انتخاب، مطرح و مقایسه شده و سیستم مناسب برای این منظور، انتخاب شود و در خاتمه، مشخصات فنی پویش‌گر[های] انتخابی ارائه شود.

### ۴-۳-۳-۷- مشخصات فنی سیستم‌های مدیریتی

در این بخش، ابتدا باید لیستی از اجزاء مدیریتی امنیت مورد استفاده در طرح، ارائه شده و در ادامه، حداقل مشخصات فنی موردنیاز برای هر یک از اجزاء ارائه شوند.

موارد مدیریتی که بطور مستقیم با امنیت شبکه در ارتباط هستند عبارتند از:

۱- مدیریت تجهیزات امنیتی شبکه، شامل مدیریت IDSهای مبتنی بر شبکه، میزبان و سرویس‌دهنده، مدیریت ضدویروس‌های مبتنی بر شبکه، میزبان و سرویس‌دهنده، و مدیریت فایروال

۲- مدیریت کاربران شامل تصدیق‌اصالت، تعیین حدود اختیارات و حسابرسی(AAA)

۳- مدیریت Patch

۴- مدیریت تهیه پشتیبان

۵- مدیریت رویدادنامه‌ها

همچنین مواردی که بطور غیرمستقیم به امنیت ارتباط دارند، عبارتند از مدیریت خطا، مدیریت کارآیی، مدیریت توان مصرفی ، مدیریت تجهیزات، سرویس‌ها و حتی خطوط شبکه.

اگر چه با توجه به پیچیدگی‌های شبکه‌های کنونی، بحث جدا کردن مدیریت شبکه و مدیریت امنیت شبکه بسیار مشکل می‌باشد، اما می‌توان با تقسیم مناسب وظایف و ایجاد راهکارهای همکاری لازم، از انجام شدن مناسب کارها اطمینان حاصل کرد.

### ۴-۳-۳-۷-۱) مدیریت و نظارت بر شبکه

در حالت کلی وقتی صحبت از مدیریت شبکه به‌میان می‌آید، توقع مدیریت و کنترل تمام جنبه‌های شبکه ایجاد می‌شود و همین مسأله به‌نوعی مشکل ساز است. برخی مجموعه‌های نرم‌افزاری با چنین دیدگاهی سعی می‌کنند که مؤلفه‌های

بسیار فراوان جدا از هم تشکیل‌دهندهٔ یک شبکه را درک و به روش یکسانی ارائه کنند که البته دشواری چنین کاری سبب هزینهٔ مالی بسیاری می‌شود.

برخی از مشخصاتی که لازم است در انتخاب نرم‌افزار مدیریت و نظارت شبکه به آنها توجه شود، عبارتند از:

۱- محصولاتی که روی یک جنبه تمرکز می‌کنند معمولا کارآتر و ارزانتر هستند و استفاده از آنها ساده‌تر می‌باشد ولی سادگی آنها سبب قابلیت‌های کمتر آنها می‌شود. از طرف دیگر، نسخه‌های کوچک‌تر محصولات پرقابلیت‌تر، تقریباً هر کدام از جنبه‌های مدل FCAPS را ، اگر چه با محدودیت‌هایی، ولی با قیمت مناسب پوشش می‌دهند. بر اساس مدل FCAPS مدیریت شبکه می‌تواند به پنج دسته کلی تقسیم شوند که عبارتند از:

1- Security Management
2- Fault Management
3- Configuration Management
4- Performance Management
5- Accounting Management

اهمیت هر کدام از این جنبه‌ها نیز برای مدیران شبکه معمولاً بر اساس ترتیب ذکر شده است. محدودیت‌هایی که معمولاً ابزارهای ارزان‌قیمت‌تر دارند به‌خاطر محدودیت کارهایی است که SNMP می‌تواند انجام دهد. ابزارهایی که تنها متکی بر SNMP هستند، تنها می‌توانند بخش‌های Performance و Fault از مدل FCAPS را پوشش دهند، بنابراین بسیاری از ابزارهای مدیریت جامع، به منظور انجام عملیات مدیریت، از عامل‌های خاص خود بهره می‌برند. به هر حال باید توجه داشت که ابزارهای امنیتی که بتوانند تمام جنبه‌های مدل FCAPS را پوشش دهند، محدود و بسیار گران‌قیمت هستند.

اغلب محصولات مدیریت شبکهٔ ارزان‌قیمت تنها ابزارهای مانیتورینگ هستند. این محصولات اطلاعات شبکه را به صورت گستره وسیعی از روش‌ها از system-tray pop-up ها و نمایه‌های چشمک زن گرفته تا گراف‌های

پیچیده مقادیر حداقل و حداکثر و آستانه بر حسب زمان نشان می‌دهند. تعداد محصولات مدیریت شبکهٔ ارزان‌قیمت بسیار فراوان است. این محصولات با هر ترکیبی از ویژگی‌های مختلف که بتوان تصور کرد، ارائه شده‌اند.

۲- کشف شبکه یا ارائه نقشهٔ شبکه یکی از اهداف اولیهٔ ابزارهای مدیریت شبکه محسوب می‌شود. اغلب محصولات سعی می‌کنند که نقشهٔ لایهٔ ۳ شبکه را با استفاده از ping، SNMP، و پورتهای TCP و UDP استخراج کنند. ابزارهای پیشرفته‌تر سعی می‌کنند نقشهٔ لایهٔ دو را نیز استخراج کنند، اگرچه اکثراً به دلیل مشکلاتی نظیر یکسان نبودن پیاده‌سازیهای SNMP نمی‌توانند نقشهٔ دقیقی در این مورد ارائه کنند. به هرحال هیچ ابزاری که بتواند توپولوژی فیزیکی شبکه را استخراج کند ارائه نشده است.

۳- مسألهٔ مهم دیگری که باید مدنظر قرار داد، پشتیبانی محصولات می‌باشد. ابزارهای مدیریت شبکهٔ ارزان‌قیمت، معمولاً از پایگاه داده‌های معمول پشتیبانی نمی‌کنند وبا شبکه‌های بسیار بزرگ مشکل پیدا می‌کنند.

در ادامه، با توجه به مشخصات ارائه شده برای نرم‌افزار مدیریت و نظارت، گزینه‌های مختلف قابل انتخاب، مطرح و مقایسه شده و نرم‌افزار[های] مناسب برای این منظور، انتخاب شود و در خاتمه، مشخصات فنی نرم‌افزار[های] انتخابی ارائه شود.

### ۴-۳-۳-۷-۲) سرویس‌دهندهٔ AAA

یقینا بحث تصدیق اصالت، تعیین و اعمال اختیارات و پی‌گیری فعالیت‌های کاربران، جزء مهمترین مقوله‌های امنیتی محسوب می‌شود. سرویس‌دهنده‌های AAA درواقع امکان مدیریت متمرکز سه سرویس Authentication،

Authorization و Accounting را فراهم می‌کنند و بنابراین باعث راحتی، قابلیت انعطاف و سودمندی فعالیتهای مدیریتی می‌شوند.

اگر چه سرویس‌دهنده‌های AAA اغلب توسط ارائه‌کنندگان خدمات اینترنتی و برای تصدیق اصالت و پی‌گیری میزان استفاده کاربران Dialup مورد استفاده قرار می‌گیرد، با توجه به ساختار و تجهیزات شبکه، این سرویس‌دهنده‌ها می‌توانند برای تصدیق اصالت، تعیین و اعمال اختیارات و پی‌گیری فعالیت‌های کاربران داخلی و کاربران راه‌دور اعم از کاربران LAN ، کاربران WAN ، مدیران شبکه و کاربران VPN بکار روند.

در این بخش، ابتدا باید لیستی از سرویس‌دهنده‌های AAA مورد استفاده در طرح، ارائه شده و در ادامه، حداقل مشخصات فنی موردنیاز برای هر یک از سرویس‌دهنده‌ها، ارائه شوند.

برخی از مشخصاتی که لازم است در نیازمندی‌های سرویس‌دهنده‌های AAA به آنها اشاره شود، عبارتند از:

۱- پشتیبانی از Radius و +Tacacs

۲- پشتیبانی از پروتکلهای تصدیق اصالت شامل:

- PAP
- CHAP
- MSCHAP v1 & v2
- پروتکلهای تصدیق اصالت EAP شامل :EAP-MD5، EAP-TLS، EAP-LEAP، EAP-PEAP

۳- امکان تصدیق اصالت کاربران از منابع داده‌ای غیر از پایگاه دادهٔ محلی شامل:

- Flat file
- Windows 2000 Active Directory
- Native Windows NT user database and domains
- پایگاه داده‌های SQL مهم نظیر Microsoft SQL Server و Oracle
- Proxy به AAA Serverهای دیگر

- LDAP
- پشتیبانی از Token-Server های شرکتهای مهم نظیر RSA و Cryptocard.
- Kerberos

٤- امکان ذخیرهٔ اطلاعات Accounting به روش‌های مختلف

- Flat file
- پایگاه داده‌های SQL مهم نظیر Microsoft SQL Server و Oracle
- Proxy به AAA Serverهای دیگر

٥- امکان مانیتورینگ بلادرنگ وضعیت فعالیت‌های کاربران و قابلیت فراهم آوردن گزارشات دقیق و مناسب

٦- پشتیبانی از SNMP برای IETF Radius Server MIB

۷- قابلیت رویدادنگاری مؤثر از طریق پشتیبانی از Syslog Server

۸- امکانات پشتیبان‌گیری

۹- امکان تخصیص اتوماتیک IP بوسیلهٔ DHCP و Sql Server

۱۰- داشتن امکانات لازم برای ایجاد محدودیت روی روز و ساعت استفاده، میزان استفاده، طول نشست‌ها، تعداد نشست‌های همزمان، تلاشهای ناموفق login ومشخصات محل دسترسی نظیر آدرس IP

۱۱- پشتیبانی از Radius Tunneling

در ادامه، با توجه به مشخصات ارائه شده، بازاء هر یک از سرویس‌دهنده‌های AAA موردنیاز، گزینه‌های مختلف قابل انتخاب، مطرح و مقایسه شده و سیستم[های] مناسب برای این منظور، انتخاب شود و در خاتمه، مشخصات فنی سرویس‌دهنده[های] AAA انتخابی ارائه شود.

**۴-۳-۳-۷-۳) مدیریت رویدادنامه‌ها**

در این بخش، ابتدا باید لیستی از سیستم‌های رویدادنگاری مورد استفاده در طرح، ارائه شده و در ادامه، حداقل مشخصات فنی موردنیاز برای هر یک از سیستم‌ها، ارائه شوند.

برخی از مشخصاتی که لازم است در نیازمندی‌های سیستم‌های رویدادنگاری به آنها اشاره شود، عبارتند از:

۱- قابلیت عملکرد بصورت Syslog Server، SNMP Trap Receiver، SETP Server
۲- پشتیبانی از پروتکل ایمن SETP و SETP مبتنی بر SSL برای انتقال اطلاعات
۳- قابلیت فیلتر کردن و جستجوی رویدادنامه‌ها
٤- تولید گزارشهای روزانه به فرمت html با اطلاعات مناسب در مورد رویدادها
٥- امکان تولید اخطار به روش‌های گوناگون شامل نوشتن در فایل و پایگاه داده، ارسال email ، ارسال به syslog server و SETP server، شروع یک برنامهٔ دلخواه، و اخطار بوسیلهٔ NET SEND
٦- امکان نظارت بر سیستمهای دیگر با استفاده از Ping & Port Probe
۷- نظارت بر NT Service و فضای Disk

در ادامه، با توجه به مشخصات ارائه شده، به ازاء هر یک از سیستم‌های رویدادنگاری موردنیاز، گزینه‌های مختلف قابل انتخاب، مطرح و مقایسه شده و سیستم[های] مناسب برای این منظور، انتخاب شود و در خاتمه، مشخصات فنی سیستم[های] رویدادنگاری انتخابی ارائه شود.

**۴-۳-۴) جریان اطلاعات در شبکه متصل به اینترنت**

در این بخش، لازم است جریان اطلاعات دسترسی کاربران به کلیه سرویس‌های شبکه، بررسی شده و نشان داده شود که سیستم امنیتی انتخاب شده، قادر به جلوگیری از دسترسی‌های غیرمجاز به سرویس‌های شبکه می‌باشد. ترسیم جریان اطلاعات هر یک از سرویس‌ها پس از انتخاب سیستم امنیتی، کمک قابل توجهی به طراح، بابت بازبینی کفایت اجزاء سیستم امنیتی خواهد بود. همچنین این امر، مشخص خواهد نمود که ترافیک هر یک از سرویس‌های شبکه، از چند لایه از سیستم امنیتی عبور می‌کند.

البته کنترل دسترسی، تنها بخشی از وظایف سیستم امنیتی می‌باشد و مثلا تشخیص حملات یا ویروس‌های موجود در دسترسی‌های مجاز، توسط IDSها و آنتی‌ویروس‌های بکار گرفته شده نیز بخش دیگری از وظایف سیستم امنیتی است.

**۴-۳-۴-۱- جریان اطلاعات در دسترسی به شبکه از طریق LAN داخلی**

به‌منظور وضوح مناسب، جریان اطلاعات دسترسی کاربران باید بر اساس مقصد دسترسی مشخص شود. بنابراین در ابتدا باید مقاصد دسترسی یا سرویس‌های قابل ارائه به کاربران مشخص شود. مقصد دسترسی کاربران داخلی و علت‌های دسترسی عبارتند از:

۱- دسترسی به منابع سیستم شخصی به‌منظور انجام فعالیتهای کاری و برقراری ارتباط با سیستم‌های دیگر
۲- دسترسی به منابع domain به‌منظور استفاده از فایل‌ها، اطلاعات و کاربردهای به اشتراک گذاشته شده
۳- دسترسی به سرویس‌دهنده‌های عمومی از قبیل پست الکترونیکی، وب و سایر سرویس‌ها
۴- دسترسی به سرویس‌دهنده‌های داخلی

۵- دسترسی به سرویس‌های سایر شبکه‌ها

لازم به ذکر است که علاوه بر جریان اطلاعات دسترسی در هر یک از دسترسی‌های فوق، یک جریان اطلاعات تصدیق اصالت، تعیین مجوز، حسابرسی (AAA) و رویدادنگاری (logging) نیز قابل تعریف و تعیین است که لازم است در این بخش به آن نیز پرداخته شود.

**۴-۳-۴-۲- جریان اطلاعات در دسترسی به شبکه از طریق Dialup**

دسترسی کاربران DialUp به شبکهٔ مورد نظر شامل سه گونه دسترسی است:

۱- دسترسی به سرویس‌های عمومی
۲- دسترسی به سرویس‌های داخلی
۳- دسترسی به سرویس‌های سایر شبکه‌ها

مشابه بخش قبل در زیربخش‌های این قسمت نیز جریان اطلاعات دسترسی، AAA ، و logging هر یک از دسترسی‌های فوق نیز باید بررسی شوند.

**۴-۳-۴-۳- جریان اطلاعات در دسترسی به شبکه از طریق اینترنت**

دسترسی کاربران اینترنتی به شبکهٔ مورد نظر شامل دو گونه دسترسی است:

۱- ارسال نامهٔ الکترونیکی به آدرس‌های سرویس‌دهندهٔ پست‌الکترونیکی سازمان
۲- دسترسی به وب‌سایت سازمان به‌منظور کسب اطلاعات عمومی منتشره توسط سازمان

مشابه بخش‌های قبل، در این قسمت نیز جریان اطلاعات دسترسی، AAA ، و logging هر یک از دسترسی‌های فوق نیز باید بررسی شود.

### ۴-۳-۴-۴- جریان اطلاعات در دسترسی به شبکه سازمان از طریق سایر شبکه‌ها

در این بخش، جریان اطلاعات دسترسی کاربران سایر شبکه‌های متصل به شبکه سازمان، به سرویس‌دهنده‌های عمومی شبکه سازمان و جریان اطلاعات AAA و Logging مرتبط با آن ترسیم خواهد شد.

### ۴-۳-۴-۵- جریان اطلاعات در دسترسی به شبکه از طریق ایستگاه مدیریت

دسترسی‌های مدیریتی قابل تصور برای بررسی جریان اطلاعات، عبارتند از:

۱- مدیریت دروازهٔ امنیتی
۲- مدیریت فایروال
۳- مدیریت سیستم تشخیص تهاجم مبتنی بر شبکه
۴- مدیریت و به‌روز رسانی سیستم تشخیص تهاجم مبتنی بر میزبان
۵- مدیریت سیستم ضدویروس
۶- مدیریت و پیکربندی سرویس‌دهنده‌ها
۷- مدیریت سوئیچ‌ها و مسیریاب‌ها
۸- مانیتورینگ شبکه
۹- مدیریت Domain
۱۰-مدیریت Patch

در این بخش، لازم است جریان اطلاعات دسترسی از هر یک از ایستگاه‌های مدیریتی فوق، به اجزاء مدیریت شونده، به همراه جریان اطلاعات AAA و Logging مرتبط با آن ترسیم شود.

### ۴-۳-۴-۶- جمع‌بندی نحوه کنترل جریان اطلاعات توسط سیستم امنیتی شبکه

با توجه به جریان اطلاعات مربوط به دسترسی انواع کاربران شبکه سازمان به سرویس‌های این شبکه، در این بخش جمع‌بندی نحوه عبور جریان اطلاعات دسترسی کاربران به سرویس‌های شبکه و کفایت اجزاء و کنترل‌های سیستم امنیتی شبکه بر جریان اطلاعات انجام خواهد شد.

برای این منظور، جدولی مشابه آنچه در جدول (۴-۲) نشان داده شده است، تهیه می‌شود. سطرهای این جدول، نمایانگر دسترسی انواع کاربران به سرویس‌های مجاز و ستون‌های آن، نمایانگر اجزاء سیستم امنیتی شبکه می‌باشد. بر اساس نتایج حاصل از بخش قبیل، در هر خانه از این جدول، تعداد اجزاء سیستم امنیتی که ترافیک دسترسی کاربران به هر یک از سرویس‌ها از آنها عبور می‌نماید، قید خواهد شد.

نتایج این جدول، جمع‌بندی مناسبی از تعداد اجزاء سیستم امنیتی تاثیر گذار در ترافیک کلیه سرویس‌های شبکه را نشان خواهد داد.

| Content Filter | Anti Virus | | | Intrusion Detection & Prevention | | | Firewall | سیستم امنیتی / دسترسی به سرویس‌ها | |
|---|---|---|---|---|---|---|---|---|---|
| | Client | Server | Network | H-IDS | N-IDS | N-IPS | | | |
| | | | | | | | | سرویس دسترسی به اینترنت | کاربران داخلی |
| | | | | | | | | سرویس‌دهنده Web | |
| | | | | | | | | سرویس‌دهنده Email | |
| | | | | | | | | سایر سرویس‌ها | |
| | | | | | | | | سرویس دسترسی به اینترنت | کاربران Dialup |
| | | | | | | | | سرویس‌دهنده Web | |
| | | | | | | | | سرویس‌دهنده Email | |
| | | | | | | | | سایر سرویس‌ها | |
| | | | | | | | | سرویس‌دهنده Web | کاربران اینترنت |
| | | | | | | | | سرویس‌دهنده Email Forwarder | |
| | | | | | | | | سایر سرویس‌ها | |
| | | | | | | | | سرویس‌دهنده Web ویژه سرویس‌دهی به شبکه دولت | کاربران شبکه دولت |
| | | | | | | | | سایر سرویس‌ها | |

جدول (۴-۲): جمع‌بندی تاثیر اجزاء سیستم امنیتی شبکه روی ترافیک سرویس‌ها

## ۴-۴- تخمین هزینه و اجرای طرح امنیت شبکه

### ۴-۴-۱- لیست و تخمین هزینه طرح امنیت شبکه

در این بخش از طرح، باید لیست سخت‌افزارها و نرم‌افزارهای امنیت شبکه، تجهیزات شبکه و کامپیوترهای اضافه شده به شبکه، در جداولی حاوی مولفه‌های زیر، ارائه شوند:

- شماره مشخصه (Part Number)
- توضیح
- تعداد
- قیمت تقریبی

### ۴-۴-۲- اجرای طرح امنیت شبکه

در این بخش از طرح، باید لیست و مشخصات فعالیت‌های مورد نیاز جهت اجرای طرح، در جداولی حاوی مولفه‌های زیر، ارائه گردد:

- شرح فعالیت
- زمان شروع و خاتمه هر فعالیت
- تخمین نفر/ماه نیروی انسانی موردنیاز جهت اجرای فعالیت
- تخمین هزینه موردنیاز جهت اجرای فعالیت

# ۵

# چارچوب پیشنهادی برای طرح پشتیبانی حوادث شبکه

## ۵-۱- مقدمه

اجرای طرح امنیت شبکه سازمان، موجب ایجاد امنیت در شبکه خواهد شد. لیکن با گذشت زمان، روش‌های نفوذ به شبکه‌ها تغییر نموده و سیستم امنیتی شبکه بر اساس تنظیمات قبلی، قادر به مقابله با روش‌های جدید نخواهد بود. از سوی دیگر، هر روزه آسیب‌پذیری تعدادی از نرم‌افزارها و سخت‌افزارها کشف و اعلام می‌گردد و شرکت‌های سازنده نیز پس از گذشت مدت زمانی، اقدام به ارائه وصله‌های امنیتی سیستم‌های خود می‌نمایند. در صورتی که این وصله‌های امنیتی نصب نشوند، شبکه سازمان در مقابل حملات جدیدی که از آسیب‌پذیریهای جدید استفاده می‌نمایند، آسیب‌پذیر خواهد بود. بسیاری از ویروس‌ها و کرم‌های مشهوری که طی چند سال اخیر، زیان‌های زیادی را به شبکه‌های کامپیوتری وارد نمودند، به سرعت از آسیب‌پذیری‌های اعلام شده استفاده نموده و قبل از آن‌که سازندگان سیستم‌ها، وصله‌های امنیتی را ارائه دهند و یا حتی در مواردی، به واسطه کوتاهی صاحبان شبکه‌ها در نصب به‌موقع وصله‌های امنیتی، زیان‌های بسیاری را وارد نمودند.

در سیستم مدیریت امنیت شبکه، تشکیلات پشتیبانی امنیت شبکه و طرح‌های پشتیبانی امنیت شبکه، به همین منظور پیش‌بینی شده است. مهم‌ترین طرح

پشتیبانی امنیت شبکه، طرح پشتیبانی حوادث می‌باشد. این طرح که توسط تیم پشتیبانی حوادث ( یکی از تیم‌های پشتیبانی امنیت شبکه )، اجراء خواهد شد، متضمن تداوم امنیت در شبکه سازمان می‌باشد. مطالب این فصل، برگرفته از مرجع [۱۰] می‌باشد.

### ۵-۱-۱- اهداف و ابعاد

در این بخش از طرح، باید اهداف تدوین طرح پشتیبانی حوادث سازمان و همچنین ابعادی که طرح پشتیبانی حوادث پوشش می‌دهد، تشریح شوند. اصولا مهم‌ترین هدف سازمان از ارائه چنین طرحی، تامین تداوم امنیت شبکه خود می باشد. در ضمن علاوه براین موضوع باید ابعاد عملی اجرای این طرح نیز مشخص گردد. به عبارت دیگر باید گفته شود که طرح ارائه شده در رده چه سازمان‌هایی قابل اجرا می باشد. به عنوان مثال: سازمان‌های کوچک و بدون شعبه، سازمان‌های متوسط به همراه تعداد کمی شعبه و یا تعداد زیادی شعبه اما در داخل کشور و یا سازمان‌های بزرگ با تعداد زیادی شعبه حتی در خارج از کشور

### ۵-۱-۲- مخاطبین

در این بخش باید مخاطبین این طرح اعم از فرد/افراد، سازمان/سازمان‌ها عنوان شود. لذا لازم است لیست تمامی مخاطبین طرح، اعم از حقیقی یا حقوقی به همراه سطح دسترسی آن‌ها مشخص شود. نمونه‌هایی از مخاطبین این طرح، عبارتند از: تیم پشتیبانی حوادث، مدیریت فن آوری اطلاعات، پرسنل امنیت شبکه، پرسنل پشتیبانی شبکه و سایر پرسنل سازمان.

### ۵-۱-۳- ساختار طرح

در این بخش، ساختار رعایت شده در این طرح شامل قسمت‌های مختلف طرح و موضوعات مطرح شده در هر بخش و ضمیمه‌های طرح، به صورت مختصر عنوان می گردد.

## ۵-۲- ساختار تیم پشتیبانی حوادث

از عوامل موثر در ساختار تیم پشتیبانی حوادث سازمان، می‌توان از ساختار تشکیلاتی سازمان، ساختار تیم امنیت شبکه و متمرکز یا توزیع شده بودن سازمان نام برد.

### ۵-۲-۱- دسته بندی حوادث

در این قسمت از طرح، دسته بندی از انواع حوادث امنیتی ممکن به همراه عوامل آن‌ها ارائه می گردد. به عنوان مثال، حوادث را می توان به شکل زیر دسته بندی نمود:

- ممانعت از سرویس
- کدهای مخرب
- دسترسی غیرمجاز
- استفاده نامناسب

### ۵-۲-۲- پاسخ به حوادث

پاسخ گویی به حوادث امری ضروری می باشد، زیرا تکرار حملات می تواند منجر به افزایش دامنه خسارات و زیان‌هایی بر سرمایه‌های سازمان گردد. ضرورت پاسخ گویی به حوادث و فواید تیم پشتیبانی حوادث در این بخش ذکر می گردد.

### ۵-۲-۳- سیاست‌ها و روال‌های پشتیبانی حوادث

سیاست‌ها و روال‌های مربوط به پشتیبانی حوادث در این بخش عنوان می گردد. در این بخش باید نحوه ارتباط تیم پشتیبانی حوادث سازمان با تیم پشتیبانی حوادث سایر سازمان‌ها نیز تعیین گردد.

### ۵-۲-۴- ساختار تیم پشتیبانی حوادث

اعضای تیم، انواع مدل‌های تیم پاسخ گویی به حوادث و اصول راهبردی برای انتخاب مدل مناسب، از موضوعاتی هستند که در این بخش، ارائه خواهد شد. محتوای موجود در این بخش عبارت است از:

- **معرفی انواع تیم‌های پشتیبانی حوادث و انتخاب مورد مناسب برای سازمان**-سه نوع تیم به منظور پاسخ گویی به حوادث وجود دارد که عبارتند از: تیم پاسخ به حوادث مرکزی، تیم پاسخ به حوادث توزیع شده و تیم اطلاع رسانی.
- **معرفی انواع سیستم‌های پرسنلی و انتخاب مورد مناسب برای سازمان**- مدل‌های سیستم پرسنلی تیم پاسخ گویی به حوادث سه نوع می باشند که عبارتند از: سیستم خود گردانی، سیستم جزئی سفارشی و سیستم تمام سفارشی.
- **انتخاب پرسنل تیم و تعیین وظایف**- به منظور انجام هرچه بهتر و دقیق تر امور و همچنین پی‌گیری دقیق و سریع وقایع، ضرورت دارد لیست پرسنل به همراه شرح وظایف و مسئولیت‌ها و جایگاه سازمانی آن‌ها تعیین و در این بخش از طرح ارائه گردد.
- **وابستگی‌های سازمانی**-ضرورت دارد گروه‌های دخیل در امر پاسخ گویی به حوادث که نقش حیاتی و مؤثر در این امر دارند معرفی گردند. بدیهی است تیم پشتیبانی حوادث به تجارب، قضاوت و توانایی این قبیل گروه‌ها وابسته است. این گروه‌ها عبارتند از: مدیریت، امنیت اطلاعات، ارتباطات، پشتیبانی

IT، دایره حقوقی، بخش اطلاع رسانی عمومی، منابع انسانی، مدیریت سیستم‌ها و امنیت فیزیکی.

### ۵-۲-۵- سرویس‌های تیم پشتیبانی حوادث

علاوه بر عملیات پاسخ دهی به حوادث، سرویس‌های دیگری نیز لازم است توسط این تیم ارائه شوند. سرویس‌های ارائه شده توسط این تیم در این بخش تشریح می شود. به عبارت دیگر وظایفی که تیم مذکور در سازمان بر عهده خواهد داشت عنوان می گردد. اهم سرویس‌هایی که توسط این تیم قابل ارائه می‌باشند، عبارتند از:

- سرویس مشاوره ای آسیب پذیری‌ها
- ارزیابی آسیب پذیری‌ها
- تشخیص تهاجم
- آموزش و اطلاع رسانی
- تحقیق و توسعه
- مدیریت وصله‌ها

### ۵-۲-۶- توصیه‌ها

توصیه‌های کلیدی برای پیاده سازی هرچه بهتر ساختار تیم در این بخش عنوان می گردد. نمونه ای از این توصیه‌ها عبارتند از:

۱- در هر شرایطی سعی شود ملزومات رسمی پاسخ گویی حوادث مهیا گردد.

۲- سیاست پاسخ گویی به حوادث تدوین شده و از آن به عنوان پایه ای برای تنظیم روال‌های پاسخ گویی به حوادث استفاده گردد.

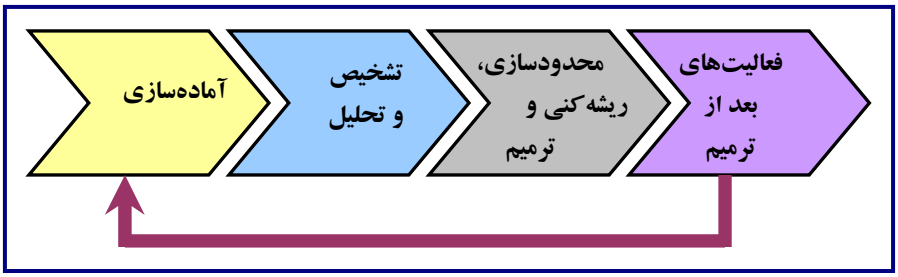
۳- سیاست‌ها و همچنین روال‌هایی راجع به حوادث مربوط به تسهیم اطلاعات، تدوین شده و به اجرا گذارده شود.

۴- از سیستم اطلاع رسانی مناسبی برای اعلام حوادث استفاده شود.

۵- به هنگام انتخاب مدلی مناسب برای تیم پشتیبانی حوادث، از فاکتورهای مناسب استفاده گردد.
۶- از افرادی که از مهارت بالا در تخصص مورد نیاز برخوردارند، استفاده شود.
۷- با سایر واحدهای موجود در سازمان که در فرآیند کنترل حوادث سهیم می باشند، همکاری گردد.
۸- سرویس‌های ارائه شده توسط تیم تعیین و اعلام شود.

## ۵-۳- متدولوژی پشتیبانی حوادث

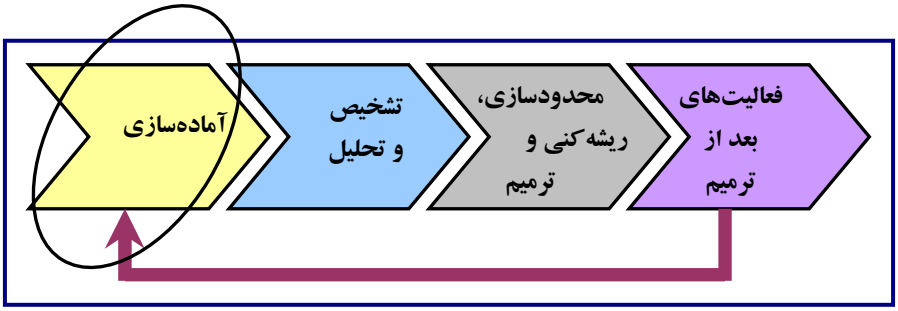
متدولوژی پشتیبانی حوادث مطابق شکل (۵-۱) دارای چندین فاز می باشد. هریک از این فازها در یک چرخه تحت عنوان چرخه حیات پشتیبانی حوادث از جایگاه مشخصی برخوردار می‌باشند. فازهای مختلف چرخه پشتیبانی حوادث، در این قسمت تشریح خواهد شد.




شکل (۵-۱): متدولوژی پشتیبانی حوادث [۱۰]

### ۵-۳-۱- آماده سازی

اولین فاز از متدولوژی پشتیبانی حوادث، مطابق شکل (۵-۲)، مرحله آماده سازی است. این مرحله از جایگاه خاصی در متدولوژی پشتیبانی حوادث برخوردار می‌باشد. زیرا فعالیت‌هایی که در این مرحله انجام می‌گیرد، علاوه بر این‌که زمینه‌ساز ایجاد قابلیت پاسخ‌گویی به حوادث در سازمان است، موجب اعمال کنترل‌های امنیتی بر روی سیستم‌ها و رعایت اصول امنیتی در سازمان نیز می‌باشد. در نتیجه، اقدامات این مرحله، جنبه پیش‌گیری از وقوع حوادث بعدی را نیز دارد. لذا نقش این مرحله، در متدولوژی پشتیبانی حوادث، بسیار حساس می‌باشد.




شکل (۵-۲): متدولوژی پشتیبانی حوادث – فاز آماده‌سازی [۱۰]

در این بخش از طرح، لازم است موارد ذیل مطرح شوند:

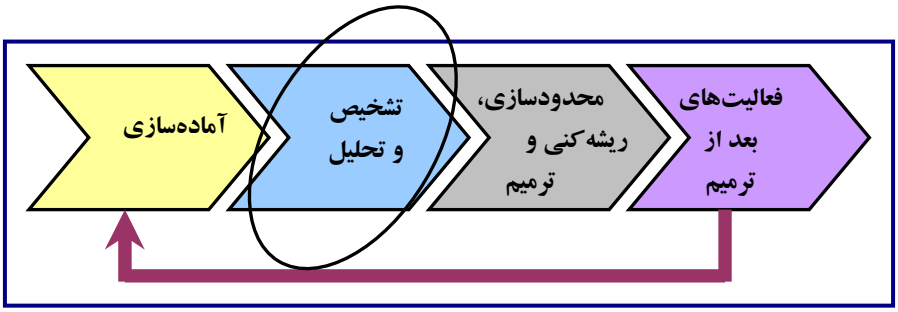
- **آماده‌سازی امکانات تیم در جهت پاسخ‌گویی به حوادث** – این امکانات شامل سیستم‌های ارتباطی، سیستم‌های ذخیره سازی امن، نرم افزار و سخت افزار تحلیل حوادث، ابزارهای کاهش حوادث، منابع تحلیل حوادث اعم از مستندات، لیست پورت‌های مورد استفاده و سایر موارد می باشد. در این بخش، لازم است امکانات و اقدامات موردنیاز جهت آماده‌سازی تیم پاسخ‌گویی به حوادث، تشریح شوند.

- **طراحی و پیاده سازی اقدامات تأمینی در جهت جلوگیری از حوادث-** چنانچه اقدامات امنیتی ناکافی باشد امکان وقوع حوادث زیادی وجود خواهد داشت که با پیاده سازی اقدامات امنیتی در حد معقول، می توان جلوی بسیاری از این حوادث را گرفت. تعدادی از اقدامات امنیتی لازم برای سازمان عبارتند از: مدیریت وصله‌ها، امنیت میزبان‌ها، امنیت اطلاعات، امنیت شبکه، ممانعت از سرایت کدهای مخرب، اطلاع رسانی امنیتی و آموزش. در این بخش، لازم است امکانات و اقدامات پیش‌گیرانه موردنیاز، تشریح شوند.

### ۵-۳-۲- تشخیص و تحلیل حوادث

تشخیص و تحلیل، مطابق شکل (۵-۳)، دومین فاز از متدولوژی پشتیبانی حوادث محسوب می‌گردد. این بخش شامل قسمت‌های زیر است:

- **دسته بندی حوادث ممکن** – حوادث به طرق مختلفی امکان وقوع دارند بنابراین امکان پیاده سازی روال‌های جامعی با ساختار دقیق و مرحله به مرحله در جهت کنترل هر حادثه ای وجود ندارد. لذا بهترین کاری که یک تیم می تواند در این مورد انجام دهد، کسب آمادگی لازم برای مواجهه با هرگونه حملات شناخته شده و رایج می باشد. دسته‌ای از حوادث ممکن عبارتند از حوادث ناشی از حملات ممانعت از سرویس، کدهای مخرب، دسترسی غیرمجاز و استفاده نامناسب از منابع شبکه. در این بخش، لازم است با توجه به مشخصات سازمان، ساختار و ویژگی‌های شبکه، مشخصات سرمایه‌های شبکه، کاربران و سایر پارامترهای موثر در وقوع حادثه، انواع حوادثی که احتمال وقوع آن‌ها در شبکه سازمان وجود دارد، شناسایی و دسته‌بندی شوند.




شکل (۵-۳): متدولوژی پشتیبانی حوادث – فاز تشخیص و تحلیل [۱۰]

- **تدوین روال‌هایی برای قطعی‌سازی وقوع حوادث** – در بسیاری از سازمان‌ها، حساس‌ترین قسمت فرآیند پشتیبانی حوادث، تشخیص و تحلیل حوادث ممکن می باشد. تعیین اینکه حادثه ای اتفاق افتاده است یا خیر و در صورت مثبت بودن جواب، تعیین وسعت، شدت و میزان خرابی ناشی از آن. در این بخش، باید روال‌های لازم جهت تشخیص قطعیت هر حادثه و تعیین وسعت، شدت و میزان خرابی ناشی از آن حادثه ارائه شوند.

- **تعیین ابزار[های] تشخیص حوادث** – تشخیص حوادث با استفاده از ابزارهای مختلف، شگردهای گوناگون و روش‌های مختلف امکان پذیر است. در این میان، ابزارهای خودکار قادرند بر اساس الگوهای تعریف شده برای آن‌ها، حوادث رایج را تشخیص دهند. اما می توان با استفاده از شگردهای مختلفی اعم از تحلیل رویدادنامه‌ها و وضعیت موجود، حوادثی را تشخیص داد. بعضی از ابزارهای رایج در این زمینه عبارتند از: سیستم‌های تشخیص تهاجم مبتنی بر میزبان و شبکه، نرم افزار ضدویروس، نرم افزارهای تست تمامیت فایل و پوشه و دست آخر، نرم‌افزارهای نظارت شبکه. در این بخش، لازم است کلیه ابزارهای نرم‌افزاری و سخت‌افزاری موردنیاز جهت تشخیص حوادثی که احتمال وقوع آن‌ها در شبکه وجود دارد، ارائه گردند.

- **تحلیل حوادث و روش‌های آن** – در این بخش، انواع روش‌های رایج برای تحلیل حوادث عنوان می شود و از بین آن‌ها روش‌های مناسب انتخاب، بررسی و برای سازمان سفارشی می شوند. برخی از این روش‌ها عبارتند از:
  - تدوین شناسنامه سیستم‌ها و شبکه‌های موجود در سازمان و استفاده از آن‌ها در مواقع لزوم
  - آشنایی با رفتار نرمال سیستم‌ها، شبکه‌ها و نرم‌افزارها
  - استفاده از سیستم رویدادنگاری متمرکز و تحلیل آن و همچنین سیاست نگهداری رویدادنامه‌ها
  - سعی در انتساب ارتباط مابین وقایع
  - یکسان سازی زمان دربین تمامی میزبان‌ها
  - ایجاد، حفظ و استفاده از یک پایگاه داده مبتنی بر دانش
  - استفاده از موتورهای جستجوگر برای تحقیق

- **گزارش‌دهی حوادث** – به محض این‌که تیم پشتیبانی حوادث به وقوع حادثه ای مظنون می شوند، ضرورت دارد تمامی اطلاعات مربوط به حادثه، ثبت گردد. روش‌های مناسب برای تحقق این امر عبارتند از: استفاده از کتابچه رویداد که روشی کارا و در عین حال ساده برای این امر می باشد، استفاده از ابزارهای PDA، کامپیوترهای همراه، ابزارهای ضبط صدا و تصویر. همچنین لازم است در این بخش از طرح، فرم‌های لازم برای ثبت حوادث، متناسب با مشخصات سازمان، طراحی و ارائه گردند.

- **اولویت‌دهی به حوادث** – اولویت‌دهی به حوادث، حساس‌ترین مقطع تصمیم گیری در فرآیند پشتیبانی حوادث می باشد. پاسخ‌گویی به حوادث نباید بصورت منظم و تنها بر اساس ترتیب تشخیص و اعلام حوادث صورت

پذیرد، بلکه با توجه به ارزش سرمایه‌ها باید در رسیدگی بـه حـوادث تقـدم و تأخر را به خوبی رعایت کرد. دو فاکتور موثر در فرآیند تصمیم‌گیـری بـرای رسیدگی به حوادث، عبارتند از:

- میزان اهمیت سرمایه حادثه دیده
- اثرات تکنیکی حال حاضر و بعدی حوادث

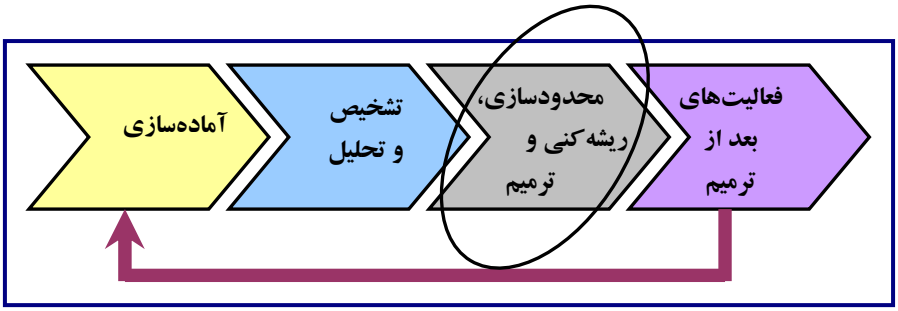
- **هشدار حوادث** – به هنگام وقوع یک حادثـه در سـازمان، تمـامی پرسـنل آن سازمان به نوعی در وقـوع، تشـخیص و کنتـرل آن سـهیم مـی باشـند و لـذا ضرورت دارد این پرسنل نقش خود را به خوبی در کنترل حوادث ایفا نمایند. پرسنل می توانند از طریق اعلام حادثه و خسارات ناشی از آن، موجب کنترل به‌موقع حادثه و مانع از گسترش دامنه و خسارات حادثه شوند. در این بخش از طرح، باید امکانات موردنیاز جهت ایفـای نقـش پرسـنل، از قبیـل فـرم‌هـای اعلام حادثه، امکانات تلفنی و سایر تجهیـزات و امکانـات اعـلام حادثـه ارائـه شده و همچنین اقدامات موردنیاز جهت افزایش میـزان مشـارکت پرسـنل، از قبیل موارد آگاهی‌رسانی موردنیاز برای این امر، پیش‌بینی و ارائه گردد.

### ۵-۳-۳- محدودسازی، ترمیم و ریشه کنی

مطـابق بـا **Error! Reference source not found.** (۵-۴)، ایـن مرحلـه سومین گام از متدولوژی پشتیبانی حوادث می باشد. این بخش شامل قسمت‌هـای زیر است:

- **انتخاب راهبرد/راهبردها برای محدودسـازی** – بعـد از فرآینـد تشـخیص و تحلیل حوادث، ضرورت دارد در جهت جلوگیری از گسترش حادثـه و تبعـات آن، محدودسازی صورت پذیرد. قسمت اصلی فرآیند محدود سازی، تصـمیم گیری مـی باشـد. تصـمیم گیـری مـی توانـد در خصـوص مـواردی از قبیـل:

خاموش کردن سیستم، جدانمودن سیستم از کابل‌های شبکه یا مودم و غیرفعال سازی ویژگی‌های خاص نرم افزاری باشد. این گونه تصمیم گیری‌ها در صورتی که راهبردها و روال‌هایی برای آن اتخاذ شده باشد، آسان تر بوده و از ریسک کمتری نیز برخوردار خواهد بود. در این بخش از طرح، لازم است راهبردهای سازمان در خصوص محدودسازی حوادث، تعیین و تشریح گردند.




شکل (۵-۴): متدولوژی پشتیبانی حوادث – فاز محدود سازی، ترمیم و ریشه‌کنی [۱۰]

- **جمع آوری اسناد و مدارک** – جمع آوری اسناد و مدارک، علاوه بر تسریع در رفع حادثه، در جهت پی‌گیری مراحل قانونی نیز نقش موثری دارد. در این بخش از طرح، لازم است ضمن تاکید بر جمع‌آوری اسناد و مدارک، امکانات موردنیاز برای این امر نیز ارائه گردند.

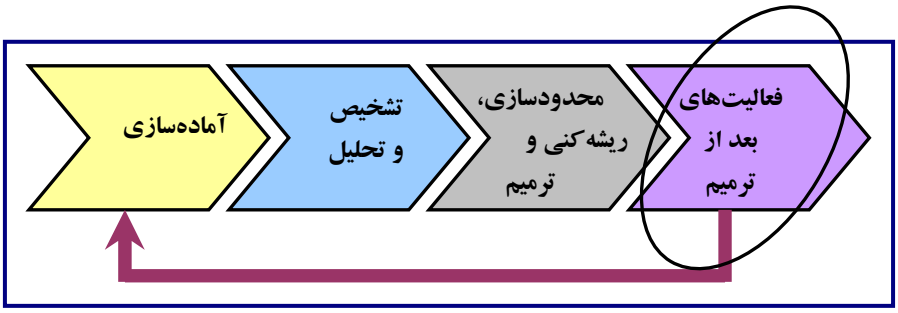
- **معرفی مهاجم/مهاجمان** – در خلال فرایند پشتیبانی حوادث، مدیریت ارشد تیم و به دنبال آن سازمان اقدام به معرفی مهاجم/مهاجمان به مراجع ذی صلاح می نمایند اما در این بین اعضای تیم همچنان به فعالیت خود در فرآیند محدود سازی، ترمیم و ریشه کنی ادامه می دهند. مهمترین آیتم‌ها در معرفی مهاجم/مهاجمان عبارتند از: آدرس IP سیستم مهاجم/مهاجمان، پویش سیستم مهاجم/مهاجمان، تحقیقات بر روی سیستم مهاجم/مهاجمان با

استفاده از موتورهای جستجوگر. در این بخش از طرح، لازم است اقدامات موردنیاز جهت شناسایی و معرفی مهاجم/مهاجمان تشریح و امکانات موردنیاز برای این منظور، ارائه گردند.

- **ترمیم و ریشه کنی** – بعد از محدودسازی حادثه، ضرورت دارد تمامی تبعات حادثه از قبیل: کدهای مخرب، مجوزهای دسترسی غیرمجاز و همچنین حساب‌های غیرمجاز و غیره ریشه کن شوند. اما در مورد بعضی از حوادث، این مرحله به ریشه کنی ختم نمی شود و ضرورت دارد خرابی‌های ناشی از حادثه، ترمیم شوند تا سیستم به وضعیت عادی خود برگردد. در این بخش از طرح، لازم است اقدامات موردنیاز به منظور ریشه‌کنی حوادث و ترمیم خرابی‌ها تشریح و امکانات موردنیاز برای این منظور ارائه گردند.

### ۵-۳-۴ فعالیت‌های بعد از ترمیم حوادث

بعد از اتمام فاز محدودسازی، ترمیم و ریشه کنی، سه فاز اولیه متدولوژی پشتیبانی حوادث انجام پذیرفته و نوبت به انجام آخرین فاز، یعنی فعالیت‌های بعد از ترمیم حوادث می رسد. این قسمت یکی از مهمترین قسمت‌های متدولوژی پشتیبانی حوادث می باشد که متأسفانه در اغلب موارد از قلم می‌افتد. این بخش شامل قسمت‌های زیر می باشد:




شکل (۵-۵): متدولوژی پشتیبانی حوادث – فاز فعالیت‌های بعد از حوادث [۱۰]

- **بررسی و تدوین تجارب اندوخته شده** - هر تیم پشتیبانی حوادث باید در این مرحله، اقدام به یادگیری و افزایش دانش و تجربه خود نماید. با بازتاب تهدیدات جدید و همچنین فن آوری‌های جدید در این عرصه می توان قابلیت‌ها و مهارت تیم را افزایش داد. در این بخش از طرح، ضمن تشریح تجربیاتی که می‌توان اندوخت، باید امکانات موردنیاز برای ثبت تجربیات نیز ارائه گردند.

- **استفاده از اطلاعات جمع آوری شده و تحلیل آنها** – با استفاده از اطلاعات جمع‌آوری شده و تحلیل آماری آن‌ها می توان به نتایج قابل توجهی در مورد حوادث رسید که بررسی آن‌ها در فرایند مدیریت امنیت می تواند بسیار مفید باشد. برخی از پارامترهای مناسب برای تحلیل آماری عبارتند از تعداد حوادث کنترل شده و مدت زمان پاسخ گویی به هر یک از حوادث.از سوی دیگر، این پارامترها نمایانگر کارآیی تیم پشتیبانی حوادث سازمان نیز می‌باشند. در این بخش از طرح، ضمن تشریح اقدامات موردنیاز در این خصوص، باید امکانات لازم جهت ثبت اطلاعات و ارائه گزارش‌های مدیریتی نیز ارائه شوند.

- **بایگانی اطلاعات** – هر سازمان باید سیاستی برای بایگانی اطلاعات تیم پشتیبانی حوادث داشته باشد. از مهمترین موضوعات این سیاست، مدت زمان نگهداری اطلاعات می باشد. در این بخش از طرح، ضمن تشریح سیاست‌های سازمان در خصوص بایگانی اطلاعات حوادث، باید امکانات لازم جهت ایجاد سیستم بایگانی نیز پیش‌بینی شود.

### ۵-۳-۵- تدوین چک لیست پشتیبانی حوادث

در زمان وقوع حادثه، تصمیم‌گیری در خصوص اقداماتی که باید انجام گیرند بسیار مشکل است، لذا چک‌لیست[هایی] برای انجام هر یک از مراحل پشتیبانی حوادث، تدوین و در اختیار تیم ÷شتیبانی حوادث قرار می‌گیرد. این چک‌لیست[ها] معمولا در دو سطح کلی و جزئی تدوین و در طرح پشتیبانی حوادث ارائه می‌شوند. چک‌لیست اولیه، شامل اقدامات موردنیاز و چک‌لیست‌های سطح دوم، شامل جزئیات فنی اقدامات موردنیاز می‌باشند. در این بخش از طرح، ضمن ارائه کلیه چک‌لیست‌های موردنیاز، موارد کاربرد و نحوه به‌کارگیری هر یک از آن‌ها نیز تشریح می‌شوند.

### ۵-۳-۶- توصیه‌ها

در این بخش، توصیه‌های کلیدی برای عملیات پشتیبانی حوادث ذکر می گردد. تعدادی از این توصیه‌ها عبارتند از:

- در طی عملیات پشتیبانی حوادث از ابزارها و منابع مناسب موجود، حداکثر بهره‌برداری ممکن انجام گیرد.
- با اعمال امنیت برروی سیستم‌ها، شبکه‌ها و نرم افزارهای کاربردی تا حد امکان از بروز حوادث پیش‌گیری شود.
- برای سیستم‌ها، شبکه‌ها و نرم‌افزارهای سازمان، شناسنامه تدوین گردد.

## ۵-۴- الگوی پشتیبانی حوادث

در این بخش با استفاده از متدولوژی پشتیبانی حوادث، الگوهای مناسب پشتیبانی حوادث برای هریک از حوادث دسته‌بندی شده در بخش ۵-۲-۱

(دسته‌بندی حوادث) عنوان می گردد. روند تدوین این بخش به این شکل است که ابتدا توضیحی از حادثه مربوطه به همراه مثال‌هایی از آن عنوان شده و سپس کلیه موارد مطرح شده در بخش ۵-۳ (متدولوژی پشتیبانی حوادث)، برای آن دسته از حوادث، ارائه می شود و در انتها نیز چک لیستی برای مقابله با آن دسته از حوادث در سطح سازمان ارائه می گردد. به عبارت دیگر، اگر در بخش ۵-۲-۱ (دسته‌بندی حوادث) طرح پشتیبانی حوادث سازمان، حوادث ممکن در ۴ دسته قرار گیرند، لازم است این طرح، بخش ۵-۳ (متدولوژی پشتیبانی حوادث) را ۴ بار تکرار و هر بار، برای یک دسته از حوادث، تنظیم نماید.

# ۶

# چارچوب پیشنهادی برای برنامه آگاهی‌رسانی، تربیت نیروی انسانی و آموزش امنیت شبکه

### ۶-۱- مقدمه

یکی از عواملی که هم در ایجاد امنیت شبکه و هم در تداوم آن، نقش موثری ایفا می‌کند، آگاهی پرسنل سازمان از حقوق، وظایف، مسئولیت‌ها و پاسخ‌گویی خود در برنامه امنیت شبکه سازمان می‌باشد. بخش قابل توجهی از سیاست‌های امنیتی شبکه سازمان، اختصاص به تبیین نقش پرسنل در تامین امنیت شبکه دارد، همچنین در طرح‌های امنیت شبکه سازمان، لازم است فرم‌ها و روال‌های اجرایی موردنیاز برای اجرای آن طرح‌ها، پیش‌بینی شود. از سوی دیگر، لازم است تیم امنیت شبکه سازمان با برخورداری از دانش امنیت شبکه، توانایی لازم جهت دفاع از شبکه سازمان و تامین اهداف امنیتی پیش‌بینی شده را داشته باشد. برنامه آگاهی‌رسانی، تربیت نیروی انسانی و آموزش امنیت شبکه، در این راستا و با ساختاری که در این فصل ارائه شده است، تدوین می‌شود. مطالب این فصل، برگرفته از مرجع [۱۱] می‌باشد.

#### ۶-۱-۱- اهداف

در این بخش، هدف از ارائه این برنامه و ابعاد عملی و اجرایی این برنامه عنوان می‌گردد. بالطبع هدف از ارائه چنین برنامه‌ای، بسترسازی و ارائه اطلاعات به

سطوح مختلف پرسنل سازمان، در راستای تامین تداوم امنیت شبکه سازمان می‌باشد. به دنبال چنین هدفی، در این برنامه لازم است موضوعاتی از قبیل موارد زیر، مطرح شوند:

- انتخاب موضوعات آگاهی‌رسانی امنیتی، تربیت نیروی انسانی و آموزش
- انتخاب مراجع مربوطه و سرفصل‌ها
- پیاده‌سازی ارکان آگاهی‌رسانی امنیتی، تربیت نیروی انسانی و آموزش
- ارزیابی میزان کارایی برنامه‌ها
- به روزرسانی و بهبود برنامه‌ها

### ۶-۱-۲- مخاطبین

در این بخش، لیست تمامی مخاطبین برنامه آگاهی‌رسانی، آموزش و تربیت نیروی انسانی در زمینه امنیت، به همراه موارد پیش‌بینی شده در برنامه برای هر یک از مخاطبین، ارائه می‌گردد. به عنوان مثال، می‌توان در این بخش از برنامه، لیست زیر را به همراه دوره‌هائی که افراد باید شرکت نمایند، ارائه داد:

- **سازمان/سازمان‌های مطبوع** –بخش‌هائی از سازمان که طراحی، توسعه و اجرای برنامه آگاهی‌رسانی، تربیت نیروی انسانی و آموزش امنیت در آنها مورد نظر می‌باشد
- **حمایت کنندگان برنامه**
  - **مدیر سازمان** – تائید و حمایت اجرای برنامه
- **طراح، مجری و ناظر اجرای برنامه**
  - **مدیر فن‌آوری اطلاعات (CIO )** – مدیریت و نظارت بر تدوین و اجرای برنامه
  - **مدیر امنیت اطلاعات** – طراح و مسئول اجرای برنامه آگاهی‌رسانی، تربیت نیروی انسانی و آموزش امنیت

- **فن‌آموزان**
  - **پرسنل تیم پشتیبانی امنیت شبکه** – شرکت در دوره‌های آموزشی تخصصی امنیت شبکه و دوره‌های تربیت نیروی انسانی سیستم امنیتی شبکه سازمان
  - **مسؤولین سیستم‌ها و نرم‌افزارها** – شرکت در برنامه‌های آگاهی‌رسانی امنیتی و تربیت نیروی انسانی امنیت شبکه، مطابق با نوع تخصص و حوزه کاری آن‌ها
  - **عموم پرسنل سازمان** – شرکت در برنامه‌های آگاهی‌رسانی امنیتی

**۶-۱-۳- ابعاد**

در این بخش، ابعاد مختلف برنامه آگاهی‌رسانی امنیتی، آموزش و تربیت نیروی انسانی در راستای تامین اهداف امنیت شبکه سازمان و بر اساس سیاست‌های امنیتی ارائه شده، تبیین می‌شود. این ابعاد شامل: طراحی، توسعه، پیاده‌سازی و پشتیبانی آگاهی‌رسانی امنیتی، آموزش و تربیت نیروی انسانی در سازمان می‌باشد.

**۶-۱-۴- سیاست**

سیاست‌های امنیتی سازمان در خصوص آگاهی‌رسانی امنیتی، آموزش و تربیت نیروی انسانی در زمینه امنیت شبکه، در این بخش عنوان می‌شود. این سیاست‌ها، خط‌مشی سازمان را در قبال آگاهی‌رسانی امنیتی، آموزش و تربیت نیروی انسانی بیان می‌کنند.

### ۶-۱-۵- وظایف و مسؤولیت‌ها

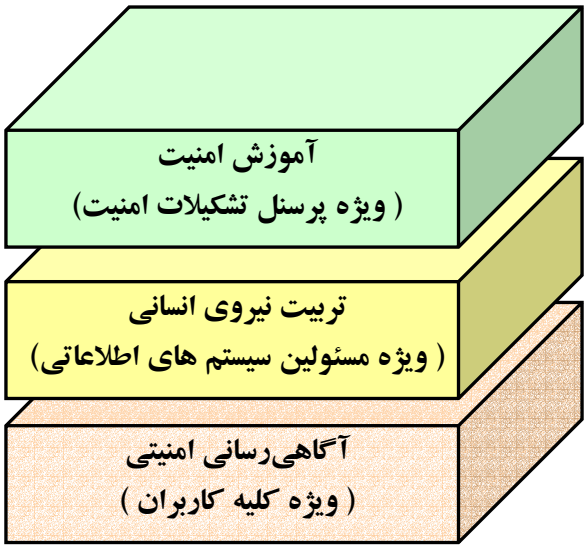
تعیین وظایف و مسؤولیت‌ها در قبال مقوله آگاهی‌رسانی امنیتی، آموزش و تربیت نیروی انسانی از اهمیت ویژه‌ای برخوردار است. لذا ضرورت دارد به منظور تضمین تاثیر هر چه بیشتر اجرای برنامه آگاهی‌رسانی امنیتی، آموزش و تربیت نیروی انسانی در زمینه امنیت، وظایف و مسؤولیت‌های مربوط به کلیه مخاطبین برنامه، صریحا تعیین و اعلام گردد. مخاطبین آگاهی‌رسانی امنیتی، آموزش و تربیت نیروی انسانی شامل موارد زیر می‌باشند:

- رئیس سازمان
- مدیر فن‌آوری اطلاعات سازمان
- مدیر امنیت شبکه سازمان
- مسؤولین سیستم‌ها و نرم‌افزارهای IT
- پرسنل سازمان ( بویژه کاربران شبکه سازمان )

## ۶-۲- آگاهی‌رسانی امنیتی، تربیت نیروی انسانی و آموزش امنیت

هریک از مقولات آگاهی‌رسانی امنیتی، تربیت نیروی انسانی و آموزش امنیت، مفهوم و جایگاه خاص خود را در فرآیند ایجاد و تامین استمرار ثبات امنیت شبکه سازمان ایفا می‌نماید. مطابق شکل(۶-۱) هریک از این محورها در یکی از سطوح یادگیری امنیت شبکه قرار دارند.

در این بخش، لازم است سطوح مختلف یادگیری، شامل آگاهی‌رسانی امنیتی، تربیت نیروی انسانی و آموزش امنیت، عنوان و مفاهیم و کاربردهای هریک در سازمان بررسی شوند و در انتها، این سطوح از لحاظ ویژگی‌های مختلف با هم مقایسه شوند.




شکل(۶-۱) : سطوح یادگیری امنیت شبکه [۱۱]

### ۶-۲-۱- آگاهی‌رسانی امنیتی

آگاهی‌رسانی امنیتی، مختص تمامی پرسنل سازمان می‌باشد. هدف آگاهی‌رسانی امنیتی، به‌صورت ساده، جلب توجه مخاطبین به اهمیت مقوله امنیت در سطح سازمان و ایجاد هوشیاری امنیتی بیشتر در بین مخاطبین می‌باشد، به‌طوری‌که پرسنل به سادگی از کنار مسائل به ظاهر جزئی نگذرند و به موقع نگرانی‌های امنیتی را تشخیص داده و عملکرد مناسبی در سطح وظایف و اختیارات خود انجام دهند. ابزارهای مناسب برای این امر عبارتند از: پوستر، بروشور، بولتن، روزنامه، مجله، رسانه‌ی صوتی و تصویری و غیره.

در این بخش، لازم است ضمن تبیین ضرورتها و اهداف آگاهی‌رسانی امنیتی، روش‌های اجرائی مناسب برای این منظور نیز انتخاب و اعلام گردد.

### ۶-۲-۲- تربیت نیروی انسانی

مقوله تربیت نیروی انسانی، مختص پرسنلی است که با سیستم‌های IT در سازمان ارتباط داشته و همچنین عهده‌دار وظایف و مسؤولیت‌هایی در این سطح می‌باشند. هدف تربیت نیروی انسانی، تلاش در جهت کسب مهارت و شایستگی برای راهبری هرچه بهتر سیتسم‌های IT می‌باشد. فرآیند تربیت نیروی انسانی در سه سطح: مقدماتی، متوسطه و پیشرفته صورت می‌پذیرد. لذا در این بخش، لازم است ضمن تبیین ضرورتها و اهداف تربیت نیروی انسانی در زمینه امنیت، سطوح مختلف تربیت نیروی انسانی و روش‌های اجرائی مناسب برای این منظور، انتخاب و اعلام گردد.

### ۶-۲-۳- آموزش امنیت

آموزش متخصص در زمینه امنیت شبکه، مختص متخصصین امنیت شبکه سازمان می‌باشد. هدف از آموزش، کسب دانش و تجربه در امر طراحی، پیاده‌سازی و پشتیبانی سیستم‌های امنیت شبکه می‌باشد. فرایند آموزش در سه سطح: مقدماتی، متوسطه و پیشرفته صورت می‌پذیرد. لذا در این بخش، لازم است ضمن تبیین ضرورتها و اهداف آموزش متخصصین امنیت شبکه سازمان، سطوح مختلف آموزش و روش‌های اجرائی مناسب برای این منظور، انتخاب و اعلام گردد.

### ۶-۲-۴- مقایسه

در این بخش مطابق با چارچوب ارائه شده در جدول (۶-۱)، مقایسه‌ای بین سطوح مختلف یادگیری فراهم می‌شود. هرچند تمایز قائل شدن بین این سطوح آن‌چنان سهل و آسان نمی‌باشد اما اجرای هرچه بهتر برنامه آگاهی‌رسانی، تربیت

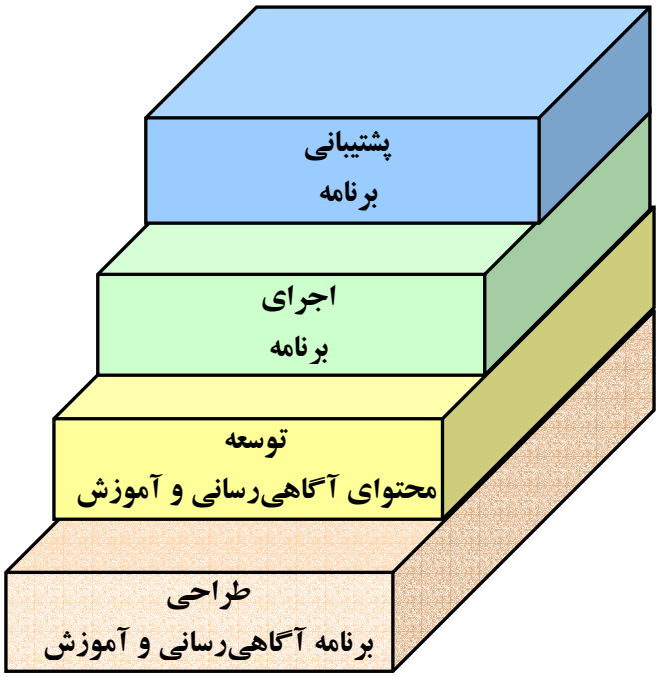
نیروی انسانی و آموزش، نیاز به ارائه دسته‌بندی دقیق و به‌دنبال آن کسب فهم بهتر در این زمینه داشته و لذا ضرورت دارد این امر به‌خوبی تبیین گردد.

| دوره<br>ویژگی‌ها | آگاهی‌رسانی | تربیت | آموزش |
|---|---|---|---|
| مشخصه | "What" | "How" | "Why" |
| سطح | اطلاعات | دانش | بینش |
| موضوعات یادگیری | شناخت و نگهداری | مهارت | فهم |
| نمونه‌هایی از روش‌های یادگیری | رسانه<br>ویدیو<br>روزنامه<br>پوستر | آموزش کاربردی<br>سخنرانی<br>مطالعه نمونه<br>تمرین دستی | آموزش تئوری<br>سمینار و بحث<br>خواندن و مطالعه<br>تحقیق |
| مقیاس سنجش | درست / غلط<br>چند جوابی<br>( سنجش دانش) | حل مسئله<br>شناسایی و تحلیل<br>( بکاربردن دانش) | مقاله<br><br>(تفسیر دانش) |
| مدت دوره | کوتاه مدت | میان مدت | بلند مدت |

جدول (۱): چارچوب مقایسه بین سطوح مختلف یادگیری [۱۱]

## ۶-۳- متدولوژی آگاهی‌رسانی، تربیت نیروی انسانی و آموزش امنیت

متدولوژی آگاهی‌رسانی امنیتی، تربیت نیروی انسانی و آموزش، مطابق با شکل (۶-۲) دارای چهار فاز می‌باشد. هریک از این فازها در چرخه‌ای تحت عنوان چرخه حیات یادگیری در سازمان اعمال می‌شوند. در این بخش لازم است جزئیات هریک از فازهای این چرخه، ارائه شوند.




شکل (۶-۲): متدولوژی آگاهی‌رسانی امنیتی، تربیت نیروی انسانی و آموزش [۱۱]

### ۶-۳-۱- طراحی

در مرحله طراحی برنامه آگاهی‌رسانی امنیتی، تربیت نیروی انسانی و آموزش، نیازهای پرسنل سازمان در هر یک از این زمینه‌ها مشخص می‌گردد چراکه ضرورت دارد سیستم یادگیری، مطابق با نیازهای سازمان و پرسنل آن باشد.

این بخش شامل قسمت‌های زیر می باشد:

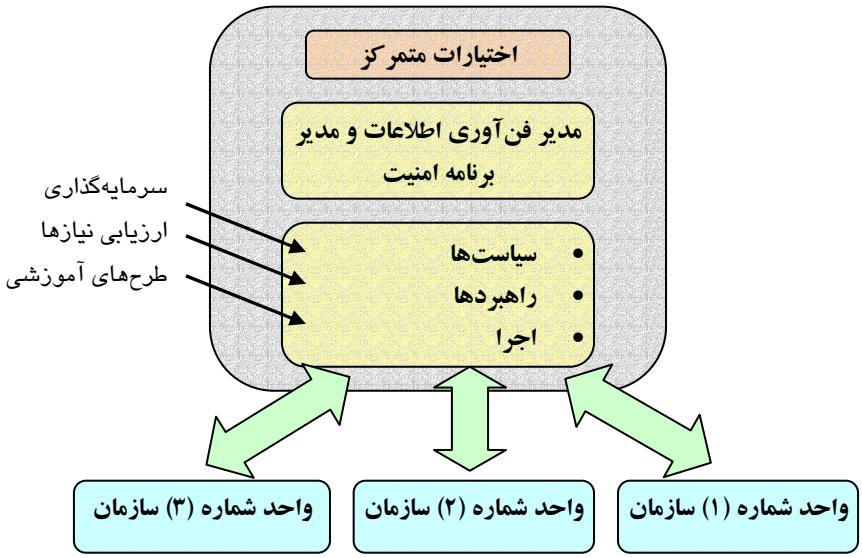
۱. **ارائه ساختار برای برنامه آگاهی‌رسانی امنیتی، تربیت نیروی انسانی و آموزش** – برای شکل دهی به برنامه آگاهی‌رسانی، آموزش و تربیت نیروی انسانی سازمان، سه مدل به شرح زیر، وجود دارد:

- مدل ۱: سیاست‌گذاری، راهبرددهی و پیاده‌سازی به‌صورت متمرکز، مطابق شکل ((۶-۳)
- مدل ۲: سیاست‌گذاری و راهبرددهی به‌صورت متمرکز و پیاده‌سازی به‌صورت توزیع‌شده، مطابق شکل (۶-۴)
- مدل ۳: سیاست‌گذاری به‌صورت متمرکز و راهبرددهی و پیاده‌سازی به‌صورت توزیع‌شده، مطابق شکل (۶-۵)

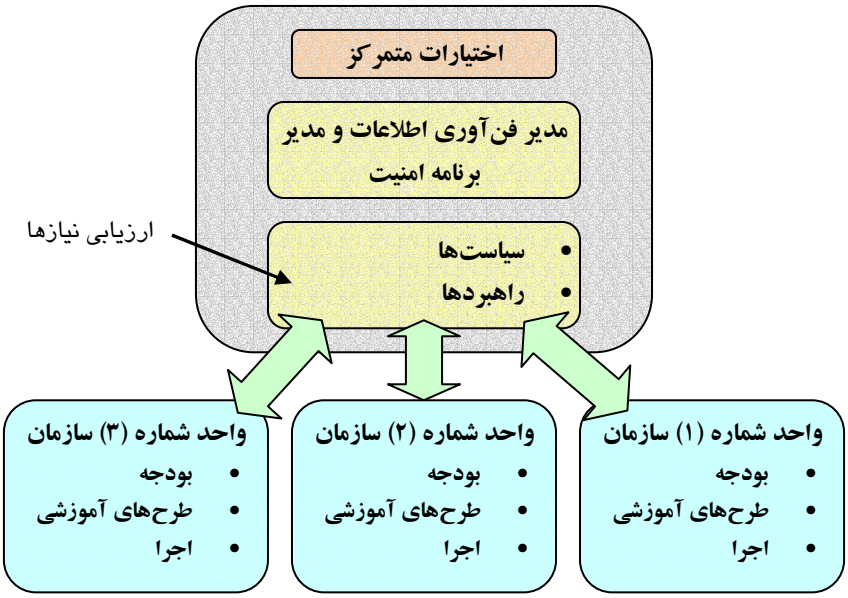
در این بخش از برنامه، لازم است ضمن معرفی مدلهای موجود، مدل مناسب جهت استفاده در سازمان، انتخاب گردد. انتخاب هریک از این سه مدل برای سازمان، وابسته به پارامترهای زیر می‌باشد:

- وسعت و پراکندگی جغرافیایی سازمان
- ماموریت‌ها و مسؤولیت‌های سازمان
- میزان اختصاص بودجه و قدرت اجرایی سازمان

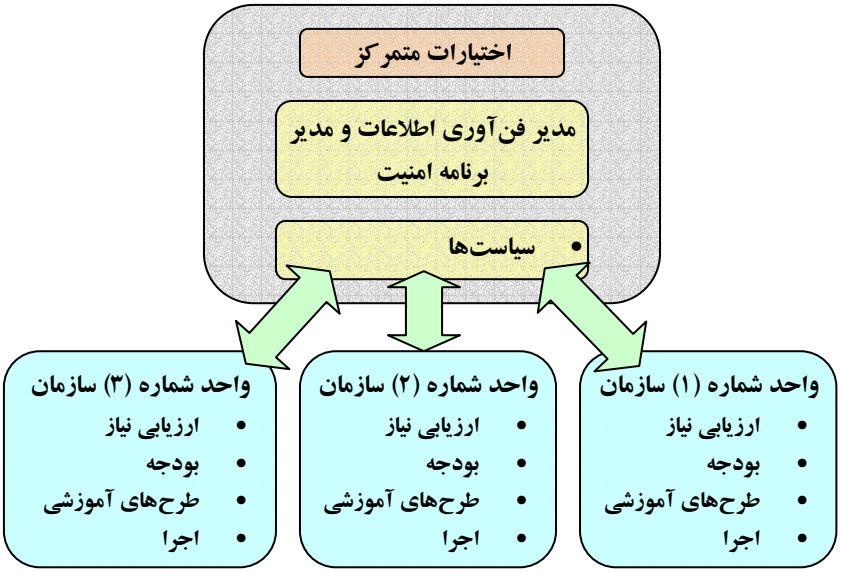
در هریک از این سه مدل، کمیته راهبری امنیت شبکه سازمان که ساختار و اعضاء آن در فصل دوم معرفی شدند، اقدام به سیاست‌گذاری، راهبرددهی و نظارت بر پیاده‌سازی می‌نمایند. همچنین مدیریت اجرایی سازمان به عنوان تصمیم‌گیرنده اصلی سازمان و مدیر فن‌آوری اطلاعات و مدیر امنیت شبکه سازمان به عنوان مجری طرح، ایفای نقش می‌کنند.




شکل (۶-۳): مدل اول – مدیریت برنامه به‌صورت متمرکز [۱۱]

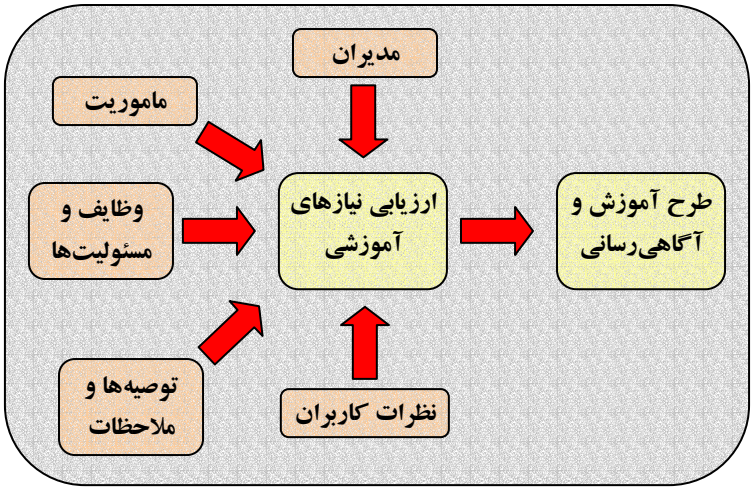



شکل (۶-۴): مدل دوم – مدیریت برنامه به‌صورت نیمه‌متمرکز [۱۱]




شکل (۶-۵): مدل سوم – مدیریت برنامه به‌صورت تمام توزیع‌شده [۱۱]

۲. **برآورد نیاز** – برآورد نیازها، فرآیندی است که توسط آن نیازهای مرتبط با آگاهی‌رسانی امنیتی، آموزش و تربیت نیروی انسانی تعیین می‌شود. نتایج حاصل از برآورد نیازها می‌تواند در جهت متقاعد کردن مدیریت برای صرف هزینه و سایر منابع، مؤثر واقع گردد. عواملی که در برآورد نیازها می‌توانند مؤثر واقع شوند مطابق با شکل (۶-۶) عبارتنداز: رهنمودهای مدیریتی، مأموریت تحقیقی، تعیین وظایف و مسؤولیت‌ها، توصیه‌ها، مشاهدات عینی و بازخوردهای کاربران.




شکل (۶-۶): عوامل مؤثر در برآورد نیازهای آگاهی‌رسانی، آموزش و تربیت نیروی انسانی [۱۱]

۳. **توسعه راهبردها و برنامه** – پس از تأیید مدیریت ارشد سازمان مبنی‌بر ضرورت اجرای برنامه آگاهی‌رسانی امنیتی، آموزش و تربیت نیروی انسانی، راهبردهایی به‌منظور توسعه، پیاده‌سازی و پشتیبانی برنامه‌های آگاهی‌رسانی امنیتی، آموزش و تربیت نیروی انسانی ارائه می‌گردد. پس از این مرحله، برنامه‌ای به‌منظور تحقق راهبردهای مذکور ارائه می‌شود.

۴. **اولویت‌دهی به نیازها** – پس از نهایی شدن راهبردها و برنامه آگاهی‌رسانی امنیتی، آموزش و تربیت نیروی انسانی، باید زمان‌بندی مشخصی برای فاز پیاده‌سازی برنامه ارائه شود. پارامترهای مهم در تعیین اولویت‌دهی عبارتنداز:

- بهره‌مندی از وسایل و امکانات مورد نیاز

- پروژه‌های درحال انجام
- مخاطرات موجود در سازمان و تأثیر آن‌ها
- مجوزدهی

۵. **تعیین میزان پیچیدگی** – در توسعه برنامه آگاهی‌رسانی امنیتی، آموزش وتربیت نیروی انسانی، باید میزان پیچیدگی هریک از اجزای برنامه مشخص گردد. تعیین میزان پیچیدگی برپایه دو عامل مهم صورت می‌گیرد:
   - موقعیت سازمانی شرکت‌کنندگان در برنامه
   - میزان دانش و مهارت مورد نیاز برای موقعیت مورد نظر

۶. **بودجه مالی مورد نیاز** – پس‌ازاینکه برنامه آگاهی‌رسانی امنیتی، آموزش و تربیت نیروی انسانی مبتنی بر اولویت‌های کاری ارائه شده مورد موافقت واقع شد، میزان بودجه مالی مورد نیاز که در برنامه پیش‌بینی شده نیز باید به اجرای برنامه تخصیص یابد. روش های بیان میزان بودجه مورد نیاز در برنامه عبارتنداز:
   - درصدی از کل بودجه آگاهی‌رسانی، آموزش و تربیت نیروی انسانی سازمان
   - درصدی از کل بودجه فن‌آوری اطلاعات سازمان
   - میزان هزینه به ازای هرنفر با بیان مسؤولیت مربوطه
   - بیان صریح هزینه مورد نیاز

**۶-۳-۲- توسعه**

در مرحله توسعه برنامه آگاهی‌رسانی امنیتی، آموزش و تربیت نیروی انسانی، لازم است موارد مورد نیاز به همراه موضوعات و مراجع مربوطه در مورد هریک

از محورهای سه‌گانه یادگیری شامل آگاهی‌رسانی امنیتی، آموزش و تربیت نیروی انسانی تعیین گردد. این بخش، شامل موضوعات زیر می‌باشد:

۱. موارد، موضوعات و مراجع مربوط به آگاهی‌رسانی امنیتی
۲. موارد، موضوعات و مراجع مربوط به آموزش
۳. موارد، موضوعات و مراجع مربوط به تربیت نیروی انسانی

### ۶-۳-۳- پیاده‌سازی

پیاده‌سازی برنامه آگاهی‌رسانی امنیتی، آموزش و تربیت نیروی انسانی بعداز طی مراحل زیر صورت می‌پذیرد:

- انجام فرایند برآورد نیازها
- توسعه راهبردها
- تدوین برنامه آگاهی‌رسانی امنیتی، آموزش و تربیت نیروی انسانی به‌منظور پیاده‌سازی راهبردها
- توسعه برنامه آگاهی‌رسانی امنیتی، آموزش و تربیت نیروی انسانی

در این بخش از برنامه، لازم است موارد زیر مطرح شوند:

۱. **آگاهی‌رسانی برنامه به قسمت‌های مختلف سازمان** – به منظور کسب موافقت‌های اداری و تهیه امکانات مورد نیاز و همچنین بالابردن ضمانت اجرایی برنامه، ضرورت دارد برنامه مزبور به قسمت‌های تاثیرگذار در برنامه و تاثیر پذیر از برنامه ارائه گردد.

۲. **تعیین روش‌های آگاهی‌رسانی** – روش‌های زیادی برای آگاهی‌رسانی امنیتی وجود دارد. این روش‌ها بسته به نوع و پیچیدگی پیام‌ها متفاوت می‌باشند. دسته‌ای از این روش‌ها عبارتند از: جلسات مبتنی‌بر وب، جلسات

مبتنی بر کامپیوتر، جلسات کنفرانس ویدیویی، بولتن‌های خبری و غیره. در این بخش از برنامه، لازم است روش[های] مناسب، انتخاب و اعلام شوند.

۳. **تعیین روش‌های تربیت نیروی انسانی** – در فرایند تربیت نیروی انسانی در جهت حصول کارایی بالا، ضرورت دارد از تجهیزات مناسبی استفاده گردد. بعضی از ویژگی‌های این تجهیزات عبارتند از: سهولت استفاده، مقیاس‌پذیری، قابلیت پشتیبانی. همچنین بعضی از روش‌های رایج برای تربیت نیروی انسانی عبارتند از: آموزش تصویری تعاملی، آموزش مبتنی‌بر وب و آموزش مبتنی‌بر کامپیوتر. در این بخش از برنامه، لازم است روش[های] مناسب، انتخاب و اعلام شوند.

۴. **تعیین روش‌های آموزش** – این مقوله بسیار تخصصی بوده و ضرورت دارد از حداکثر امکانات در این امر بهره گرفته شود. بهترین روش موجود برای این امر، اعزام نیروهای مورد نظر به دانشگاه‌ها، آموزشگاه‌ها و سایر مراکز تخصصی می‌باشد. اما در صورتی‌که سازمان امکانات لازم اعم از: تجهیزات، آزمایشگاه و اساتید مجرب را دارا باشد، می‌توان آموزش متخصصین را نیز در داخل سازمان به انجام رسانید. در این بخش از برنامه، لازم است روش[های] مناسب برای آموزش، انتخاب و اعلام شوند.

### ۶-۳-۴- پشتیبانی

چنانچه توجه کافی به مقوله پشتیبانی برنامه آگاهی‌رسانی امنیتی، آموزش و تربیت نیروی انسانی نشود، امکان تنزل این برنامه به سطح روزمرگی وجود دارد. همچنین با توجه به اینکه در اثر مرور زمان، زیرساختار فن‌آوری اطلاعات، تشکیلات سازمانی و نیازهای آگاهی‌رسانی و آموزش پرسنل تغییر می‌یابند، لذا

ضرورت دارد نتایج حاصل از اجرای این برنامه بصورت مداوم بررسی شده و محتوای این برنامه، مرتباً مورد بازنگری قرار گیرد.

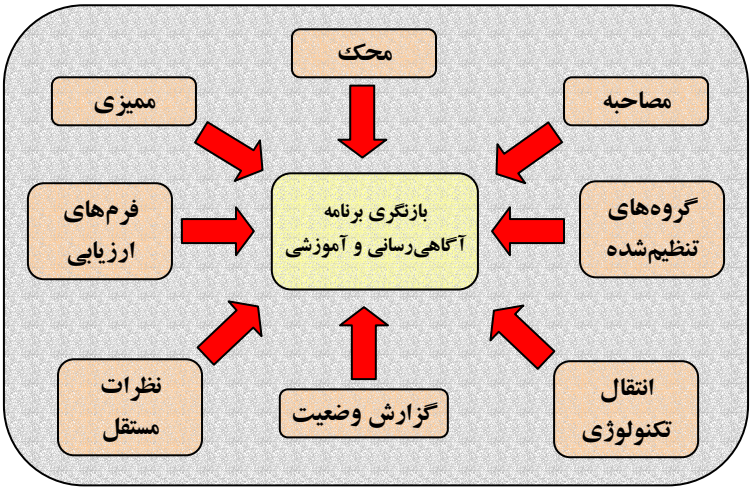
در این بخش، لازم است موارد زیر مطرح شوند:

۱. **نظارت‌بر مناسب بودن برنامه‌ها** – به‌منظور بررسی صحت برنامه آگاهی‌رسانی امنیتی، آموزش و تربیت نیروی انسانی ارائه شده، باید به‌صورت منظم و از طریق مراجع موجود در سازمان و مشخص شده در برنامه، بر درستی عملکرد این برنامه، نظارت شود. برخی از این مراجع عبارتند از: مدیر فن‌آوری اطلاعات سازمان، مدیر امنیت شبکه، مدیر منابع انسانی، مدیر آموزش سازمان، سایر مدیران اجرایی سازمان. لذا در این بخش از برنامه، لازم است مراجع و روش نظارت بر مناسب بودن برنامه، پیش‌بینی شود.

۲. **انجام ارزیابی و بازخورد** – مکانیسم‌های ارزیابی و بازخورد، از مهمترین اجزای برنامه آگاهی‌رسانی امنیتی، آموزش و تربیت نیروی انسانی می‌باشند. بهبود وضع برنامه امکان نخواهد داشت مگر با بررسی وضع عملکرد موجود برنامه. شکل (۶-۷) برخی از تکنیک‌های ارزیابی و بازخورد را نشان می‌دهد. در این بخش از برنامه، لازم است مراجع و تکنیکهای مناسب برای ارزیابی برنامه، پیش‌بینی شود.

۳. **مدیریت تغییرات** – در صورتی که انجام ارزیابی و بازخورد، ضرورت انجام بعضی تغییرات را نشان دهد، لازم است این تغییرات انجام گیرد. دامنه این تغییرات بستگی به نتایج ارزیابی دارد. تغییرات می‌تواند برروی راهبردها و سیاست‌های برنامه آگاهی‌رسانی امنیتی، آموزش و تربیت نیروی انسانی، اصل برنامه، وظایف و مسؤولیت‌ها یا سایر موارد باشد. مدیریت این تغییرات باید به نحوی انجام گیرد که نقش مثبتی در روند برنامه آگاهی‌رسانی امنیتی، آموزش و تربیت نیروی انسانی سازمان ایفا نماید.

۴. **تداوم آموزش** – استمرار آگاهی‌رسانی و آموزش و افزایش مهارت و توان پرسنل سازمان، نکته‌ای است که لازم است همیشه مورد توجه مدیران سازمان قرار داشته باشد. در این بخش از برنامه، لازم است روش‌های مناسب برای تداوم برنامه، پیش‌بینی شوند.




شکل (۶-۷): تکنیک‌های ارزیابی و بازخورد [۱۱]

۵. **حمایت، ضامن موفقیت** – مدیریت ارشد سازمان اعم از: مدیر سازمان، مدیر فن‌آوری اطلاعات سازمان، مدیر امنیت شبکه سازمان و سایر مدیران، درموفقیت برنامه آگاهی‌رسانی امنیتی، آموزش و تربیت نیروی انسانی نقشی به‌سزا ایفا می‌نمایند. حمایت این مدیران، بویژه مدیر سازمان و مدیر فن‌آوری اطلاعات سازمان هم در درازمدت و هم در مواقع بحرانی می‌تواند اثرات شگرفی بر نتایج حاصل از اجرای این برنامه داشته باشد. در این بخش از برنامه، لازم است ضمن تبیین حمایت مدیران فوق از اجرای برنامه، روش‌های مناسب جهت تداوم حمایت مدیران و انتقال این مطلب به مخاطبین برنامه، پیش‌بینی شود.

# مراجع

[1]. British standard institute, “Information security management – part 1: code of practice for information security management (BS7799-1)”, 1999

[2]. British standard institute, “Information security management – part 2: specification for information security management system (BS7799-2)”, 1999

[3]. International Standard Organization, “Information technology – Code of practice for information security management (ISO/IEC 17799)”, 2000

[4]. International Standard Organization, “Information technology – Guidelines for the management of IT security – Part 1: Concepts and models for IT security (ISO/IEC TR 13335-1)”, 1996

[5]. International Standard Organization, “Information technology – Guidelines for the management of IT security – Part 2: Managing and planning IT security (ISO/IEC TR 13335-2)”, 1997

[6]. International Standard Organization, “Information technology – Guidelines for the management of IT security – Part 3: Techniques for the Management of IT security (ISO/IEC TR 13335-3)”, 1998

[7]. International Standard Organization, “Information technology – Guidelines for the management of IT security – Part 4: Selection of safeguards (ISO/IEC TR 13335-4)”, 2000

[8]. International Standard Organization, “Information technology – Guidelines for the management of IT security – Part 5: Management guidance on network security (ISO/IEC TR 13335-5)”, 2001

[۹]. محمد سپهری راد، سعید جلیلی، سید فرشید یعسوبی، مریم نراقی، هوشنگ بشارتیان، ناهید خزائی و مریم فصیحی، "مقررات مربوط به سیستم مدیریت حفاظت اطلاعات – بخش دو:

ویژگیهای مدیریت سیستم‌های حفاظت اطلاعات"، استاندارد ملی ایران، موسسه استاندارد و تحقیقات صنعتی ایران

[10]. Tim Grance, Karen Kent, Brian Kim, "NIST Special publication 800-61: Computer security incident handling Guide", 2004

[11]. Mark Wilson, Joan Hash, "NIST Special publication 800-50: Building an information technology security awareness and training program", 2003

# عبارات اختصاری

| | |
|---|---|
| AAA | Authentication, Authorization, Accounting |
| FTP | File Transfer Protocol |
| H-IDS | Host based Intrusion Detection System |
| H-IPS | Host based Intrusion Prevention System |
| HTTP | Hyper Text Transmission Protocol |
| IDS | Intrusion Detection System |
| IETF | Internet Engineering Task Force |
| IP | Internet Protocol |
| ISMS | Information Security Management System |
| ISMS IUG | ISMS International User Group |
| ISS | Internet Security Systems |
| IPS | Intrusion Prevention System |
| MIB | Management Information Base |
| N-IDS | Network based Intrusion Detection System |
| N-IPS | Network based Intrusion Prevention System |
| POP | Post Office Protocol |
| SMTP | Simple Mail Transfer Protocol |
| SNMP | Simple Network Management Protocol |
| VPN | Virtual Private Network |

# واژه‌نامه فارسی به انگلیسی

**الف**

| | |
|---|---|
| ابزار | Tools |
| اختیار | Authority |
| ارزیابی | Assessment |
| ارزیابی | Evaluation |
| آسیب‌پذیری | Vulnerability |
| اطمینان | Assurance |
| افزونگی | Redundancy |
| آگاهی‌رسانی امنیتی | Security Awareness |
| آماده‌سازی | Preparation |
| آموزش امنیت | Security Education |
| آنالیز مخاطره | Risk Analysis |
| انتخاب | Selection |
| انضباطی | Disiplinary |
| انکار | Repudiation |
| اهداف نهایی | Goals |
| اهداف مقطعی | Objectives |

**ب**

| | |
|---|---|
| بازبینی | Review |
| بازخورد | Feedback |

| | |
|---|---|
| بازرسی | Audit |
| بازیابی | Recovery |
| بررسی سازگاری | Compliance checking |
| برنامه | Program |
| بی‌قاعده | Promiscuous |

**پ**

| | |
|---|---|
| پاسخ‌گویی | Accountability |
| پذیرش | Acceptance |
| پشتیبانی | Handling |
| پشتیبانی | Follow-Up |
| پویش‌گر | Scanner |
| پیاده‌سازی | Implementation |
| پیش‌گیری | Prevention |
| پیغام‌رسانی فوری | Instant Messaging |
| پیکربندی | Configuration |
| پیمان | Contract |

**ت**

| | |
|---|---|
| تداوم | Continuity |
| تربیت نیروی انسانی در زمینه امنیت | Security Training |
| ترکیبی | Combined |
| ترمیم خرابی | Disaster Recovery |
| تشخیص | Detection |
| تشخیص نفوذ | Intrusion detection |

| | |
|---|---|
| تشخیص هویت | Authentication |
| تشکیلات امنیت | Security organization |
| تصدیق اصالت / تصدیق هویت | Authentication |
| تفصیلی | Detailed |
| توصیه | Recommendation |
| تهدید | Threat |

**چ**

| | |
|---|---|
| چارچوب | Framework |
| چرخه حیات | Life Cycle |

**ح**

| | |
|---|---|
| حریم خصوصی | Privacy |
| حفاظ | Safeguard |
| حوادث | Incidents |

**خ**

| | |
|---|---|
| خرابی | Disaster |
| خسارت | Loss |
| خصوصی | Private |

**د**

| | |
|---|---|
| دسترس‌پذیری | Availability |
| دسته‌بندی | Categorization |

**ر**

| | |
|---|---|
| راهبرد | Strategy |
| رمزنگاری | Encryption |
| روال | Procedure |
| رویدادنامه | Log |
| رهنمود | Guidance |
| ریسک باقیمانده | Residual risk |

**ز**

| | |
|---|---|
| زیرساختار | Infrastructure |

**س**

| | |
|---|---|
| سازگاری | Compliance |
| سرمایه | Asset |
| سیاست امنیتی | Security policy |
| سیستم مدیریت امنیت اطلاعات | Information Security Management System (ISMS) |
| سیستم‌های تشخیص نفوذ | Intrusion detection system (IDS) |
| سیستم‌های پیش‌گیری از نفوذ | Intrusion Prevention system (IPS) |

**ش**

| | |
|---|---|
| شبکه خصوصی مجازی | Virtual Private Network (VPN) |
| شخص ثالث | Third party |
| شناسایی | Identification |

**ص**

| | |
|---|---|
| صحت | Integrity |

**ض**

| | |
|---|---|
| ضربه | Impact |
| ضعف | Weakness |

**ط**

| | |
|---|---|
| طبقه‌بندی | Classification |
| طرح | Plan |

**ع**

| | |
|---|---|
| عدم انکار | Non-Repudiation |

**غ**

| | |
|---|---|
| غیررسمی | Informal |
| غیرمجاز | UnAuthorize |

**ف**

| | |
|---|---|
| فرآیند | Process |
| فشار | Constraint |
| فعالیت | Business |
| فن‌آوری اطلاعات | Information Technology (IT) |
| فیزیکی | Physical |
| فیلترینگ محتوا | Content Filtering |

**ق**

| | |
|---|---|
| قابلیت اعتماد | Reliability |
| قابلیت دسترسی | Availability |
| قلمرو | Scope |

**ک**

| | |
|---|---|
| کار از راه دور | Teleworking |
| کاربرد | Application |
| کرم | Worm |
| کلمه عبور | Password |
| کمیته راهبری | Steering Committee |
| کنترل دسترسی | Access control |

**گ**

| | |
|---|---|
| گزارش فنی | Technical report |
| گذرگاه | Gateway |
| گواهی | Certification |

**م**

| | |
|---|---|
| مارک | Brand |
| ماموریت | Mission |
| محافظت فیزیکی | Physical security |
| محتوا | Content |
| محدودسازی | Containment |

| | |
|---|---|
| محرمانگی | Confidentiality |
| محیطی | Environmental |
| مخاطره | Risk |
| مخرب | Malicious |
| مدیر امنیت | Security officer |
| مدیریت تغییرات | Change Management |
| مدیریت مخاطره | Risk management |
| مدیریت وصله | Patch Management |
| مستندسازی | Documentation |
| مسئولیت | Responsibility |
| مشورت | Advice |
| مطمئن | Trust |
| معماری | Architecture |
| معیارهای مشترک | Common Criteria |
| مفهوم | Concept |
| ممانعت از سرویس | Denial of Service |
| میز پاک | Clear desk |

**ن**

| | |
|---|---|
| ناحیه | Zone |
| ناحیه غیرنظامی | De militarize Zone |
| نامناسب | Inappropriate |
| نظارت | Monitoring |
| نفوذ | Intrusion |
| نگرانی | Concern |

| | |
|---|---|
| نگهداری | Maintenance |
| نیاز | Requirement |

**و**

| | |
|---|---|
| واگذاری فعالیت‌ها به خارج از سازمان | Outsourcing |
| وصله | Patch |
| وظیفه | Duty |
| وقایع | Event |

**ه**

| | |
|---|---|
| هماهنگ‌کننده | Co-ordinator |
| هم‌زمانی | Synchrinization |
| همه جانبه | Detailed |