جمهوري اسلامي ايران

**Islamic Republic of Iran**

مؤسسه استاندارد و تحقيقات صنعتی ايران

**Institue of Standards and Industrial Research of Iran –1**

# مقررات مربوط به
# سيستم مديريت حفاظت اطلاعات -

بخش دو : ويژگي‌هاي سيستم مديريت حفاظت اطلاعات

# Information Security Management System -

# Part 2 : Specification Information Security Management System

## مدیریت حفاظت اطلاعات قسمت 2- ویژگی‌های سیستم مدیریت حفاظت اطلاعات

| رئیس | سمت یا نمایندگی |
|---|---|
| دکتر محمد سپهری‌راد<br>(دکترای فیزیک) | دبیر شورای عالی انفورماتیک کشور |

**اعضاء**

| | |
|---|---|
| سعید جلیلی<br>(دکترای کامپیوتر) | عضو هیأت علمی دانشگاه تربیت مدرس |
| سید فرشید یعسوبی<br>(فوق‌لیسانس برق الکترونیک) | شرکت مهندسی سیستم یاس ارغوانی |
| مریم نراقی<br>(لیسانس کامپیوتر) | شرکت مهندسی سیستم یاس ارغوانی |
| هوشنگ بشارتیان<br>(فوق لیسانس - مدیریت سیستم) | شرکت مهندسی سیستم یاس ارغوانی |
| ناهید خزاعی<br>(فوق لیسانس مدیریت تکنولوژی اطلاعات) | شرکت مهندسی سیستم یاس ارغوانی |

**دبیر**

**مریم فصیحی** **مؤسسه استاندارد و تحقیقات صنعتی ایران**

**(لیسانس علوم کامپیوتر)**

**فهرست مندرجات** **صفحه**

**پیش‌گفتار** ..... **4**

**1 دامنه** ..... **5**

**2 اصطلاحات و تعریف‌ها** ..... **5**

2-1 دستورالعمل اجرایی ..... 5

**3 الزامات سیستم مدیریت حفاظت اطلاعات** ..... **5**

3-1 کلیات ..... 5

3-2 ایجاد چارچوب مدیریتی ..... 6

3-3 پیاده‌سازی ..... 8

3-4 مستندسازی ..... 8

3-5 کنترل مستندات ..... 8

3-6 ثبت‌ها ..... 9

**4 کنترل‌های همه جانبه** ..... **9**

4-1 سیاست حفاظت ..... 9

4-2 سازمان حفاظت ..... 10

4-3 طبقه‌بندی و کنترل دارایی‌ها ..... 11

4-4 حفاظت کارکنان ..... 12

4-5 حفاظت فیزیکی و محیطی ..... 14

4-6 مدیریت ارتباطات و عملیات ..... 16

4-7 کنترل دسترسی ..... 19

4-8 توسعه و نگهداری سیستم‌ها ..... 24

4-9 مدیریت تداوم فعالیت ..... 26

4-10 سازگاری ..... 27

– واژه‌نامه لاتین ..... 30

– واژه‌نامه فارسی ..... 33

## پیش گفتار

استاندارد "مدیریت حفاظت اطلاعات- قسمت 2، ویژگی‌های سیستم مدیریت حفاظت اطلاعات" که توسط کمیسیون‌های مربوط تهیه و تدوین شده و در جلسه کمیته ملی استاندارد رایانه و فرآوری داده‌ها مورخ 82/7/29 مورد تصویب قرار گرفته است، اینک به استناد بند یک ماده 3 قانون اصلاح قوانین و مقررات مؤسسه استاندارد و تحقیقات صنعتی ایران مصوب بهمن ماه 1371 به عنوان استاندارد ملی ایران منتشر می‌شود.

برای حفظ همگامی و هماهنگی با تحولات و پیشرفت‌های ملی و جهانی در زمینه صنایع، علوم و خدمات، در استانداردهای ملی ایران در مواقع لزوم تجدید نظر خواهد شد و هرگونه پیشنهادی که برای اصلاح یا تکمیل این استانداردها ارائه شود، در هنگام تجدید نظر در کمیسیون فنی مربوط مورد توجه قرار خواهد گرفت. بنابراین برای مراجعه به استانداردهای ایران باید همواره از آخرین تجدیدنظر آنها استفاده کرد.

در تهیه و تدوین این استاندارد سعی شده است که ضمن توجه به شرایط موجود و نیازهای جامعه، در حد امکان بین این استاندارد، استانداردهای بین‌المللی و استاندارد ملی کشورهای صنعتی و پیشرفته هماهنگی ایجاد می‌شود.

منابع و مآخذی که برای تهیه این استاندارد به کار رفته به شرح زیر است :


1- گزارش بررسی و شناخت - پروژه استانداردسازی حفاظت اطلاعات (پروژه شماره 1224 شورای پژوهش‌های علمی کشور)

2- BS 7799-2 :1999 Information Security Management
Part 2 : Specification Information Security Management Systems

# مدیریت حفاظت اطلاعات قسمت 2- ویژگی‌های سیستم مدیریت حفاظت اطلاعات

## 1 دامنه

هدف از تدوین این استاندارد، ارائه مقررات و ویژگی‌های یک سیستم مدیریت حفاظت اطلاعات است. این استاندارد برای حوزه فناوری اطلاعات تهیه شده است و به دلیل اینکه ارائه‌کننده یک سیستم مدیریت حفاظت اطلاعات می‌باشد، مستقل از فناوری قابل پیاده‌سازی است و در برگیرنده کلیه مسائل ایجاد، پیاده‌سازی و مستندسازی یک سیستم امن می‌باشد. کلیه سازمانها و دستگاه‌های دولتی و غیردولتی به منظور حفظ و نگهداری و حراست از اطلاعات در روال‌ها و سیستم‌های خود می‌توانند از آن بهره‌برداری نمایند.

## 2 اصطلاحات و تعریف‌ها

در این استاندارد اصلاحات و تعاریف بکار رفته در گزارش بررسی و شناخت - پروژه استانداردسازی حفاظت اطلاعات (پروژه شماره 1224 شورای پژوهش‌های علمی کشور) کاربرد دارد.

دستورالعمل اجرایی

بررسی و نقد اهداف و کنترل‌های متناسب با نیازهای سازمان

## 3 الزامات[1] سیستم مدیریت حفاظت اطلاعات

### 3-1 کلیات

هر سازمانی باید یک سیستم مدیریت حفاظت اطلاعات را برای خود به‌صورت مستند؛ تعریف، ایجاد و نگهداری نماید. این سیستم باید دربرگیرندهٔ حفاظت دارایی‌ها، ارائهٔ روش مدیریت مخاطره[2]، هدف‌های کنترل[3]، کنترل‌ها و درجهٔ اطمینان[4] از آنها باشد.

1. Requirements
2. Risk
3. Control Objectives
4. Degree of assurance

## 2-3 ایجاد چارچوب[1] مدیریتی

به منظور ایجاد چارچوبی معین، مراحل زیر برای شناسایی و مستندسازی "اهداف کنترل" و "کنترل‌ها" باید پذیرفته شوند (شکل 1) :

الف : سیاست‌های حفاظت اطلاعات تعریف شوند.

ب : دامنه سیستم مدیریت حفاظت اطلاعات تعریف شده باشد و مرزبندی‌های آن متناسب با نوع سازمان و نیازهای آن ارائه گردد.

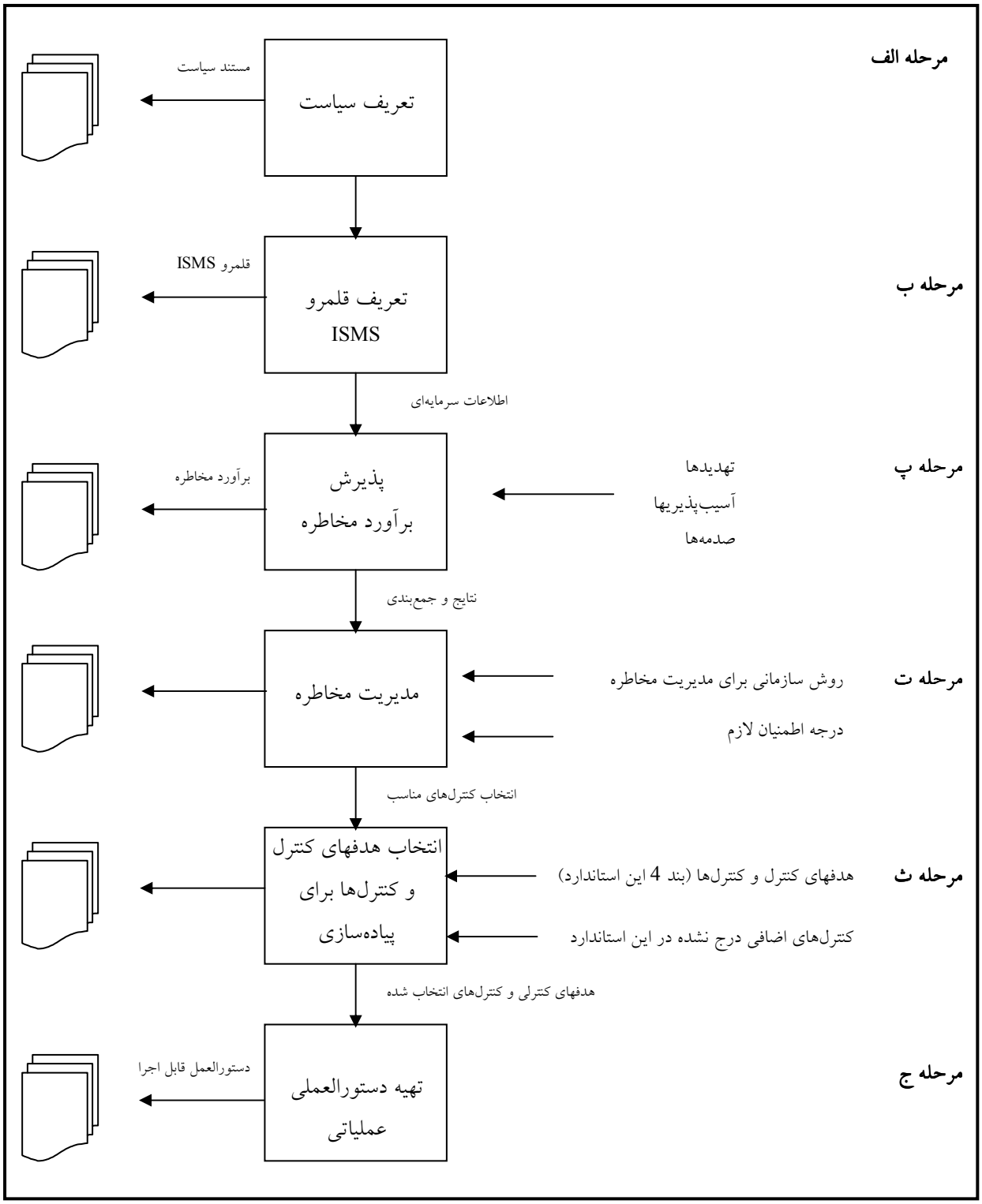
پ : هماهنگ با نوع و نیازهای سازمان، برآوردی مناسب از مخاطره صورت گیرد و پذیرفته شود.

ت : زمینه‌های مخاطره‌ای که بایستی مدیریت شوند، باید بر اساس سیاست‌های حفاظت اطلاعات سازمان و درجه اطمینان مورد نیاز مشخص گردند.

ث : برای پیاده‌سازی در سازمان، هدف‌های کنترل و کنترل‌های مناسبی که قابل توجیه هستند، از بند 4 انتخاب گردند.

ج : دستورالعملی عملیاتی تهیه شود.

1. Frame work




**شکل 1- ایجاد چارچوب مدیریتی**

### 3-3 پیاده‌سازی[1]

اهداف کنترلی و کنترل‌های انتخاب شده، باید به‌صورت مؤثری توسط سازمان پیاده‌سازی گردند. اثربخشی رویه‌های بکارگرفته شده برای پیاده‌سازی این کنترل‌ها، بایستی توسط بازبینی‌هایی که مطابق با بند 4-10-2 می‌باشد، تأیید گردد.

### 4-3 مستندسازی[2]

مستندات ISMS [3] باید شامل اطلاعات ذیل باشند:

الف- مدرک [4] اقدامات انجام شده منطبق بر بند 3-2

ب - خلاصه‌ای از چارچوب مدیریت حفاظت، شامل سیاست‌ها، اهداف کنترلی و کنترل‌های پیاده‌سازی شده مندرج در دستورالعمل بکارگیری

پ - روال‌های تطبیق یافته متناسب با پیاده‌سازی کنترل‌های تعیین شده در بند 3-3 (این روال‌ها باید دقیقاً مسئولیت‌ها، وظایف و کارهای مربوط را مشخص نمایند.)

ت - روال‌هایی که مسئولیت‌ها و اجرای وظایف ISMS را تشریح می‌کند و پوشش می‌دهند.

### 5-3 کنترل مستندات

سازمان باید روال‌هایی را برای ایجاد و نگهداری همهٔ مستندات لازم در بند 3-4 فراهم نماید. این مستندات باید دارای خصوصیات ذیل باشند:

الف- همواره آماده و در دسترس باشند.

ب - به صورت منظم و دوره‌ای مطابق با سیاست حفاظت سازمان، مرور و بازنگری شوند.

پ - در همهٔ محل‌هایی که ISMS اجرا می‌شود، به‌صورت نسخه‌برداری کنترل شده در دسترس باشند.

ث : به هنگام غیرقابل استفاده شدن یا قدیمی شدن، باید بازپس‌گیری شوند.

ج : به منظور حفظ دانش یا اهمیت حقوقی، همه مستندات از رده خارج شده، باید شناسایی و نگهداری شوند.

---

1. Implementation
2. Documentation
3. Information Security Management System
4. Evidence

مستندات باید خوانا، تاریخ‌دار (همراه با تاریخ‌های نسخه‌های مختلف) و به صورت کاملاً آماده و قابل شناسایی تهیه و با یک روش منظم و به صورت دوره‌ای نگهداری گردند، به همین منظور، برای ایجاد، نگهداری، اصلاح و به کارگیری مستندات باید روال‌های مناسبی ایجاد شوند.
یادآوری : مستندات می‌توانند در هر محیطی، نظیر مکتوبات یا محیط‌های ذخیره الکترونیکی باشند.

### 6-3 ثبت‌ها[1]

ثبت‌ها، مدارکی هستند که در توالی منطقی عملیات ISMS تولید می‌شوند. آنها باید برای نشان دادن مطابقت با نیازهای سیستم مدیریت حفاظت اطلاعات سازمان نگهداری شوند. دفتر ثبت ورود و خروج بازدیدکنندگان، گزارش‌های بازرسی و کنترل صحت دسترسی‌ها از جمله این ثبت‌ها می‌باشند. سازمان باید برای شناسایی، نگهداری، حفظ و آشکارسازی مدارک ثبت شده، روال‌هایی را ایجاد و نگهداری نماید. ثبت‌ها باید خوانا، قابل شناسایی و پیگیری برای فعالیت‌های مربوطه باشند. همچنین به روش‌هایی ذخیره و نگهداری شوند، که در دسترس، قابل استخراج و حفاظت شده در برابر هرگونه صدمات و گم‌شدن باشند.
یادآوری : ثبت‌ها می‌توانند در هر محیطی، نظیر مکتوبات یا محیط‌های ذخیره الکترونیکی باشند.

## 4 کنترل‌های همه‌جانبه[2]

### 4-1 سیاست حفاظت[3]

#### 4-1-1 سیاست حفاظت اطلاعات

| |
|---|
| **مقصود :** فراهم آوردن رهنمود و حمایت مدیریت جهت حفاظت اطلاعات است. |

6-1-1-1- سند سیاست حفاظت اطلاعات

سندی است محتوی سیاست حفاظت اطلاعات، که بایستی به وسیلهٔ مدیران تأیید و به نحو مناسب در دسترس کلیهٔ همکاران سازمان قرار گیرد.

6-1-1-2- مرور و ارزیابی

1 . Records
2 . Detailed Controls
3 . Security Policy

سیاست حفاظت اطلاعات، باید به‌طور منظم و باتوجه به تغییرات احتمالی و به منظور اطمینان از مؤثر بودن آن، بازنگری شود.

## 4-2 سازمان حفاظت[1]

### 4-2-1 زیرساخت حفاظت اطلاعات

| |
|---|
| **مقصود :** مدیریت کردن حفاظت اطلاعات در داخل سازمان است. |

6-2-1-1- گروه مدیریتی حفاظت اطلاعات

به منظور اطمینان از توجه روشن و حمایت شفاف مدیران از اصول حفاظت، باید یک گروه مدیریتی تشکیل گردد.

6-2-1-2- هماهنگی حفاظت اطلاعات

به منظور هماهنگی در پیاده‌سازی کنترل‌های حفاظت اطلاعات، متناسب با اندازهٔ سازمان باید یک گروه عملیاتی[2] از مدیران بخش‌های مختلف سازمان، وجود داشته باشد.

6-2-1-3- تعیین مسئولیت‌های حفاظت اطلاعات

به منظور صیانت از دارایی‌های شخصی و اجرای دقیق فرایند حفاظتی باید، مسئولیت‌ها به طور واضح تعریف شود.

6-2-1-4- فرایند مجازسازی برای امکان پردازش اطلاعات

برای امکانات جدید پردازش اطلاعات، باید یک فرایند مدیریت مجازسازی ایجاد گردد.

6-2-1-5- مشورت با نیروهای متخصص حفاظت اطلاعات

به منظور مؤثر کردن روش‌های حفاظتی، آگاهی از نظرات نیروهای داخلی یا مشاورین مرتبط با سازمان الزامی است.

1 . Security Organization

2 . Cross - Functional

6-2-1-6- همکاری بین سازمان‌ها

در سازمان حفاظت، ارتباط‌های مناسب با اشخاص و مؤسسات حقوقی، تأمین‌کنندگان خدمات اطلاعاتی[1] و اپراتورهای مخابرات راه دور بایستی در نظر گرفته شود.

6-2-1-7- مرور مستقل حفاظت اطلاعات

نحوه پیاده‌سازی سیاست حفاظت اطلاعات، باید بطور جداگانه دیده شده باشد.

### 4-2-2 حفاظت از دستیابی شخص ثالث

| |
|---|
| **مقصود:** حفاظت از امکانات پردازشی و دارایی‌های اطلاعاتی سازمان، از دسترسی اشخاص ثالث |

6-2-2-1- شناسایی مخاطرات ناشی از دسترسی شخص ثالث

مخاطراتی که به وسیله دسترسی شخص ثالث (حقوقی و حقیقی) به امکانات پردازش اطلاعات سازمان وجود دارد، باید ارزیابی شده و کنترل‌های حفاظتی مناسب، در آن موارد پیاده شوند.

6-2-2-2- پیش‌بینی الزامات حفاظتی در قراردادهای شخص ثالث

دسترسی شخص ثالث به امکانات پردازش اطلاعات سازمان بایستی بر اساس قراردادی رسمی حاوی کلیه الزامات حفاظتی لازم باشد.

### 4-2-3 واگذاری فعالیت به بیرون سازمان

| |
|---|
| **مقصود:** رعایت حفاظت اطلاعات، هنگامی که مسئولیت پردازش اطلاعات به سازمان دیگری واگذار می‌شود. |

6-2-3-1- الزامات حفاظتی در قراردادهای واگذاری فعالیت به بیرون سازمان

هنگامی که تمام یا بخشی از مدیریت و کنترل سیستم‌های اطلاعاتی، شبکه و فعالیت‌های دفتری سازمان به سازمان دیگری واگذار می‌شود، الزامات حفاظتی، باید در قرارداد بین طرفین در نظر گرفته شده باشد.

## 6-3- طبقه‌بندی و کنترل دارایی‌ها[2]

### 4-3-1 قابلیت حسابرسی دارایی‌ها

| |
|---|
| **مقصود:** هدف ایجاد حفاظت مناسب از دارایی‌های سازمانی است. |

1. Information Service Providers
2 . Asset classification and control

6-3-1-1-ایجاد فهرستی از دارایی‌ها

یک فهرست از همهٔ دارایی‌های مهم، باید تنظیم و نگهداری شود.

### 4-3-2 طبقه‌بندی اطلاعات

| |
|---|
| **مقصود** : اطمینان از اینکه دارایی‌های اطلاعاتی به یک سطح حفاظتی مناسب رسیده است. |

**4-3-2-1** رهنمودهای طبقه‌بندی[1]

طبقه‌بندی‌ها و کنترل‌های حفاظت اطلاعات مربوطه، بایستی متناسب با نیازهای سازمانی جهت به اشتراک گذاشتن و یا محدودسازی اطلاعات و تأثیرات سازمانی مرتبط با این نیازها باشند.

**4-3-2-2** جابجایی و علامت‌گذاری اطلاعات[2]

برای جابجایی و علامت‌گذاری اطلاعات، مطابق با رویه‌های طبقه‌بندی سازمان، باید مجموعه‌ای از روال‌ها تعریف شوند.

## 4-4- حفاظت کارکنان[3]

### 4-4-1 حفاظت در شرح شغل و کاریابی

| |
|---|
| **مقصود :** کاهش مخاطرات ناشی از خطای انسانی، سرقت، تقلب و استفاده نادرست از منابع و قابلیت‌ها است. |

**4-4-1-1** لحاظ نمودن مسائل حفاظتی در مسئولیت‌های شغلی

نقش‌ها و مسئولیت‌های حفاظتی، باید در سیاست حفاظت اطلاعات سازمان در نظر گرفته شود و به صورت مناسب و مستند در شرح شغل درج گردد.

**4-4-1-2** گزینش کارکنان

در مورد کارکنان دائم، باید در زمان درخواست کار کنترل‌ها و تأییدهای لازم صورت گیرد.

**4-4-1-3** توافق‌نامهٔ محرمانه بودن اطلاعات سازمانی

کارکنان، باید توافق‌نامهٔ محرمانه بودن اطلاعات سازمانی را به عنوان بخشی از شرایط قراردادی خود، در هنگام استخدام امضاء نمایند.

1 . Classification guidelines
2 . Information labelling and handling
3 . Personel Security

**4-4-1-4** ضوابط استخدامی

ضوابط استخدامی بایستی حاوی مسئولیت‌های کارکنان در زمینه حفاظت اطلاعات باشد.

**4-4-2** آموزش کاربر

| |
|---|
| **مقصود:** اطمینان از اینکه کاربران آگاهی لازم را از تهدیدها و نگرانی‌های حفاظت اطلاعات دارند و در انجام وظایف خود، می‌توانند پشتیبانی لازم را از سیاست‌های حفاظتی سازمان به عمل آورند. |

**4-4-2-1** آموزش دانش حفاظت اطلاعات

همهٔ کارکنان سازمان و در مواقع لزوم اشخاص ثالث، باید به نحوی مناسب و منظم در مورد روال‌ها و سیاست‌های حفاظتی سازمان آموزش ببینند.

**4-4-3** پاسخ به حوادث و اشتباهات مربوط به حفاظت

| |
|---|
| **مقصود:** کمینه کردن صدمات ناشی از حوادث و اشتباهات حفاظتی و یادگیری و مراقبت از چنین حوادثی است. |

**4-4-3-1** گزارش حوادث حفاظتی

حوادث حفاظتی پس از کشف، باید در کوتاه‌ترین زمان ممکن از طریق مجاری مدیریتی مناسب گزارش شوند.

**4-4-3-2** گزارش ضعف‌های حفاظتی

کاربران خدمات اطلاعاتی، ضروری است هرگونه ضعف و تهدید حفاظتی روی خدمات و سیستم‌ها را یادداشت و گزارش نمایند.

**4-4-3-3** گزارش اشتباهات نرم‌افزاری

روال‌هایی به منظور پیگیری گزارش‌های اشتباهات نرم‌افزاری، باید ایجاد شوند.

**4-4-3-4** یادگیری از حوادث

برای اینکه، نوع، اندازه و هزینه اشتباهات و حوادث قابل اندازه‌گیری و نمایش شوند باید مکانیزم‌هایی ایجاد شوند.

**4-4-3-5** فرایند انضباطی

یک فرایند انضباطی رسمی برای تخلف از سیاست‌های حفاظتی سازمان و روال‌هایی که کارکنان لازم است رعایت نمایند، باید ایجاد گردد.

## 5-4 حفاظت فیزیکی و محیطی[1]

### 1-5-4 محیط‌های ایمن

| |
|---|
| **مقصود:** جلوگیری از دسترسی غیرمجاز، صدمات و تداخل در اطلاعات و خصوصیات تجاری سازمان است. |

**1-1-5-4** میدان حفاظت فیزیکی

سازمان‌ها، باید از میدان‌های حفاظتی، برای حفاظت از محل‌های نگهداری تجهیزات پردازش اطلاعات استفاده کنند.

**2-1-5-4** کنترل‌های ورودی فیزیکی

محل‌های ایمن، باید بوسیله کنترل‌های ورودی مناسب محافظت شوند تا اطمینان حاصل شود فقط افراد مجاز می‌توانند دسترسی داشته باشند.

**3-1-5-4** ایمن‌سازی دفاتر، اتاقها و امکانات

به منظور حفاظت از دفاتر، اتاق‌ها و امکانات با نیازهای حفاظتی خاص، باید محل‌های ایمن ایجاد گردند.

**4-1-5-4** کار در محل‌های ایمن

برای کار در محل‌های ایمن، باید کنترل‌های اضافی و رهنمودهای تکمیلی مورد استفاده قرار گیرد تا از ایمن بودن این محل‌ها اطمینان لازم حاصل شود.

**5-1-5-4** مجزاسازی محل‌های انتقال و بارگیری اطلاعات

محل‌های انتقال و بارگیری اطلاعات، باید کنترل شود و درصورت امکان مجزا از محل تجهیزات پردازش اطلاعات باشد، تا از دستیابی‌های غیرمجاز جلوگیری شود.

1 . Physical and environmental security

### 4-5-2 حفاظت تجهیزات

| |
|---|
| **مقصود:** جلوگیری از اتلاف، صدمات و لطمه به دارایی‌ها و ایجاد وقفه در فعالیت‌های سازمان است. |

**4-5-2-1** استقرار و حفاظت تجهیزات

تجهیزات، باید در محل مناسب و محافظت شده‌ای قرار داشته باشند. تا مخاطرات و تهدیدهای محیطی و امکان دسترسی غیرمجاز کاهش یابد.

**4-5-2-2** منابع تغذیه

تجهیزات، باید از هرگونه صدمات ناشی از قطع یا خرابی منابع تغذیه محافظت شوند.

**4-5-2-3** حفاظت کابل‌کشی

به منظور جلوگیری از هرگونه خسارت یا قطع شدن، باید کابل‌کشی‌های برق، داده‌ها و تلفن مورد استفاده در خدمات اطلاعاتی، محافظت شوند.

**4-5-2-4** نگهداری تجهیزات

تجهیزات، جهت اطمینان از تداوم فعالیت و یکپارچگی، متناسب با دستورالعمل‌های سازنده یا روال‌های مستند شده، باید نگهداری شوند.

**4-5-2-5** حفاظت از تجهیزات در هنگام استفاده بیرونی

به منظور حفاظت از تجهیزات در هنگام استفاده در بیرون سازمان، باید روال‌های حفاظتی ایجاد شوند.

**4-5-2-6** دور ریختن یا استفاده مجدد از تجهیزات به صورت مطمئن

قبل از دور ریختن یا استفادهٔ مجدد از تجهیزات، اطلاعات باید از روی آنها پاک شود.

### 4-5-3 کنترل‌های عمومی[1]

| |
|---|
| **مقصود:** جلوگیری از تساهل یا سرقت اطلاعات و امکانات پردازش اطلاعات است. |

1 . General controls

**4-5-3-1** سیاست میز و صفحه پاک

به منظور کاهش مخاطرات ناشی از دسترسی غیرمجاز و فقدان یا صدمه به اطلاعات، سازمان‌ها بایستی سیاست میز پاک و صفحه پاک را اختیار و اجرا کنند.

**4-5-3-2** جابجایی اموال

تجهیزات، اطلاعات یا نرم‌افزار متعلق به سازمان، نباید بدون اجازه جابجا شود.

## 4-6 مدیریت ارتباطات[1] و عملیات

### 4-6-1 روال‌های عملیاتی و مسئولیت‌ها

| |
|---|
| **مقصود:** ایجاد اطمینان از صحت و امن بودن عملیات و تجهیزات پردازش اطلاعات است. |

**4-6-1-1** روال‌های عملیاتی مستند شده

روال‌های عملیاتی شناسایی شده در سیاست حفاظت (4-1-1-1) باید مستند و نگهداری شوند.

**4-6-1-2** کنترل تغییر عملیاتی

تغییرات در تجهیزات و سیستم‌های پردازش اطلاعات، باید کنترل شده باشند.

**4-6-1-3** روال‌های مدیریت حادثه

به منظور اطمینان از پاسخ سریع، مؤثر و مناسب به حوادث، باید روال‌ها و مسئولیت‌های مدیریت حادثه برقرار گردند.

**4-6-1-4** تفکیک وظایف

به منظور کاهش فرصت‌های تغییرات غیرمجاز و استفادهٔ نابجا از اطلاعات و خدمات، وظایف و محدودهٔ مسئولیت‌ها باید تفکیک گردند.

**4-6-1-5** جداسازی امکانات توسعه و عملیاتی

امکانات آزمایش و توسعه باید از امکانات عملیاتی مجزا شوند.

1 . Communications and operations management

**4-6-1-6** مدیریت امکانات خارج سازمانی

قبل از استفاده از خدمات قابل ارائه توسط مدیریت امکانات خارج از سازمان، باید مخاطرات دقیقاً شناسایی و روش‌های کنترلی مناسب که مورد توافق طرف قرارداد و سازمان باشد، در قرارداد گنجانده شوند.

**4-6-2** برنامه‌ریزی و پذیرش سیستم [1]

| |
|---|
| **مقصود :** کمینه کردن مخاطره خرابی سیستم‌ها است. |

**4-6-2-1** برنامه‌ریزی ظرفیت

برنامه‌ریزی لازم برای توان پردازش و ظرفیت ذخیره‌سازی اطلاعات در دسترس، باید با در نظر گرفتن تقاضاهای فعلی و آتی سیستم صورت پذیرد.

**4-6-2-2** پذیرش سیستم

معیار پذیرش سیستم‌های اطلاعاتی جدید و نسخه‌های جدید و به روز شده سیستم‌ها، باید مستند شده و قبل از پذیرش و جایگزینی سیستم قبلی، آزمایش‌های کافی صورت گیرد.

**4-6-3** حفاظت در برابر نرم‌افزار مخرب

| |
|---|
| **مقصود :** محافظت از یکپارچگی اطلاعات و نرم‌افزار است. |

**4-6-3-1** کنترل‌ها در برابر نرم‌افزار مخرب

روال‌های کنترلی، برای شناسایی، مقابله با نرم‌افزار مخرب و آگاهی کاربران از آنها باید پیاده شوند.

**4-6-4** اداره کردن

| |
|---|
| **مقصود :** نگهداری یکپارچگی و در دسترس بودن خدمات ارتباطی و پردازش اطلاعات است. |

**4-6-4-1** ایجاد پشتیبان اطلاعات

از اطلاعات مهم و اساسی و نرم‌افزارها، باید به طور منظم نسخه‌های پشتیبان تهیه گردد.

**4-6-4-2** ثبت‌های مجری [2]

کارکنان عملیاتی، باید فعالیت‌های خود را ثبت نمایند.

**4-6-4-3** ثبت خرابی

1. System planning and acceptance
2. Operator

خرابی‌ها باید گزارش شده و عملیات تصحیح آنها، انجام شوند.

**4-6-5** مدیریت شبکه

| |
|---|
| **مقصود :** اطمینان از محفوظ بودن اطلاعات در شبکه‌ها و حفاظت از زیربنای پشتیبانی آن است. |

**4-6-5-1** کنترل‌های شبکه

به منظور دستیابی به امنیت شبکه و حفظ آن باید مجموعه‌ای از کنترل‌ها اعمال گردد.

**4-6-6** جابجایی محیط ذخیره و حفاظت

| |
|---|
| **مقصود :** جلوگیری از صدمه به دارایی‌ها و وقفه در فعالیت‌های سازمان است. |

**4-6-6-1** مدیریت محیط‌های رایانه‌ای قابل جابجایی

مدیریت محیط‌های رایانه‌ای قابل جابجایی نظیر نوار، دیسک، کاست و گزارش‌های چاپ شده، باید کنترل شده باشد.

**4-6-6-2** دور انداختن محیط‌های ذخیره[1]

محیط‌های ذخیره‌ای که دیگر مورد نیاز نیستند، باید بصورت امن و محافظت‌شده دور ریخته شوند.

**4-6-6-3** روال‌های جابجایی اطلاعات

به منظور حفاظت اطلاعات در مقابل استفاده نابجا و غیرمجاز باید، روال‌هایی جهت جابجایی و انبار کردن (محیط‌های ذخیره) اطلاعات ایجاد شود.

**4-6-6-4** حفاظت از مستندات سیستم

مستندات سیستم، باید از دسترسی غیرمجاز محافظت گردند.

**4-6-7** تبادل اطلاعات و نرم‌افزار

| |
|---|
| **مقصود :** جلوگیری از گم شدن، تغییر یا استفاده نابجا از اطلاعات مبادله شده بین سازمان‌ها است. |

**4-6-7-1** توافق‌نامه‌های تبادل اطلاعات و نرم‌افزار

چه برای تبادل دستی و چه برای تبادل الکترونیکی اطلاعات و نرم‌افزار بین سازمان‌ها، باید توافق‌نامه‌هایی که می‌توانند رسمی باشند، تهیه گردند.

**4-6-7-2** حفاظت محیط‌های ذخیره در حال حمل و نقل

محیط ذخیره‌ای که جابه‌جا می‌شود باید از دسترسی غیرمجاز، صدمه یا استفادهٔ نابجا حفاظت گردد.

**4-6-7-3** حفاظت تجارت الکترونیکی

1. Media

تجارت الکترونیکی، باید در مقابل فعالیت‌های غیرقانونی، آشکارسازی یا تغییر در اطلاعات آن، محافظت شود.

**4-6-7-4** حفاظت از پست الکترونیکی

برای استفاده از پست الکترونیکی، باید سیاست ویژه‌ای تدوین گردد و کنترل‌های لازم برای کاهش مخاطرات حفاظتی آن صورت گیرد.

**5-6-7-4** حفاظت سیستم‌های دفتری الکترونیکی

برای حفاظت از سیستم‌های دفتری الکترونیکی و کنترل مخاطرات همراه با سیستم‌های الکترونیکی، باید سیاست‌ها و رهنمودهای معینی پیاده شوند.

**6-6-7-4** سیستم‌های در دسترس عموم

قبل از اینکه اطلاعات به طور عمومی در دسترس قرار بگیرند باید، یک فرآیند رسمی برای مجازسازی وجود داشته باشد و حفاظت‌های مربوط برای یکپارچگی و تغییر نکردن اطلاعات آن صورت بگیرد.

**7-6-7-4** شکل‌های دیگر مبادله اطلاعات

به منظور حفاظت تبادل اطلاعات در هنگام بکارگیری صوت، فاکس و امکانات ارتباطی ویدئویی باید، رویه‌ها و کنترل‌هایی تعبیه گردد.

## 7-4 کنترل دسترسی[1]

**1-7-4** الزامات سازمانی برای کنترل دسترسی

| |
|---|
| **مقصود :** کنترل کردن دسترسی به اطلاعات است. |

1 . Access control

**4-7-1-1** سیاست کنترل دسترسی

الزامات سازمانی برای کنترل دسترسی، باید به خوبی تعریف و مستند شوند و دسترسی، باید به آنچه که سیاست کنترل و دسترسی تعریف کرده است، محدود شود.

**4-7-2** مدیریت دسترسی کاربر

| |
|---|
| **مقصود :** جلوگیری از دسترسی غیرمجاز به سیستم‌های اطلاعاتی است. |

**4-7-2-1** ثبت نام کاربر

برای ثبت نام و حذف کاربران، به منظور دسترسی به همهٔ سیستم‌های اطلاعاتی چند کاربره و سرویس‌های آنها، باید روال‌هایی رسمی وجود داشته باشد.

**4-7-2-2** مدیریت اختیارات ویژه

اختصاص و استفاده از اختیارات ویژه باید محدود و کنترل شده باشد.

**4-7-2-3** مدیریت کلمهٔ عبور کاربر

اختصاص کلمات عبور به کاربران، باید کنترل شده و بر اساس یک فرایند مدیریت رسمی صورت گیرد.

**4-7-2-4** بازنگری حق دسترسی کاربر

یک فرایند رسمی به طور منظم و در فواصل زمانی مناسب، باید حق دسترسی کاربران را مرور ودر صورت لزوم بازنگری نماید.

**4-7-3** مسئولیت‌های کاربر

| |
|---|
| **مقصود:** جلوگیری از دسترسی کاربر غیرمجاز است. |

**4-7-3-1** استفادهٔ کلمهٔ عبور

کاربران، باید در انتخاب و استفاده از کلمهٔ عبور نهایت دقت را بنمایند.

**4-7-3-2** تجهیزات بدون مسئول مستقیم

کاربران، باید از حفاظت تجهیزات بدون مسئول مستقیم اطمینان داشته باشند.

**4-7-4** کنترل دسترسی شبکه

| |
|---|
| **مقصود :** حفاظت از خدمات شبکه‌ای است. |

**4-7-4-1** سیاست استفاده از خدمات شبکه

کاربران، باید فقط بطور مستقیم به خدماتی که برای آنها مجاز است، دسترسی داشته باشند.

**4-7-4-2** مسیر تأکید شده

مسیر پایانه کاربر تا رایانه سرویس‌دهنده، باید کنترل شده باشد.

**4-7-4-3** تصدیق اصالت کاربر برای ارتباطات از بیرون

دسترسی برای کاربران راه‌دور، باید بخشی از روال شناسایی و تصدیق اصالت باشد.

**4-7-4-4** تصدیق اصالت گره

اتصال به سیستم‌های رایانه‌ای راه‌دور، باید تصدیق اصالت شده باشند.

**4-7-4-5** حفاظت از پورت‌های عیب‌یابی از راه‌دور

دسترسی به پورت‌هایی که برای عیب‌یابی از راه‌دور استفاده می‌شوند، باید کنترل شده باشد.

**4-7-4-6** جداسازی در شبکه‌ها

در شبکه‌ها، کنترل‌هایی برای گروه‌های مختلف خدمات اطلاعاتی، کاربران و سیستمهای اطلاعاتی باید تعریف شوند.

**4-7-4-7** کنترل اتصال شبکه

ظرفیت اتصال کاربران در شبکه‌های اشتراکی، بر اساس سیاست کنترل دسترسی (4-7-1-1)، باید محدود شود.

**4-7-4-8** کنترل مسیریابی شبکه

شبکه‌های مشترک باید دارای کنترل مسیریابی باشند تا اطمینان حاصل شود که ارتباط رایانه‌ها و جریان اطلاعات در آنها، سیاست کنترل دسترسی به سیستم‌های کاربردی برای سازمان را که در 4-7-1-1 تعیین شده است، نقض نمی‌نماید.

**4-7-4-9** حفاظت از خدمات شبکه

یک توصیف شفاف از خواص حفاظتی همهٔ خدمات شبکهٔ مورد استفاده توسط سازمان، باید تهیه شود.

**4-7-5** کنترل دسترسی به سیستم عامل

| |
|---|
| **مقصود :** جلوگیری از دسترسی غیرمجاز به رایانه است. |

**4-7-5-1** شناسایی خودکار پایانه

به منظور تصدیق اصالت اتصالات در محل‌های معین و تجهیزات قابل حمل باید، شناسایی خودکار پایانه صورت گیرد.

**4-7-5-2** روال‌های ورود پایانه

دسترسی به خدمات اطلاعاتی، باید با استفاده از یک فرایند ورود (آغاز به کار) امن صورت گیرد.

**4-7-5-3** شناسایی و تصدیق اصالت کاربر

همه کاربران برای فعالیت‌هایشان، باید دارای یک شناسه منحصر به فرد (شناسه کاربر) باشند، که مخصوص خودشان باشد و از طریق آن بتوان افراد مسئول را ردیابی کرد.

**4-7-5-4** سیستم مدیریت کلمهٔ عبور

یک سیستم مدیریت کلمهٔ عبور که بتواند به طور مؤثر و متعامل از کیفیت کلمهٔ عبور اطمینان حاصل نماید، باید به وجود بیاید.

**4-7-5-5** استفاده از برنامه‌های کمکی سیستم [1]

استفاده از برنامه‌های کمکی سیستم، باید به دقت کنترل و محدود شده باشد.

**4-7-5-6** هشدار اضطرار برای ایمن کردن کاربران

برای کاربرانی که ممکن است تحت فشار قرار گیرند، باید، هشدارهای لازم تهیه شود.

**4-7-5-7** خروج زمانی پایانه [2]

به منظور جلوگیری از دسترسی افراد غیرمجاز، ارتباط پایانه‌هایی که در محل‌های با مخاطره بالا هستند، یا سیستم‌های پر مخاطره توسط آنها اجرا می‌شود چنانچه در یک بازه زمانی تعریف شده غیر فعال باشند، باید به‌صورت خودکار قطع شود.

**4-7-5-8** محدودیت زمان اتصال

به منظور اعمال حفاظت اضافی در استفاده از کاربردهای پر مخاطره، باید محدودیت‌هایی در زمان اتصال در نظر گرفته شود.

1. System Utilities
2. Terminal Time-out

### 4-7-6 کنترل دسترسی به برنامه‌های کاربردی

| |
|---|
| **مقصود :** جلوگیری از دسترسی غیرمجاز به اطلاعات نگهداری شده در سیستم‌های اطلاعاتی است. |

#### 4-7-6-1 محدودیت دسترسی به اطلاعات

دسترسی به اطلاعات و سیستم کاربردی، باید بر اساس با سیاست تعریف شده کنترل دسترسی (4-7-1-1)، محدود شود.

#### 4-7-6-2 مجزا سازی سیستم‌های حساس

سیستم‌های حساس، باید یک محیط اختصاصی و مجزای محاسباتی داشته باشند.

### 4-7-7 نظارت بر دسترسی و استفاده سیستم

| |
|---|
| **مقصود :** شناسایی فعالیت‌های غیرمجاز است. |

#### 4-7-7-1 ثبت وقایع

وقایع به ویژه استثنایی، باید برای یک مدت مورد توافق، ثبت و نگهداری شوند تا در رسیدگی‌های آتی جهت نظارت بر کنترل دسترسی استفاده شوند.

#### 4-7-7-2 نظارت بر استفاده از سیستم

به منظور نظارت بر استفاده از امکانات پردازش اطلاعات باید روال‌هایی ایجاد شود و نتیجه‌های آن، به صورت منظم مرور شود.

#### 4-7-7-3 همزمانی ساعت

ساعت رایانه‌ها، باید به منظور ثبت دقیق وقایع همزمان باشند.

### 4-7-8 محاسبه سیار و کار از راه دور

| |
|---|
| **مقصود :** اطمینان از حفاظت اطلاعات در مواقعی که از امکانات پردازش سیار و از راه دور استفاده می‌شود. |

#### 4-7-8-1 پردازش سیار

کنترل‌های مربوطه، برای مقابله با مخاطرات کار با امکانات محاسبه سیار، به ویژه در محیط‌های غیر حفاظت شده، بایستی پذیرفته شوند و یک سیاست رسمی تدوین شود.

**4-7-8-2** کار از راه دور

به منظور کنترل و مجازسازی در فعالیت‌های راه‌دور، باید سیاست‌ها و روال‌هایی تدوین و اجرا گردند.

## 4-8 توسعه و نگهداری سیستم‌ها[1]

### 4-8-1 الزامات حفاظتی سیستم‌ها

| |
|---|
| **مقصود :** اطمینان از حفاظت قرار داده شده در سیستم‌های اطلاعاتی است. |

**4-8-1-1** تحلیل و تعیین الزامات حفاظتی

نیازمندی‌های سازمان به سیستم‌های جدید یا گسترش سیستم‌های موجود، باید حاوی الزامات کنترلی باشد.

### 4-8-2- حفاظت در سیستم‌های کاربردی

| |
|---|
| **مقصود :** جلوگیری از فقدان، تغییر یا استفاده نادرست کاربر از داده در سیستم‌های کاربردی است. |

**4-8-2-1-** تأیید داده ورودی

صحت و تناسب داده ورودی سیستم‌های کاربردی، باید تأیید شوند.

**4-8-2-2** کنترل حین پردازش

برای تأیید و قابل قبول بودن داده‌های پردازش شده، باید کنترل‌هایی در سیستم‌ها تعبیه شود تا انحراف تشخیص داده شود.

**4-8-2-3** تصدیق اصالت پیام

برای برنامه‌های کاربردی که نیاز به حفاظت از یکپارچگی محتویات پیام دارند، باید تصدیق اصالت پیام صورت گیرد.

**4-8-2-4** تأیید داده‌های خروجی

برای اطمینان از اینکه پردازش اطلاعات ذخیره شده، صحیح و متناسب با شرایط بوده، باید خروجی سیستم‌های کاربردی مورد تأیید قرار گیرند.

**4-8-3** کنترل‌های رمزنگاری

1 . Systems development and maintenance

| |
|---|
| **مقصود :** محافظت از محرمانه بودن، تصدیق اصالت یا یکپارچگی اطلاعات است. |

**4-8-3-1** سیاست استفاده از کنترل‌های رمزنگاری

برای حفاظت اطلاعات، باید سیاستی در جهت استفاده از کنترل‌های رمزنگاری، تدوین و از آن پیروی گردد.

**4-8-3-2** رمزگذاری

برای حفاظت از اطلاعات حساس و مهم، باید رمزگذاری صورت گیرد.

**4-8-3-3** امضاء رقومی[1]

به منظور حفاظت از تصدیق اصالت، مجازسازی و یکپارچگی اطلاعات الکترونیکی، باید امضاءهای رقومی به کار برده شوند.

**4-8-3-4** خدمات غیرقابل انکار [2]

به منظور حل اختلافات در مورد وقوع یا عدم وقوع یک رویداد یا عمل، باید خدمات غیرقابل انکار مورد استفاده قرار گیرند.

**4-8-3-5** مدیریت کلید

به منظور پشتیبانی از روش‌های رمزنگاری، باید یک سیستم مدیریت کلید، بر طبق مجموعه استانداردها، روال‌ها و روش‌های مورد توافق، پیاده شود.

**4-8-4** حفاظت از پرونده‌های سیستم

| |
|---|
| **مقصود :** اطمینان از اینکه پروژه‌های فناوری اطلاعات و فعالیت‌های پشتیبانی آن، بوسیله یک روش امن انجام گردند. (امنیت در تمام مسیر روش انجام پروژه). |

**4-8-4-1** کنترل نرم‌افزار عملیاتی

در بکارگیری نرم‌افزار، در سیستم‌های عملیاتی، باید کنترل صورت گیرد.

**4-8-4-2** حفاظت از داده‌های آزمایش سیستم

داده‌های آزمایش سیستم، باید کنترل و محافظت شوند.

**4-8-4-3** کنترل دسترسی به کتابخانه منبع برنامه‌ها[3]

1. Digital
2. Non-repudiation
3. Program Source

برای دسترسی به کتابخانه منبع برنامه‌ها، باید کنترل شدیدی صورت گیرد.

### 4-8-5 حفاظت در فرایندهای توسعه و پشتیبانی

**مقصود :** نگهداری و حفاظت از اطلاعات و نرم‌افزار سیستم کاربردی است.

#### 4-8-5-1 روال‌های کنترل تغییر

پیاده‌سازی تغییرات، باید دقیقاً بوسیله استفاده از روال‌های رسمی کنترل تغییر، کنترل شوند تا میزان اتفاقات ناخواسته سیستم‌های اطلاعاتی کمینه گردد.

#### 4-8-5-2 مرور فنی تغییرات سیستم عامل

در هنگام وقوع تغییرات، باید سیستم‌های کاربردی مرور و آزمایش شوند.

#### 4-8-5-3 محدودیت‌هایی روی تغییرات در بسته‌های نرم‌افزاری

از اصلاحات روی بسته‌های نرم‌افزاری، باید اجتناب شده و تغییرات اساسی باید شدیداً کنترل شوند.

#### 4-8-5-4 کانال‌های مخفی و کد تروا[1]

خرید، استفاده و اصلاح نرم‌افزارها، باید در مقابل هرگونه احتمال وجود کانال‌های مخفی و کد تروا کنترل شوند.

#### 4-8-5-5 توسعه نرم‌افزار توسط شخص ثالث

برای اطمینان از توسعه نرم‌افزار توسط شخص ثالث، باید کنترل‌هایی صورت گیرد.

## 4-9 مدیریت تداوم فعالیت[2]

### 4-9-1 جنبه‌های مدیریت تداوم فعالیت

**مقصود :** بی‌اثر کردن وقفه‌های فعالیت‌های سازمان و حفاظت از فرایندهای مهم سازمان در مقابل اثرات ناشی از خرابی‌ها یا بلاها است.

1. Trojan Code
2. Business continuity management

**4-9-1-1** فرایند مدیریت تداوم فعالیت

برای توسعه و نگهداری تداوم فعالیت در سازمان، باید یک فرایند مدیریت شده وجود داشته باشد.

**4-9-1-2** تداوم فعالیت و تحلیل موانع

به منظور تداوم فعالیت، باید یک برنامهٔ راهبردی متناسب با برآورد مخاطره، مناسب برای کلیهٔ فعالیت‌ها ایجاد شود.

**4-9-1-3** تدوین و پیاده‌سازی طرح‌های لازم جهت حفظ تداوم در روال کارها

به منظور نگهداری یا ازسرگیری فعالیت‌های کاری عادی سازمان در یک زمان مطلوب، پس از بروز وقفه و یا خرابی در کارهای بحرانی باید طرح‌هایی تدوین گردد.

**4-9-1-4** چارچوب طراحی تداوم فعالیت

یک چارچوب واحد از طرح‌های تداوم فعالیت باید ایجاد و نگهداری شود تا اطمینان حاصل گردد همهٔ طرح‌ها فراگیر بوده و حاوی اولویت‌های آزمایش و نگهداری هستند.

**4-9-1-5** آزمایش، نگهداری و ارزیابی دوباره طرح‌های تداوم فعالیت

طرح‌های تداوم فعالیت، باید به طور منظم آزمایش و نگهداری شوند، به طوری که همواره اطمینان از به روز بودن و مؤثر بودن آنها وجود داشته باشد.

## 4-10 سازگاری[1]

**4-10-1** سازگاری با الزامات قانونی

| |
|---|
| **مقصود :** اجتناب از نقض قوانین مدنی و جنایی و التزام به معاهدات قوانین و قواعد حفاظتی است. |

**4-10-1-1** شناسایی قوانین مرتبط

همهٔ الزامات قانونی و قراردادی مرتبط، برای هر سیستم اطلاعاتی، باید به طور شفاف تعریف و مستند شده باشد.

**4-10-1-2** حقوق دارائی‌های فکری

برای اطمینان از سازگاری با محدودیت‌های قانونی حقوق دارایی‌های فکری و استفادهٔ صحیح از محصولات نرم‌افزاری، باید روال‌های مناسب پیاده شوند.

**4-10-1-3** حفاظت از مدارک و سوابق سازمانی

1 . Compliance

مدارک و سوابق مهم سازمان باید از گم شدن، خرابی یا استفاده نادرست حفاظت شوند.

**4-1-10-4** حفاظت داده و محرمانه بودن اطلاعات کارکنان

به منظور حفاظت از اطلاعات شخصی مطابق با قوانین و مقررات مربوطه، باید کنترل‌هایی صورت گیرد.

**5-1-10-4** جلوگیری از استفاده نادرست از امکانات پردازش اطلاعات

استفاده از امکانات پردازش اطلاعات بایستی با اجازه مدیر باشد و کنترل‌های لازم برای جلوگیری از استفاده نادرست از این امکانات باید صورت گیرد.

**6-1-10-4** مقررات حاکم بر رمزنگاری

برای اطمینان از سازگاری با قوانین رمزنگاری ملی و دیگر قوانین و مقررات، باید کنترل‌های لازم صورت گیرد.

**7-1-10-4** جمع‌آوری مدرک

به منظور ارائه به مراجع ذیصلاح در محاکم دعاوی سازمان، باید مدرک لازم در تمام زمینه‌ها براساس استانداردها جمع‌آوری و نگهداری شده باشد.

**2-10-4** مرور سیاست حفاظتی و سازگاری فنی

**مقصود :** اطمینان از سازگاری سیستم‌ها با سیاست‌های حفاظتی سازمان و استانداردهای مربوط است.

**1-2-10-4** سازگاری با سیاست حفاظت

مدیران باید اطمینان کسب کنند که روال‌های حفاظتی متناسب با مسئولیت‌ها، به درستی اجرا می‌شوند و بازنگری‌های لازم بر طبق سیاست و استانداردها، به طور مداوم صورت می‌گیرد.

**2-2-10-4** کنترل سازگاری فنی

برای سازگاری با استانداردهای پیاده‌سازی حفاظت باید سیستم‌های اطلاعاتی به طور منظم، کنترل شوند.

### 4-10-3 ملاحظات ممیزی[1] سیستم

| |
|---|
| **مقصود :** بیشینه کردن تأثیرپذیری و کاهش تداخل در فرایند ممیزی سیستم است. |

#### 4-10-3-1 کنترل‌های ممیزی سیستم

ممیزی‌های سیستم‌های عملیاتی، باید بر اساس برنامه و توافق‌های انجام شده برای کاهش وقفه در فعالیت‌های سازمان، صورت بگیرد.

#### 4-10-3-2 حفاظت از ابزارهای ممیزی سیستم

به منظور استفاده نادرست یا مصالحه، دسترسی به ابزارهای ممیزی سیستم، باید کنترل شوند.

1. Audit

## واژه‌نامه لاتین

| | |
|---|---|
| Acceptance | پذیرش |
| Access Control | کنترل دسترسی |
| Allocation | تخصیص |
| Areas of risk | نواحی مخاطره |
| Asset | دارایی |
| Authentication | تصدیق اصالت |
| Authorization | مجازسازی |
| Business | فعالیت (تجارت) |
| Classification | طبقه‌بندی |
| Clear desk | میز پاک |
| Communication | ارتباطات |
| Compliance | سازگاری |
| Computing | محاسبه |
| Continuity | تداوم |
| Control objectives | هدف‌های کنترل |
| Cryptography | علم رمزنگاری |
| Degree of assurance | درجه اطمینان |
| Detailed Control | کنترل‌های همه جانبه |
| Disciplinary | انضباطی |
| Documentation | مستندسازی |
| Duty | وظیفه |
| Encryption | رمزگذاری |
| Enforced | تأکید شده |
| Environmental | محیطی |

| | |
|---|---|
| Events | وقایع/ رویدادها |
| Evidence | مدرک |
| Framework | چارچوب |
| General | عمومی |
| Guidelines | رهنمود |
| Handling | بکار بردن |
| Housekeeping | اداره کردن |
| Implementation | پیاده‌سازی |
| Incidents | حوادث |
| Information Security Management System (ISMS) | سیستم مدیریت حفاظت اطلاعات |
| Labelling | علامت گذاری |
| Log | سابقه |
| Log – on | ورود (آغاز به کار) |
| Malfunctions | اشتباهات |
| Malicious | مخرب |
| Media | محیط ذخیره |
| Mobile | سیار |
| Monitoring | نظارت |
| Network | شبکه |
| Non – repudiation | غیرقابل انکار |
| Operation | عملیات |
| Password | کلمه عبور |
| Personel | کارکنان |
| Physical | فیزیکی |
| Policy | سیاست |
| Privilege | اختیارات ویژه |

| | |
|---|---|
| Procedure | روال |
| Process | فرآیند |
| Processing | پردازش |
| Record | ثبت |
| Registration | نام نویسی |
| Requirements | الزامات |
| Responsibility | مسئولیت |
| Risk management | مدیریت مخاطره |
| Scope | دامنه |
| Screen | صفحه |
| Security Oraganization | سازمان حفاظت |
| Select | انتخاب |
| Statement | دستورالعمل |
| Synchronization | همزمانی |
| Teleworking | کار از راه دور |
| Terminal | پایانه |
| Third party | شخص ثالث |
| Time out | زمان خروج |
| Trojan | تروا |
| Undertake | پذیرفتن |

## واژه‌نامه فارسی

| | |
|---|---|
| Privilege | اختیارات ویژه |
| Housekeeping | اداره کردن |
| Communication | ارتباطات |
| Malfunctions | اشتباهات |
| Select | انتخاب |
| Disciplinary | انضباطی |
| Handling | بکار بردن |
| Terminal | پایانه |
| Acceptance | پذیرش |
| Undertake | پذیرفتن |
| Processing | پردازش |
| Implementation | پیاده‌سازی |
| Enforced | تأکید شده |
| Allocation | تخصیص |
| Continuity | تداوم |
| Trojan | تروا |
| Authentication | تصدیق اصالت |
| Record | ثبت |
| Framework | چارچوب |
| Incidents | حوادث |
| Asset | دارایی |
| Scope | دامنه |
| Degree of assurance | درجه اطمینان |

| | |
|---|---|
| Statement | دستورالعمل |
| Encryption | رمزگذاری |
| Procedure | روال |
| Guidelines | رهنمود |
| Requirements | الزامات |
| Time out | زمان خروج |
| Log | سابقه |
| Compliance | سازگاری |
| Security Oraganization | سازمان حفاظت |
| Mobile | سیار |
| Policy | سیاست |
| Information Security Management System (ISMS) | سیستم مدیریت حفاظت اطلاعات |
| Network | شبکه |
| Third party | شخص ثالث |
| Screen | صفحه |
| Classification | طبقه‌بندی |
| Labelling | علامت گذاری |
| Cryptography | علم رمزنگاری |
| Operation | عملیات |
| General | عمومی |
| Non – repudiation | غیرقابل انکار |
| Process | فرآیند |
| Business | فعالیت (تجارت) |
| Physical | فیزیکی |
| Teleworking | کار از راه دور |
| Personel | کارکنان |

| | |
|---|---|
| Password | کلمه عبور |
| Access Control | کنترل دسترسی |
| Detailed Control | کنترل‌های همه جانبه |
| Authorization | مجازسازی |
| Computing | محاسبه |
| Media | محیط ذخیره |
| Environmental | محیطی |
| Malicious | مخرب |
| Evidence | مدرک |
| Risk management | مدیریت مخاطره |
| Responsibility | مسئولیت |
| Documentation | مستندسازی |
| Clear desk | میز پاک |
| Registration | نام نویسی |
| Monitoring | نظارت |
| Areas of risk | نواحی مخاطره |
| Log – on | ورود (آغاز به کار) |
| Duty | وظیفه |
| Events | وقایع/ رویدارها |
| Control objectives | هدف‌های کنترل |
| Synchronization | همزمانی |