

بسمه تعالی

# پیاده‌سازی سیستم‌های مدیریت امنیت اطلاعات

مؤلف :

محمد علی ترکمانی

انتشارات ارسطو (چاپ و نشر ایران)

1394

شابک : 978-600-7558-50-8

شماره کتابشناسی ملی : ۳۷۶۶۴۴۰

عنوان و نام پدیدآور : پیاده‌سازی سیستمهای مدیریت امنیت

اطلاعات : راهنمای کامل اخذ گواهینامه... ISO 27000

مشخصات نشر : مشهد: ارسطو، ۱۳۹۴.

مشخصات ظاهری : ۲۰۲ص.: مصور، جدول، نمودار. : ۱۷×۲۴س.م.

یادداشت : این مدرک در آدرس <http://opac.nlai.ir> قابل

دسترسی است.

سرشناسه : ترکمانی، محمدعلی، ۱۳۵۴-

وضعیت فهرست نویسی : فیپای مختصر

نام کتاب : پیاده‌سازی سیستم های مدیریت امنیت اطلاعات

مولف : محمد علی ترکمانی

ناشر : ارسطو ( با همکاری سامانه اطلاع رسانی چاپ و نشر ایران )

صفحه آرایي ، تنظيم و طرح جلد : پروانه مهاجر

تیراژ : ۱۰۰۰ جلد

نوبت چاپ : اول - ۱۳۹۴

چاپ : مهتاب

قیمت : ۱۸۰۰۰ تومان

شابک : ۹۷۸ - ۶۰۰ - ۷۵۵۸ - ۵۰ - ۸

تلفن های مرکز بخش : ۳۵۰۹۶۱۴۵ - ۳۵۰۹۶۱۴۶ - ۳۵۱ - ۵۱

[www.chaponashr.ir](http://www.chaponashr.ir)

## فهرست مطالب

|                                                           |    |
|-----------------------------------------------------------|----|
| فصل اول: تعاریف و قراردادها                               | ۱۷ |
| ۱-۱- تعریف امنیت اطلاعات و سیستم امن                      | ۱۷ |
| ۱-۱-۱- سیستم امن                                          | ۱۷ |
| ۲-۱- اصطلاحات امنیتی                                      | ۱۸ |
| ۱-۲-۱- آسیب پذیری                                         | ۱۸ |
| ۲-۲-۱- حمله                                               | ۱۸ |
| ۳-۲-۱- تهدید                                              | ۱۸ |
| ۴-۲-۱- مفهوم AAA در امنیت اطلاعات                         | ۱۹ |
| ۳-۱- سرویس های امنیتی                                     | ۲۰ |
| ۴-۱- مکانیزم های امنیتی                                   | ۲۰ |
| ۵-۱- سیاست های امنیتی                                     | ۲۱ |
| ۱-۵-۱- سیاست های کلمه عبور                                | ۲۲ |
| ۲-۵-۱- سیاست های اینترنتی                                 | ۲۲ |
| ۳-۵-۱- پشتیبان گیری و احیای اطلاعات                       | ۲۳ |
| ۶-۱- مفهوم سیستم مدیریت امنیت اطلاعات                     | ۲۳ |
| ۷-۱- استانداردهای مدیریتی ارائه شده در خصوص امنیت اطلاعات | ۲۳ |
| ۸-۱- استانداردهای خانواده ISO27000                        | ۲۴ |
| ۹-۱- گزارش فنی ISO/IEC TR ۱۳۳۳۵                           | ۲۴ |
| ۱۰-۱- مراحل ایمن سازی براساس گزارش فنی ISO/IEC TR ۱۳۳۳۵   | ۲۵ |
| ۱۱-۱- مزایای پیاده سازی و صدور گواهینامه ایزو ۲۷۰۰۱       | ۲۶ |

۱۲-۱- مشکلات پیاده‌سازی I.S.M.S ..... ۲۶

۱۳-۱- مستندات I.S.M.S ..... ۲۷

۱۴-۱- سئوالات تشریحی ..... ۲۸

۱۵-۱- سئوالات چهارگزینه‌ای ..... ۲۸

..... پاسخ سئوالات ..... ۳۰

## فصل دوم: مدیریت ریسک ..... ۳۱

۱-۲- مقدمه ..... ۳۱

۲-۲- ارزیابی مدیریت و کاهش خطر ..... ۳۱

۱-۲-۲- مخاطره (ریسک) چیست؟ ..... ۳۲

۲-۲-۱۴- ریسک‌های مرتبط با امنیت اطلاعات ..... ۳۳

۳-۲- مراحل مدیریت مخاطرات ..... ۳۳

۱-۳-۲- شناسایی دارایی‌ها ..... ۳۳

۲-۳-۲- شناسایی تهدیدها ..... ۳۵

۳-۳-۲- شناسایی نقاط آسیب‌پذیری ..... ۳۶

۴-۳-۲- ارزیابی مخاطرات ..... ۳۷

۵-۳-۲- روش‌های مواجه شدن با ریسک‌ها ..... ۴۰

۴-۲- نحوه مقاوم سازی سیستم در برابر ریسک‌های احتمالی ..... ۴۲

۵-۲- عوامل موفقیت پروژه مدیریت خطرات امنیتی ..... ۴۳

۶-۲- رویکردهای متفاوت مدیریت خطرات امنیتی ..... ۴۵

۷-۲- حوزه های یازده گانه استاندارد ISO/IEC 17799:2005 ..... ۴۶

۸-۲- تمرین: پروژه NSC ..... ۴۶

۹-۲- سئوالات تشریحی ..... ۴۷

۴۸ ..... ۱۰-۲ سوالات چهارگزینه‌ای

۵۰ ..... پاسخ سوالات

## ۵۱ ..... فصل سوم: خط مشی امنیتی سازمان

۵۱ ..... ۱-۳ مقدمه

۵۱ ..... ۲-۳ خط مشی های امنیتی

۵۲ ..... ۱-۲-۳ اجزاء مستند خط مشی امنیت اطلاعات

۵۲ ..... ۲-۲-۳ جهت گیری و حمایت مدیران سازمان در خصوص تامین نیازمندی ها و

۵۳ ..... مقررات امنیت اطلاعات

۵۳ ..... ۲-۳-۳ مستند خط مشی امنیت اطلاعات و سیاست گذاری اطلاعات سازمان

۵۴ ..... ۲-۳-۴ بازنگری و ارزیابی خط مشی امنیت اطلاعات سازمان

۵۴ ..... ۳-۳ سوالات تشریحی

۵۵ ..... ۴-۳ سوالات چهارگزینه‌ای

۵۶ ..... پاسخ سوالات

## ۵۷ ..... فصل چهارم: سازماندهی امنیت اطلاعات

۵۷ ..... ۱-۴ مقدمه

۵۷ ..... ۲-۴ سازماندهی مدیریت امنیت اطلاعات در داخل سازمان

۵۸ ..... ۱-۲-۴ دبیرخانه مرکزی مدیریت امنیت اطلاعات

۵۹ ..... ۲-۲-۴ پابندی مدیریت سازمان به امنیت اطلاعات

۶۰ ..... ۲-۴-۳ ایجاد هماهنگی بین واحدهای تامین امنیت اطلاعات

۶۰ ..... ۲-۴-۴ تعیین و تخصیص مسئولیت های افراد مرتبط با امنیت اطلاعات

۶۰ ..... ۴-۲-۴ شرح وظائف و مسئولیت های کمیته راهبردی امنیت

۶۱ ..... ۴-۲-۴ شرح وظائف و مسئولیت های مدیر امنیت شبکه

|    |                                                                               |
|----|-------------------------------------------------------------------------------|
| ۶۱ | ۲-۴-۳-شرح وظایف و مسئولیت‌های واحد پشتیبانی امنیت                             |
| ۶۴ | ۲-۴-۴-شرح وظائف نظارت و بازرسی امنیتی                                         |
| ۶۵ | ۲-۴-۵-شرح وظائف مدیریت تغییرات                                                |
| ۶۶ | ۲-۴-۶-شرح وظائف نگهداری امنیت شبکه کامپیوتری                                  |
| ۶۶ | ۲-۵-مجوز دهی فرآیندهای مجاز برای پردازش اطلاعات                               |
| ۶۷ | ۲-۶-توافقنامه محرمانگی اطلاعات سازمان                                         |
| ۶۷ | ۲-۷-تامین ارتباط با مسئولین و بالاترین مقام سازمان                            |
| ۶۷ | ۲-۸-پشتیبانی ارتباط با گروه‌های مشاور مجامع تخصصی امنیت                       |
| ۶۸ | ۲-۹-بازنگری مستقل وضعیت امنیت اطلاعات سازمان ( مستقل از زمان بندی طراحی شده ) |
| ۶۸ | ۳-۴-سازماندهی مدیریت امنیت اطلاعات در تعاملات با طرف‌های خارج از سازمان       |
| ۶۸ | ۳-۱-شناسایی مخاطرات دسترسی طرف‌های خارج از سازمان                             |
| ۶۸ | ۳-۲-گام‌های تامین نیازمندی‌های امنیت اطلاعات مشتریان طرف‌های خارج از سازمان   |
| ۶۸ | ۳-۳-توجه به امنیت در قرارداد با طرف‌های خارج از سازمان                        |
| ۶۸ | ۴-سئوالات تشریحی                                                              |
| ۶۹ | ۵-سئوالات چهارگزینه‌ای                                                        |
| ۷۰ | پاسخ سئوالات                                                                  |
| ۷۱ | <b>فصل پنجم: مدیریت دارایی‌ها</b>                                             |
| ۷۱ | ۱-۵-مقدمه                                                                     |
| ۷۱ | ۲-۵-دستورالعمل تدوین راهنمای طبقه‌بندی اطلاعات                                |
| ۷۱ | ۲-۱-تعاریف                                                                    |
| ۷۲ | ۳-۵-نشانه‌گذاری (برچسب) و پشتیبانی از اطلاعات                                 |

۷۲ ..... ۴-۵- فهرست کلی اقدامات حفاظتی

۷۴ ..... ۵-۵- اصول حفاظتی

۷۶ ..... ۶-۵- سئوالات تشریحی

۷۶ ..... ۷-۵- سئوالات چهارگزینه‌ای

۷۷ ..... پاسخ سئوالات

## ۷۹ ..... فصل ششم: امنیت منابع انسانی

۷۹ ..... ۱-۶- لحاظ نمودن امنیت قبل از به کارگیری

۸۰ ..... ۲-۶- اطمینان از اطلاع کارکنان از مسئولیت‌ها و صلاحیت افراد برای انجام وظایف

۸۱ ..... ۳-۶- لحاظ نمودن امنیت در حین خدمت

۸۱ ..... ۱-۳-۶- مسئولیت مدیران

۸۱ ..... ۲-۳-۶- آگاهی‌رسانی کسب مهارت و آموزش امنیت

۸۱ ..... ۳-۳-۶- فرآیندهای انضباطی

۸۲ ..... ۴-۶- شیوه مناسب خاتمه دادن به همکاری کارکنان

۸۲ ..... ۵-۶- سئوالات تشریحی

۸۲ ..... ۶-۶- سئوالات چهارگزینه‌ای

۸۳ ..... پاسخ سئوالات

## ۸۵ ..... فصل هفتم: امنیت فیزیکی و محیط

۸۵ ..... ۱-۷- مقدمه

۸۵ ..... ۲-۷- جلوگیری از دسترسی فیزیکی غیرمجاز، خسارت و توقف فعالیت‌های سازمان

۸۵ ..... ۱-۲-۷- ایجاد محیط امن فیزیکی برای اطلاعات و سیستم‌های اطلاعاتی

۸۵ ..... ۲-۲-۷- کنترل تردد فیزیکی (ورود و خروج)

۸۶ ..... ۳-۲-۷- امن‌سازی دفاتر اتاق‌ها و تاسیسات

- ۸۶ ..... ۴-۲-۷-محافظت در مقابل تهدیدات محیطی و خارج
- ۸۷ ..... ۵-۲-۷-کار در محیط امن
- ۸۷ ..... ۶-۲-۷-جداسازی فضاهای دسترسی عمومی تخلیه، بارگیری و ارسال و دریافت
- ۳-۷-پیشگیری از صدمه خسارت دزدی یا لو رفتن دارایی‌های سازمان و توقف در فعالیت‌های سازمان. ۸۸
- ۸۸ ..... ۱-۳-۷-تجهیزات
- ۸۸ ..... ۱-۳-۷-۱-۱-میز کار
- ۸۸ ..... ۱-۳-۷-۲-ابزارهای قابل حمل (Portabe)
- ۸۹ ..... ۲-۳-۷-امکانات پشتیبانی (منابع تغذیه)
- ۹۰ ..... ۳-۳-۷-امنیت کابل کشی
- ۹۱ ..... ۴-۳-۷-نگهداری از تجهیزات
- ۹۱ ..... ۵-۳-۷-امنیت تجهیزات خارج از محل‌های اصلی
- ۹۱ ..... ۶-۳-۷-اسقاط یا استفاده مجدد از تجهیزات
- ۹۲ ..... ۶-۳-۷-۱-خط‌مشی اسقاط یا استفاده مجدد از تجهیزات
- ۹۳ ..... ۷-۳-۷-راه‌های خروج تجهیزات از سازمان
- ۹۳ ..... ۴-۷-سئوالات تشریحی
- ۹۳ ..... ۵-۷-سئوالات چهارگزینه‌ای
- ۹۴ ..... پاسخ سئوالات

## ۹۵ ..... فصل هشتم: مدیریت عملیات و ارتباطات

- ۹۵ ..... ۱-۸-مقدمه
- ۹۵ ..... ۲-۸-اطمینان از عملکرد صحیح و امن امکانات پردازش اطلاعات
- ۳-۸-پیاده سازی و نگهداری سطح مناسب امنیت اطلاعات و سرویس‌های تحویلی منطبق با توافقنامه ..... ۹۶

- ۸-۳-۱-ارائه خدمات مورد نیاز ..... ۹۶
- ۸-۳-۲-نظارت و بازنگری در نحوه ارائه خدمات ..... ۹۶
- ۸-۳-۳-مدیریت تغییرات در ارائه خدمات ..... ۹۶
- ۸-۴-۴-به حداقل رساندن خرابی سیستم(طراحی و تست قبولی سیستم) ..... ۹۶
- ۸-۴-۱-مدیریت ظرفیت ..... ۹۶
- ۸-۴-۲-پذیرش سیستم ..... ۹۷
- ۸-۵-۵-محافظت از صحت اطلاعات و نرم افزارها در مقابل نرم افزارهای نفوذگر ..... ۹۷
- ۸-۵-۱-کنترل در مقابل کدهای مخرب ، نفوذگر و موبایل ..... ۹۷
- ۸-۵-۲-کنترل در مقابل کدهای متحرک ..... ۹۸
- ۸-۶-۶-مدیریت نسخه های پشتیبان انجام شود به منظور صحت و دسترسی پذیری اطلاعات و امکانات پردازش اطلاعات ( سیستم گردانی ) ..... ۹۸
- ۸-۶-۱-تهیه نسخه پشتیبان از اطلاعات ..... ۹۸
- ۸-۶-۱-نگهداری از نسخه پشتیبان ..... ۹۹
- ۸-۷-۷-اطمینان از امنیت اطلاعات در شبکه های کامپیوتری و امنیت زیر ساخت شبکه کامپیوتری ..... ۹۹
- ۸-۷-۱-مکانیزهای کنترل شبکه کامپیوتری ..... ۹۹
- ۸-۷-۲-امنیت در سرویس های شبکه ..... ۹۹
- ۸-۸-۸-اطمینان از عدم لو رفتن، تغییر یا انهدام سرمایه ها و یا توقف در فعالیتهای سازمان. ۱۰۰
- ۸-۹-۹-تامین امنیت مبادله اطلاعات و نرم افزارها در داخل سازمان یا بین سازمان ها. ۱۰۰
- ۸-۹-۱-پیمان نامه ها، رویه ها و سیاست های مبادله اطلاعات ..... ۱۰۰
- ۸-۹-۲-قرارداد مبادله اطلاعات ..... ۱۰۰
- ۸-۹-۳-محیط فیزیکی در انتقال ..... ۱۰۰

۸-۹-۴- مدیریت امنیت پست الکترونیک، سیستم اتوماسیون اداری و سیستم‌های

اطلاعات M.I.S ..... ۱۰۱

۸-۱۰-۱- اطمینان از امنیت در سرویس‌های تجارت الکترونیک و استفاده امن از آنها ..... ۱۰۱

۸-۱۱-۱- تشخیص فعالیت‌های غیرمجاز پردازش اطلاعات ..... ۱۰۱

۸-۱۱-۱- نظارت بر ثبت وقایع ..... ۱۰۲

۸-۱۱-۲- استفاده از سیستم‌های مانیتورینگ ..... ۱۰۲

۸-۱۱-۳- محافظت از اطلاعات log ..... ۱۰۴

۸-۱۱-۴- ثبت عملکرد مدیران و اپراتورهای سیستم‌ها ..... ۱۰۴

۸-۱۱-۵- ثبت خطاها ..... ۱۰۴

۸-۱۱-۶- هم زمان نمودن ساعت سیستم‌ها ..... ۱۰۴

۸-۱۲- سئوالات تشریحی ..... ۱۰۴

۸-۱۳- سئوالات چهارگزینه‌ای ..... ۱۰۵

پاسخ سئوالات ..... ۱۰۶

## فصل نهم: کنترل دسترسی ..... ۱۰۷

۹-۱- نیازهای دسترسی کنترل دسترسی به اطلاعات ..... ۱۰۷

۹-۱-۱- سیاست‌گذاری و خط‌مشی کنترل دسترسی ..... ۱۰۷

۹-۲- اطمینان از دسترسی مجاز به اطلاعات و سیستم‌ها ..... ۱۰۷

۹-۳- پیشگیری از دسترسی کاربران غیرمجاز ..... ۱۰۸

۹-۳-۱- خط‌مشی پیشگیری از دسترسی کاربران غیرمجاز ..... ۱۰۸

۹-۳-۱-۱- استفاده از رمز عبور ..... ۱۰۸

۹-۳-۲- تجهیزات رها شده و بدون مراقبت توسط کاربر ..... ۱۰۹

۹-۳-۳- سیاست نمایشگر پاک و میز پاک ..... ۱۱۰

- ۱۱۰ ..... ۱-۳-۳-۹ خطمشی نمایشگر پاک
- ۱۱۱ ..... ۴-۹- پیشگیری از دسترسی غیرمجاز به سرویس‌های شبکه
- ۱۱۱ ..... ۵-۹- پیشگیری از دسترسی غیرمجاز به سیستم عامل‌ها
- ۱۱۲ ..... ۶-۹- پیشگیری از دسترسی غیرمجاز به اطلاعات داخل سیستم‌های اطلاعاتی
- ۱۱۲ ..... ۶-۹- محدودیت دسترسی به اطلاعات سیستم
- ۱۱۲ ..... ۶-۹- جداسازی اطلاعات سیستم‌های حساس
- ۱۱۳ ..... ۷-۹- اطمینان از امنیت اطلاعات در زمان استفاده از کامپیوترهای قابل حمل
- ۱۱۳ ..... ۷-۹- ارتباط کامپیوترهای قابل حمل
- ۱۱۳ ..... ۷-۹- کار از راه دور
- ۱۱۳ ..... ۸-۹- سئوالات تشریحی
- ۱۱۴ ..... ۹-۹- سئوالات چهارگزینه‌ای
- ۱۱۵ ..... پاسخ سئوالات
- ۱۱۷ ..... فصل دهم: تهیه، توسعه و نگهداری سیستم**
- ۱۱۷ ..... ۱-۱۰- اطمینان از امنیت سیستم‌های اطلاعاتی
- ۱۱۷ ..... ۲-۱۰- پیشگیری از خطاها؛ تغییر یا سوء استفاده از اصلاحات نرم افزارهای کاربردی
- ۱۱۷ ..... ۳-۱۰- تأمین محرمانگی، اصالت و صحت اطلاعات
- ۱۱۷ ..... ۱-۳-۱۰- سیاست استفاده از مکانیزم کنترل‌های رمزنگاری
- ۱۱۸ ..... ۲-۳-۱۰- مدیریت کلید
- ۱۱۸ ..... ۳-۳-۱۰- امضاء الکترونیکی (دیجیتال)
- ۱۱۸ ..... ۱-۳-۳-۱۰- حملات ممکن علیه امضای دیجیتالی
- ۱۱۹ ..... ۴-۱۰- اطمینان از امنیت نرم افزارهای کاربردی
- ۱۱۹ ..... ۵-۱۰- تداوم امنیت اطلاعات و سیستم‌های عملیاتی

۱۰-۶- کاهش مخاطرات ناشی از بهره‌برداری از آسیب‌پذیری‌های فنی منتشر شده. .... ۱۱۹

۱۰-۷- سئوالات تشریحی ..... ۱۱۹

۱۰-۸- سئوالات چهارگزینه‌ای ..... ۱۲۰

پاسخ سئوالات ..... ۱۲۱

## **فصل یازدهم: مدیریت حوادث امنیتی ..... ۱۲۳**

۱۱-۱- اطمینان از گزارش به موقع حوادث و ضعف‌های سیستم‌های اطلاعاتی ..... ۱۲۳

۱۱-۲- اطمینان از اعمال رویه‌های یکنواخت و موثر در مورد حوادث امنیتی. (مدیریت

حوادث امنیت اطلاعات و راه‌های بهبود آنها) ..... ۱۲۳

۱۱-۳- سئوالات تشریحی ..... ۱۲۴

۱۱-۴- سئوالات چهارگزینه‌ای ..... ۱۲۴

پاسخ سئوالات ..... ۱۲۵

## **فصل دوازدهم: مدیریت تداوم کسب و کار ..... ۱۲۷**

۱۲-۱- مقدمه ..... ۱۲۷

۱۲-۲- جوه امنیتی مدیریت تداوم کسب و کار ..... ۱۲۷

۱۲-۳- توجه به امنیت در فرآیند مدیریت کسب و کار سازمان ..... ۱۲۸

۱۲-۴- پیوستگی کسب و کار و ارزیابی مخاطرات ..... ۱۲۸

۱۲-۵- مزایای پیاده‌سازی مدیریت تداوم کسب و کار ..... ۱۲۸

۱۲-۶- چارچوب طرح پیوستگی کسب و کار ..... ۱۲۹

۱۲-۷- تست، نگهداری و ارزیابی مجدد طرح‌های پیوستگی کسب و کار ..... ۱۳۰

۱۲-۸- سئوالات تشریحی ..... ۱۳۰

۱۲-۹- سئوالات چهارگزینه‌ای ..... ۱۳۰

پاسخ سئوالات ..... ۱۳۱

## فصل سیزدهم: سازگاری با قوانین ..... ۱۳۳

۱۳-۱- مفهوم سازگاری با قوانین ..... ۱۳۳

۱۳-۲- جلوگیری از نقض قوانین، مقررات، مسئولیت‌های قراردادی و نیازمندی‌های امنیتی ..... ۱۳۳

۱۳-۳- اطمینان از سازگاری سیستم‌ها با سیاست‌ها و استانداردهای امنیتی سازمان ..... ۱۳۵

۱۳-۴- سئوالات تشریحی ..... ۱۳۵

۱۳-۵- سئوالات چهارگزینه‌ای ..... ۱۳۵

پاسخنامه ..... ۱۳۷

## فصل چهاردهم: پیاده‌سازی سیستم مدیریت امنیت اطلاعات ..... ۱۳۹

۱۴-۱- مقدمه ..... ۱۳۹

۱۴-۲- نحوه پیاده‌سازی ISMS در سازمانها و مراحل اخذ گواهینامه ..... ۱۳۹

۱۴-۳- چرخه استمرار پیاده‌سازی ISMS ..... ۱۳۹

۱۴-۳-۱- مراحل اجرای ISMS بر اساس چرخه دمیثگ ..... ۱۴۱

۱۴-۴- مدل‌ولوژی اجرای I.S.M.S ..... ۱۴۴

۱۴-۴-۱- پایه‌گذاری I.S.M.S ..... ۱۴۴

۱۴-۴-۲- تعریف هدف نهایی سیستم مدیریت امنیت اطلاعات ..... ۱۴۵

۱۴-۴-۳- واگذاری طراحی سیستم مدیریت امنیت اطلاعات ..... ۱۴۷

۱۴-۴-۴- ارزیابی مخاطرات و رفع مخاطرات با تاثیر زیاد ..... ۱۴۸

۱۴-۴-۵- طراحی سیستم مدیریت امنیت اطلاعات ..... ۱۴۹

۱۴-۴-۶- واگذاری پیاده‌سازی سیستم مدیریت امنیت اطلاعات ..... ۱۴۹

۱۴-۴-۷- پیاده‌سازی سیستم مدیریت امنیت اطلاعات ..... ۱۵۰

۱۴-۴-۸- آموزش امنیت اطلاعات ..... ۱۵۰

۱۴-۴-۹- پشتیبانی I.S.M.S برای مدت ۲ تا ۳ ماه ..... ۱۵۰

۱۴-۵-مستندات تعریف و واگذاری طراحی / پیاده‌سازی ..... ۱۵۱

۱۴-۵-۱ RFP-پروژه I.S.M.S ..... ۱۵۱

۱۴-۵-۱-۱ I.S.M.S ..... ۱۵۱

۱۴-۵-۲-قرارداد عدم افشاء اطلاعات کارفرما ..... ۱۵۳

۱۴-۵-۲-جدول ارزیابی پیشنهاد ..... ۱۵۴

۱۴-۵-۲-۱-متدولوژی ارزیابی ریسک بر اساس NIST SP 800-30 ..... ۱۵۷

۱۴-۵-۲-۲-طرح Risk Treatment ..... ۱۵۷

۱۴-۶-طرح پشتیبانی حوادث بر اساس مستند NIST SP800-61 ..... ۱۵۸

۱۴-۷-متدولوژی پشتیبانی حوادث بر اساس مستند NIST SP800-61 ..... ۱۵۸

۱۴-۸-طرح آگاهی رسانی، کسب مهارت و آموزش امنیت بر اساس NIST SP800-50 ..... ۱۶۰

۱۴-۹-متدولوژی آگاهی رسانی، کسب مهارت و آموزش امنیت بر اساس NIST SP800-50 ..... ۱۶۱

۱۴-۱۰-سئوالات تشریحی ..... ۱۶۲

۱۴-۱۱-سئوالات چهارگزینه‌ای ..... ۱۶۳

پاسخ سئوالات ..... ۱۶۶

## فصل پانزدهم: نمونه‌ای از سیاست‌های امنیتی ..... ۱۶۷

۱۵-۱-مقدمه ..... ۱۶۷

۱۵-۲-سیاست‌های امنیتی اطلاعات ..... ۱۶۷

۱۵-۲-سیاست‌های امنیتی کامپیوتری ..... ۱۷۳

۱۵-۳-سیاست‌های امنیتی شبکه ..... ۱۷۶

۱۵-۴-سیاست‌های امنیتی کنترل دسترسی ..... ۱۷۹

۱۵-۵-سیاست‌های امنیتی کنترل دسترسی از راه دور ..... ۱۸۶

۱۵-۶-سیاست‌های امنیتی دیوار آتش ..... ۱۹۱

۱۵-۷-سیاست امنیتی پست الکترونیک ..... ۱۹۴

۱۵-۸-سئوالات تشریحی ..... ۱۹۷

۱۵-۹-سئوالات چهارگزینه‌ای ..... ۱۹۷

پاسخنامه ۲۰۲

منابع: ..... ۲۰۲

www.ketab.ir

## مقدمه مولف:

علیرغم پیشرفت تکنیک‌ها و مکانیزم‌های امنیتی، باز هم شاهد انتشار اخبار نفوذ مهاجمین به شبکه‌های رایانه‌ای سازمان‌ها هستیم. ظاهراً همزمان با پیشرفت‌های امنیت شبکه مهاجمین نیز از تکنیک‌های جدیدی برای حمله سیستم‌های رایانه‌ای استفاده می‌کنند. این موضوع باعث شده است که حفظ محرمانگی، صحت اطلاعات حیاتی سازمان‌ها و جلوگیری از قطع سرویس‌های ارائه شده توسط سازمان‌ها به یک چالش اساسی برای مدیران تبدیل شود. برای مقابله با این چالش سازمان‌ها باید به صورت نظام‌مند و سیستماتیک با مسئله امنیت اطلاعات برخورد کنند. راه حلی که برای این مسئله ارائه شده است، استقرار سیستم مدیریت امنیت اطلاعات (ISMS) در سازمان و دریافت گواهینامه مربوط به آن می‌باشد. در حال حاضر محبوب‌ترین استاندارد در حوزه امنیت اطلاعات، استانداردهای خانواده ISO 27000 است که در کشور ما نیز به شدت در حال گسترش می‌باشد. در این کتاب مجموعه استانداردهای امنیتی ISO 27000 مورد بررسی قرار می‌گیرد. در کنار این استاندارد می‌توان استانداردهای دیگری را نیز به کار برد که متخصصین به این کار اجرای موازی استانداردها در سازمان می‌گویند. لذا در این کتاب برخی از استانداردهای دیگر نظیر استاندارد مدیریتی BS7799 موسسه استاندارد انگلیس، استاندارد ISO/IEC 17799، گزارش فنی ISO/IEC TR 13335، استاندارد BS25999 منتشر شده توسط موسسه استاندارد انگلستان (BSI) و همچنین برخی از مستندات مهم در حوزه امنیت اطلاعات نظیر مستندات NIST SP 800-30، NIST SP800-61 و NIST SP800-50 بررسی شده است. این کتاب راهنمای مناسبی برای اخذ گواهینامه ISO 27000 بوده و مرجعی برای متقاضیان شرکت در آزمونهای مرتبط خواهد بود. همچنین از این کتاب می‌توان به عنوان مرجع دروس معماری امنیت اطلاعات و مدیریت امنیت اطلاعات در رشته‌های فناوری اطلاعات و کامپیوتر استفاده نمود. در پایان هر فصل تعدادی سؤال چهارگزینه‌ای آورده شده است تا خوانندگان بهتر بتوانند خود را برای آزمون‌هایی که در پیش رو دارند آماده نمایند. در فصل آخر کتاب نیز نمونه‌هایی از سیاست‌های امنیتی ارائه شده است. امید است این اثر مورد توجه اساتید، دانشجویان، سازمان‌های متقاضی دریافت استاندارد و همچنین ممیزین ISO 27000 قرار گیرد. از خوانندگان عزیز تقاضا دارم نقطه نظرات خود را از طریق ایمیل [m.a.torkamani@gmail.com](mailto:m.a.torkamani@gmail.com) با اینجانب در میان بگذارند تا انشالله در ویرایش‌های بعدی اشکالات یا کاستی‌های احتمالی کتاب مورد تجدید نظر قرار گیرد. در پایان از زحمات آقای مهندس علی بیات به خاطر طراحی جلد کتاب و همچنین از مدیریت انتشارت ارسطو جناب آقای حسین قنبری تشکر و قدردانی نمایم.