بسم الله الرحمن الرحیم

سیاست های امنیت اطلاعات و ارتباطات

تالیف و تدوین

دکتر ناصر مدیری

مهندس بنفشه فشارکی

مهندس مریم گریوانی

Publication Mehregane Ghalam

سرشناسه	:	مدیری، ناصر، ۱۳۴۱
عنوان	:	سیاست‌های امنیت اطلاعات و ارتباطات
نام پدیدآور	:	تدوین و تالیف ناصر مدیری، بنفشه فشارکی، مریم گریوانی.
مشخصات نشر	:	تهران: مهرگان قلم، ۱۳۹۵.
مشخصات ظاهری	:	۳۵۰ص.: مصور.
شابک	:	۹۷۸-۶۰۰-۶۲۳۶-۹۱-۹
وضعیت فهرست نویسی	:	فیپا
یادداشت	:	کتابنامه.
موضوع	:	تکنولوژی اطلاعات -- تدابیر ایمنی
موضوع	:	حفاظت داده‌ها
موضوع	:	شبکه‌های کامپیوتری -- تدابیر ایمنی
موضوع	:	کامپیوترها -- ایمنی اطلاعات
موضوع	:	منابع اطلاعاتی -- مدیریت
شناسه افزوده	:	فشارکی، بنفشه، ۱۳۶۳
شناسه افزوده	:	گریوانی، مریم، ۱۳۶۶
رده بندی کنگره	:	T۵۸/۸/۹س۹۵ ۱۳۹۵
رده بندی دیویی	:	۳۰۳/۴۸۳۳
شماره کتابشناسی ملی	:	۴۵۸۵۴۳۰

نام کتاب : سیاست های امنیت اطلاعات و ارتباطات

مولف : ناصر مدیری-بنفشه فشارکی-مریم گریوانی

ناشر: مهرگان قلم

نوبت چاپ اول: زمستان ۹۵

شابک: ۹۷۸-۶۰۰-۶۲۳۶-۹۱-۹

تیراژ: ۵۰۰

قیمت: ۳۵۰۰۰ تومان

مرکز پخش

انتشارات مهرگان قلم:

تهران - میدان انقلاب - خیابان کارگرجنوبی - بعد از خیابان وحید نظری - کوچه گشتاب-پلاک۷ واحد۲

تلفن تماس: ۵-۶۶۴۷۷۲۲۴ - ۰۹۱۲۳۱۴۶۰۵۸

WWW.MEHREGANEGHALAM.COM

اطمینان به هر کس قبل از تحقیق، ضعف و ناتوانی است. حضرت علی (ع)

پیشگفتار

گسترش سریع فناوری‌های اطلاعاتی و ارتباطی، به ویژه اینترنت و افزایش پیوسته کاربرد آن‌ها، قابلیـ
دسترسی و سرعت عملیات را بهبود بخشیده و منجر به تغییـرات قابـل تـوجهی در اداره سـازمان‌هـا شـ
است. اما به موازات امکانات و مزیت‌هایی که فناوری اطلاعات فراهم آورده ریسک‌هـای قابـل تـوجهی
نیز متوجه سیستم‌های اطلاعاتی و به ویژه منابع حساس نموده است. این واقعیت سازمان‌هـا را مجبـور بـ
اطمینان یافتن از برقراری امنیت اطلاعات در سازمان می‌نماید. در دنیای امروز بـرای بقـای یـک سـازمان
پیاده سازی سیستم مدیریت امنیت اطلاعات[1] ضرورتی انکار ناپذیر شناخته می‌شود و پـر واضـح اسـ
قرار گرفتن در زیر بار امنیت، حز با گام برداشتن در سایه استانداردهای امنیتی و مـدیریتی میسـر نیسـت
بنابراین موفقیت در اخذ گواهنامه ISO/IEC 270 و بررسی دوره‌ای آن به منزلـه تـداوم هـر سـازمان
محسوب می‌شود. اما لازم است قبل این مراحل، سیاست های امنیتی متناسب با سازمان تـدوین شـود
بر اساس نیازها و کاربرد خاص سازمان سراغ سیستم مدیریت امنیت اطلاعـات (یـا همـان ISMS) رفـت
حال باید دید سیاست امنیتی چیست؟

در ابتدا دیدگاه اولیه و سنتی مبتنی بر این موضوع بود که همه چیز در دو حوزه سخت افزار و نرم افز
شکسته و تعریف شود. اما در دهه گذشته حوزه کاربردهای مبتنی بر وب افزایش یافته و در چند سال اخی
نیاز به امنیت کاری در سه حوزه پیشین اهمیت یافته است. آنچه مشخص اسـت ایـن اسـت کـه حلقـه‌ا
مفقوده که شاید بتوان با عنوان فرهنگ اطلاعات و ارتباطات به آن اشاره نمود، وجـود دارد. ایـن فرهنـگ
همان سیاست‌های امنیتی است که می‌تواند در سطحی بالاتر نقش اتصال ایـن نـواحی بـه یکـدیگر را ایفـ
نماید. شکل زیر تا حدودی گویای نقش سیاست های امنیتی در پیوند این سه حوزه به یکدیگر می‌باشد.

[1] Information security management system (ISMS)

سیاست‌های امنیتی را می‌توان سرآغاز امنیت دانست. از آنجایی که ایجاد یک سیاست امنیتی خوب، پایه‌های پیاده سازی موفق امنیت اطلاعات در آینده را فراهم می‌کند، اولین گام به سمت افزایش امنیت سازمان، معرفی یک سیاست امنیتی دقیق و قابل اجرا، آگاه کردن کارکنان از مسئولیت‌هایشان و پیاده سازی و استقرار سیاست امنیتی می‌باشد. عموماً انجام یک کار پیچیده بدون داشتن برنامه ریزی به همراه جزئیات اجرای آن غیر ممکن است، می‌توان سیاست امنیتی اطلاعات را در حکم برنامه ریزی برای انجام عمل امنیت اطلاعات دانست که فقط در مورد کلیات بحث می‌کند و از چگونگی انجام کار صحبتی به میان نمی‌آورد.

نکته مهم اینست که هر سازمان با توجه به اهداف و شرایط خاص خود، مشمول بخشی از سیاست‌ها می باشد و به اجرای تمامی سیاست ها نیازی ندارد و چه بسا بکارگیری سیاست های غیر لازم سبب تحمیل هزینه های اضافی بر سازمان شود. پس از تدوین سیاست امنیتی، با ستی سیاست ها، اجرایی شوند. هر سیاست می تواند راهنماها و استاندارد هایی همراه با بکارگیری رویه ها، برای پیاده سازی داشته باشد.

در حال حاضر یک سلسله قوانین مجازات اسلامی و نیز قوانین سایبر در کشور وجود آمده است اما آنچه اهمیت دارد این است که این قوانین باید به یک سلسله سیاست تبدیل شوند و مرتبط با سیاست‌های امنیتی باشند و به طور خاص منظوره تر گسترش یابند. سیاست‌های امنیتی باید به شکل سلسله قوانین تدوین شوند و با توجه به نیاز و کاربرد خاص به ISMS مرتبط شوند. در ادامه به دو نمونه از قوانین مجازات اسلامی که در ایران وجود دارد اشاره شده است:

ماده 501 قانون مجازات اسلامی

هر کس نقشه‌ها یا اسرار یا اسناد و تصمیمات راجع به سیاست داخلی یا خارجی کشور را عملاً و عامداً در اختیار افرادی که صلاحیت دسترسی به آن‌ها را ندارند، قرار دهد یا از مفاد آن مطلع کند به نحوی که متضمن نوعی جاسوسی باشد، نظر به کیفیات و مراتب جرم به یک تا ده سال حبس محکوم می‌شود.

ماده 503 قانون مجازات اسلامی

هر کس به قصد سرقت یا نقشه برداری یا کسب اطلاع از اسرار سیاسی یا نظامی یا امنیتی به مواضع مربوطه داخل شود و همچنین شخصی که بدون اجازه مأموران یا مقامات ذی‌صلاح در حال نقشه برداری یا گرفتن فیلم یا عکس برداری از استحکامات نظامی یا اماکن ممنوعه دستگیر شود به شش ماه تا سه سال حبس محکوم می‌شود.

با توجه به عدم آشنایی اکثر سازمان‌ها و نهادهای کشور با سیاست‌های امنیتی و لزوم به کار گیری آن‌ها و ایجاد فرهنگ استفاده از تکنولوژی و کاهش هزینه‌های اضافی، ضرورت نوشتن کتابی در زمینه فراهم آوردن آشنایی با این مفاهیم و اصول برنامه ریزی آن‌ها احساس شد. فرهنگ استفاده از فناوری اطلاعات در ایران چندان تعریف نشده و این امر نیازمند اصلاح و بهبود است. تعریف فرهنگ استفاده از فناوری اطلاعات کمک می‌کند تا آسیب‌ها در این زمینه به پایین ترین میزان ممکن برسد و استفاده از این امکانات، موجب به وجود آوردن مشکلات جدید نشود.

این کتاب شامل ده فصل و چهار ضمیمه می‌باشد که به طور خلاصه مطالب هر فصل به صورت زیر می‌باشد:

- فصل اول، شامل مقدمه‌ای بر فناوری‌های اطلاعاتی و ارتباطی و اهمیت آن‌ها و نیز معرفی برخی از استانداردهای موجود در حوزه فناوری اطلاعات می‌باشد.
- فصل دوم، با توجه به مطالب فصل اول و افزایش انواع تهدیدات و آسیب پذیری های ایجاد شده در مورد اطلاعات، امنیت اطلاعات را به عنوان یک نیاز اساسی مطرح می‌کند و به تعریف آن و برخی از مهم‌ترین موارد مرتبط با آن می‌پردازد. پس از بیان اهمیت و موارد مرتبط با امنیت اطلاعات، امنیت اطلاعات در چهار بخش اصلی تقسیم بندی می‌شود تا در فصول سوم تا ششم به بیان آن‌ها و سیاست‌های مرتبط با هر یک پرداخته شود.

- فصل سوم، در مورد تأمین امنیت کامپیوتر و بیان سیاست‌های مرتبط با کامپیوتر و اجزای کامپیوتری می‌باشد.
- فصل چهارم، سیاست‌های امنیتی مطرح در شبکه را مورد بررسی قرار می‌دهد و زمینه‌های مختلف برای امنیت شبکه را مطرح می‌کند.
- فصل پنجم، سیستم مدیریت امنیت اطلاعات (ISMS) را به عنوان پیش‌نیاز سیاست‌های امنیتی بیان کرده یازده حوزه مرتبط با آن را مورد بررسی قرار می‌دهد و بیان می‌کند برای اطلاعاتی که سیستم‌ها تولید می‌کنند و اطلاعاتی که برنامه‌های کاربردی دارند، چگونه می‌توانیم یک ساختار امن داشته باشیم و چه کارهایی را باید به طور متداول انجام داده باشیم.
- فصل ششم، به طور مفصل به سیاست‌های کنترل دسترسی که یکی از حوزه‌های یازده‌گانه مطرح در فصل پنجم بود، می‌پردازد. به دلیل متکی شدن هر چه بیشتر ما به نرم افزارها و اتوماسیون شدن سیستم‌ها و نیز به دلیل مبتنی بر IP بودن و متحرک شدن وسایل، کنترل دسترسی دارای اهمیتی دوچندان شده و به همین دلیل در فصلی مجزا مورد بررسی قرار گرفته است و به معرفی سیاست‌ها و موضوعات مهم در این زمینه پرداخته شده است.
- فصل هفتم، به معرفی نمونه مثال‌هایی از پرکاربردترین سیاست‌های امنیتی که حاصل گردآوری نمونه سیاست‌های برخی دانشگاه‌ها و سازمان‌های معتبر می‌باشد، می‌پردازد.
- فصل هشتم، به چگونگی عملیاتی کردن یک سیاست امنیتی و مراحل لازم برای پیاده سازی سیستم مدیریت امنیت اطلاعات می‌پردازد. در فصول قبلی، عمدتاً به بررسی علم سیاست‌های امنیت بحث شد که بر خلاف این فصل هیچ کدام از فصول جنبه اجرایی نداشتند.
- فصل نهم، به بیان مشخصات سیاست امنیتی و چگونگی فرآیند نگارش، فرمت و اجزای تشکیل دهنده یک سیاست امنیتی پرداخته است و راهنمایی‌هایی را جهت نوشتن یک نمونه سیاست امنیتی فراهم می‌آورد.
- فصل دهم، در ابتدا به معرفی مراحل لازم برای شروع فرآیند استمرار کسب و کار می‌پردازد. در ادامه استانداردهای مرتبط با استمرار کسب و کار و نیز مراحل متداول یک طرح ریزی (برنامه ریزی) برای استمرار کسب و کار معرفی شده است. داشتن سیاست‌های امنیتی یکی از مهم‌ترین عوامل در استمرار کسب و کار است. در انتهای فصل بیان می‌کند پس از پیاده سازی ISMS و انجام فرآیند لازم برای آن، چگونه می‌توان با کمک ITIL، معیاری برای پیاده سازی موفق امنیت ارائه داد. همان‌طور که در فصل

هشتم در مورد چگونگی پیاده سازی صحبت شد بخش پایانی این فصل باید ما را قادر به ارزیابی و اندازه گیری امنیت اطلاعات سازد که ملاک این ارزیابی، یک سری نقاط کنترلی که همان KPI های امنیت اطلاعات ITIL هستند، می‌باشد. در واقع این فصل، این موضوع را بیان می‌کند که امنیت و استمرار کسب و کار بایستی انجام شوند تا بتوان سیستم مدیریت امنیت اطلاعات (ISMS) را روی آن اجرایی کرد و در نهایت پس از آن با KPI های امنیتی ITIL و نگاشت آن‌ها به سرویس‌های امنیتی ISO 27001 می‌توان در مورد بهینه کردن و ارزیابی ISMS صحبت نمود.

راهنمایی جهت مطالعه کتاب:

این کتاب را از چه منظر می‌توان مورد مطالعه قرار داد:

در صورتیکه خواننده مباحث امنیت اطلاعات آشنایی ندارد، پیشنهاد می‌شود 7 فصل ابتدای کتاب را که عمدتاً در مورد علم سیاست امنیت اطلاعات می‌باشد، مورد بررسی قرار دهد. اما چنانچه خواننده با این مباحث آشنایی داشته و از دید مدیریتی و اجرایی بخواهد به موضوع امنیت اطلاعات و سیاست‌های آن بنگرد مطالعه فصول 8 تا 10 توصیه می‌شود.

در خاتمه بر خود لازم می‌دانیم از تمامی عزیزانی که به نوعی در گردآوری مطالب این کتاب ما را یاری رساندند کمال تشکر و قدردانی را به عمل آوریم.

بی‌صبرانه منتظر نظرات، انتقادات و پیشنهادات شما هستیم.

پست الکترونیکی انعکاس نظرات:

info@27000.Ir
www.27000.Ir

ناصر مدیری – بنفشه فشارکی – مریم گریوانی

فهرست مطالب

1. سیستم‌های اطلاعاتی و ارتباطی 16
1-1 : خلاصه فصل 16
1-2 : مقدمه 16
1-3 : سیستم‌های ارتباطی 17
1-4 : شبکه‌های کامپیوتری 19
1-4-1: اهمیت و کاربرد شبکه‌های کامپیوتری 19
1-4-2: شبکه متصل (شبکه شبکه‌ها) 20
1-5 : سیستم‌های اطلاعاتی 22
1-6 : حاکمیت فناوری اطلاعات 25
1-6-1: چارچوب‌ها و استانداردهای حوزه حاکمیت فناوری اطلاعات 26
1-6-2: چارچوب COBIT 28
1-6-3: کتابخانه زیربنایی فناوری اطلاعات (ITIL) 31
1-6-4: استانداردهای سری 27000 ISO 32
1-7 : نتیجه گیری 33
1-8 : سوالات متداول 33
1-9 : منابعی برای مطالعه بیشتر 34

2.امنیت اطلاعات و ارتباطات 36
2-1 : خلاصه فصل 36
2-2 : مقدمه 36
2-3 : تعریف امنیت 37
2-4 : تعریف امنیت اطلاعات 38
2-5 : معرفی برخی دیگر از مؤلفه‌های امنیت اطلاعات 41
2-6 : مدل امنیتی NSTISSC 43
2-7 : حملات 44
2-7-1: انواع حملات 44
2-7-2: آشنایی با مفاهیم تهدیدات، آسیب پذیری ها و ریسک 46
2-7-3: انواع کنترل‌های امنیت اطلاعات 48
2-8 : دفاع (پدافند) در عمق 49
2-9 : برخی مسئولیتهای امنیتی در یک سازمان 51
2-10 :مدیریت امنیت اطلاعات 53
2-10-1: مدیریت ریسک (مخاطرات) 54
2-11 :سیاست امنیتی 59
2-12 :نتیجه گیری 63

2-13 :سوالات متداول 63
2-14 :منابعی برای مطالعه بیشتر 64

3.سیاست‌های امنیتی کامپیوتری 66
3-1 : خلاصه فصل 66
3-2 : امنیت کامپیوتر 66
3-2-1: تأمین امنیت با طراحی 67
3-2-2: معماری امنیت 68
3-2-3: مکانیسم‌های سخت افزاری 69
3-2-4: سیستم عامل‌های امن 69
3-2-5: مدل نهایی امن 70
3-3 : فاکتورهای امنیت کامپیوتر 71
3-4 : سیاست امنیت کامپیوتر 76
3-4-1: سیاست برنامه 78
3-4-2: سیاست‌های موضوع خاص 79
3-4-3: سیاست‌های سیستم‌های خاص 83
3-5 : وابستگی سیاست‌های کامپیوتری 86
3-6 : پیش بینی هزینه 87
3-7 : نتیجه گیری 87
3-8 : سوالات متداول 87
3-9 : منابع برای مطالعه بیشتر 88

4.سیاست‌های امنیتی شبکه 90
4-1 : خلاصه فصل 90
4-2 : مقدمه 90
4-3 : سیاستهای امنیتی پایه 91
4-4 : امنیت شبکه 92
4-4-1: دسترسی به شبکه داده 93
4-4-2: منابع شبکه 94
4-4-3: حمله 95
4-4-4: تحلیل خطر 95
4-4-5: سیاست امنیتی 96
4-4-6: طرح امنیت شبکه 96
4-4-7: نواحی امنیتی 97
4-4-8: امنیت در شبکه‌های بیسیم 98
4-5 : سیاستهای امنیتی شبکه 98
4-5-1: امنیت تجهیزات شبکه 108

4-5-2: امنیت فیزیکی و محیطی 109
4-5-3: امنیت منطقی 114
4-6 : ملزومات و مشکلات امنیتی ارائه دهندگان خدمات 117
4-6-1: مشکلات اعمال ملزومات امنیتی 118
4-7 : نتیجه گیری 118
4-8 : سوالات متداول 119
4-9 : مراجعی برای مطالعه بیشتر 120
5.سیاست‌های امنیتی اطلاعات 122
5-1 : خلاصه فصل 122
5-2 : مقدمه 122
5-3 : حداقل نیازمندیهای امنیتی 123
5-4 : امنیت اطلاعات 126
5-4-1: دسته بندی امنیتی برای اطلاعات 126
5-5 : سیاستهای امنیت اطلاعات 127
5-5-1: محرمانه بودن اطلاعات 127
5-5-2: چرخه حیات اطلاعات 128
5-5-3: مدیریت چرخه حیات اطلاعات (ILM) 129
5-5-4: داده گردانی 129
5-5-5: ذخیره سازی داده 129
5-5-6: انتقال دادهها 130
5-5-7: تخریب دادهها 130
5-6 : سیستم مدیریت امنیت اطلاعات (ISMS) 132
5-6-1: آشنائی با مراحل طی شده در زمینه امنیت اطلاعات 133
5-6-2: چگونگی روند رو به رشد استاندارد BS7799 133
5-6-3: استاندارد BS7799 134
5-6-4: سری استاندارد ISO/IEC 27000 134
5-7 : حوزه تحت پوشش ISMS در سازمان‌ها 136
5-7-1: تدوین سیاست امنیت 137
5-7-2: امنیت اطلاعات سازمان 138
5-7-3: مدیریت داراییها 138
5-7-4: برقراری امنیت منابع انسانی و پرسنل 139
5-7-5: برقراری امنیت محیطی و فیزیکی 140
5-7-6: مدیریت عملیات و ارتباطات 141
5-7-7: کنترل دسترسی 144
5-7-8: نگهداری و توسعه سیستم‌های اطلاعات 145

5-7-9: گزارش و پاسخ به حوادث امنیتی اطلاعات 145
5-7-10: مدیریت استمرار فعالیت‌های سازمان 145
5-7-11: الزام انطباق با قانون و سازگاری 146
5-8 : پروسه دریافت گواهی‌نامه بین‌المللی ISO/IEC 27001 146
5-9 : فواید استاندارد ISO27001 و لزوم پیاده سازی 147
5-10 : نتیجه گیری 148
5-11 : سوالات متداول 149
5-12 : منابعی برای مطالعه بیشتر 149

6.سیاست‌های امنیتی کنترل دسترسی 151
6-1 : خلاصه فصل 152
6-2 : تعریف کنترل دسترسی 153
6-3 : کنترل دسترسی امنیت کامپیوتر 154
6-4 : اهمیت کنترل دسترسی 157
6-5 : کنترل دسترسی در ISO/IEC 27001-2005 158
6-6 : کنترل‌های فیزیکی 159
6-6-1: عملکرد سیستم‌های کنترل دسترسی فیزیکی 160
6-7 : سیاست‌های کنترل دسترسی 162
6-8 : مدل‌ها و سیاست‌های کنترل دسترسی 163
6-8-1: پیشینه سیاست‌های کنترل دسترسی 165
6-8-2: کنترل دسترسی خصوصیت محور 166
6-8-3: کنترل دسترسی بصیرتی 167
6-8-4: کنترل دسترسی الزامی 168
6-8-5: سیاست‌های کنترل دسترسی نقش محور 173
6-8-6: مقایسه مدل‌های کنترل دسترسی 177
6-9 : ابزارهای سیاست کنترل دسترسی 178
6-10 : نتیجه گیری 180
6-11 : سوالات متداول 180
6-12 : مراجع برای مطالعه بیشتر 181

7.نمونه سیاست‌های امنیتی 184
7-1 : خلاصه فصل 184
7-2 : سیاست‌های امنیتی اطلاعاتی 184
7-3 : سیاست‌های امنیتی کامپیوتری 191
7-4 : سیاست‌های امنیتی شبکه 194
7-5 : سیاست‌های امنیتی کنترل دسترسی 198
7-6 : سیاست‌های امنیتی کنترل دسترسی از راه دور 205

7-7 : سیاست‌های امنیتی دیوار آتش 209
7-8 : سیاست‌های امنیتی پست الکترونیک 213
7-9 : نتیجه گیری 216
7-10 :سوالات متداول 217
7-11 :منابعی برای مطالعه بیشتر 217

8.پیاده سازی سیاست‌های امنیتی 219
8-1 : خلاصه فصل 220
8-2 : مقدمه 221
8-3 : یک روش پیاده سازی سیستم مدیریت امنیت اطلاعات 222
8-4 : جایگاه چرخه مدیریتی دمینگ در پیاده سازی ISMS 235
8-5 : اندازه گیری سیستم مدیریت امنیت اطلاعات 254
8-5-1: چارچوبی برای اندازه گیری پیاده سازی ISMS 260
8-5-2: تشریح چرخه مدیریت ضربه امنیتی 263
8-5-3: خلاصه چارچوب اندازه گیری ISMS 265
8-6 : اشتباهات رایج در پیاده سازی 268
8-7 : نتیجه گیری 268
8-8 : سوالات متداول 269
8-9 : مراجع 270

9.نگارش سیاست‌های امنیتی 272
9-1 : خلاصه فصل 272
9-2 : ارتباط سیاست امنیتی با دیگر ابعاد مطرح در سازمان 272
9-3 : مراحل توسعه یک سیاست امنیتی 275
9-4 : نمونه چک لیستی از فرآیند توسعه 282
9-5 : مؤلفه‌های تشکیل دهنده یک سیاست امنیتی 283
9-6 : نتیجه گیری 290
9-7 : سوالات متداول 290
9-8 : منابعی برای مطالعه بیشتر 291

10.سیاست‌های امنیتی و تداوم کسب و کار 294
10-1 :خلاصه فصل 294
10-2 :مقدمه 295
10-3 :پایه‌ها و اصول مبنا برای استمرار کسب و کار 296
10-4 :استانداردهای مرتبط با استمرار کسب و کار 301
10-5 :طرح ریزی (برنامه ریزی) برای استمرار کسب و کار 302
10-5-1 مدیریت ریسک 306

10-5-2:آنالیز تأثیر کسب و کار 308
10-5-3:طرح پاسخ 312
10-5-4:بازیابی و ترمیم 313
10-5-5:تست، نگهداری و بازبینی 318
10-6 :نمونه چک لیست ارزیابی استمرار کسب و کار 320
10-7 :مدیریت سرویس‌های سیاست‌های امنیتی بر مبنای مدل ITIL 322
10-7-1:سرویس‌های سیاست‌های امنیتی 323
10-7-2:مدل ITIL 324
10-7-3:شاخص‌های کلیدی عملکرد امنیت ITIL 326
10-7-4:پیاده سازی سیاست‌های امنیت بر مبنای ITIL 327
10-8 :نتیجه گیری 329
10-9 :منابعی برای مطالعه بیشتر 330
11. ضمایم 331
11-1 :ضمیمه اول 332
11-2 :ضمیمه دوم 336
11-3 :ضمیمه سوم 337
11-4 :ضمیمه چهارم 345