پیوست

شورای اجرایی (عالی) فناوری اطلاعات کشور

کمیسیون توسعه دولت الکترونیکی

چارچوب معماری سازمانی ایران

معماری مرجع امنیت

استانداردهای امنیتی حوزه نرم افزار

نسخه ۱,۰ – اردیبهشت‌ماه ۱۳۹۶

پیشگفتار

نرم‌افزار نقش اساسی در ایجاد امنیت ایفا می‌کند، همچنین منبع اصلی مشکلات امنیتی است و پایبندی نرم‌افزارها به یک مدل فرایند و یا یک مدل چرخه حیات خاص، امنیت نرم‌افزار را از نظر مصون بودن از آسیب پذیری‌های امنیتی ناخواسته تضمین نمی‌کند. بنابراین به منظور ایجاد نرم‌افزاری امن، بایستی در طی مراحل اصلی چرخه توسعه نرم‌افزار (SDLC)[1] شامل نیازمندی‌ها، طراحی، کدنویسی، صحت‌سنجی[2]، پذیرش[3] و استقرار[4]، مفاهیم امنیتی را پیاده‌سازی نمود که این امر باعث صرفه‌جویی در زمان، هزینه و همچنین تاثیرپذیری بیشتر می‌شود.

چرخه حیات توسعه سیستم

چرخه حیات توسعه سیستم (SDLC) یک فرایند کلی از توسعه، پیاده‌سازی، آزمایش، استقرار و نگهداری سیستم‌های نرم‌افزاری است. SDLC مدل‌ها و روش‌های متفاوتی دارد اما به طور کلی شامل مجموعه‌ای از مراحل تعریف شده می‌باشد. امنیت اطلاعات باید به صورت یکپارچه برای هر مدل SDLC به منظور اطمینان از حفاظت اطلاعات مورد استفاده قرار بگیرد. اگر امنیت از ابتدایی‌ترین مرحله چرخه حیات سیستم لحاظ شود باعث صرفه‌جویی در زمان، هزینه و همچنین تاثیرپذیری بیشتر می‌شود. برخی از مزایای یکپارچه‌سازی امنیت در چرخه حیات توسعه سیستم عبارت است از:

- شناسایی و کاهش آسیب‌پذیری‌های امنیتی و مشکلات پیکربندی سیستم، در نتیجه هزینه‌های پایین‌تر برای پیاده‌سازی کنترل‌های امنیتی و کاهش آسیب‌پذیری.
- آگاهی از چالش‌های مهندسی بالقوه ناشی از کنترل‌های امنیتی اجباری

---

[1] Software Development Lifecycle (SDLC)

[2] Verification

[3] Acceptance

[4] Deployment

- شناسایی سرویس‌های امنیتی مشترک و استفاده مجدد از استراتژی‌ها و ابزارهای امنیتی که هزینه-های توسعه را کاهش و وضعیت امنیتی سیستم را با استفاده از روش‌ها و تکنیک‌های اثبات شده بهبود می‌دهند.
- بهبود سازمان و اعتماد مشتریان به منظور تسهیل پذیرش و استفاده از سیستم‌ها، و بهبود اعتماد در ادامه سرمایه‌گذاری در سیستم‌های دولتی.
- بهبود سیستم‌های با قابلیت همکاری و ادغام

به صورت کلی چرخه حیات توسعه سیستم به پنج مرحله اصلی: آغاز، تهیه و توسعه، اجرا/ ارزیابی، عملیات/ نگه‌داری و امحاء دسته‌بندی می‌شود:

❖ مرحله آغاز

در طی مرحله آغاز، سازمان‌ها بایستی نیازهای سیستم را ایجاد و اهداف آن‌ها را ثبت نمایند. برنامه‌ریزی امنیت باید در این مرحله آغاز و قانون‌های کلیدی امنیت شناسایی شود. اطلاعات برای ارزیابی نیازمندی‌های امنیت پردازش، انتقال یا ذخیره می‌شوند و همه اعضا باید درک مشترکی از ملاحظات امنیتی داشته باشند. همچنین نیازمندی‌های موردنیاز برای محرمانگی، یکپارچگی و دسترس‌پذیری بایستی در این مرحله مورد ارزیابی قرار بگیرد. لیستی از استانداردهای این مرحله در جدول زیر آمده است.

جدول ۱: استانداردهای امنیتی مرحله آغاز

شماره استاندارد	نام استاندارد
SP 800-36	Guide to Selecting Information Technology Security Products, (2003)
	راهنمای انتخاب محصولات امنیتی فناوری اطلاعات
SP 800-35	Guide to Information Technology Security Services, (2003)
	راهنمای سرویس‌های امنیتی فناوری اطلاعات
SP 800-48	Guide to Securing Legacy IEEE 802.11 Wireless Networks, Rev.1, (2008)

شماره استاندارد	نام استاندارد
	راهنمایی برای تامین امنیت شبکه‌های بی‌سیمIEEE 802.11
SP 800-47	Security Guide for Interconnecting Information Technology Systems, (2002) راهنمای امنیت برای ارتباطات سیستم‌های فناوری اطلاعات
SP 800-46	Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security, Rev.2 (2016) راهنمایی برای امنیت دورکاری سازمان‌ها، دسترسی از راه دور و استفاده از دستگاه‌های شخصی (BYOD)
SP 800-45	Guidelines on Electronic Mail Security, V.2, (2007) راهنمایی در مورد امنیت پست الکترونیک
SP 800-44	Guidelines on Securing Public Web Servers, V.2, (2007) راهنمایی در مورد امنیت وب سرورهای عمومی
SP 800-41	Guidelines on Firewalls and Firewall Policy, (2009) راهنمایی‌هایی در مورد دیواره آتش و سیاست‌های آن
SP 800-40	Guide to Enterprise Patch Management Technologies Rev.3, (2013) راهنمایی برای فناوری‌های مدیریت وصله سازمان
SP 800-33	Underlying Technical Models for Information Technology Security, (2001) مدل فنی بنیادی برای امنیت فناوری اطلاعات
SP 800-31	Intrusion Detection systems, (2001) سیستم‌های تشخیص نفوذ
SP 800-28	Guidelines on Active Content and Mobile Code, V.2, (2008) راهنما در مورد محتوا فعال و کد موبایل
SP 800-67	Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, Rev.1, (2012) توصیه‌ای برای الگوریتم رمزگذاری داده سه‌گانه (TDEA) رمز قطعه‌ای
SP 800-38A	Recommendation for Block Cipher Modes of Operation: Methods and Techniques, (2001) توصیه‌ای برای مدهای عملیاتی رمز قطعه‌ای: روش‌ها و تکنیک‌ها
SP 800-38B	Recommendation for Block Cipher Modes of Operation: the CMAC Mode for Authentication, (2016) توصیه‌ای برای مدهای عملیاتی رمز قطعه‌ای: مد CMAC برای احرازهویت
SP 800-38C	Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality, (2007)

نام استاندارد	شماره استاندارد
توصیه‌ای برای مدهای عملیاتی رمز قطعه‌ای: مد CCM برای احرازهویت و محرمانگی	
A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, Rev 1a, (2010)	SP 800-22
یک مجموعه آزمون آماری برای مولد اعداد تصادفی و شبه تصادفی برای برنامه‌های کاربردی رمزنگاری	
Modes of Operation Validation System for the Triple Data Encryption Algorithm (TMOVS): Requirements and Procedures, (2012)	SP 800-20
سیستم اعتبارسنجی مد عملیاتی برای الگوریتم رمزنگاری داده سه‌گانه (TMOVS): الزامات و روش‌ها	
An Introduction to Computer Security, Rev.1, (2017)	SP 800-12
مقدمه‌ای بر امنیت کامپیوتر	
Engineering Principles for Information Technology Security (A Baseline for Achieving Security) , Revision A, Rev. A, (2004)	SP 800-27
اصول مهندسی برای امنیت فناوری اطلاعات	
Integrating IT Security into the Capital Planning and Investment Control Process, (2005)	SP 800-65
یکپارچه‌سازی امنیت فناوری اطلاعات در فرایند برنامه‌ریزی سرمایه و کنترل سرمایه‌گذاری	
Guide for Mapping Types of Information and Information Systems to Security Categories, (2008)	SP 800-60
راهنمایی برای نگاشت انواع اطلاعات و سیستم‌های اطلاعاتی به دسته‌های امنیت	
Guideline for Identifying an Information System as a National Security System, (2003)	SP 800-59
راهنمایی برای شناسایی یک سیستم اطلاعاتی به عنوان یک سیستم امنیت ملی	
Guidelines to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products, (2000)	SP 800-23
راهنمایی‌هایی برای سازمان‌های فدرال جهت تضمین امنیت و کسب یا استفاده از محصولات تست یا ارزیابی شده	
An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, (2008)	SP 800-66
یک راهنمای منابع مقدماتی مورد نیاز برای پیاده‌سازی قانون امنیتی پاسخگویی و انتقال بیمه سلامت	
Risk Management Guide for Information Technology Systems	SP 800-30
راهنمای مدیریت ریسک برای سیستم‌های فناوری اطلاعات	
Federal S/MIME V3 Client Profile	SP 800-49
مشخصات سرویس‌گیرنده S/MIME فدرال	
Secure Hash Standard (SHS), (2015)	

شماره استاندارد	نام استاندارد
FIPS 180-4	استاندارد درهم‌سازی امن
FIPS 186	Digital Signature Standard (DSS), (2013) استاندارد امضای دیجیتال
FIPS 197	Advanced Encryption Standard (AES), (2001) استاندارد رمزگذاری پیشرفته
FIPS 198-1	The Keyed-Hash Message Authentication Code(HMAC), (2008) کد اصالت‌سنجی پیام مبتنی‌بر درهم‌سازی
FIPS 199	Standards for Security Categorization of Federal Information and Information Systems, (2004) استانداردهایی برای دسته‌بندی امنیت سیستم‌های اطلاعاتی و اطلاعات فدرال

در این قسمت هریک از استانداردهای امنیتی مرحله آغاز شرح داده شده است:

- **SP 800-36: Guide to Selecting Information Technology Security Products, (2003)**

یک زیرساخت اطلاعاتی امن محرمانگی، صحت و دسترس‌پذیری اطلاعات حیاتی را تضمین می‌کند. محصولات امنیتی فناوری اطلاعات جزء جدایی ناپذیر طراحی، توسعه و نگهداری زیرساخت‌های امن می‌باشند. این راهنما مجموعه‌ای از محصولات امنیتی فناوری اطلاعات را پوشش می‌دهد که به عنوان کنترل‌های امنیتی عملیاتی و فنی استفاده می‌شود. این راهنما شامل دسته‌بندی محصولات امنیتی فناوری اطلاعات می‌باشد، اما یک لیست جامع و کامل از محصولات امنیتی را پوشش نمی‌دهد. این راهنما لیستی از مشخصات و سوالات مربوط به یک سازمان که بایستی در طول فرایند انتخاب محصولات پرسیده شوند را توضیح و ارایه می‌دهد.

- **SP 800-35: Guide to Information Technology Security Services, (2003)**

هدف از این راهنما کمک به سازمان‌ها در انتخاب[5]، اجرا[6] و مدیریت سرویس‌های فناوری اطلاعات در مراحل مختلف چرخه حیات سرویس‌های امنیتی فناوری اطلاعات می‌باشد. چرخه حیات سرویس‌های امنیتی فناوری اطلاعات با ارایه یک چارچوب، تصمیم‌گیرندگان امنیت فناوری اطلاعات را قادر می‌سازد تا تلاش‌های امنیتی فناوری اطلاعات خود را از شروع تا پایان سازماندهی کنند. مدیریت سیستماتیک سرویس‌های امنیت فناوری اطلاعات بسیار مهم است. عدم در نظر گرفتن بسیاری از مسایل و مدیریت ریسک سازمانی، می‌تواند به طور جدی سازمان را تحت تاثیر قرار دهد. تصمیم‌گیرندگان امنیت فناوری اطلاعات باید هزینه‌ها و نیازمندی‌های امنیتی، همچنین تاثیر بالقوه تصمیم‌گیری‌های خود بر روی ماموریت‌ها، عملیات و استراتژی‌های سازمانی و طبقه‌بندی ارایه‌دهندگان سرویس و پرسنل را مدنظر قرار دهند.

- **SP 800-48: Guide to Securing Legacy IEEE 802.11 Wireless Networks, (2008)**

هدف این سند فراهم نمودن راهنمایی برای سازمان‌ها جهت امنیت شبکه‌های بی‌سیم خود براساس استاندارد IEEE 802.11 است که نمی‌توانند از استاندارد IEEE 802.11i استفاده کنند. جزئیات درباره امن نمودن قابلیت WLANها در استاندارد IEEE 802.11i که می‌تواند در استاندارد NIST 800-97 یافت شود. توصیه‌نامه‌ها برای امنیت در به‌کارگیری WLAN خارجی، از جمله نقاط دسترسی عمومی بی‌سیم، خارج از حیطه این سند می‌باشد.

- **SP 800-47: Security Guide for Interconnecting Information Technology Systems, (2002)**

این سند سیستم‌های فناوری اطلاعات، شناسایی اجزای اصلی یک اتصال، شناسایی روش‌ها و سطح اتصال را توصیف و در مورد خطرات امنیتی بالقوه در ارتباط با اتصال توضیح می‌دهد. این سند یک رویکرد مدیریت چرخه حیات برای اتصال سیستم‌های فناوری اطلاعات، با تاکید بر امنیت فراهم می‌کند. همچنین شامل

---

[5] Selection

[6] Implementation

راهنماها و نمونه‌هایی برای توسعه یک قرارداد امنیت ارتباطات[۷] و یک تفاهم نامه/ توافقنامه[۸] می‌باشد. قرارداد امنیت ارتباطات نیازمندی‌های فنی و امنیتی ارتباطات را مشخص و تفاهم نامه مسئولیت‌های سازمان‌های شرکت کننده را تعریف می‌کند. در نهایت، این سند شامل راهنمایی برای توسعه یک برنامه جهت پیاده‌سازی ارتباطات سیستمی می‌باشد که فرایند برقراری ارتباطات، از جمله برنامه‌ریزی و هزینه را تعریف می‌کند.

- **SP 800-46: Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security, (2016)**

هدف از این سند، کمک به سازمان‌ها در کاهش ریسک‌های مرتبط با فناوری‌های سازمانی مورداستفاده در دورکاری، مانند دسترسی از راه دور سرویس‌دهنده‌ها، دستگاه‌های مورداستفاده در دورکاری (از جمله BYOD) و ارتباطات دسترسی از راه دور است. این سند بر اهمیت تامین امنیت اطلاعات حساس ذخیره شده در دستگاه‌های دورکاری و انتقال از طریق دسترسی از راه دور در سراسر شبکه خارجی تاکید کرده و همچنین توصیه‌هایی برای ایجاد سیاست‌های مرتبط با دورکاری و برای انتخاب، پیاده‌سازی و حفظ کنترل‌های امنیتی لازم برای دسترسی از راه دور به سرور و سرویس‌گیرنده را ارایه می‌دهد.

- **SP 800-45: Guidelines on Electronic Mail Security, (2007)**

هدف این سند ارایه توصیه‌هایی برای در نظر گرفتن اقدامات امنیتی در طراحی، پیاده‌سازی سیستم‌های ایمیل در شبکه‌های عمومی و خصوصی می‌باشد.

سرویس‌دهنده پست الکترونیک اغلب توسط مهاجمان مورد هدف قرار می‌گیرد. همچنین به طور گسترده به عنوان یک بردار ارایه حملات استفاده می‌شود که از آسیب‌پذیری‌ها در محیط کاری کاربر سو استفاده و از روش‌های مهندسی اجتماعی برای فریب کاربران استفاده می‌کند. این سند توسط سازمان‌ها برای افزایش امنیت در سیستم‌های پست الکترونیک موجود و اینده استفاده شده تا تعداد و تکرار حوادث امنیتی مربوط به پست الکترونیک را کاهش دهد.

---

[۷] Interconnection Security Agreement (ISA)

[8] Memorandum of Understanding/Agreement(MOU/A)

این سند جنبه‌های مربوط به تامین امنیت سرویس دهنده پست الکترونیک را پوشش نمی‌دهد. از جمله:

- امنیت پروتکل پیام استاندارد X.400
- امن کردن انواع متفاوت سرورهای شبکه
- دیواره‌های آتش و مسیریاب‌های مورد استفاده برای حفاظت سرویس‌دهنده پست الکترونیک

➢ **SP 800-44: Guidelines on Securing Public Web Servers, (2007)**

هدف این سند ارایه توصیه‌هایی در مورد اقدامات امنیتی برای طراحی و پیاده‌سازی سرورهای وب در دسترس عموم، از جمله مسایل مربوط به زیرساخت‌های شبکه می‌باشد. این سند توسط سازمان‌ها برای افزایش امنیت سرورهای وب موجود و آینده استفاده شده تا تعداد و تکرار حوادث امنیتی مربوط به سرورهای وب را کاهش دهد. همچنین اصول عمومی ارایه شده را به تمام سیستم عامل‌ها اعمال می‌کند.

این سند جنبه‌های مربوط به تامین امنیت وب سرور را پوشش نمی‌دهد. از جمله:

- ملاحظات امنیتی مربوط به سرویس‌گیرنده وب
- امن کردن انواع متفاوت سرورهای شبکه
- دیواره‌های آتش و مسیریاب‌های مورد استفاده برای حفاظت سرویس‌دهنده پست الکترونیک

➢ **SP 800-41: Guidelines on Firewalls and Firewall Policy, (2009)**

هدف این سند کمک به سازمان‌ها در درک قابلیت‌های فناوری‌های دیواره آتش و سیاست‌های دیواره آتش می‌باشد. در واقع قابلیت‌های امنیتی و مزایا و معایب دیواره آتش را بررسی کرده و همچنین راهنمایی‌های کاربردی را در توسعه سیاست‌های دیواره‌آتش و انتخاب، پیکربندی، تست، استقرار و مدیریت دیواره آتش فراهم می‌کند.

برای بهبود اثربخشی و امنیت دیواره‌آتش، سازمان‌ها باید توصیه‌های زیر را پیاده‌سازی کنند:

- ایجاد سیاست دیواره آتش که مشخص می‌کند دیواره آتش چگونه باید ترافیک شبکه‌های ورودی و خروجی خود را مدیریت کند.

- شناسایی تمام نیازمندی‌هایی که بایستی در زمان تعیین دیواره آتش برای پیاده‌سازی در نظر گرفته شود.
- مدیریت معماری دیواره آتش، سیاست‌ها، نرم‌افزار،و دیگر اجزا در سراسر حیات راه‌حل‌های دیواره آتش

- **SP 800-40: Guide to Enterprise Patch Management Technologies, (2013)**

این سند برای کمک به سازمان‌ها در درک اصول اولیه فناوری‌های مدیریت وصله سازمان طراحی شده است. این سند اهمیت مدیریت وصله را توضیح داده و به بررسی چالش‌های ذاتی در انجام مدیریت وصله می‌پردازد و یک دید کلی از فناوری‌های مدیریت وصله سازمان فراهم نموده و معیارهایی را برای سنجش کارایی فناوری‌ها و مقایسه اهمیت نسبی وصله‌ها شرح می‌دهد.

- **SP 800-33: Underlying Technical Models for Information Technology Security, (2001)**

هدف از این سند ارایه یک توصیف فنی بنیادی، به اصطلاح مدل، برای زیرساخت‌های امن فناوری اطلاعات می‌باشد. در واقع هدف، ارایه مدل‌هایی است که بایستی به صورت مختصر در طراحی و توسعه قابلیت‌های امنیتی فنی در نظر گرفته شوند. این مدل شامل مطالب آموخته شده، رویه‌های خوب و ملاحظات خاص می‌باشد.

مخاطبان درنظر گرفته شده شامل بخش‌های دولتی و خصوصی از جمله کاربران فناوری اطلاعات که درک بهتری از امنیت دارند، مهندسین و معماران طراحی قابلیت‌های امنیتی و کسانی که در حال توسعه قابلیت‌های امنیتی می‌باشند.

هدف از امنیت فناوری اطلاعات این است که سازمان‌ها قادر باشند به تمام اهداف کسب و کار و ماموریتی خود از طریق پیاده‌سازی سیستم‌ها با توجه به ریسک‌های مربوط به فناوری اطلاعات دست یابند که این از طریق اهداف امنیتی زیر برآورده می‌شود:

- دسترس‌پذیری
- جامعیت داده و سیستم
- محرمانه بودن داده و اطلاعات سیستم
- مسئولیت پذیری[۹]

➢ **SP 800-31: Intrusion Detection systems, (2001)**

سیستم‌های تشخیص نفوذ، سیستم‌های سخت‌افزاری یا نرم‌افزاری هستند که به طور خودکار فرایند نظارت بر حوادث سیستم کامپیوتری یا شبکه را انجام داده و آن‌ها را تحلیل می‌کنند. با توجه به افزایش حملات چند سال اخیر، سیستم‌های تشخیص نفوذ برای زیرساخت‌های امنیتی اغلب سازمان‌ها مورد نیاز می‌باشند. این سند برای کسانی که نیازمند درک اهداف امنیتی روش‌های تشخیص نفوذ جهت انتخاب و پیکربندی سیستم‌های تشخیص نفوذ برای سیستم‌ها و شبکه‌های خاص می‌باشند، توسعه یافته است.

➢ **SP 800-28: Guidelines on Active Content and Mobile Code, (2008)**

هدف از این سند ارایه یک دید کلی از تکنولوژی‌های محتوای فعال و کد موبایل در استفاده امروزی و درکی برای تصمیم‌گیری‌های امنیت فناوری اطلاعات آگاهانه در برنامه‌های خود می‌باشد. همچنین در مورد تهدیدات، ریسک‌های تکنولوژی و حفاظت سیستم‌های کاربر نهایی (مانند دسکتاپ و لپ تاپ) جزئیاتی را ارایه می‌دهد.

این سند ممکن است توسط سازمان‌ها به منظور افزایش امنیت برای استفاده موجود و آینده از محتوای فعال به منظور کاهش حوادث امنیتی مرتبط استفاده شود. این سند جنبه‌های مربوط به تامین امنیت محتوای فعال را پوشش نمی‌دهد:

---

[۹] Accountability

- ملاحظات امنیتی عمومی مربوط به وب سرور و مروگر
- توسعه نرم‌افزار وب امن

➢ **SP 800-67: Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, (2012)**

این سند، الگوریتم رمزگذاری داده سه گانه[10] (TDEA) را مشخص می‌کند که شامل اجزای اولیه موتور رمزنگاری، الگوریتم رمزنگاری داده[11](DEA) می‌باشد. این الگوریتم توسط سازمان فدرال برای محافظت از داده‌های حساس طبقه بندی نشده استفاده می‌شود. حفاظت از داده در زمان انتقال یا هنگام ذخیره‌سازی برای حفظ محرمانگی و صحت اطلاعات ارایه شده توسط داده‌ها ضروری می‌باشد. این سند مراحل رمزنگاری موردنیاز به منظور حفاظت از اطلاعات را با استفاده از این الگوریتم تعریف می‌کند.

➢ **SP 800-38A: Recommendation for Block Cipher Modes of Operation: Methods and Techniques, (2001)**

این سند توصیه‌های مربوط به مد عملیاتی با استفاده از الگوریتم رمزنگاری قطعه‌ای کلید متقارن را فراهم می‌کند. این راهنما پنج مد عملیاتی محرمانه را برای استفاده با یک الگوریتم رمزنگاری قطعه‌ای کلید متقارن تعریف می‌کند:

- Electronic Codebook (ECB)
- Cipher Block Chaining (CBC)
- Cipher Feedback (CFB)
- Output Feedback (OFB)
- Counter (CTR)

این مدها می‌توانند حفاظت از رمزنگاری را برای داده‌های حساس طبقه بندی نشده فراهم نمایند.

➢ **SP 800-38B: Recommendation for Block Cipher Modes of Operation: the CMAC Mode for Authentication, (2016)**

---

[10] Triple Data Encryption Algorithm

[11] Data Encryption Algorithm

این سند (بخش دوم) شامل یک سری از توصیه‌های مربوط به مدهای عملیاتی رمزنگاری قطعه‌ای کلید متقارن می‌باشد.

این توصیه یک الگوریتم کد تصدیق پیام [۱۲](MAC) مبتنی بر رمزنگاری قطعه‌ای کلید متقارن را مشخص می‌کند. الگوریتم MAC مبتنی بر رمزنگاری قطعه‌ای ، CMAC نامیده می‌شود، ممکن است برای اطمینان از صحت و جامعیت داده‌های باینری استفاده شود.

- **SP 800-38C: Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality, (2007)**

این سند شامل یک سری از توصیه‌های مربوط به مدهای عملیاتی رمزنگاری قطعه‌ای کلید متقارن می‌باشد.

این توصیه یک مد عملیاتی به نام CCM، را برای الگوریتم رمزنگاری قطعه‌ای کلید متقارن تعریف می‌کند. مد CCM ممکن است به منظور اطمینان از محرمانگی و صحت داده‌های کامپیوتری به وسیله ترکیب تکنیک‌هایی مانند مد شمارنده[۱۳] (CTR) و الگوریتم کد اصالت‌سنجی زنجیره رمز-قطعه [۱۴] (CBC-MAC) استفاده شود.

- **SP 800-22: A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, (2010)**

این سند برخی از جنبه‌های انتخاب و تست مولد اعداد تصادفی و شبه تصادفی را بررسی می‌کند. خروجی چنین مولدهایی ممکن است در بسیاری از کاربردهای رمزنگاری استفاده شود. مولدهای سازگار ممکن است برای استفاده در کاربردهای رمزنگاری نیاز داشته باشند که الزامات قوی‌تری را نسبت به سایر برنامه‌های کاربردی درنظر بگیرند. این سند برخی از معیارها را برای توصیف و انتخاب مولد مناسب بررسی می‌کند.

---

[12] Message Authentication Code

[13] Counter mode

[14] Cipher Block Chaining-Message Authentication Code

موضوع آزمایش آماری و ارتباط آن با تحلیل رمز را توضیح و برخی از آزمون‌های آماری توصیف شده را ارایه می‌دهد.

- **SP 800-20: Modes of Operation Validation System for the Triple Data Encryption Algorithm (TMOVS): Requirements and Procedures, (2012)**

سیستم اعتبارسنجی مد عملیاتی الگوریتم رمزنگاری سه گانه، روش‌های مورداستفاده در اعتبارسنجی پیاده‌سازی الگوریتم DES سه‌گانه در استاندارد رمزنگاری داده (DES) را مشخص می‌کند. این سند دید کلی از الگوریتم DES سه گانه فراهم می‌کند و طراحی اولیه و پیکربندی TMOVS را معرفی می‌کند.

- **SP 800-12: An Introduction to Computer Security, (2017)**

این استاندارد، راهنمایی‌هایی را در رابطه با امنیت کامپیوتر از جمله امنیت سخت‌افزار، نرم‌افزار و منابع اطلاعاتی، مفاهیم مرتبط با امنیت کامپیوتر، ملاحظات هزینه و روابط بین کنترل‌های امنیتی ارایه می‌دهد. کنترل امنیتی در سه دسته کنترل‌های مدیریتی، کنترل‌های عملیاتی و کنترل‌های تکنولوژی قرار می‌گیرد. بخشی از این استاندارد به امنیت و برنامه‌ریزی در چرخه حیات سیستم‌های کامپیوتری اختصاص داده شده است. همچنین مزایای کنترل‌های امنیتی مختلف و حالات آن‌ها که برای اجرا مناسب است، موردبحث قرار گرفته است.

- **SP 800-27: Engineering Principles for Information Technology Security (A Baseline for Achieving Security), (2004)**

این استاندارد، مبنایی برای دستیابی به امنیت فناوری اطلاعات است. برخی از اصول این سند عبارتست از:

- ایجاد سیاست امنیتی بی‌عیب به عنوان مبنا برای طراحی
- پرداختن به امنیت به عنوان بخش جدایی‌ناپذیر از طراحی کل سیستم
- ترسیم شفاف مرزهای امنیتی فیزیکی و منطقی با توجه به سیاست‌های امنیتی
- کاهش ریسک تا حد مجاز

- فرض بر ناامن بودن سیستم‌های خارجی
- پیاده‌سازی مناسب، اقدامات امنیتی سیستم برای پاسخگویی به اهداف
- طراحی و راه‌اندازی سیستم فناوری اطلاعات به منظور محدودسازی آسیب‌پذیری و انعطاف در پاسخ‌گویی

➢ **SP 800-65: Integrating IT Security into the Capital Planning and Investment Control Process, (2005)**

این سند برای کمک به سازمان فدرال جهت یکپارچه‌سازی امنیت فرایندهای برنامه‌ریزی سرمایه و کنترل سرمایه‌گذاری[۱۵](CPIC) مورد استفاده قرار می‌گیرد که ارایه رویکرد هدفمند آن به انتخاب مدیریت و سنجش سرمایه‌گذاری‌های امنیتی کمک می‌کند. این رویکرد هدفمند به طور خاص منظوره می‌تواند به فعالیت‌های زیر کمک کند:

✓ چگونگی نیازمندی‌های مربوط به امنیت را توضیح می‌دهد و از فرایند برنامه‌ریزی سرمایه و کنترل سرمایه‌گذاری فناوری اطلاعات حمایت می‌کند.

✓ درک مراحل فرایند مدیریت سرمایه‌گذاری مانند انتخاب، کنترل و ارزیابی که به سرمایه‌گذاری‌های امنیتی وابسته هستند.

✓ شناسایی نقش‌های وابسته به برنامه‌ریزی سرمایه و کنترل سرمایه‌گذاری و مسئولیت مورد نیاز جهت مدیریت سرمایه‌گذاری‌های امنیتی

✓ توضیح بهترین روش فرایند مدیریت امنیت فناوری اطلاعات و چرایی اهمیت اخذ تصمیمات صحیح امنیت فناوری اطلاعات

✓ درک چگونگی توسعه نیازمندی‌های امنیتی و پشتیبانی مناسب از اسناد و مدارک مربوط به فناوری اطلاعات

---

[15] capital planning and investment control

- ✓ شناسایی مراحل و موارد مورد نیاز جهت تکمیل کسب وکار مناسب در حمایت از درخواست‌های سرمایه‌گذاری
- ✓ درک مسائل مرتبط با ترکیب امنیت در فرایند برنامه‌ریزی سرمایه و کنترل سرمایه‌گذاری

- **SP 800-60: Guide for Mapping Types of Information and Information Systems to Security Categories, (2008)**

شناسایی اطلاعات پردازش شده در یک سیستم اطلاعات برای انتخاب کنترل‌های امنیتی مناسب و اطمینان از محرمانگی، یکپارچگی و در دسترس بودن سیستم و اطلاعات آن ضروری است. این راهنما برای کمک به سازمان‌ها به منظور نگاشت سطوح تاثیر امنیت به انواع اطلاعات (به عنوان مثال اطلاعات حریم خصوصی، پزشکی، مالی و...) و سیستم‌های اطلاعاتی (به عنوان مثال ماموریت بحرانی، مدیریت و ...) در نظر گرفته شده است.

مخاطبان این سند عبارتند از:

- اشخاصی که با مدیریت امنیت اطلاعات و سیستم‌های اطلاعات و مسئولیت‌های نظارت آشنا هستند.
- مقامات سازمانی دارای منافع ویژه در انجام ماموریت‌های سازمانی
- افرادی که دارای مسئولیت توسعه سیستم اطلاعات هستند.
- افرادی که پیاده‌سازی امنیت اطلاعات و مسئولیت عملیاتی را انجام می‌دهند.

- **SP 800-59: Guideline for Identifying an Information System as a National Security System, (2003)**

این سند راهنمایی‌هایی را در رابطه با وزارت دفاع، از جمله سازمان امنیت ملی، برای شناسایی یک سیستم اطلاعاتی به عنوان سیستم امنیت ملی فراهم می‌کند. اساس و مبنای این راهنمایی‌ها قانون مدیریت امنیت اطلاعات فدرال است که الزامات دولتی را برای امنیت اطلاعات ارایه می‌دهد.

- **SP 800-23: Guidelines to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products, (2000)**

این سند دستورالعمل‌هایی را برای سازمان‌های فدرال جهت دستیابی و استفاده از محصولات امنیتی فناوری اطلاعات فراهم می‌کند و همچنین مشاوره‌هایی برای سیستم‌های حساس طبقه بندی نشده ارایه می‌دهد.

- **SP 800-66: An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, (2008)**

هدف از این سند کمک به آموزش خوانندگان در مورد استانداردهای امنیتی موجود در قانون امنیتی HIPAA است. این سند یک دید کلی از قانون امنیتی HIPAA فراهم نموده و فعالیت‌های عمومی یک سازمان که باید در اجرای یک برنامه امنیت اطلاعات درنظر گرفته شود را شناسایی می‌کند.

- **SP 800-30: Risk Management Guide for Information Technology Systems**

مدیریت ریسک، یکی از جنبه‌های کلیدی مدیریت امنیت است که نقش مهمی در حفاظت از دارایی‌های اطلاعاتی دارد. این سند با مرور کلی از مدیریت ریسک آغاز شده و مواردی که منجر به موفقیت برنامه مدیریت ریسک می‌شود را پوشش می‌دهد. این راهنما همچنین نشان می‌دهد که چگونه مدیریت ریسک، قادر به یکپارچه‌سازی چرخه حیات توسعه سیستم می‌شود. این سند همچنین مواردی مانند طبقه‌بندی کنترل، تحلیل سود و زیان، ارزیابی ریسک باقی‌مانده و گزینه‌های کاهش آن و نیز مراحلی که باید پس از اتمام روند ریسک درنظر گرفته شوند را شامل می‌شود.

- **SP 800-49 Federal S/MIME V3 Client Profile**

S/MIME[16] مجموعه‌ای از مشخصات برای تامین امنیت پست الکترونیک است. S/MIME پروتکلی را برای افزودن سرویس‌های امنیتی رمزنگاری از طریق کپسوله‌سازی[17] اشیای رمزگذاری شده و امضا شده MIME به صورت دیجیتالی توصیف می‌کند. سرویس‌های امنیتی ارایه شده توسط S/MIME احرازهویت، عدم انکار مبدا، یکپارچگی پیام و حفظ حریم خصوصی پیام می‌باشد. S/MIME V3 آخرین نسخه S/MIME است. هدف این سند ارایه ویژگی‌های امنیتی ایمیل مانند رمزگذاری ایمیل، رسید امضا و... می‌باشد.

---

[16] Secure / Multipurpose Internet Mail Extensions

[17] encapsulation

- **FIPS 180-4: Secure Hash Standard (SHS), (2015)**

این استاندارد الگوریتم‌های چکیده امنی مانند SHA-1, SHA-224, SHA-256, SHA-384, SHA-256 و... را مشخص می‌کند که برای تولید خلاصه پیام استفاده می‌شوند. این خلاصه‌ها برای تعیین تغییر پیام استفاده می‌شوند. این الگوریتم قادر به تعیین یکپارچگی یک پیام است. این ویژگی در تولید و تایید امضاهای دیجیتال، کد تایید هویت پیام و در تولید اعداد تصادفی یا بیت‌ها مفید می‌باشد.

- **FIPS 186: Digital Signature Standard (DSS), (2013)**

این استاندارد مجموعه‌ای از الگوریتم‌های مشخص است که برای تولید امضای دیجیتال مورد استفاده قرار می‌گیرند. از این سند همچنین جهت تشخیص تغییرات غیرمجاز استفاده می‌شود. امضای دیجیتال می‌تواند برای احراز هویت به کار گرفته شود. DSS دستورالعمل‌هایی را برای تولید امضای دیجیتال، صحت‌سنجی و اعتبارسنجی توصیه می‌کند.

- **FIPS 197: Advanced Encryption Standard (AES), (2001)**

این استاندارد برای اطمینان از محرمانه بودن اطلاعات الکترونیکی تصویب شده است. الگوریتم AES، نوعی رمزنگاری متقارن قطعه‌ای است که برای رمزنگاری و رمزگشایی کاربرد دارد. این استاندارد جایگزین رمزنگاری استاندارد داده (DES) FIPS 46-3 شد که در آن برای حفاظت از داده‌ها، از یکی از دو الگوریتم DES یا الگوریتم رمزنگاری داده سه‌گانه (TDEA) استفاده می‌شد. الگوریتم AES سریع‌تر و قوی‌تر از DES در حفاظت از داده‌ها است.

- **FIPS 198-1: The Keyed-Hash Message Authentication Code(HMAC), (2008)**

این استاندارد یک کد اصالت‌سنجی پیام مبتنی‌بر درهم‌سازی (HMAC)، مکانیسمی برای تایید پیام با استفاده از توابع درهم‌ساز رمزنگاری، را توصیف می‌کند. HMAC می‌تواند با هر تابع درهم‌ساز رمزنگاری

تایید شده، در ترکیب با یک کلید محرمانه مشترک استفاده شود. قدرت رمزنگاری HMAC بستگی به خواص تابع درهم‌ساز دارد.

- **FIPS 199: Standards for Security Categorization of Federal Information and Information Systems, (2004)**

این سند، استانداردهایی را برای طبقه‌بندی امنیت اطلاعات و سیستم‌های اطلاعاتی ایجاد می‌کند. استانداردهای طبقه‌بندی امنیتی برای اطلاعات و سیستم‌های اطلاعاتی یک چارچوب مرسوم را فراهم می‌نمایند و برای دولت فدرال مواردی مانند مدیریت موثر و نظارت بر برنامه‌های امنیت اطلاعات، کفایت و اثربخشی سیاست‌های امنیت اطلاعات، روش‌ها و شیوه‌ها را توسعه می‌دهد.

❖ مرحله تهیه/توسعه

در طی این مرحله سیستم طراحی، خریداری، برنامه‌ریزی و توسعه داده می‌شود. فعالیت‌های کلیدی در این مرحله شامل ارزیابی ریسک و استفاده از نتایج تکمیلی کنترل‌های امنیتی پایه است.

جدول ۲: استانداردهای امنیتی مرحله تهیه/ توسعه

شماره استاندارد	نام استاندارد
SP 800-64	Security Considerations in the System Development Life Cycle, Rev.2 (2008)
	ملاحظات امنیتی در چرخه حیات توسعه سیستم
SP 800-61	Computer Security Incident Handling Guide, Rev. 2 (2012)
	راهنمای رسیدگی به حوادث امنیتی کامپیوتری
* SP 800-36	Guide to Selecting Information Technology Security Products, (2003)
	راهنمای انتخاب محصولات امنیتی فناوری اطلاعات
* SP 800-35	Guide to Information Technology Security Services, (2003)
	راهنمای سرویس‌های امنیتی فناوری اطلاعات
SP 800-70	National Checklist Program for IT Products: Guidelines for Checklist Users and Developers, Rev.3, (2016)
	برنامه چک لیست ملی برای محصولات فناوری اطلاعات: راهنمایی برای چک لیست کاربران و توسعه‌دهندگان
SP 800-58	Security Considerations for Voice Over IP Systems, (2005)

شماره استاندارد	نام استاندارد
	ملاحظات امنیتی برای سیستم‌های VOIP
* SP 800-48	Guide to Securing Legacy IEEE 802.11 Wireless Networks, Rev.1, (2008) راهنمایی برای تامین امنیت شبکه‌های بی‌سیمIEEE 802.11
* SP 800-46	Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security, Rev.2, (2016) راهنمایی برای امنیت دورکاری سازمان‌ها، دسترسی از راه دور و استفاده از دستگاه‌های شخصی (BYOD)
* SP 800-45	Guidelines on Electronic Mail Security, V.2, (2007) راهنمایی در مورد امنیت پست الکترونیک
* SP 800-44	Guidelines on Securing Public Web Servers, V.2, (2007) راهنمایی در مورد امنیت وب سرورهای عمومی
* SP 800-41	Guidelines on Firewalls and Firewall Policy, (2009) راهنمایی‌هایی در مورد دیواره آتش و سیاست‌های آن
* SP 800-40	Guide to Enterprise Patch Management Technologies Rev.3, (2013) راهنمایی برای فناوری‌های مدیریت وصله سازمان
* SP 800-33	Underlying Technical Models for Information Technology Security, (2001) مدل فنی بنیادی برای امنیت فناوری اطلاعات
* SP 800-31	Intrusion Detection systems سیستم‌های تشخیص نفوذ
* SP 800-28	Guidelines on Active Content and Mobile Code, V.2, (2008) راهنما در مورد محتوا فعال و کد موبایل
SP 800-55	Performance Measurement Guide for Information Security, Rev.1, (2008) راهنمای سنجش عملکرد برای امنیت اطلاعات
SP 800-37	Guide for Applying the Risk Management Framework to Federal Information Systems: a Security Life Cycle Approach, Rev.1 (2014) راهنمایی برای امنیت گواهی و مجوز رسمی از سیستم اطلاعات فدرال
SP 800-53A	Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans, Rev. 4 (2014) راهنمایی برای ارزیابی کنترل‌های امنیتی و حریم خصوصی در سازمان‌ها و سیستم‌های اطلاعات فدرال: ایجاد طرح‌های ارزیابی موثر
* SP 800-12	An Introduction to Computer Security, Rev.1 (2017) مقدمه‌ای بر امنیت کامپیوتر

شماره استاندارد	نام استاندارد
* SP 800-65	Integrating IT Security into the Capital Planning and Investment Control Process, 2005 یکپارچه‌سازی امنیت فناوری اطلاعات در فرایند برنامه‌ریزی سرمایه و کنترل سرمایه‌گذاری
* SP 800-23	Guidelines to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products, 2000 راهنمایی‌هایی برای سازمان‌های فدرال جهت تضمین امنیت و کسب یا استفاده از محصولات تست یا ارزیابی شده
* SP 800-66	An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, 2008 یک راهنمای منابع مقدماتی موردنیاز برای پیاده‌سازی قانون امنیتی پاسخگویی و انتقال بیمه سلامت
* SP 800-30	Risk Management Guide for Information Technology Systems راهنمای مدیریت ریسک برای سیستم‌های فناوری اطلاعات
SP 800-53	Recommended Security and Privacy Controls for Federal Information Systems and Organizations, Rev 4 (2013) کنترل‌های امنیتی و حریم خصوصی برای سازمان‌ها و سیستم‌های اطلاعاتی فدرال
SP 800-18	Guide for Developing Security Plans for Federal Information Systems, 2006 راهنمایی برای توسعه برنامه‌های امنیتی برای سیستم‌های اطلاعاتی فدرال
SP 800-50	Building an Information Technology Security Awareness and Training Program, 2003 ایجاد یک برنامه آموزشی و آگاهی از امنیت فناوری اطلاعات
SP 800-16	A Role-Based Model for Federal Information Technology/Cybersecurity Training, Rev. 1, 2014 یک مدل مبتنی بر نقش برای آموزش امنیت سایبری/ فناوری اطلاعات فدرال
FIPS 140-2	Security Requirements for Cryptographic Modules, 2001 نیازمندی‌های امنیتی برای ماژول‌های رمزنگاری
FIPS 196	Entity Authentication Using Public Key Cryptography احرازهویت موجودیت با استفاده از رمزنگاری کلید عمومی

* برای مطالعه بیشتر در مورد این استانداردها به توضیحات مرحله آغاز مراجعه شود.

در این قسمت هریک از استانداردهای امنیتی مرحله تهیه/توسعه شرح داده شده است:

- **SP 800-64: Security Considerations in the System Development Life Cycle**

در نسخه‌دوم این استاندارد به طور مستقیم به امنیت نرم‌افزار پرداخته شده است چرا که این سند، راهنمایی‌هایی را برای پیاده‌سازی امنیت درون چرخه حیات توسعه سیستم یا نرم‌افزار ارایه می‌دهد و به طیف گسترده‌ای از مخاطبان سیستم‌های اطلاعاتی و کارشناسان امنیت اطلاعات اعم از صاحبان سیستم، صاحبان اطلاعات، توسعه‌دهندگان و مدیران برنامه خدمت می‌کند.

- **SP 800-61: Computer Security Incident Handling Guide**

تهدیدهایی که در گذشته عمر کوتاهی داشته و به آسانی پیدا می‌شدند، امروزه جای خود را به تهدیدات مداوم پیشرفته[۱۸] (APTها) داده‌اند و این امر، ضرورت استفاده از رویه‌های رسیدگی به حوادث را نشان می‌دهد. استاندارد SP 800-61، سازمان‌ها را در توسعه رویه‌های رسیدگی به حوادث و کنترل تهدیدات امنیتی یاری می‌کند. این استاندارد برای تیم‌های پاسخگویی به حوادث[۱۹] مفید است.

- **SP 800-70: National Checklist Program for IT Products: Guidelines for Checklist Users and Developers**

این سند استفاده، منافع و مدیریت چک لیست‌ها را توصیف کرده و چگونگی استفاده از برنامه چک لیست ملی[۲۰] NIST را به منظور دستیابی و بازیابی چک لیست‌ها توضیح می‌دهد. این سند برای کاربران و توسعه‌دهندگان بالقوه و بالفعل چک لیست برای فناوری اطلاعات چه در بخش خصوصی و چه بخش عمومی درنظر گرفته شده است. این سند برای کاربران چک لیست، توصیه‌هایی را جهت نحوه انتخاب چک لیست از مخزن چک لیست ملی NIST و اعمال آن‌ها بر محصولات فناوری اطلاعات ارایه می‌کند. برای

---

18 Advanced Persistent Threats

19 Incident Response Team

20 National Checklist Program

توسعه‌دهندگان چک لیست، این سند سیاست‌ها، روش‌ها و نیازمندی‌های عمومی جهت شرکت در برنامه چک لیست امنیتی NIST را تنظیم می‌کند.

- **SP 800-58: Security Considerations for Voice Over IP Systems**

این نشریه به معرفی VOIP، چالش‌های امنیتی و اقدامات متقابل بالقوه برای آسیب‌پذیری‌های VOIP می‌پردازد. هدف از این سند ارایه راهنمایی‌هایی برای ایجاد شبکه‌های VOIP امن است و همچنین فناوری VOIP و راه‌حل‌های آن را مورد بررسی قرار می‌دهد. ملاحظات امنیتی VOIP برای شبکه تلفن عمومی تا حد زیادی خارج از محدوده این سند است. اگر چه مسایل حقوقی مربوط به VOIP فراتر از محدوده این سند می‌باشد، خوانندگان بایستی با احکام و قوانین حاکم بر رهگیری و یا نظارت بر خطوط VOIP آگاه باشند و رکوردهای تماس را نگهداری کنند، که ممکن است از رکوردهای سیستم‌های تلفنی متعارف متفاوت باشد.

- **SP 800-55: Performance Measurement Guide for Information Security**

این سند راهنمایی برای توسعه، انتخاب و اجرای خاصی از معیارهای سطح برنامه و سیستم اطلاعاتی جهت مشخص کردن راندمان/تاثیر اجرا، تاثیر کنترل‌های امنیتی و دیگر فعالیت‌های مربوط به امنیت می‌باشد. این دستورالعمل چگونگی استفاده سازمان از معیارها، شناسایی مناسب بودن کنترل‌های امنیتی در مکان، سیاست‌ها و رویه‌ها را مشخص می‌کند.

همچنین این سند روشی را ارایه می‌دهد که به مدیریت در رابطه یا اعمال منابع اطلاعاتی اضافی کمک می‌کند همچنین کنترل‌های امنیتی ناکارآمد را بررسی کرده و کنترل‌های امنیتی را برای ادامه نظارت اولویت‌بندی می‌کند. همچنین استفاده از معیارهایی که در سرمایه‌گذاری امنیت اطلاعات توجیه کافی دارند را توضیح می‌دهد و از تصمیم‌گیری‌های مبتنی بر ریسک پشتیبانی می‌کند.

- **SP 800-37: Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach**

هدف از این سند ارایه راهنمایی برای استفاده از چارچوب مدیریت ریسک در سیستم‌های اطلاعاتی فدرال شامل فعالیت‌های طبقه‌بندی امنیت، انتخاب، اجرا، ارزیابی و نظارت‌بر کنترل‌های امنیتی است. این راهنما برای موارد زیر توسعه یافته است:

- اطمینان از این که مدیریت ریسک‌های امنیتی مربوط به سیستم اطلاعاتی مطابق با اهداف کسب‌وکار سازمان است.
- اطمینان از این که نیازمندی‌های امنیت اطلاعات از جمله کنترل‌های امنیتی ضروری، در معماری سازمان و فرایندهای چرخه حیات توسعه سازمان در نظر گرفته شده است.
- دستیابی به اطلاعات و سیستم‌های اطلاعاتی امن‌تر در دولت فدرال، از طریق پیاده‌سازی استراتژی‌های کاهش ریسک مناسب.

- **SP 800-53A: Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans**

هدف از این نشریه ارایه راهنمایی‌هایی برای ایجاد طرح‌های ارزیابی امنیتی موثر و مجموعه‌ای جامع از روش‌ها برای اثربخشی کنترل‌های امنیتی به کار گرفته شده در سیستم‌های اطلاعاتی می‌باشد. این دستورالعمل‌ها برای کنترل‌های امنیتی تعریف شده در استاندارد SP 800-53 استفاده می‌شود.

مخاطبان این نشریه:

- افراد مسئول توسعه و یکپارچه‌سازی سیستم اطلاعات
- افرادی که مسئول ارزیابی و نظارت امنیت اطلاعات هستند.
- افراد مسئول نظارت، مدیریت امنیت
- افرادی که مسئول پیاده‌سازی امنیت اطلاعات هستند.

- **SP 800-53: Recommended Security and Privacy Controls for Federal Information Systems and Organizations**

این نشریه یک کاتالوگ از کنترل‌های امنیتی و حفظ حریم خصوصی برای سیستم‌های اطلاعات فدرال و سازمان‌ها فراهم می‌کند. همچنین فرایندی برای انتخاب کنترل‌های مناسب برای محافظت از عملیات

سازمانی (رسالت، توابع، نمود و شهرت)، دارایی‌های سازمانی، افراد، سازمان‌های دیگر و ملت از مجموعه‌ای متنوع از تهدیدات از جمله حملات خصمانه سایبری، بلایای طبیعی، شکست‌های ساختاری و خطاهای انسانی ارایه می‌دهد. لازم به ذکر است که نسخه پنج این سند در دست تهیه است.

- **SP 800-18: Guide for Developing Security Plans for Federal Information Systems**

هدف اصلی از طرح‌ریزی امنیت اطلاعات، بهبود حفاظت از منابع سیستم اطلاعات است. طرح امنیت باید به صورت دوره‌ای و مداوم، صحت مفهومی و کاربردی را بررسی کند. این سند، چارچوبی را برای توسعه برنامه‌های امنیتی ارایه می‌دهد. این چارچوب دارایی‌های اطلاعاتی را بر اساس تاثیر آن‌ها بر سه هدف اصلی امنیت شامل محرمانگی، صحت و دسترسی‌پذیری، طبقه‌بندی می‌کند.

- **SP 800-50: Building an Information Technology Security Awareness and Training Program**

این سند دستورالعمل‌هایی را به منظور ایجاد و حفظ یک برنامه آموزشی و آگاهی جامع به عنوان بخشی از برنامه امنیت فناوری اطلاعات سازمان درنظرگرفته می‌شود. این دستورالمل‌ها در چرخه حیات سیستم اعم از طراحی، توسعه، اجرا و سنجش عملکرد ارایه شده است.

این سند دستورالعمل‌هایی است در رابطه با این که، متخصصان امنیت فناوری اطلاعات چگونه می‌توانند نیازهای آموزشی را شناسایی و یک طرح آموزشی را توسعه دهند. همچنین این سند، نحوه انجام موارد زیر را توضیح می‌دهد:

- انتخاب عناوین آموزش
- یافتن منابع و مواد آموزشی
- ارزیابی اثربخشی برنامه
- به روزرسانی و بهبود تمرکز بر روی تغییر اولویت‌های سازمانی و فناوری

- **SP 800-16: A Role-Based Model for Federal Information Technology /Cybersecurity Training**

این سند یک چارچوب مفهومی جدید را برای آموزش امنیت فناوری اطلاعات ارایه می‌دهد. این چارچوب شامل نیازمندی‌های آموزش امنیت فناوری اطلاعات برای محیط محاسبات توزیع شده است. رویکرد آموزش در این سند براساس اصول زیر طراحی شده است:

- تمرکز بر روی توابع کار، یا نقش‌ها و مسئولیت‌ها
- ترسیم تفاوت میان آگاهی و آموزش
- ارایه یک چارچوب یکپارچه برای شناسایی نیازمندی‌های آموزشی و اطمینان از اموزش‌های مناسب
- ارایه یک ابزار توسعه
- ارایه یک ساختار برای ارزیابی اثربخشی یادگیری

- **FIPS 140-2: Security Requirements for Cryptographic Modules**

این استاندارد نیازمندی‌های خاص ماژول رمزنگاری را مشخص می‌کند و چهار سطح افزایش کیفی (از سطح یک تا چهار) برای پوشش طیف گسترده‌ای از قابلیت‌های برنامه و محیط ارایه می‌دهد. این سند، نیازمندی‌های امنیتی مناطقی را که در رابطه با طراحی و اجرای ماژول رمزنگاری است را پوشش می‌دهد که شامل مشخصات ماژول، پورت‌ها و رابط‌ها، نقش‌ها، سرویس‌ها، احرازهویت، مدل وضعیت محدود، امنیت فیزیکی، محیط عملیاتی، مدیریت کلید رمزنگاری، رابط مغناطیسی، مطابقت مغناطیسی (EMI/EMC)، خودآزمایی و طراحی مطمئن می‌شود. همچنین این استاندارد تعیین می‌کند که توسعه‌دهندگان ماژول‌های رمزنگاری و فروشندگان آن‌ها چه کنترل‌های امنیتی خاصی نیاز دارند تا حملات را کاهش دهند.

- **FIPS 196: Entity Authentication Using Public Key Cryptography**

این سند دو پروتکل برای احراز هویت یک موجودیت که با استفاده از الگوریتم رمزنگاری کلید عمومی برای تولید و تایید امضای دیجیتال مشخص کند. یک موجودیت می‌تواند هویت خود را به موجودیت دیگری با استفاده از یک کلید خصوصی برای تولید یک امضای دیجیتال در یک چالش تصادفی اثبات کند. استفاده

از رمزنگاری احرازهویت قوی را فراهم می‌کند، که نهادهای احرازهویت به اشتراک گذاشتن اطلاعات محرمانه نیاز ندارد.

❖ مرحله اجرا/ارزیابی

در این مرحله ویژگی‌های امنیتی سیستم پیکربندی، فعال و عملکرد این ویژگی‌ها آزموده می‌شود. همچنین سیستم نصب یا اجرا و مجوز رسمی عملکرد سیستم دریافت می‌گردد.

بررسی طراحی و تست سیستم باید قبل از بهره‌داری سیستم انجام شود تا از مطابقت با مشخصات امنیتی اطمینان حاصل گردد. همچنین اگر کنترل جدید به نرم‌افزار یا سیستم پشتیبانی اضافه گردید باید ازمون پذیرش کنترل جدید انجام شود. این کار مطابقت کنترل‌های جدید را با مشخصات امنیتی تضمین می‌کند.

جدول ۳: استانداردهای امنیتی مرحله اجرا / ارزیابی

شماره استاندارد	نام استاندارد
** SP 800-64	Security Considerations in the System Development Life Cycle, Rev.2 (2008) ملاحظات امنیتی در چرخه حیات توسعه سیستم
SP 800-51	Guide to Using Vulnerability Naming Schemes, Rev.1 (2011) راهنمایی برای استفاده از طرح‌های نام‌گذاری آسیب‌پذیری
** SP 800-61	Computer Security Incident Handling Guide, Rev. 2 (2012) راهنمای رسیدگی به حوادث امنیتی کامپیوتری
* SP 800-36	Guide to Selecting Information Technology Security Products (2003) راهنمای انتخاب محصولات امنیتی فناوری اطلاعات
* SP 800-35	Guide to Information Technology Security Services (2003) راهنمای سرویس‌های امنیتی فناوری اطلاعات
SP 800-56A	Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, (2013) توصیه‌ای برای طرح‌های تولید جفت کلید با استفاده از رمزنگاری لگاریتم گسسته
SP 800-57	Recommendation for Key Management Part 1: General, (2016) Part 2: Best Practices for Key Management Organization, (2005) Part 3: Application-Specific Key Management Guidance, (2015)

شماره استاندارد	نام استاندارد
	توصیه‌ای برای مدیریت کلید بخش ۱: کلیات بخش ۲: بهترین روش برای سازمان مدیریت کلید بخش ۳: راهنمایی‌هایی جهت مدیریت کلید خاص حوزه نرم‌افزار
** SP 800-70	National Checklist Program for IT Products: Guidelines for Checklist Users and Developers, Rev.3 (2016) برنامه چک لیست ملی برای محصولات فناوری اطلاعات: راهنمایی برای چک لیست کاربران و توسعه‌دهندگان
SP 800-68	Guide to Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist, Rev.1 (2008) راهنمای امنیت سیستم‌های مایکروسافت ویندوز XP برای متخصصان فناوری اطلاعات
** SP 800-58	Security Considerations for Voice Over IP Systems (2005) ملاحظات امنیتی برای سیستم‌های VOIP
* SP 800-48	Guide to Securing Legacy IEEE 802.11 Wireless Networks, Rev.1 (2008) راهنمایی برای تامین امنیت شبکه‌های بی‌سیمIEEE 802.11
* SP 800-47	Security Guide for Interconnecting Information Technology Systems (2002) راهنمای امنیت برای ارتباطات سیستم‌های فناوری اطلاعات
* SP 800-46	Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security, Rev.2 (2016) راهنمایی برای امنیت دورکاری سازمان‌ها، دسترسی از راه دور و استفاده از دستگاه‌های شخصی (BYOD)
* SP 800-45	Guidelines on Electronic Mail Security, V.2 (2007) راهنمایی در مورد امنیت پست الکترونیک
* SP 800-44	Guidelines on Securing Public Web Servers, V.2 (2007) راهنمایی در مورد امنیت وب سرورهای عمومی
* SP 800-41	Guidelines on Firewalls and Firewall Policy (2009) راهنمایی‌هایی در مورد دیواره آتش و سیاست‌های آن
* SP 800-40	Guide to Enterprise Patch Management Technologies Rev.3 (2013) راهنمایی برای فناوری‌های مدیریت وصله سازمان
* SP 800-33	Underlying Technical Models for Information Technology Security (2001) مدل فنی بنیادی برای امنیت فناوری اطلاعات
* SP 800-31	Intrusion Detection systems (2001) سیستم‌های تشخیص نفوذ
* SP 800-28	Guidelines on Active Content and Mobile Code, V.2 (2008) راهنما در مورد محتوا فعال و کد موبایل
** SP 800-55	Performance Measurement Guide for Information Security, Rev.1 (2008)

شماره استاندارد	نام استاندارد
	راهنمای سنجش عملکرد برای امنیت اطلاعات
** SP 800-37	Guide for Applying the Risk Management Framework to Federal Information Systems: a Security Life Cycle Approach, Rev.1 (2014)
	راهنمایی برای امنیت گواهی و مجوز رسمی از سیستم اطلاعات فدرال
** SP 800-53A	Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans, Rev. 4 (2014)
	راهنمایی برای ارزیابی کنترل‌های امنیتی و حریم خصوصی در سازمان‌ها و سیستم‌های اطلاعات فدرال: ایجاد طرح‌های ارزیابی موثر
** FIPS 140-2	Security Requirements for Cryptographic Modules, 2001
	نیازمندی‌های امنیتی برای ماژول‌های رمزنگاری
** FIP S 196	Entity Authentication Using Public Key Cryptography
	احرازهویت موجودیت با استفاده از رمزنگاری کلید عمومی

* برای مطالعه بیشتر در مورد این استانداردها به توضیحات مرحله آغاز مراجعه شود.

** برای مطالعه بیشتر در مورد این استانداردها به توضیحات مرحله تهیه/ توسعه مراجعه شود.

در این قسمت هریک از استانداردهای امنیتی مرحله اجرا/ ارزیابی شرح داده شده است:

- **SP 800-51: Guide to Using Vulnerability Naming Schemes**

هدف از این سند ارایه توصیه‌هایی برای استفاده از طرح‌های نام‌گذاری آسیب‌پذیری است. این سند دو طرح CVE [۲۱] و CCE [۲۲] را تحت پوشش قرار می‌دهد. این سند مقدمه‌ای را برای هر دو طرح و توصیه‌هایی برای سازمان کاربر نهایی در رابطه با استفاده از اسامی تولید شده توسط این طرح‌ها ارایه می‌دهد. همچنین این سند توصیه‌هایی را برای فروشندگان نرم‌افزار و خدمات به منظور چگونگی استفاده از نام‌گذاری آسیب‌پذیری و طرح‌های نامگذاری در ارایه محصولات و خدمات خود ارایه می‌دهد.

مخاطبان در نظر گرفته شده برای این سند افرادی هستند که مسئولیت‌های مربوط به مدیریت آسیب‌پذیری را دارند.

- **SP 800-56A: Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography**

---

[21] Common Vulnerabilities and Exposures

[22] Common Configuration Enumeration

این توصیه مشخصاتی را برای طرح‌های تولید جفت کلید با استفاده از رمزنگاری لگاریتم گسسته فراهم می‌کند که برای استفاده در دولت فدرال ایالات متحده و نیز برای استفاده به همراه استاندارد SP 800-57 در نظر گرفته می‌شود. طرح تولید کلید می‌تواند به صورت طرح توافق کلید یا طرح انتقال کلید مشخص شود. طرح تولید کلید مبتنی بر کلید نامتقارن در این سند، بر اساس الگوریتم دیفی هلمن (DH) و الگوریتم Menezes-QuVanstone در نظر گرفته شده است و همچنین طرح‌های تولید کلید مبتنی بر کلید نامتقارن در استاندارد SP 800-56B نیز آمده است.

- **SP 800-57: Recommendation for Key Management**

این راهنما چارچوبی را برای پشتیبانی از تصمیم‌گیری‌های مناسب در هنگام انتخاب و استفاده از مکانیزم‌های رمزنگاری ایجاد می‌کند. همچنین این سند بر روی مسایل مربوط به مدیریت کلیدهای رمزنگاری متمرکز است. از جمله این موضوعات مرتبط، انتخاب الگوریتم و سایز کلید مناسب، سیاست‌های رمزنگاری، و انتخاب ماژول رمزنگاری می‌باشد. این سند جزئیات پیاده‌سازی ماژول رمزنگاری را بررسی نمی‌کند.

انتشارات ویژه 57-800 شامل سه بخش است:

- بخش ۱ راهنمایی کلی و بهترین شیوه برای مدیریت کلید رمزنگاری را فراهم می‌کند.
- بخش ۲ راهنمایی‌هایی را در رابطه با سیاست‌ها و برنامه‌ریزی امنیتی مورد نیاز برای سازمان‌های دولتی ایالات متحده فراهم می‌کند.
- بخش ۳ راهنمایی‌هایی را در هنگام استفاده از ویژگی‌های رمزنگاری سیستم‌های فعلی فراهم می‌کند.

- **SP 800-68: Guide to Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist**

هدف این سند کمک به متخصصان فناوری اطلاعات در تامین امنیت سیستم‌های ماکروسافت ویندوز XP می‌باشد و همچنین اطلاعات دقیق در مورد ویژگی‌های امنیتی ویندوز XP، دستورالعمل تنظیمات امنیتی

برای برنامه‌های کاربردی محبوب و سیستم عامل ویندوز XP را فراهم می‌کند. هدف اصلی از این سند توصیه و توضیح تنظیمات امن، تست شده برای ایستگاه کاری ویندوز XP می‌باشد.

❖ مرحله عملیات/ نگه‌داری

در این مرحله، سیستم و محصولات در جای خود قرار داده می‌شود و/یا تغییراتی در سیستم توسعه‌یافته و تست شده انجام می‌گردد. و همچنین اجزای سخت‌افزاری و نرم‌افزاری اضافه یا جایگزین می‌شوند.

سازمان باید به طور مداوم بر عملکرد سیستم نظارت داشته باشد و از مطابقت نیازمندی‌های امنیتی از پیش‌تعیین شده اطمینان حاصل کند. مدیریت پیکربندی و فعالیت‌های کنترلی هر گونه تغییر و پیشنهاد حقیقی در طرح امنیت سیستم را مکتوب می‌کنند. سیستم‌های اطلاعاتی ممکن است نیاز به تغییر و ارتقا سخت‌افزار، نرم‌افزار، سیستم‌عامل داشته باشند، ثبت این تغییرات و ارزیابی بالقوه آن‌ها در امنیت یک سیستم، از فعالیت‌های ضروری برای اطمینان از نظارت مستمر است. در ادامه لیستی از استانداردهای امنیتی این مرحله در جدول زیر آمده است.

جدول ۴: لیستی از استانداردهای امنیتی مرحله عمیات/ نگه‌داری

شماره استاندارد	نام استاندارد
*** SP 800-51	Guide to Using Vulnerability Naming Schemes, Rev.1 (2011) راهنمایی برای استفاده از طرح‌های نام‌گذاری آسیب‌پذیری
**SP 800-61	Computer Security Incident Handling Guide, Rev. 2 (2012) راهنمای رسیدگی به حوادث امنیتی کامپیوتری
* SP 800-36	Guide to Selecting Information Technology Security Products (2003) راهنمای انتخاب محصولات امنیتی فناوری اطلاعات
* SP 800-35	Guide to Information Technology Security Services (2003) راهنمای سرویس‌های امنیتی فناوری اطلاعات
* SP 800-14	Generally Accepted Principles and Practices for Securing Information Technology Systems (1996) روش‌ها و اصول پذیرفته شده عمومی برای امنیت سیستم‌های فناوری اطلاعات
* SP 800-41	Guidelines on Firewalls and Firewall Policy (2009) راهنمایی‌هایی در مورد دیواره آتش و سیاست‌های آن
* SP 800-40	Guide to Enterprise Patch Management Technologies Rev.3 (2013) راهنمایی برای فناوری‌های مدیریت وصله سازمان

شماره استاندارد	نام استاندارد
* SP 800-31	Intrusion Detection systems سیستم‌های تشخیص نفوذ
* SP 800-28	Guidelines on Active Content and Mobile Code, V.2 (2008) راهنما در مورد محتوا فعال و کد موبایل
** SP 800-55	Performance Measurement Guide for Information Security, Rev.1 (2008) راهنمای سنجش عملکرد برای امنیت اطلاعات
** SP 800-37	Guide for Applying the Risk Management Framework to Federal Information Systems: a Security Life Cycle Approach, Rev.1 (2014) راهنمایی برای امنیت گواهی و مجوز رسمی از سیستم اطلاعات فدرال
** SP 800-53A	Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans, Rev. 4 (2014) راهنمایی برای ارزیابی کنترل‌های امنیتی و حریم خصوصی در سازمان‌ها و سیستم‌های اطلاعات فدرال: ایجاد طرح‌های ارزیابی موثر
* SP 800-67	Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, Rev.1 (2012) توصیه‌ای برای الگوریتم رمزگذاری داده سه‌گانه (TDEA) رمز قطعه‌ای
* SP 800-38A	Recommendation for Block Cipher Modes of Operation: Methods and Techniques (2001) توصیه‌ای برای مدهای عملیاتی رمز قطعه‌ای: روش‌ها و تکنیک‌ها
* SP 800-38B	Recommendation for Block Cipher Modes of Operation: the CMAC Mode for Authentication (2016) توصیه‌ای برای مدهای عملیاتی رمز قطعه‌ای: مد CMAC برای احرازهویت
* SP 800-38C	Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality (2007) توصیه‌ای برای مدهای عملیاتی رمز قطعه‌ای: مد CCM برای احرازهویت و محرمانگی
* SP 800-22	A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, Rev 1a (2010) یک مجموعه آزمون آماری برای مولد اعداد تصادفی و شبه تصادفی برای برنامه‌های کاربردی رمزنگاری
* SP 800-20	Modes of Operation Validation System for the Triple Data Encryption Algorithm (TMOVS): Requirements and Procedures (2012) سیستم اعتبارسنجی مد عملیاتی برای الگوریتم رمزنگاری داده سه‌گانه (TMOVS): الزامات و روش‌ها
* SP 800-12	An Introduction to Computer Security, Rev.1 (2017) مقدمه‌ای بر امنیت کامپیوتر

شماره استاندارد	نام استاندارد
SP 800-34	Contingency Planning Guide for Federal Information Systems, Rev.1 (2010) راهنمای برنامه‌ریزی وقوع حادثه احتمالی سیستم‌های اطلاعاتی فدرال
** FIPS 140-2	Security Requirements for Cryptographic Modules, 2001 نیازمندی‌های امنیتی برای ماژول‌های رمزنگاری
* FIPS 180-4	Secure Hash Standard (SHS) (2015) استاندارد درهم‌سازی امن
* FIPS 186	Digital Signature Standard (DSS), (2013) استاندارد امضای دیجیتال
* FIPS 197	Advanced Encryption Standard (AES), (2001) استاندارد رمزگذاری پیشرفته
* FIPS 198	The Keyed-Hash Message Authentication Code(HMAC), (2008) کد اصالت‌سنجی پیام مبتنی‌بر درهم‌سازی- رمزشده

* برای مطالعه بیشتر در مورد این استانداردها به توضیحات مرحله آغاز مراجعه شود.

** برای مطالعه بیشتر در مورد این استانداردها به توضیحات تهیه/ توسعه آغاز مراجعه شود.

*** برای مطالعه بیشتر در مورد این استانداردها به توضیحات مرحله اجرا/ ارزیابی مراجعه شود.

در این قسمت هریک از استانداردهای امنیتی مرحله عملیات/ نگه‌داری شرح داده شده است:

- **SP 800-34: Contingency Planning Guide for Federal Information Systems**

این راهنما، دستورالعمل‌ها، توصیه‌ها و ملاحظاتی را برای برنامه‌ریزی وقوع حادثه احتمالی سیستم‌های اطلاعات فدرال ارایه می‌دهد. برنامه‌ریزی وقوع حادثه احتمالی به اقدامات موقت برای بازیابی خدمات سیستم اطلاعات پس از یک اختلال اشاره دارد. اقدامات موقت ممکن شامل جابجایی سیستم‌های اطلاعاتی و عملیات به یک سایت دیگر، بازیابی توابع سیستم اطلاعاتی با استفاده از تجهیزات دیگر، یا عملکرد توابع سیستم اطلاعاتی با استفاده از روش‌های دستی باشد. این راهنما در حال حاضر برای سه نوع پلت فرم موجود است از جمله: سیستم‌های سرویس‌گیرنده/سرویس‌دهنده، سیستم‌های ارتباطات، سیستم‌های پردازنده مرکزی.

این راهنما اطلاعاتی را در روابط متقابل بین برنامه‌ریزی وقوع حادثه احتمالی سیستم اطلاعات و انواع دیگر از امنیت و مدیریت اضطراری مربوط به برنامه‌های وقوع حادثه احتمالی، انعطاف‌پذیری سازمانی، و چرخه حیات توسعه سیستم ارایه می‌دهد. همچنین راهنمایی برای کمک به پرسنل ارزیابی سیستم‌های اطلاعات و عملیات برای تعیین الزامات برنامه‌ریزی وقوع حادثه احتمالی و اولویت‌ها فراهم می‌کند.

❖ امحاء [۲۳]

در این مرحله اطلاعات، سخت‌افزار و نرم‌افزار ممکن است بایگانی، به سیستم دیگری منتقل، دورانداخته و یا نابود شود. اگر این مرحله به صورت نادرست انجام شود، امکان افشای غیرمجاز داده‌های حساس وجود دارد. در ادامه لیستی از استانداردهای امنیتی این مرحله در جدول زیر آمده است.

جدول ۵: لیستی از استانداردهای امنیتی مرحله امحاء

شماره استاندارد	نام استاندارد
** SP 800-64	Security Considerations in the System Development Life Cycle, Rev.2 (2008) ملاحظات امنیتی در چرخه حیات توسعه سیستم
* SP 800-36	Guide to Selecting Information Technology Security Products (2003) راهنمای انتخاب محصولات امنیتی فناوری اطلاعات
* SP 800-35	Guide to Information Technology Security Services (2003) راهنمای سرویس‌های امنیتی فناوری اطلاعات
* SP 800-14	Generally Accepted Principles and Practices for Securing Information Technology Systems (1996) روش‌ها و اصول پذیرفته شده عمومی برای امنیت سیستم‌های فناوری اطلاعات
* SP 800-47	Security Guide for Interconnecting Information Technology Systems (2002) راهنمای امنیت برای ارتباطات سیستم‌های فناوری اطلاعات
* SP 800-46	Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security, Rev.2 (2016) راهنمایی برای امنیت دورکاری سازمان‌ها، دسترسی از راه دور و استفاده از دستگاه‌های شخصی (BYOD)
* SP 800-45	Guidelines on Electronic Mail Security, V.2 (2007) راهنمایی در مورد امنیت پست الکترونیک

[۲۳] Disposal

Guidelines on Securing Public Web Servers, V.2 (2007) راهنمایی در مورد امنیت وب سرورهای عمومی	* SP 800-44
Guidelines on Firewalls and Firewall Policy (2009) راهنمایی‌هایی در مورد دیواره آتش و سیاست‌های آن	* SP 800-41
An Introduction to Computer Security, Rev.1 (2017) مقدمه‌ای بر امنیت کامپیوتر	* SP 800-12
Engineering Principles for Information Technology Security (A Baseline for Achieving Security), Revision A, Rev. A (2004) اصول مهندسی برای امنیت فناوری اطلاعات	* SP 800-27