سازمان بورس و اوراق بهادار
SECURITIES & EXCHANGE ORGANIZATION

الزامات امنیت اطلاعات بازار سرمایه

مرکز نظارت بر امنیت اطلاعات بازار سرمایه (مکنا)

طبقه بندی محرمانگی: عادی

نسخه ۴.۰

آذرماه ۱۳۹۸

صلاحیت و اعتبار

این الزامات توسط مرکز نظارت بر امنیت اطلاعات بازار سرمایه (مکنا) با توجه به مسئولیت‌های کنترلی و نظارتی آن بر اساس مصوبه چهار صد و چهل و هشتمین جلسه هیأت مدیره سازمان بورس و اوراق بهادار تدوین شده است.

این الزامات امنیتی بر اساس آخرین استانداردهای معتبر بین‌المللی امنیت اطلاعات (از جمله ISMS[1]، SANS[2]، NIST[3]، PCI-DSS[4] و Secure SDLC[5])، الزامات امنیت اطلاعات در بازارهای سرمایه بین‌المللی و سایر مطالعات تطبیقی، الزامات قانونی و مقرراتی کشور از جمله قوانین و مقررات بازار اوراق بهادار و همچنین اصول علمی امنیت اطلاعات تدوین شده است. این الزامات با دیگر الزامات کاربردی و امنیتی بازار سرمایه، سازگاری داشته و امکان تفسیر آن‌ها، به منظور مخالفت یا رد دیگر استانداردها، قوانین، مقررات و الزامات حاکم بر بازار سرمایه وجود ندارد.

این الزامات به عنوان یکی از خطوط راهنمای حداقلی جهت نظارت مرکز مکنا بر اجرای صحیح الزامات امنیتی در زیرساخت‌ها و سامانه‌های فناوری اطلاعات بازار سرمایه به شمار می‌آید.

با توجه به تغییرات تکنولوژی و توسعه ابزارهای فناوری اطلاعات و ایجاد روش‌های جدید هک و نفوذ، در صورت نیاز مرکز نظارت بر امنیت اطلاعات بازار سرمایه اصلاحات مقتضی این مستند را تدوین و در قالب نسخه جدید به صورت رسمی ابلاغ و جایگزین نسخه قبلی خواهد نمود. الزامات این مستند و سایر الزامات امنیتی حسب مورد، توسط مرکز نظارت بر امنیت اطلاعات بازار سرمایه تدوین و ابلاغ می‌گردد.

---

[1] به طور مثال ISO 27001 و ISO 27002

[2] https://www.sans.org/security-resources/

[3] National Institute of Standards and Technology

[4] Payment Card Industry Data Security Standard

[5] Secure Software Development Life Cycle

تغییرات نسبت به نسخه قبل

تغییرات مستند حاضر (نسخه ۴.۰) نسبت به نسخه قبلی (نسخه ۳.۰) در برخی از موارد، نگارشی و به صورت جزئی بوده است. تغییرات عمده در کنترل‌ها در جدول ذیل لیست شده است:

شماره کنترل در نسخه قبلی	شماره کنترل در نسخه فعلی	شرح تغییرات
۱-۱	۱-۱	محتوای کنترل کامل‌تر شده است.
۲-۱	۲-۱	محتوا و عنوان کنترل با حفظ ماهیت تغییر یافته است.
----	۶-۱	این کنترل اضافه گردیده است.
۱-۲	۱-۲	محتوای کنترل کامل‌تر شده است.
----	۵-۲	این کنترل اضافه گردیده است.
----	۳-۳	این کنترل اضافه گردیده است.
۴-۴	۳-۴	محتوا و عنوان کنترل با حفظ ماهیت تغییر یافته است.
۸-۴	----	این کنترل حذف گردیده است.
۶-۶	۶-۶	محتوا و عنوان کنترل با حفظ ماهیت تغییر یافته است.
----	۱۲-۶	این کنترل اضافه گردیده است.
۱۲-۶	۱۵-۶	محتوای کنترل کامل‌تر شده است.
----	۱۶-۶	این کنترل اضافه گردیده است.
۱۳-۶	۱۷-۶	محتوای کنترل با حفظ ماهیت تغییر یافته است.
۲۳-۶	۲۴-۶	محتوای کنترل با حفظ ماهیت تغییر یافته است.
۲۵-۶	۲۷-۶	محتوای کنترل کامل‌تر شده است.
۳-۷	۶-۷	محتوای کنترل کامل‌تر شده است.
۵-۷	----	این کنترل از این بخش حذف گردیده است.
۶-۷	۱۶-۷	محتوای کنترل کامل‌تر شده است.
۷-۷	۱۱-۷	محتوای کنترل کامل‌تر شده است.
۱۱-۷	۵-۷	محتوای کنترل با حفظ ماهیت تغییر یافته است.
۲۰-۷	۱۴-۷	محتوای کنترل با حفظ ماهیت تغییر یافته است.
----	۱۵-۷	این کنترل اضافه گردیده است.
----	۲۲-۷	این کنترل اضافه گردیده است.

----	۷-۸	این کنترل اضافه گردیده است.
۵-۹	۵-۹	محتوای کنترل با حفظ ماهیت تغییر یافته است.
۶-۹	۶-۹	محتوای کنترل با حفظ ماهیت تغییر یافته است.
----	۷-۹	این کنترل اضافه گردیده است.
۷-۹	۸-۹	محتوای کنترل با حفظ ماهیت تغییر یافته است.
----	۳-۱۰	این کنترل اضافه گردیده است.
۷-۱۰	۸-۱۰	محتوای کنترل با حفظ ماهیت تغییر یافته است.
۱۰-۱۰	۱۱-۱۰	محتوای کنترل با حفظ ماهیت تغییر یافته است.

فهرست

پیشگفتار

اغلب فرآیندهای بازار سرمایه، از درگاه‌های اطلاع رسانی و سامانه‌های مکاتبات اداری تا سامانه‌های معاملاتی بر روی زیرساخت‌ها و سامانه‌های فناوری اطلاعات در حال انجام است و در صورت پیدایش مشکل امنیتی در آن‌ها، ممکن است چالش‌هایی برای فعالان بازار سرمایه ایجاد شود.

امنیت اطلاعات از سه بعد محرمانگی، صحت و دسترس‌پذیری تشکیل شده است. جهت امن‌سازی سامانه‌های اطلاعاتی باید توجهی جامع به این ابعاد داشت. وجود الزامات فنی در کنار الزامات فرایندی می‌تواند آسیب‌پذیری‌ها، تهدیدات و در نتیجه ریسک‌ها را به میزان قابل توجهی کاهش دهد. از این رو، مرکز مکنا با هدف یکپارچه‌سازی و ارتقاء سطح امنیت اطلاعات بازار سرمایه و در راستای سیاست‌های کلی نظام در امور «امنیت فضای تولید و تبادل اطلاعات و ارتباطات (افتا)»، ابلاغیه رهبر معظم انقلاب اسلامی ایران به تاریخ ۱۳۸۹/۱۱/۲۹، اقدام به تدوین این الزامات نموده است. تدوین این الزامات، از سال ۱۳۹۲ در دستور کار مرکز مکنا قرار گرفت و در سال ۱۳۹۳ ابلاغ گردید. پس از آن، در مواردی که نیاز به تکمیل و یا اصلاح بوده است، نسخه‌های جدید این الزامات تدوین و ابلاغ شده‌اند.

الزامات مستند حاضر، حوزه‌های ذیل را در مقوله امنیت اطلاعات پوشش داده است:

- سازمان‌دهی و مدیریت امنیت اطلاعات
- خط‌مشی‌ها و فرایندهای امنیتی
- امنیت در تعامل با طرف‌های ثالث
- امنیت منابع انسانی
- امنیت شبکه و ارتباطات
- امنیت سیستم‌عامل‌ها و پایگاه‌های داده
- امنیت برنامه‌های کاربردی
- حفاظت از داده‌ها و اطلاعات
- امنیت فیزیکی مرکز داده
- ممیزی داخلی، بازنگری و بهبود

این الزامات، با دو نگاه فنی و فرایندی تدوین شده‌اند، به طوری که مکمل یکدیگر باشند. در فصل اول، الزامات مدیریتی و فرایندی امنیت اطلاعات و در فصل دوم، الزامات فنی امنیتی تبیین گردیده است.

اهداف

این الزامات به منظور حفاظت از اطلاعات بازار سرمایه و زیرساخت‌های فناوری اطلاعات آن، اهداف زیر را دنبال می‌کند:

- نظام‌مند نمودن امنیت اطلاعات در ساختار بازار سرمایه
- ارائه چارچوبی به منظور ارتقاء سطح امنیت سامانه‌های بازار سرمایه و انجام اقدامات پیشگیرانه و پدافندی
- بیان حداقل نیازمندی‌ها، الزامات و کنترل‌های امنیت اطلاعات مطابق با نیازهای بازار سرمایه
- ارائه ساختاری برای شناسایی و رفع نقاط آسیب‌پذیر امنیت اطلاعات در بازار سرمایه
- ارائه ساختاری پایه برای ارزیابی و کنترل امنیت اطلاعات در بازار سرمایه

شرکت باید با تبعیت از این الزامات و با استفاده از سایر استانداردها و بهترین تجربیات امنیتی، در پی تحقق اهداف ذیل در مجموعه خود باشد:

- پایه‌گذاری یک نظام مدیریت امنیت اطلاعات در حوزه اجرا
- برقراری رویه‌هایی به منظور رسیدن به سطح مناسبی از امنیت اطلاعات در حوزه اجرا
- پیاده‌سازی و اجرای الزامات و کنترل‌های امنیت اطلاعات کاربردپذیر در حوزه اجرا
- ارتقاء سطح آگاهی و دانش فنی و علمی امنیت اطلاعات نیروی انسانی در حوزه اجرا
- بهبود مستمر سطح امنیت اطلاعات در حوزه اجرا

تعریف واژگان

آسیب‌پذیری: ضعفی از سیستم است که می‌تواند موجب نقض امنیت اطلاعات شود.

اختیارات ویژه: به دسترسی‌های منطقی یا فیزیکی که جهت مدیریت، پیکربندی، راه‌اندازی و یا پشتیبانی یک تجهیز یا سیستم یا کاربران یک سیستم، به فرد یا سیستم دیگری داده می‌شود، اختیارات ویژه می‌گویند.

اصل حداقل دسترسی: اعطای اختیارات و دسترسی‌های مجاز به هر سیستم یا کاربر، باید مستدل، مکتوب و تنها بر اساس نیاز و ضرورت ارائه شود.

افزونگی[1]: هر سیستم یا تجهیزی که به عنوان پشتیبان سیستم یا تجهیز دیگری، درحال فعالیت بوده یا به طور خودکار آماده به کار باشد، افزونه آن سیستم یا تجهیز نامیده می‌شود. به این مکانیزمِ افزایش دسترس‌پذیری، افزونگی گفته می‌شود.

اطلاعات نهانی (بند ۳۲ ماده ۱ فصل اول قانون بازار اوراق بهادار ج.ا.ا.): هرگونه اطلاعات افشا نشده برای عموم که به طور مستقیم یا غیرمستقیم، به اوراق بهادار، معاملات یا ناشر آن مربوط می‌شود و در صورت انتشار، بر قیمت یا تصمیم سرمایه‌گذاران برای معامله اوراق بهادار مربوط تأثیر می‌گذارد.

بهترین تجربیات امنیتی[2]: بهترین تجربیات امنیتی شامل راهبردهایی می‌شوند که عموماً توسط شرکت‌ها و سازمان‌های بین المللی معتبر و متخصص در این حوزه، قبلاً مورد بررسی و آزمون قرار گرفته و تجربه شده‌اند و تأثیر مناسب و قابل قبول متناسب با اهداف امنیتی را نشان داده‌اند. مستندات راهنمای امن‌سازی ارائه شده توسط مرکز مدیریت راهبردی افتای ریاست جمهوری از جمله بهترین تجربیات امنیتی می‌باشند.

دسترسی مدیریتی از راه دور: دسترسی با اختیارات ویژه به درگاه‌های پیکربندی تجهیزات، سیستم‌ها یا برنامه‌های کاربردی[3] حوزه اجرا از خارج از شبکه، دسترسی مدیریتی از راه دور نامیده می‌شود.

---

[1] Redundancy
[2] Security Best Practices
[3] Application

زون[1] (ناحیه شبکه): در این الزامات، به تقسیمات منطقی شبکه در قالب VLAN، زون گفته می‌شود. هر زون، دارای یک بازه آدرس IP است که ارتباطات ماشین‌های درون آن با یکدیگر، به صورت لایه ۲ می‌باشد.

شرکت: در این الزامات، منظور از "شرکت"، شرکتی است که این الزامات به وی ابلاغ شده و ملزم به رعایت آن می‌باشد.

مرکز داده: به محل قرارگیری تجهیزات شبکه‌ای و امنیتی و سرورهای عملیاتی، مرکز داده گفته می‌شود.

معماری استقرار سامانه‌ها[2] : نقشه‌ای که سرورها و سرویس‌ها، ارتباطات میان آن‌ها و تجهیزات ارتباطی مربوط به هر سامانه، به همراه نام هر سرور، آدرس IP و شماره پورت‌های مربوط به هر یک را نمایش می‌دهد.

مرکز مکنا: به مرکز نظارت بر امنیت اطلاعات بازار سرمایه، به اختصار، مرکز مکنا اطلاق می‌گردد.

SPoF[3]: نقطه‌ای از شبکه است که اختلال در آن قسمت، باعث ایجاد اختلال در بخش عمده‌ای از شبکه و سرویس‌ها می‌شود.

[1] Zone
[2] Deployment Diagram
[3] Single Point of Failure

فصل اول

الزامات مدیریتی و فرایندی

۱- سازمان‌دهی امنیت اطلاعات		
۱-۱	ساختار سازمانی امنیت اطلاعات	شرکت باید در راستای اهداف تعیین شده، ساختار سازمانی امنیت اطلاعات را مستقیما زیرنظر عالی‌ترین مقام شرکت، جهت استقرار و حفظ این الزامات و دیگر الزامات مقرراتی امنیت اطلاعات، ایجاد نماید.
۱-۲	مسئول امنیت اطلاعات	شرکت می‌بایست مسئول امنیت اطلاعات خود را تعیین و به مرکز مکنا معرفی نماید.
۱-۳	بیانیه خط‌مشی امنیت اطلاعات	بیانیه خط‌مشی امنیت اطلاعات شرکت شامل تعهد مدیریت به ارتقاء مداوم سطح امنیت اطلاعات می‌بایست تدوین گردیده و به تایید عالی‌ترین مقام شرکت برسد.
۱-۴	مستند مسئولیت‌های افراد	مستند مسئولیت‌های افراد در رابطه با مدیریت، پیاده‌سازی، نگهداری و اجرای این الزامات، از جمله در ساختار واحد امنیت اطلاعات می‌بایست تدوین و مکتوب گردد.
۱-۵	طرح‌های بهبود سطح امنیت اطلاعات	طرح‌های انجام شده، طرح‌های در حال انجام و طرح‌های آتی که در راستای بهبود سطح امنیت اطلاعات شرکت باشد، باید به همراه وضعیت انجام هر یک، فهرست و مستند شود. مستند مذکور باید همواره به‌روزرسانی گردد.
۱-۶	تایید امنیتی تغییرات	هرگونه تغییر و یا توسعه در سامانه‌ها و زیرساخت حوزه اجرای این الزامات باید توسط مسئول امنیت اطلاعات به صورت مستند مورد تایید امنیتی قرار گیرد و به مدت دو سال در سوابق نگه‌داری شود.

۲- استقرار الزامات		
۲-۱	تعیین حوزه اجرا	شرکت باید حوزه اجرای این الزامات شامل حوزه فیزیکی، حوزه کسب‌وکار، حوزه فناوری (تجهیزات، برنامه‌های کاربردی، پایگاه‌های داده و سرورها) و حوزه منابع انسانی را برای تمام سامانه و زیرساخت‌های فناوری اطلاعات خود در نظر بگیرد. در صورت وجود استدلال کافی برای محدود نمودن حوزه اجرا، شرکت باید مستندات خود به همراه دلایل را به مرکز نظارت بر امنیت اطلاعات بازار سرمایه ارسال نماید و در صورت دریافت تأییدیه، می‌تواند حوزه اجرای محدود و تأیید شده را برای این الزامات لحاظ نماید.
۲-۲	محدودسازی حوزه اجرا	در راستای تسهیل در اجرای این الزامات، شرکت می‌بایست بخش‌هایی از مجموعه خود را که از نقطه نظر فیزیکی، شبکه‌ای و سیستمی در حوزه اجرای این الزامات نقش ندارند، از حوزه اجرا به روشی امن، مستند و مستدل، به طور کامل تفکیک نماید.
۲-۳	حوزه پیاده‌سازی الزامات	شرکت باید تمامی الزامات و کنترل‌های امنیتی مستند حاضر را در محدوده حوزه اجرای مجموعه خود پیاده‌سازی و مستند نماید.
۲-۴	پیاده‌سازی کنترل‌ها	کنترل‌های این مستند، باید به طور کامل پیاده‌سازی شوند. در صورتی‌که بخش یا تمامی آن کنترل برای حوزه اجرای شرکت کاربرد نداشته باشد، شرکت باید دلایل مستدل و کافی خود را جهت عدم کاربرد بخش یا تمامی آن کنترل، به صورت مستند به مرکز مکنا ارائه نماید و تنها در صورت تایید مرکز مکنا، شرکت مجاز به عدم پیاده‌سازی کامل کنترل مربوطه خواهد بود.
۲-۵	پیاده‌سازی سایر الزامات امنیتی	شرکت نسبت به اجرای کامل سایر الزامات امنیتی ابلاغ شده توسط مرکز مکنا متعهد و مسئول است. شرکت همواره می‌تواند از طریق درخواست مکتوب از مرکز مکنا، لیست تمام الزامات و ابلاغیات امنیتی را دریافت نماید.

۳- تعامل با طرف‌های ثالث		
۳-۱	وجود و اجرای رویه استفاده از خدمات طرف‌های ثالث[1]	شرکت برای استفاده از خدمات طرف‌های ثالث در حوزه اجرا، باید رویه‌ای تهیه، مستند، اجرا و به‌روزرسانی نماید به نحوی که بتواند امنیت اطلاعات را حداقل در سطح این الزامات فراهم نماید. این رویه باید حداقل دارای موارد کنترل ۳-۲ باشد.
۳-۲	مفاد رویه استفاده از خدمات طرف‌های ثالث	سرویس‌دهی به (یا دریافت سرویس از) طرف‌های ثالث و واگذاری حقوق دسترسی به آن‌ها، باید بر مبنای یک چارچوب مشخص باشد و محدوده‌ی دسترسی طرف‌های ثالث در ابعاد فیزیکی و منطقی، سیستمی، فرآیندی، فناوری و منابع اطلاعاتی، بر اساس اصل حداقل دسترسی باشد و به صورت دقیق و شفاف مستند گردد. تمامی طرف‌های ثالث باید تعهدنامه عدم افشای اطلاعات حداقل شامل تعهد به تمامی خط‌مشی‌ها و قوانین امنیتی شرکت، محرمانگی اطلاعات، مسئولیت‌های متناظر و نتایج عدم اجرای آن‌ها و محدودیت‌های نسخه‌برداری از اطلاعات را پذیرفته و امضا نمایند.
۳-۳	مسئولیت شرکت در صورت برون‌سپاری	مسئولیت پاسخگویی در قبال اجرا و نگهداری این الزامات و سایر الزامات و ابلاغیات مرتبط، حتی در صورت برون‌سپاری به طرف ثالث، بر عهده شرکت می‌باشد.

[1] Third Party

۴- الزامات منابع انسانی		
۴-۱	تأمین نیروی متخصص	شرکت باید حداقل دو نفر کارشناس با تجربه امنیت اطلاعات را به منظور پیشبرد الزامات امنیت اطلاعات به کار گیرد. شرکت برای جذب کمتر از دو نفر، باید با ارائه دلایل و مستندات، موافقت مرکز مکنا را دریافت نماید.
۴-۲	بررسی سوابق افراد	پیشینه فنی و اخلاقی کارکنان، پیمانکاران و متقاضیان استخدام در شرکت می‌بایست توسط مراجع ذیصلاح تایید گردد.
۴-۳	تعهدنامه منع افشای اطلاعات	تمامی کارکنان، پیمانکاران و مشاوران، باید تعهدنامه حفظ محرمانگی یا عدم افشای اطلاعات به مدت حداقل ۱۰ سال را امضاء نمایند.
۴-۴	آموزش و آگاهی‌رسانی	در این رابطه شرکت باید موارد زیر را انجام دهد: • شایستگی‌ها و نیازمندی‌های علمی برای هر یک از سمت‌های کاری مرتبط با حوزه اجرا را تعریف و مستند نماید. • با برگزاری دوره‌هایی در دو سطح آموزش عمومی و آموزش تخصصی امنیت اطلاعات برای کارکنان حوزه اجرا به تناسب نقش و مسئولیت آن‌ها، از صلاحیت آن‌ها برای انجام امور اطمینان کسب نماید.
۴-۵	خط‌مشی میز پاک و صفحه پاک	خط‌مشی میز پاک برای مستندات و رسانه‌های ذخیره‌سازی قابل حمل و خط‌مشی صفحه پاک برای نمایشگرهای اطلاعات در حوزه اجرا توسط شرکت تدوین، مستند و اطلاع‌رسانی گردد. شرکت باید بر اجرای این خط‌مشی‌ها توسط کارکنان حوزه اجرا، نظارت نماید.
۴-۶	اطلاع‌رسانی تهدیدات	تمامی کارکنان، پیمانکاران و مشاوران موظفند در صورت مشاهده یا مظنون شدن به وجود هرگونه تهدید نسبت به دارایی‌های اطلاعاتی حوزه اجرا، مراتب را به مدیر مستقیم و مسئول امنیت اطلاعات شرکت گزارش نمایند.
۴-۷	اطلاع‌رسانی رخدادهای امنیتی به مرکز مکنا	مسئول امنیت اطلاعات شرکت باید تمامی رخدادهای امنیتی و یا موارد مشکوکی را که برای حوزه اجرا تهدید چشمگیری ایجاد کرده‌اند، در اسرع وقت به مرکز مکنا اطلاع دهد.
۴-۸	حذف حقوق دسترسی	به محض خاتمه استخدام/ قرارداد/ توافق‌نامه هر یک از کارکنان، پیمانکاران و طرف‌های ثالث باید حقوق دسترسی آن‌ها به اطلاعات و امکانات پردازش اطلاعات، حذف گردد. همچنین به محض تغییر شغل، تمام حقوق دسترسی باید بر اساس اصل حداقل دسترسی مجدد تنظیم شود. در این خصوص، شرکت می‌بایست دستورالعمل کاملی را تهیه، مستند، اجرا و به‌روزرسانی نماید.

۵- حفظ انطباق		
۵-۱	ممیزی داخلی	شرکت باید بر اساس یک طرح مستند، ممیزی‌های داخلی را در فواصل زمانی مشخص (با فاصله حداکثر شش ماه) انجام دهد و نتایج حاصل را مکتوب نماید. نتایج این ممیزی‌ها بیانگر این است که آیا کنترل‌ها، فرایندها و رویه‌های انتخاب شده: ۱. با الزامات و اهداف این مستند انطباق دارند؟ ۲. آن گونه که انتظار می‌رود، اجرا می‌شوند؟ ۳. به گونه‌ای اثر بخش انتخاب، اجرا و نگهداری می‌شوند؟
۵-۲	بهبود	شرکت باید بر اساس نتایج ممیزی داخلی، اقدامات اصلاحی را در راستای رفع اساسی مشکلات موجود انجام داده و در صورت نیاز طرح‌های امنیتی خود را به روز نماید.
۵-۳	بازنگری	شرکت با توجه به پایش‌های مستمر، ممیزی‌ها و تجربیات حاصل از حوادث امنیتی و به منظور تصدیق الزامات امنیتی برآورده شده، باید حوزه اجرا، کنترل‌های امنیتی و روش‌های ممیزی و پایش مستمر خود را به طور منظم و در فواصل زمانی مشخص (با فاصله حداکثر یک سال) بازنگری و در صورت نیاز تغییرات لازم را در آن‌ها اعمال و مستند نماید.

فصل دوم

الزامات فنی امنیتی

۶- امنیت شبکه و ارتباطات		
۶-۱	ساختار مدیریت شبکه	گروه‌ها، وظایف و نقش افراد برای مدیریت اجزاء شبکه و امنیت شبکه در حوزه اجرا باید تعریف، مستند و اجرا شوند.
۶-۲	فهرست تجهیزات شبکه‌ای و امنیتی	اطلاعات تمامی تجهیزات شبکه‌ای و امنیتی در محدوده حوزه اجرا باید به صورت مستند موجود باشد. موارد زیر حداقل اطلاعات ضروری برای هر تجهیز است: • نام و مدل تجهیز • آدرس IP • تعداد اینترفیس فعال • محل استقرار • مشخصات افراد مجاز به دسترسی پیکربندی
۶-۳	طرح فیزیکی شبکه	نقشه(های) مربوط به طراحی و ارتباطات فیزیکی شبکه حوزه اجرا باید تهیه، مستند و به‌روزرسانی شود. این نقشه(ها) حداقل باید اطلاعات ذیل را نمایش دهند: • تجهیزات افزونه • نام و شماره پورت‌های ارتباطی تجهیزات • وجود تمامی تجهیزات و ارتباطات فیزیکی در توپولوژی شبکه
۶-۴	طرح منطقی شبکه	نقشه جامع مربوط به طراحی منطقی شبکه حوزه اجرا باید تهیه، مستند و به‌روزرسانی شود. این نقشه حداقل باید شامل اطلاعات زیر باشد: • محل منطقی قرارگیری فایروال‌ها، سوییچ‌ها و روترها • ارتباطات منطقی بین تجهیزات • نام و بازه آدرس IP زون‌های هر بخش از شبکه
۶-۵	مدیریت تغییرات در سطح شبکه	تمامی تغییرات فیزیکی یا منطقی در ساختار شبکه در حوزه اجرا باید بر اساس یک رویه مشخص و مستند انجام شود. تنظیم رویه مدیریت تغییرات، حداقل باید بر اساس بخش 12.1.2 استاندارد ISO 27002:2013 باشد.
۶-۶	عبور ترافیک از حداقل دو لایه فایروال و IPS	ترافیک بین کاربران نهایی و سرویس‌های عملیاتی باید حداقل از دو لایه فایروال و IPS از تولیدکنندگان متفاوت عبور کند. توصیه می‌شود در لبه‌های ورودی شبکه حوزه اجرا از تجهیزات تولید داخل کشور استفاده شود.
۶-۷	فایروال برنامه‌های کاربردی تحت وب (WAF)	تمامی برنامه‌های کاربردی تحت وب در حوزه اجرا باید توسط WAF[1] محافظت شوند. (تنظیمات WAF باید به گونه‌ای باشد که از دسترسی‌های غیر مجاز و حملات احتمالی به برنامه‌های کاربردی تحت وب حوزه اجرا جلوگیری کند.)

[1] Web Application Firewall

۶-۸	ساختار امنیتی بین زون‌ها	ترافیک شبکه بین هر دو زون در حوزه اجرا، باید از فایروال، IPS و آنتی‌ویروس سخت‌افزاری با پیکربندی امن عبور کند و کنترل شود. (تنظیمات IPS و فایروال باید به گونه‌ای باشد که از دسترسی‌های غیرمجاز و حملات به حوزه اجرا جلوگیری کند.)
۶-۹	ساختار زون‌بندی شبکه	زون‌بندی شبکه در حوزه اجرا باید بر اساس سطوح حساسیت امنیتی و ماهیت کاری دارایی‌های موجود (مانند ماهیت پایگاه‌داده، ماهیت برنامه‌کاربردی تحت وب، ماهیت DMZ، سطح مدیریت، سطح Public و از این قبیل) انجام گیرد. توصیف ماهیت کاری و حساسیت امنیتی هر زون باید مستند و به‌روز باشد.
۶-۱۰	زون مدیریت تجهیزات	سیستم‌هایی که به منظور مدیریت تجهیزات، سیستم‌عامل‌ها و سرویس‌ها استفاده می‌شوند، باید دارای زون(های) اختصاصی باشند و به شبکه‌های عمومی مانند اینترنت دسترسی نداشته باشند.
۶-۱۱	زون‌بندی شبکه کلاینت‌ها	شبکه کلاینت‌های حوزه اجرا باید مطابق با کنترل ۶-۹ به زون‌های مجزا تقسیم گردیده و نباید هیچ‌گونه دسترسی میان این زون‌ها وجود داشته باشد.
۶-۱۲	نگاشت IP و MAC به کاربر	به هر کاربر، باید آدرس IP و MAC ثابت و معینی تخصیص داده شود. این مقادیر و یا تغییرات آن باید در اسرع وقت به کاربر اطلاع‌رسانی و کتباً ابلاغ گردد. مستند نگاشت IP و MAC به کاربر، باید همواره به‌روزرسانی گردد و آخرین نسخه و تغییرات آن به مدت حداقل ۵ سال نگهداری شود. شیوه تشخیص آدرس‌های IP و MAC، باید به کاربران آموزش داده شود.
۶-۱۳	تفکیک محیط‌های تست، توسعه و عملیات	محیط‌های تست، توسعه و عملیات باید به صورت فیزیکی یا منطقی تفکیک شوند و هیچ گونه دسترسی شبکه‌ای میان آن‌ها وجود نداشته باشد.
۶-۱۴	نحوه آدرس‌دهی در زون DMZ	در زون DMZ بر روی هیچ یک از سرورها، نباید IP معتبر اینترنتی تنظیم شود و باید از مکانیزم ترجمه آدرس شبکه (Network Address Translation) استفاده گردد.
۶-۱۵	رویه اعطاء و لغو دسترسی	برای اعطاء یا لغو دسترسی در سطح شبکه حوزه اجرا (مانند دسترسی به سرویس‌ها) باید رویه‌ای مطابق با اصل حداقل دسترسی تهیه، مستند و اجرا گردد. در این رویه، باید ایجاد دسترسی، مبتنی بر درخواست مستند و مکتوب متقاضی و منطبق بر خط مشی‌های امنیتی شرکت باشد. شرح دسترسی‌های ایجاد شده و نتایج بازنگری دوره‌ای دسترسی‌های ایجاد شده در سطح شبکه و حذف دسترسی‌های غیر ضروری باید مستند شود.
۶-۱۶	سیاست‌های اعمالی در فایروال‌ها	سیاست‌های دسترسی اعمال شده در فایروال‌ها باید بر اساس اصل حداقل دسترسی تنظیم گردد. در سیاست‌های اعطای دسترسی، Port Number نباید به صورت Any تنظیم شود. حتی‌الامکان در سیاست‌های اعطای دسترسی برای آدرس IP، از Any استفاده نشود.

۶-۱۷	محدودسازی دسترسی سرورها به اینترنت	هیچ کدام از سرورهای موجود در حوزه اجرا نباید به اینترنت دسترسی داشته باشند. برای سرویس ضروری خاص مانند WSUS، دسترسی صرفاً باید به IP و پورت‌های مورد نیاز آن سرویس محدود گردد.
۶-۱۸	دسترسی به درگاه‌های پیکربندی	هیچ‌یک از درگاه‌های پیکربندی تجهیزات، سیستم‌عامل‌ها و سرویس‌ها نباید از شبکه‌ای خارج از شبکه حوزه اجرا مستقیماً قابل رؤیت باشد.
۶-۱۹	دسترسی مدیریتی از راه دور	دسترسی مدیریتی از راه دور به درگاه‌های پیکربندی تجهیزات، سرویس‌ها و سیستم‌عامل‌های حوزه اجرا، باید بر اساس اصل حداقل دسترسی باشد و به صورت ارتباط نقطه به نقطه امن با شبکه حوزه اجرا، با رمزنگاری قوی (مطابق با کنترل ۸-۵) و تصدیق اصالت به روش دو فاکتوری انجام شود.
۶-۲۰	کنترل دسترسی به پورت‌های فیزیکی شبکه	در سوئیچ‌های شبکه دسترسی کاربران در حوزه اجرا باید تنظیمات Port Security اعمال گردد. بدین صورت که به هر یک از پورت‌های سوییچ تعداد آدرس MAC محدود و مشخص، بر اساس اصل حداقل دسترسی تخصیص داده شود. برای پورت‌هایی که بیشتر از یک آدرس MAC اختصاص داده شده است، باید لیست آدرس‌های MAC مجاز آن پورت و مشخصات کاربر آن، مستند شود.
۶-۲۱	به‌روزرسانی تجهیزات	تجهیزات امنیتی (مانند IDS و آنتی‌ویروس) باید به صورت مداوم به‌روزرسانی گردند. همچنین سیستم‌عامل تجهیزات شبکه و امنیت شبکه در حوزه اجرا باید نسخه معتبر، امن و پایدار باشد.
۶-۲۲	امن‌سازی[1] تجهیزات	تمامی تجهیزات شبکه و امنیت شبکه حوزه اجرا باید بر اساس یک رویه مستند، مطابق با مراجع معتبر یا بهترین تجربیات امنیتی، امن‌سازی گردد.
۶-۲۳	ارزیابی امنیتی زیرساخت شبکه	نقاط ورودی به حوزه اجرا، عملکرد افزونگی و امنیت پیکربندی تجهیزات باید به صورت دوره‌ای (هر ۶ ماه حداقل یکبار) مورد بررسی و آزمون قرار بگیرد و نتایج آن، مستند شده و در صورت نیاز اقدامات اصلاحی صورت پذیرد.
۶-۲۴	تضمین دسترس‌پذیری	در طراحی و پیاده‌سازی زیرساخت شبکه و ارتباطات، برای بخش‌هایی که در صورت اختلال در عملکردشان، مشکل قابل توجهی به بخش وسیعی از زیرساخت‌ها یا سامانه‌های شرکت وارد می‌شود، باید تمهیدات لازم از جمله افزونگی در تمام سطوح جهت افزایش ضریب دسترس‌پذیری و جلوگیری از ایجاد SPoF اعمال شود.
۶-۲۵	پشتیبان‌گیری از پیکربندی تجهیزات	باید رویه‌ای جهت پشتیبان‌گیری از پیکربندی تجهیزات شبکه‌ای و امنیتی تهیه، مستند و اجرا شود. عملیات آزمون نسخ پشتیبان باید به صورت دوره‌ای در این رویه لحاظ و اجرا گردد. پس از هرگونه تغییر عمده در پیکربندی تجهیزات نیز باید پشتیبان‌گیری انجام شده و در محلی امن نگهداری شود.

[1] Hardening

۶-۲۶	ارتباطات شبکه‌ای بین سازمانی	تمامی ارتباطات شبکه‌ای با دیگر شرکت‌ها و سازمان‌ها که حاوی اطلاعات محرمانه می‌باشند، باید به صورت ارتباطات نقطه به نقطه امن با استفاده از رمزنگاری (مطابق با کنترل ۸-۵) باشد.
۶-۲۷	شبکه بی‌سیم	استفاده از شبکه بی‌سیم برای برقراری ارتباط میان دو ساختمان یا دو شبکه، به عنوان لینک اصلی مجاز نیست و فقط می‌تواند به عنوان لینک پشتیبان با پیکربندی امن (و با رعایت کنترل ۶-۲۶) استفاده شود. شبکه بی‌سیم کاربران، صرفا می‌تواند دسترسی به سایت‌ها و سرویس‌های اینترنتی را مهیا نماید و دسترسی به سرویس‌های داخلی شبکه حوزه اجرا، برای سرویس‌های حاوی داده‌های حساس یا محرمانه از این طریق مجاز نیست.

۷- امنیت سیستم‌ها و برنامه‌های کاربردی[1]		
۷-۱	فهرست مشخصات سیستم‌عامل‌های سرورها	باید فهرستی از مشخصات تمامی سیستم‌عامل‌های سرورهای حوزه اجرا تهیه، مستند و به‌روزرسانی گردد. این فهرست حداقل باید موارد زیر را پوشش دهد: • آدرس IP • نام و نسخه سیستم‌عامل • سرویس(های) ارائه شده (مانند "برنامه کاربردی معاملات برخط"، "پایگاه داده معاملات برخط"، "DNS"، "Active Directory") • شماره پورت(های) مربوط به هر سرویس • حوزه سرویس‌دهی هر سرویس (مانند اینترنت، اینترانت، شبکه WAN یا به یک سرویس داخلی دیگر) • درجه حساسیت امنیتی هر سرویس (مقداری بین۱ تا ۱۰، کمترین حساسیت ۱ و بیشترین حساسیت ۱۰) • مشخصات مسئول هر سرویس
۷-۲	مستند معماری استقرار سامانه‌ها	مستند معماری استقرار سامانه‌های[2] حوزه اجرا باید تهیه، مستند و به‌روزرسانی گردد.
۷-۳	جداسازی سرویس‌ها	سرویس‌های با درجه حساسیت امنیتی بزرگتر یا مساوی ۵ (بر اساس کنترل ۷-۱)، باید هر کدام به تنهایی بر روی یک سیستم‌عامل مجزا قرار گیرند.
۷-۴	داده‌ها در محیط‌های تست، توسعه و عملیات	داده‌های محرمانه، شناسه‌های کاربری و کلمات عبور در محیط تست یا توسعه باید متفاوت با محیط عملیاتی باشند. استفاده از اطلاعات نهانی در محیط‌های تست یا توسعه مجاز نمی‌باشد.
۷-۵	انتقال سرویس از محیط تست به محیط عملیاتی	انتقال سرویس‌ها از محیط تست به محیط عملیاتی باید مطابق با یک رویه امن و مستند صورت پذیرد. قبل از انتقال سرویس‌ها به محیط عملیاتی حوزه اجرا و بهره‌برداری نهایی، باید ارزیابی امنیتی جامعی (مطابق کنترل ۷-۱۵) بر روی آن‌ها انجام شود و پس از اطمینان از رفع آسیب‌پذیری‌ها، با رعایت کنترل ۱-۶، انتقال به محیط عملیاتی صورت پذیرد.
۷-۶	مدیریت تغییرات	هرگونه تغییر در سیستم‌عامل‌ها و سرویس‌های حوزه اجرا باید مطابق با یک رویه امن و مستند صورت پذیرد. این تغییرات باید محدود و بر اساس ضرورت باشد. رویه مدیریت تغییرات، باید بخش 12.1.2 از استاندارد ISO 27002:2013 را پوشش دهد.

[1] Application

[2] به قسمت واژگان مراجعه شود.

۷-۷	امن‌سازی	پیکربندی تمامی سیستم‌عامل‌ها و مولفه‌های نصب شده بر روی آن (مانند IIS، نرم‌افزار[1]های پایگاه داده و غیره) باید مطابق با مراجع معتبر یا بهترین تجربیات امنیتی بر اساس یک رویه مستند امن شده و به صورت دوره‌ای بازنگری گردد.
۸-۷	جداسازی برنامه کاربردی تحت وب از پایگاه داده	نصب پایگاه داده‌ها و برنامه‌های کاربردی تحت وب بر روی یک سیستم‌عامل مشترک مجاز نیست.
۹-۷	کدنویسی امن	در فرایند تولید و توسعه برنامه‌های کاربردی تحت وب، باید آخرین استانداردها، مراجع و اصول امنیتی برنامه‌نویسی و آسیب‌پذیری‌های رایج لحاظ گردند. نمونه‌هایی از مراجع امنیتی معتبر عبارتند از: • مستندات برنامه‌نویسی امن ارائه شده توسط مرکز مدیریت راهبردی افتای ریاست جمهوری • مستندات برنامه‌نویسی امن ارائه شده توسط مرکز ماهر سازمان فناوری اطلاعات • OWASP TOP 10 • SANS: A Security Checklist for Web Application Design • CERT Secure Coding Standards • CWE/SANS TOP 25 همچنین در فرایند تولید و توسعه برنامه‌های کاربردی تحت موبایل، باید اصول امنیتی برنامه‌نویسی موبایل و آسیب‌پذیری‌های رایج لحاظ گردند. نمونه‌ای از مراجع امنیتی معتبر عبارت است از: OWASP Top 10 Mobile Risks
۱۰-۷	انقضای نشست[2]	تمامی نشست‌های سیستم‌عامل‌ها و سرویس‌ها باید به گونه‌ای باشد که در صورت عدم فعالیت کاربر وارد شده به سیستم در یک بازه زمانی مشخص، ارتباط قطع شده و کاربر برای از سرگیری فعالیت‌های خود مجدداً تصدیق اصالت گردد.
۱۱-۷	عدم استفاده اشتراکی از شناسه‌های کاربری[3]	در سیستم‌هایی که از مکانیزم تصدیق اصالت استفاده می‌کنند[4]، هر شناسه کاربری بایستی تنها متعلق به یک کاربر بوده و به صورت مکتوب مطابق کنترل ۷-۲۲ به وی تحویل شود. به عبارت دیگر، استفاده اشتراکی از شناسه‌های کاربری یا تخصیص یک شناسه کاربری به بیش از یک نفر مجاز نمی‌باشد.
۱۲-۷	وب سایت‌های آماده متن‌باز	در توسعه وب‌سایت‌های حوزه اجرا نباید از وب‌سایت‌های آماده و متن‌باز مانند CMSها استفاده گردد.
۱۳-۷	ثبت نام دامین	دامین سرویس‌های اینترنتی حوزه اجرا می‌بایست ir. باشد. دامین حتماً باید به نام شخص حقوقی شرکت ثبت شود؛ به طوری که مدیریت دامین، وابسته به دسترسی‌ها و شناسه‌های یک فرد خاص نباشد.
۱۴-۷	ارزیابی امنیتی دوره‌ای سیستم‌ها	تمام سیستم‌عامل‌ها و سرویس‌های حوزه اجرا باید بر اساس یک زمانبندی مستند به صورت دوره‌ای (هر سال حداقل یکبار) تست نفوذپذیری و ارزیابی امنیتی شده و تمام آسیب‌پذیری‌های

[1] Software
[2] Session
[3] Username
[4] مانند سیستم‌عامل‌های سرورها، کلاینت‌ها، تجهیزات، پایگاه‌های داده و برنامه‌های کاربردی و غیره

		کشف شده باید در اسرع وقت مرتفع گردند. گزارشات حاصل از این فرایند باید در اختیار مسئول امنیت اطلاعات قرار گیرد. ارزیابی امنیتی برنامه‌های کاربردی باید مطابق کنترل۷-۱۵ انجام شود.
۷-۱۵	الزامات ارزیابی امنیتی برنامه‌های کاربردی	ارزیابی امنیتی و آزمون نفوذپذیری برنامه‌های کاربردی می‌تواند توسط پرسنل متخصص شرکت انجام پذیرد اما باید حداقل یکبار در سال و یا به ازای هر تغییر عمده در برنامه، این ارزیابی، توسط حداقل یک شرکت تخصصی دارای پروانه معتبر از مرکز مدیریت راهبردی افتای ریاست جمهوری با گرایش ارزیابی امنیتی انجام شود. ارزیابی امنیتی فوق زمانی کامل محسوب می‌شود که گزارش مکتوبی توسط شرکت تخصصی مذکور مبنی بر عدم وجود آسیب‌پذیری در آن نسخه مشخص از برنامه قید شده باشد.
۷-۱۶	رویه اعطاء و لغو دسترسی	برای اعطاء و لغو دسترسی به سیستم‌عامل‌ها و سرویس‌های حوزه اجرا، باید یک رویه مستند مطابق با اصل حداقل دسترسی تهیه، اجرا و به‌روزرسانی گردد. در این رویه، باید ایجاد دسترسی، مبتنی بر درخواست مستند و مکتوب متقاضی و منطبق بر خط مشی‌های امنیتی شرکت باشد. شرح دسترسی‌های ایجاد شده، نتایج بازنگری دوره‌ای حقوق دسترسی کاربران و حذف دسترسی‌های غیر ضروری باید مستند شود.
۷-۱۷	آنتی‌ویروس	بر روی تمامی سیستم‌عامل‌های حوزه اجرا باید آنتی‌ویروس با قابلیت مدیریت متمرکز و لایسنس معتبر نصب شود و به طور مداوم به‌روزرسانی گردد. آنتی‌ویروس منتخب باید تمامی عملکردهای رایج یک آنتی ویروس از جمله امکان شناسایی و مقابله با ویروس‌ها، کرم‌واره‌ها، تروجان‌ها، باج‌افزارها و سایر بدافزارها را داشته باشد.
۷-۱۸	به‌روزرسانی	کلیه به‌روزرسانی‌های امنیتی در تمامی سیستم‌عامل‌ها و مولفه‌های نصب شده بر روی آن‌ها (مانند Apache، .NET Framework، Microsoft SQL Server و غیره) باید مطابق با زمانبندی معین و مستند و اصول مدیریت وصله[1] نصب و اعمال شوند.
۷-۱۹	فهرست نرم‌افزارهای مجاز	فهرستی از نرم‌افزارهای مجاز و دلیل موجه نیاز به هر یک جهت نصب بر روی سیستم‌عامل‌های کلاینت‌ها و سرورهای حوزه اجرا می‌بایست تهیه و مستند گردد. نصب نرم‌افزارهای خارج از این فهرست مجاز نیست.
۷-۲۰	کنترل نرم‌افزارهای سرورها	نصب هرگونه نرم‌افزار مانند Adobe Reader، Flash player، Microsoft Office و از این قبیل، بر روی سیستم‌عامل سرورهای حوزه اجرا، مجاز نمی‌باشد.
۷-۲۱	دسترس‌پذیری	در سرویس‌هایی که اختلال یا عدم سرویس‌دهی آن‌ها منجر به خسارت بر بخشی یا تمامی بازار سرمایه شود، باید افزونگی به گونه‌ای لحاظ گردد که اختلال در عملکرد یک جزء، منجر به اختلال در سرویس‌دهی نگردد.
۷-۲۲	تحویل نام کاربری و رمز عبور	باید رویه‌ای امن جهت تحویل نام‌کاربری و رمزعبور به کاربران یا مشتریان سامانه‌ها تهیه، مستند و اجرا گردد. این رویه می‌بایست به تأیید مسئول امنیت اطلاعات و واحد حقوقی شرکت برسد.

[1] Patch Management

۸- حفاظت از داده‌ها		
۸-۱	ذخیره داده‌های محرمانه	داده‌های محرمانه باید به صورت رمز شده (مطابق با کنترل ۸-۵) ذخیره شوند.
۸-۲	ذخیره کلمات عبور	کلمات عبور نباید به صورت متن واضح ذخیره شوند، بلکه باید حتی‌الامکان به صورت درهم‌سازی شده (رمز یکطرفه و غیر قابل بازگشت) و در غیر اینصورت مطابق کنترل ۸-۵ به صورت رمز شده ذخیره شوند. ذخیره کلمات عبور حتی به صورت درهم‌سازی شده در Log مجاز نمی‌باشد.
۸-۳	خط‌مشی کلمات عبور	خط‌مشی کلیه کلمات عبور در سیستم‌های حوزه اجرا باید از نظر طول، پیچیدگی، زمان انقضا و از این قبیل به شیوه‌های امنیتی صحیح، مطابق با مراجع SANS یا NIST الزام و مستند شود.
۸-۴	انتقال داده‌های محرمانه	انتقال داده‌های محرمانه بر روی بسترهای ارتباطی باید با استفاده از پروتکل‌های امن و به صورت رمز شده (مطابق با کنترل ۸-۵) صورت پذیرد. این بسترهای ارتباطی باید در برابر حملات شناخته شده (به عنوان مثال آسیب‌پذیری Heartbleed و Poodle در SSL) مقاوم باشد و انتخاب Cipher Suite باید بر اساس بهترین تجربیات امنیتی انجام شود.
۸-۵	رمزنگاری	الگوریتم‌ها، توابع رمزنگاری و درهم‌سازی و طول کلید آن‌ها باید به صورت امن، مطابق با پیشنهادات شناخته شده FIPS یا NIST باشد. در صورت منسوخ شدن یک الگوریتم رمزنگاری یا درهم‌سازی، باید نسبت به جایگزینی آن اقدام گردد.
۸-۶	امحاء	تمامی تجهیزات ذخیره‌سازی و مستنداتی که حاوی اطلاعات طبقه‌بندی‌شده باشند و نیازی به نگهداری آن‌ها نباشد، باید مطابق با یک رویه امن و مستند، به صورت فیزیکی از بین بروند یا به گونه‌ای امحاء شوند که آن اطلاعات قابل بازیابی نباشد. همچنین سوابق عملیات امحاء باید مستند گردد.
۸-۷	پشتیبان‌گیری	باید رویه‌ای جهت پشتیبان‌گیری منظم از داده‌های مهم و پیکربندی سرویس‌های حوزه اجرا، تهیه، مستند و اجرا شود. عملیات آزمون نسخ پشتیبان باید به صورت دوره‌ای در این رویه لحاظ و اجرا گردد.

۹- -ثبت وقایع[1] و پایش رخدادهای امنیتی		
۹-۱	ثبت Log	باید تمامی فعالیت‌های زیر در سطح سیستم‌عامل‌ها، پایگاه‌های داده، وب سرورها، برنامه‌های کاربردی تحت وب و تجهیزات شبکه‌ای و امنیتی، مطابق با کنترل ۹-۲ ثبت شود: • دسترسی‌های افراد به سیستم‌ها و داده‌ها • تغییر در داده‌ها و پیکربندی • فعالیت‌های افرادی که دارای اختیارات ویژه در حوزه اجرا می‌باشند • دسترسی‌ها به Log • توقف یا راه‌اندازی مکانیزم‌های ثبت وقایع • تلاش‌های دسترسی ناموفق به منابع و اطلاعات • فعالیت‌های تصدیق اصالت
۹-۲	اطلاعات Log	در ذخیره‌سازی Log حداقل اطلاعات زیر باید ثبت شوند: • شناسه منحصربفرد کاربر • نوع فعالیت یا رویداد • تاریخ و زمان رویداد • وضعیت موفقیت یا عدم موفقیت فعالیت یا رویداد • شناسه منحصربفرد سیستم مبدأ شناسه منحصربفرد سیستم مقصد و اجزای تحت تاثیر فعالیت یا رویداد
۹-۳	حفاظت از Log	به منظور حفاظت از Log موارد زیر باید رعایت شوند: • Log باید در یک سیستم مرکزی مدیریت وقایع نگهداری شوند و حداقل به مدت یک سال در دسترس باشند. • مدیران سیستم نباید مجوز تغییر، حذف و یا غیرفعال نمودن گزارش‌های فعالیت‌های خود را داشته باشند. راه‌اندازی، متوقف نمودن و یا تغییر در سیستم‌های ثبت وقایع باید ثبت شود.
۹-۴	پشتیبان‌گیری از Log	به منظور پشتیبان‌گیری منظم از کلیه Log ثبت شده، باید رویه‌ای امن تهیه، مستند و اجرا شود. عملیات آزمون نسخ پشتیبان باید به صورت دوره‌ای در این رویه لحاظ و اجرا گردد.
۹-۵	ثبت اطلاعات ترافیک شبکه[2]	تمامی اطلاعات ترافیک عبوری از فایروال‌ها باید به مدت حداقل ۱ سال ذخیره و نگهداری شده و در دسترس باشد.

[1] Log
[2] Traffic Log

۹-۶	پایش حملات و رخدادهای امنیتی	در حوزه اجرا، حملات و رخدادهای امنیتی باید به طور مستمر ثبت و توسط حداقل یک نیروی متخصص امنیت پایش شوند. این رخدادها، باید به مدت حداقل ۲ سال نگهداری شده و در دسترس باشند. در صورت بروز حملات بحرانی یا شواهدی از آن، مراتب باید بلافاصله به مرکز مکنا اطلاع داده شود.
۹-۷	شرایط و ضوابط ارسال وقایع و رویدادها	شرکت باید کلیه وقایع و Log های ثبت شده را حسب درخواست، در چارچوب و بستر ابلاغی مرکز مکنا ارائه نماید.
۹-۸	همزمان‌سازی ساعت‌ها	تاریخ و زمان تمامی سرورها، تجهیزات شبکه‌ای و امنیتی حوزه اجرا، باید با یک سیستم همزمان‌سازی یکسان تنظیم شوند.

۱۰- امنیت فیزیکی		
۱-۱۰	امنیت فیزیکی محیط کاری	اصول حفاظت فیزیکی (مانند کنترل دسترسی فیزیکی) برای محل استقرار راهبران شبکه، امنیت، سرورها و گروه‌های برنامه‌نویسی در حوزه اجرا باید رعایت گردد.
۲-۱۰	محل نگهداری تجهیزات	کلیه تجهیزات شبکه و ذخیره‌سازی و سرورهای عملیاتی حوزه اجرا، باید در محل فیزیکی اختصاصی و امن (تحت عنوان مرکز داده) در داخل کشور نگهداری شوند. توصیه می‌شود برای طراحی و نگهداری مرکز داده، از آخرین استانداردهای معتبر استفاده شود.
۳-۱۰	مرکز داده پشتیبان	ضروری است مرکز داده پشتیبان جهت جلوگیری از قطع سرویس‌دهی در زمان بروز بلایای طبیعی و اتفاقات غیرمترقبه، بر مبنای نیازمندی های تعریف شده در استاندارد تداوم کسب وکار (ISO 22301)، راه اندازی شده باشد. تمامی سرویس‌ها و تجهیزات با درجه حساسیت حیاتی در حوزه کسب و کار که عدم سرویس‌دهی آنها منجر به خسارت می‌گردد، می‌بایست در مرکز داده پشتیبان مستقر گردند. این امر باید به گونه‌ای لحاظ گردد که در صورت بروز اختلال در عملکرد مرکز داده اصلی، در مدت زمانی که تاثیر قابل توجهی بر روی تداوم کسب و کار سرویس های حیاتی شرکت نداشته باشد و SLA سرویس نیز کماکان حفظ شود، امکان جایگزینی سرویس‌های مرکز داده وجود داشته باشد.
۴-۱۰	شرایط فیزیکی مرکز داده	محل مرکز داده باید به گونه‌ای انتخاب شود که در برابر خطراتی مانند طوفان، سیل، زلزله، آتش سوزی، بمب‌های مغناطیسی و سرقت ایمن باشد. علاوه بر این، محیط مرکز داده باید در برابر دود، گرد و غبار، گرما و رطوبت ایمن باشد.
۵-۱۰	فهرست دارایی‌های فیزیکی	اطلاعات مربوط به تجهیزات فیزیکی مرکز داده در حوزه اجرا باید حداقل بر اساس موارد زیر مستند گردد. (تعداد رک‌ها، شماره رک، وجود سنسور اعلام و اطفاء حریق، وجود سیستم سرمایش، وجود برق پشتیبان، نوع کنترل ورود و خروج)
۶-۱۰	نام‌گذاری تجهیزات مرکز داده	تمامی تجهیزات و کابل‌های ارتباطی در مرکز داده باید بر اساس استانداردی مشخص مانند (ANSI/TIA/EIA/606A) نام‌گذاری گردد. این نام‌گذاری باید به صورتی باشد که برای پشتیبانی و نگهداری از مرکز داده تنها افراد مسئول بتوانند تجهیزات و ارتباطات آنها را تشخیص دهند.
۷-۱۰	کنترل دسترسی فیزیکی	دسترسی فیزیکی به تجهیزات حوزه اجرا (در داخل مرکز داده یا خارج از آن) باید کنترل شده و محدود باشد.
۸-۱۰	ورود و خروج افراد به مرکز داده	ورود و خروج افراد به مرکز داده باید محدود و تحت کنترل بوده و اطلاعات آن ثبت و حداقل به مدت دو سال نگهداری شود.

۹-۱۰	ورود و خروج رایانه‌ها و تجهیزات ذخیره‌سازی	ورود و خروج رایانه‌های شخصی و تجهیزات ذخیره‌سازی قابل‌حمل به حوزه اجرا باید محدود، کنترل شده و مستند باشد.
۱۰-۱۰	افزونگی تجهیزات پشتیبانی مرکز داده	سیستم‌های پشتیبانی برق، اطفاء حریق و سرمایش مراکز داده باید به گونه‌ای باشند که با از کار افتادن آن‌ها، تا زمان رفع مشکل، سیستم جایگزین آن، نیاز مرکز داده را تأمین نماید.
۱۱-۱۰	دوربین مداربسته	تمامی دسترسی‌های فیزیکی به مرکز داده، باید به طور کامل توسط دوربین‌های مدار بسته کنترل شوند. هرگونه حرکتی در این محدوده، باید توسط دوربین مداربسته ثبت و ضبط شده و در محلی امن ذخیره و به مدت حداقل یک سال نگهداری شود.
۱۲-۱۰	مدیریت تغییرات مرکز داده	قبل از اعمال تغییرات در مرکز داده، باید احتمال قطع شدن ارتباطات یا از کار افتادن سرویس‌ها پیش‌بینی شده و طرح برون رفت از حادثه تهیه شود. هرگونه تغییرات باید ثبت و به اطلاع مسئول امنیت اطلاعات شرکت برسد.

مرکز نظارت بر امنیت اطلاعات بازار سرمایه (مکنا)

تهران، خیابان ملاصدرا، سازمان بورس و اوراق بهادار

Email: MAKNA@SEO.IR