سازمان بورس و اوراق بهادار
SECURITIES & EXCHANGE ORGANIZATION

الزامات امنیت و فناوری اطلاعات بازار سرمایه

طبقه‌بندی محرمانگی: عادی

نسخه ۵.۰

مرداد ماه ۱۴۰۰

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 چهارصد و چهل و هشتمین جلسه هیأت مدیره سازمان بورس و اوراق بهادار تدوین شده است.

این الزامات بر اساس آخرین استانداردهای معتبر بین‌المللی امنیت و فناوری اطلاعات (از جمله ISMS[1]، SANS[2]، NIST[3]، PCI-DSS[4] ، Secure SDLC[5]، SDLC، ITIL[6] v3 و TIA[7]-942)، الزامات امنیت 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 آن‌ها 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

6 Information Technology Infrastructure Library

7 Telecommunications Industry Association

تغییرات نسبت به نسخه قبل

تغییرات مستند حاضر (نسخه ۵.۰) نسبت به نسخه قبلی (نسخه ۴.۰) عمدتا مربوط به موارد الزامات فناوری اطلاعات در زیرساخت‌ها و سامانه‌ها بوده که با همکاری مدیریت فناوری اطلاعات سازمان تدوین گردیده است. تغییرات عمده در کنترل‌ها در جدول ذیل لیست شده است:

شماره کنترل در نسخه قبلی (۴.۰)	شماره کنترل در نسخه فعلی (۵.۰)	شرح تغییرات
---	۱-۳	این کنترل اضافه شده است.
۴-۱	۱-۵	محتوای کنترل کاملتر شده است.
۵-۱	۱-۶	محتوای کنترل کاملتر شده است.
۲-۳	۳-۲	محتوای کنترل کاملتر شده است.
۵-۲	۲-۵	محتوای کنترل کاملتر شده است.
۱-۳	۳-۱	محتوای کنترل کاملتر شده است.
۳-۳	---	این کنترل حذف شده است.
۴-۱	۱-۴	محتوای کنترل کاملتر شده است.
۴-۳	۳-۴	محتوای کنترل کاملتر شده است.
---	۶-۳	این کنترل اضافه شده است.
۳-۶	۶-۴	محتوای کنترل کاملتر شده است.
---	۶-۲۱	این کنترل اضافه شده است.
---	۶-۲۹	این کنترل اضافه شده است.
---	۶-۳۰	این کنترل اضافه شده است.
---	۶-۳۱	این کنترل اضافه شده است.
---	۶-۳۲	این کنترل اضافه شده است.
---	۶-۳۳	این کنترل اضافه شده است.
---	۶-۳۴	این کنترل اضافه شده است.
---	۶-۳۵	این کنترل اضافه شده است.
---	۶-۳۶	این کنترل اضافه شده است.
---	۷-۲	این کنترل اضافه شده است.
---	۷-۳	این کنترل اضافه شده است.
---	۷-۴	این کنترل اضافه شده است.
---	۷-۵	این کنترل اضافه شده است.
---	۷-۲۵	این کنترل اضافه شده است.
---	۷-۲۷	این کنترل اضافه شده است.

---	۷-۲۸	این کنترل اضافه شده است.
---	۷-۲۹	این کنترل اضافه شده است.
---	۹-۸	این کنترل اضافه شده است.
---	۹-۹	این کنترل اضافه شده است.
---	۹-۱۰	این کنترل اضافه شده است.
---	۹-۱۱	این کنترل اضافه شده است.
---	۱۰-۳	این کنترل اضافه شده است.
---	۱۰-۴	این کنترل اضافه شده است.
---	۱۰-۵	این کنترل اضافه شده است.
---	۱۰-۶	این کنترل اضافه شده است.
۱۰-۹ و ۱۰-۸	۱۰-۹	محتوای کنترل‌ها ترکیب و کاملتر شده است.
۱۱-۱۰	۱۰-۱۱	این کنترل کاملتر شده است.
---	۱۰-۱۳	این کنترل اضافه شده است.
---	۱۰-۱۴	این کنترل اضافه شده است.
---	۱۱-۱	این کنترل اضافه شده است.
---	۱۱-۲	این کنترل اضافه شده است.
---	۱۱-۳	این کنترل اضافه شده است.
---	۱۱-۴	این کنترل اضافه شده است.
---	۱۱-۵	این کنترل اضافه شده است.
---	۱۱-۶	این کنترل اضافه شده است.
---	۱۲-۱	این کنترل اضافه شده است.
---	۱۲-۲	این کنترل اضافه شده است.
---	۱۲-۴	این کنترل اضافه شده است.
---	۱۲-۵	این کنترل اضافه شده است.
---	۱۲-۶	این کنترل اضافه شده است.
---	۱۲-۷	این کنترل اضافه شده است.
---	۱۲-۸	این کنترل اضافه شده است.

فهرست

پیشگفتار ۶
اهداف ۸
تعریف واژگان ۹
فصل اول ۱۱
۱- ساختار سازمانی ۱۲
۲- استقرار الزامات ۱۳
۳- تعامل با طرف‌های ثالث ۱۴
۴- الزامات منابع انسانی ۱۵
۵- حفظ انطباق ۱۷
فصل دوم ۱۸
۶- امنیت شبکه و ارتباطات ۱۹
۷- امنیت سیستم‌ها و برنامه‌های کاربردی ۲۴
۸- حفاظت از داده‌ها ۳۰
۹- ثبت وقایع و پایش ۳۱
۱۰- امنیت فیزیکی ۳۴
۱۱- پشتیبان‌گیری ۳۹
۱۲- تداوم کسب‌وکار و بازیابی از بحران ۴۰

پیشگفتار

اغلب فرآیندهای بازار سرمایه، از درگاه‌های اطلاع‌رسانی و سامانه‌های مکاتبات اداری تا سامانه‌های معاملاتی بر روی زیرساخت‌ها و سامانه‌های فناوری اطلاعات انجام می‌شود و در صورت وجود 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.

همچنین با توجه به اهمیت و نقش کلیدی زیرساخت‌ها و سامانه‌های فناوری اطلاعات در ارائه خدمات با بالاترین سطح قابل قبول، پایدار، امن، کارا و مؤثر به کاربران و ذینفعان بازار سرمایه، لزوم تعریف مجموعه‌ای از اصول و الزامات در استقرار، پیاده‌سازی، راهبری و توسعه سامانه‌ها و زیرساخت‌های فیزیکی، ارتباطی، پردازشی و سایر موارد مرتبط با حوزه فناوری اطلاعات در بازار سرمایه کشور و رعایت و پایبندی به آنها امری ضروری است.

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

- الزامات ساختار سازمانی امنیت اطلاعات
- الزامات ساختار سازمانی فناوری اطلاعات
- الزامات خط‌مشی‌ها و فرایندهای امنیتی
- الزامات امنیت تعامل با طرف‌های ثالث
- الزامات امنیت منابع انسانی
- الزامات امنیت شبکه و ارتباطات
- الزامات امنیت سیستم‌عامل‌ها و پایگاه‌های داده

- الزامات امنیت برنامه‌های کاربردی
- الزامات حفاظت از داده‌ها و اطلاعات
- الزامات پشتیبان‌گیری
- الزامات مرکز داده
- الزامات ممیزی داخلی، بازنگری و بهبود
- الزامات زیرساخت فیزیکی
- الزامات تداوم کسب‌وکار و بازگشت از بحران
- الزامات سرورها و سرویس‌ها
- الزامات پایش و گزارشگیری
- الزامات راهبری و پشتیبانی

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

اهداف

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

- نظام‌مند نمودن امنیت اطلاعات در ساختار بازار سرمایه
- ارتقاء نظام فناوری اطلاعات بازار سرمایه در جهت به‌کارگیری ظرفیت فناوری اطلاعات در بازار سرمایه و بهبود سطح اعتمادسازی و اتکاپذیری
- ارائه چارچوبی به منظور ارتقاء سطح امنیت و پایداری سامانه‌های بازار سرمایه و انجام اقدامات پیشگیرانه و پدافندی
- بیان حداقل نیازمندی‌ها، الزامات و کنترل‌های امنیت و فناوری اطلاعات مطابق با نیازهای بازار سرمایه
- ارائه ساختاری برای شناسایی و تقویت نقاط قوت و رفع نقاط آسیب‌پذیر امنیت و فناوری 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 فنی و امنیتی، در پی تحقق اهداف ذیل در مجموعه خود باشد:

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

تعریف واژگان

سازمان: منظور سازمان بورس و اوراق بهادار است.

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 مکانیزم 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 بین‌المللی 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.

RTO[4] : این معیار برابر با حداکثر مدت زمان قابل قبولی است که سرویس می‌تواند در دسترس نباشد. تعیین این معیار بر اساس حساسیت هر سرویس و برابر با مدت زمانی است که کسب‌وکار، عدم سرویس‌دهی را تحمل خواهد کرد.

RPO[5] **:** این معیار معادل یک بازه زمانی است که با بروز مشکل در یک سامانه و از دست رفتن داده‌های وارد شده به سامانه در این بازه، برای شرکت و کسب‌وکار قابل تحمل باشد. این معیار در تعیین سیاست‌های مربوطه به استفاده از مراکز داده و زیرساخت‌های پشتیبان و همچنین پشتیبان‌گیری بسیار مهم است.

سیستم Ticketing: سیستمی است که عمدتاً مبتنی بر ITIL در جهت ثبت و پیگیری درخواست‌های پشتیبانی از یک مجموعه پیاده‌سازی می‌گردد.

SLA[6]**:** منظور "توافق‌نامه سطح خدمات" است که در قالب قرارداد بین سرویس‌دهنده و سرویس‌گیرنده، مشخص‌کننده تعهدات، مسئولیت‌ها و اولویت‌های ارائه‌دهنده و گیرنده خدمات در قبال سرویس است.

---

[1] Zone
[2] Deployment Diagram
[3] Single Point of Failure
[4] Recovery Time Objective
[5] Recovery Point Objective
[6] Service Level Agreement

شبکه تبادل اطلاعات بازار سرمایه: منظور شبکه مستقل از شبکه اینترنت می‌باشد که سامانه‌های نظارتی و عملیاتی بازار سرمایه و هسته معاملات بر روی آن سرویس‌دهی می‌نماید.

فصل اول

الزامات عمومی

۱- ساختار سازمانی		
۱-۱	ساختار سازمانی امنیت اطلاعات	شرکت باید در راستای اهداف تعیین شده، ساختار سازمانی امنیت اطلاعات را به صورت مستقل و مستقیما زیرنظر عالی‌ترین مقام شرکت، جهت استقرار و حفظ این الزامات و دیگر الزامات مقرراتی امنیت اطلاعات، ایجاد نماید. شرکت باید در راستای اهداف تعیین شده حوزه نرم‌افزار (شامل تولید و توسعه نرم‌افزار، پشتیبانی و نگهداری آن)، حوزه زیرساخت و حوزه ممیزی فنی داخلی داشته باشد.
۱-۲	مسئول امنیت اطلاعات	شرکت می‌بایست مسئول امنیت اطلاعات خود را تعیین و به مرکز مکنا معرفی نماید.
۱-۳	مسئول فناوری اطلاعات	شرکت می‌بایست مسئول فناوری اطلاعات خود را تعیین و به مرکز مکنا معرفی نماید.
۱-۴	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.
۱-۵	مستند مسئولیت‌های افراد	مستند مسئولیت‌های افراد در رابطه با مدیریت، پیاده‌سازی، نگهداری و اجرای این الزامات، از جمله در ساختار واحد امنیت و فناوری اطلاعات می‌بایست تدوین و مکتوب گردد.
۱-۶	طرح‌های حوزه فناوری اطلاعات و بهبود سطح امنیت اطلاعات	طرح‌های انجام شده، طرح‌های در حال انجام و طرح‌های آتی که در حوزه فناوری اطلاعات و 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.
۱-۷	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 را به همراه دلایل به مرکز مکنا 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 فنی و 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 و ابلاغیات	شرکت نسبت به اجرای کامل سایر الزامات فنی و 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 فنی و 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 پایداری سرویس فناوری اطلاعات و امنیت اطلاعات را حداقل در سطح این الزامات فراهم نماید. این رویه باید حداقل دارای موارد کنترل ۲-۳ 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.

[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. همچنین شرکت می‌بایست کارشناسان با تجربه و مسلط به تمامی تخصص‌های مورد نیاز حوزه فناوری اطلاعات را متناسب با گستره سرویس‌دهی خود بصورت داخلی در اختیار داشته باشد، به نحوی که سطح سرویس مطلوب در اختیار مشتریان قرار گیرد.
۴-۲	بررسی سوابق افراد	عدم وجود سوء پیشینه کیفری، دارا بودن مهارت کافی در حوزه تخصصی و صلاحیت حرفه‌ای کارکنان، پیمانکاران، مشاوران 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 را به مدت نامحدود 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 در حوزه فناوری و 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 مستند نموده و 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	فرآیند 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 مستمر در راستای ممیزی داخلی	شرکت باید بر اساس نتایج ممیزی داخلی، اقدامات اصلاحی را در راستای رفع اساسی مشکلات موجود انجام داده و در صورت نیاز طرح‌های فنی و امنیتی خود را به‌روز نماید.
۵-۳	بازنگری مستمر	شرکت با توجه به پایش‌های مستمر، ممیزی‌ها و تجربیات حاصل از حوادث فنی و امنیتی و به منظور تصدیق الزامات فنی و امنیتی برآورده شده، باید حوزه اجرا، کنترل‌های فنی و 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

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 و در صورت هر گونه اعمال تغییر، بروزرسانی گردد. 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	فهرست ارتباطات WAN	شرکت می‌بایست لیستی از تمامی خطوط ارتباطی WAN خود، تهیه، مستند و در صورت هر گونه اعمال تغییر، بروزرسانی نماید. این لیست می‌بایست حداقل شامل موارد ذیل باشد: • مقصد ارتباط (نام شرکت، ساختمان و غیره) • نوع ارتباط (از قبیل فیبر نوری، فیبر تاریک، MPLS، بی سیم) • ظرفیت ارتباط بر حسب مگابایت بر ثانیه • واسط ارتباط (از قبیل مخابرات، شرکت‌های خصوصی ارائه دهنده) • هدف از برقراری ارتباط (از قبیل اتصال به شبکه معاملات آنلاین، دسترسی به اینترنت) • استفاده‌کنندگان و کاربران (از قبیل کاربران ایستگاه‌های معاملاتی، کلیه پرسنل) • وجود لینک‌های افزونه ارتباطات WAN • تاریخ برقراری ارتباط
۶-۴	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: • نام، مدل، محل استقرار در رک و شماره پورت‌های ارتباطی فیزیکی تجهیزات • تجهیزات افزونه • وجود تمامی تجهیزات و همچنین تجهیزات افزونه و ارتباطات فیزیکی در توپولوژی شبکه

۶-۵	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
۶-۶	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.
۶-۷	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.
۶-۸	فایروال برنامه‌های کاربردی تحت وب (WAF)	تمامی برنامه‌های کاربردی تحت وب در حوزه اجرا باید توسط WAF 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.)
۶-۹	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.)
۶-۱۰	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.
۶-۱۱	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.
۶-۱۲	زون‌بندی شبکه کلاینت‌ها	شبکه کلاینت‌های حوزه اجرا باید مطابق با کنترل ۶-۱۰ به زون‌های مجزا تقسیم گردیده و نباید هیچ‌گونه دسترسی میان این زون‌ها وجود داشته باشد.
۶-۱۳	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.

۶-۱۴	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.
۶-۱۵	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.
۶-۱۶	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 خط‌مشی‌های 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.
۶-۱۷	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.
۶-۱۸	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.
۶-۱۹	دسترسی به درگاه‌های پیکربندی	هیچ‌یک از درگاه‌های پیکربندی تجهیزات، سیستم‌عامل‌ها و سرویس‌ها نباید از شبکه‌ای خارج از شبکه حوزه اجرا مستقیماً قابل رویت باشد.
۶-۲۰	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 ۵-۸) و تصدیق اصالت به روش دو فاکتوری انجام شود.
۶-۲۱	مکانیزم مدیریت سطح دسترسی (Privilege Access Management)	دسترسی مدیریتی به سرورها و سرویس‌های عملیاتی می‌بایست توسط مکانیزم مدیریت سطح دسترسی (PAM) کنترل گردد.
۶-۲۲	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 سوئیچ 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.

۶-۲۳	به‌روزرسانی تجهیزات	سیستم‌عامل و میان‌افزار تجهیزات امنیتی (مانند IPS و آنتی‌ویروس) و شبکه باید به صورت مداوم به آخرین نسخه امن و پایدار به‌روزرسانی گردند. همچنین سیستم‌عامل تجهیزات شبکه و امنیت شبکه در حوزه اجرا باید نسخه معتبر، امن و پایدار باشد.
۶-۲۴	امن‌سازی 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.
۶-۲۵	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.
۶-۲۶	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.
۶-۲۷	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 ۵-۸) باشد.
۶-۲۸	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 ۶-۲۷) 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.
۶-۲۹	زیر ساخت Passive شبکه	در رابطه با زیرساخت passive شبکه لازم است موارد زیر عملیاتی گردد: • کلیه کابل‌های فیبر نوری از انواع OM3 یا OM4 باشند؛ • کلیه کابل‌های مسی از انواع Cat6-A یا بالاتر باشند؛ • لیبل‌گذاری و شماره‌گذاری تجهیزات و کابل‌ها می‌بایست مطابق با استاندارد TIA942 انجام پذیرد.
۶-۳۰	مدیریت آدرس‌دهی IP	شرکت می‌بایست مکانیزم تامین، تخصیص و مدیریت IP (داخلی و عمومی) را داشته باشد و مستندات مربوط به آن را نگهداری و بروزرسانی نماید.
۶-۳۱	جداسازی شبکه تبادل اطلاعات بازار سرمایه	شبکه تبادل اطلاعات بازار سرمایه می‌بایست به طرق مجازی یا فیزیکی، مستقل از سایر شبکه‌های ارتباطی اعم از اینترنت، LAN و غیره باشد.
۶-۳۲	سیستم جلوگیری از نشت داده‌ها (DLP[1])	به منظور جلوگیری از افشا اطلاعات و نشت داده‌های محرمانه در شبکه‌های دارای اطلاعات نهانی می‌بایست از سیستم جلوگیری از نشت داده‌ها استفاده گردد.

۶-۳۳	مکانیزم سوئیچینگ	مکانیزم سوئیچینگ در داخل شبکه می‌بایست با توجه به موارد ذیل باشد: • رعایت مکانیزم‌های Loop prevention درسوئیچینگ شبکه • رعایت VLANبندی شبکه • استفاده از پروتکل‌هایی مانند VTP، در صورت وجود تعداد زیاد سوئیچ‌ها • قرار دادن VLAN Gatewayها بر روی تجهیزات امنیتی لایه۳ به بالا • رعایت کامل نکات امنیتی در پروتکل‌های لایه ۲ شبکه نظیر DAI[2].
۶-۳۴	مسیریابی شبکه داخلی مرکز داده	لازم است شبکه داخلی مرکز داده دارای مسیرهای افزونه جهت مسیریابی باشد و حتی الامکان ارتباطات مسیریابی شبکه به صورت پویا با یکدیگر برقرار گردد.
۶-۳۵	ظرفیت تجهیزات مرکز داده/اتاق سرور	طرح و تجهیزات مرکز داده/اتاق سرور می‌بایست بر اساس نیازسنجی و در نظر گرفتن نرخ رشد کاربران باشد و در زمان‌های اوج استفاده از سرویس‌ها، کارایی مد نظر را پوشش دهد.
۶-۳۶	استفاده از لایسنس[3] معتبر	شرکت می‌بایست برای تمام تجهیزات شبکه و امنیت از لایسنس معتبر استفاده نماید.

[1] Data Leakage Prevention
[2] Dynamic ARP Inspection
[3] License

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 به همراه Subnet • 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 بین ۱ تا ۱۰، کمترین حساسیت ۱ و بیشترین حساسیت ۱۰) • مشخصات مسئول هر سرویس
۷-۲	فهرست سامانه‌ها/ سرویس‌ها	شرکت می‌بایست لیستی از تمامی نرم‌افزارها و سامانه‌ها از دامنه اجرا، تهیه، مستند و در صورت اعمال هر گونه تغییر بروزرسانی نماید. این لیست می‌بایست حداقل شامل موارد ذیل باشد: • شرح مختصر کارکرد سامانه/سرویس؛ • زیرسیستم‌های سامانه؛ • ماژول‌های وابسته (سایر ماژول‌هایی که به هر نحو با سامانه در ارتباط هستند و از آن سرویس می‌گیرند و یا به آن سرویس می‌دهند)؛ • مسئول سامانه/سرویس • مخاطبین سامانه • پاسخگوی فنی سامانه/سرویس؛ • قابلیت‌های عملکردی اصلی سامانه/سرویس؛ • مشخصات فنی سامانه/سرویس (شامل تکنولوژی (تحت ویندوز/وب/موبایل)، زبان برنامه‌نویسی/ نوع سیستم‌عامل/ پایگاه‌داده/ معماری/ متدلوژی طراحی/ رویکرد طراحی/ سایر)؛ • حقوق مالکیت سامانه/سرویس؛ • روش تامین سامانه (تولید داخلی یا خریداری) (در صورت خریداری، مشخصات شرکت تولیدکننده و وضعیت پشتیبانی از سامانه/سرویس مشخص شود).

[1] Application

۷-۳	مستندات نرم‌افزار	شرکت می‌بایست حداقل مستندات زیر را برای هر سامانه/سرویس تهیه، نگهداری و بروزرسانی نماید: • مستند معماری سامانه شامل اطلاعات کاملی از لایه‌بندی آن به همراه شماتیک لایه‌بندی، شرح وظیفه هر لایه، کلاس‌های مرتبط با هر لایه • مستندات پایگاه داده (شامل DataBase Diagram، جداول، ویوها، رویه‌ها و توابع) • مستندات آزمون (شامل Test Case، Test Procedure و Test Result برای آزمون‌های مختلف مانند Unit Test، Integration Test و Validating Test) • مستندات استقرار سامانه (شامل Deployment Diagram) • مستندات آموزش سامانه/سرویس • مستندات راهبری سامانه • شناسنامه سرویس
۷-۴	معماری استقرار سامانه‌ها	معماری سامانه حداقل شامل سه لایه (Presentation Layer, Business Logic Layer, Data Access Layer) باشد.
۷-۵	قابلیت‌های ضروری سامانه‌ها و سرویس‌ها	• سامانه/سرویس باید قابلیت مدیریت خطاها را بصورت دقیق و کنترل شده داشته باشد؛ • اعتبارسنجی داده‌های ورودی: واسط کاربری باید با اعمال کنترل‌های لازم بر روی تمامی فیلدهای ورودی به شکلی اعمال شود که از دریافت داده‌های نامعتبر، خطرناک و اضافی ممانعت نماید؛ • سامانه از انعطاف‌پذیری لازم جهت اعمال محدودیت‌ها و قوانین و مقررات و گزارشات مورد نیاز بازار سرمایه را داشته باشد.
۷-۶	جداسازی سرویس‌ها	سرویس‌های با درجه حساسیت امنیتی بزرگتر یا مساوی ۵ (بر اساس کنترل ۱-۷)، باید هر کدام به تنهایی بر روی یک سیستم‌عامل مجزا قرار گیرند.
۷-۷	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 و اطلاعات واقعی در محیط‌های تست یا توسعه مجاز نمی‌باشد.
۷-۸	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 ۱۸-۷) بر روی آن‌ها انجام شود و پس از اطمینان از رفع آسیب‌پذیری‌ها، با رعایت کنترل ۷-۱، انتقال به محیط عملیاتی صورت پذیرد.
۷-۹	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.

۷-۱۰	امن‌سازی	پیکربندی تمامی سیستم‌عامل‌ها و مولفه‌های نصب شده بر روی آن (مانند IIS، نرم‌افزارهای 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.
۷-۱۱	جداسازی برنامه کاربردی تحت وب از پایگاه داده	نصب پایگاه داده‌ها و برنامه‌های کاربردی تحت وب بر روی یک سیستم‌عامل مشترک مجاز نیست.
۷-۱۲	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
۷-۱۳	انقضای نشست (Session TimeOut)	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.
۷-۱۴	عدم استفاده اشتراکی از شناسه‌های کاربری	در سیستم‌هایی که از مکانیزم تصدیق اصالت استفاده می‌کنند، هر شناسه کاربری بایستی تنها متعلق به یک کاربر بوده و به صورت مستند مطابق کنترل ۷-۲۶ به وی تحویل شود. به عبارت دیگر، استفاده اشتراکی از شناسه‌های کاربری یا تخصیص یک شناسه کاربری به بیش از یک نفر مجاز نمی‌باشد.
۷-۱۵	وب سایت‌های آماده متن‌باز	در توسعه وب‌سایت‌های حوزه اجرا نباید از وب‌سایت‌های آماده و متن‌باز مانند CMSها استفاده گردد.
۷-۱۶	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.

۷-۱۷	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 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 کنترل ۷-۱۸ انجام شود.
۷-۱۸	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.
۷-۱۹	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.
۷-۲۰	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.
۷-۲۱	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 (Patch Management) نصب و اعمال شوند.
۷-۲۲	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.
۷-۲۳	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.

۷-۲۴	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.
۷-۲۵	حساب کاربری راهبران	حساب کاربری (User Account) راهبران و سیستم‌های حیاتی مانند Vcenter، تجهیزات و سرورها می بایست در Directory Service مجزایی از کاربران عادی قرار گیرد.
۷-۲۶	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 شرکت برسد.
۷-۲۷	رویه نگهداری Source Code سامانه	جهت نگهداری Source Code و جلوگیری از دسترسی غیر مجاز باید رویه‌ای امن تهیه و اجرا گردد.

۷-۲۸	توافقنامه سطح خدمت (SLA)	شرکت می‌بایست برای هر سرویس/سامانه فهرست شده در بند ۲-۷، جهت تضمین سطح خدمت ارائه شده، توافقنامه سطح خدمت (SLA) ارائه نماید. جزئیات این الزام باید در قرارداد ارائه خدمت در بند جداگانه ذکر شود. توافقنامه سطح خدمت ارائه شده باید حداقل دارای یک شاخص قابل اندازه‌گیری باشد. شاخص‌های کلیدی عملکرد باید دارای ویژگی‌های ذیل باشد: ○ شاخص/شاخص‌ها باید از سوی ارائه کننده خدمت تعیین شود. ○ شاخص/ شاخص‌های ارائه شده باید قابل‌اندازه‌گیری باشند. ○ شاخص/ شاخص‌های ارائه شده باید از سوی ارائه کننده خدمت در بازه‌های زمانی مورد توافق اندازه‌گیری شود. ○ شاخص/شاخص‌های ارائه شده باید کارکرد صحیح و کامل تمام کاربردهای خدمت ارائه شده را اندازه‌گیری نمایند. ○ شاخص/شاخص‌های ارائه شده باید تخطی از عملکرد صحیح و میزان آن را گزارش نماید. ○ شاخص/شاخص‌های ارائه شده باید از سوی ارائه کننده و دریافت کننده خدمت قابل اندازه‌گیری باشد. صحت گزارش اندازه‌گیری شاخص/ شاخص‌های تعیین شده باید به تایید دریافت کننده خدمت برسد. در توافقنامه سطح خدمت باید زمان‌های مجاز وقفه و حداکثر میزان تخطی از سطح تضمین شده تعیین گردد. در توافقنامه سطح خدمت باید نحوه اندازه‌گیری شاخص، نحوه ارائه گزارش و دوره‌های زمانی ارائه گزارش شاخص‌ها از سوی ارائه کننده خدمت مشخص گردد. در توافقنامه سطح خدمت باید نحوه برخورد با تخطی رخ داده (به تفکیک میزان تخطی) مشخص گردد.
۷-۲۹	وضعیت نسخه‌بندی سامانه /سرویس (Versioning)	• برای مدیریت و کنترل نسخه‌های سامانه/سرویس باید از رویه و ابزار استاندارد استفاده شود؛ • سامانه /سرویس باید دارای شماره‌گذاری نسخه (ورژن) براساس روش‌های مرسوم و قابل قبول باشد و در صورت توسعه یا بروزرسانی تغییرات، شماره نسخه‌ها به روش معناداری تغییر نماید؛ • در صورت تغییر در نسخه سامانه/سرویس، باید نسخه جدید با نسخه‌های قبلی آن سازگاری منطقی داشته باشد.

۸- حفاظت از داده‌ها		
۸-۱	ذخیره داده‌های محرمانه	داده‌های محرمانه باید به صورت رمز شده (مطابق با کنترل ۵-۸) 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 ۵-۸ 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 ۵-۸) 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.

۹- ثبت وقایع[1] و پایش		
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	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.
۹-۵	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.
۹-۶	شرایط و ضوابط ارسال وقایع و رویدادها	شرکت باید کلیه وقایع و Logهای ثبت شده را حسب درخواست، در چارچوب و بستر ابلاغی مرکز مکنا ارائه نماید.

[1] Log

[2] Traffic Log

۹-۷	همزمان‌سازی ساعت‌ها	تاریخ و زمان تمامی سرورها، تجهیزات شبکه‌ای و امنیتی حوزه اجرا، باید با یک سیستم همزمان‌سازی یکسان تنظیم شوند.
۹-۸	پیاده‌سازی الزامات ثبت و ارسال لاگ	شرکت باید تنظیمات مربوط به لاگ سرویس‌ها، سامانه‌ها و تجهیزات را بر اساس الزامات ثبت و ارسال لاگ پیاده‌سازی نماید.
۹-۹	پایش سرویس‌های زیرساختی فناوری اطلاعات	شرکت می‌بایست از طریق سامانه پایش تمامی تجهیزات و سرویس‌های ذیل را بطور شبانه‌روزی مورد پایش قرار داده و گزارش‌های تولیدی را بر اساس اهمیت سرویس، برای یک بازه زمانی حداقل ۶ ماهه نگهداری نماید: • تمام تجهیزات شبکه، شامل لایه ۲، لایه ۳ و فایروال ها • تمام تجهیزات ذخیره‌سازی و پردازشی • تجهیزات زیرساخت فیزیکی مانند سرمایشی، الکترونیکی و الکتریکی • سرویس‌های زیرساختی مانند DNS و Mail • ارتباطات اینترنتی و WAN • ارتباطات اینترنتی از ابعاد سرعت، تأخیر و ترافیک‌های ورودی و خروجی به مرکزداده • سرویس‌های سمت کاربر نهایی یا مشتریان
۹-۱۰	قابلیت های کلیدی سامانه پایش NOC	• سامانه پایش می‌بایست دارای داشبوردهای نمایشی متنوعی بوده و امکان دریافت و نمایش گزارش‌های مختلف بصورت نموداری و فایل را داشته باشد. • شرکت مکلف است در صورت نیاز و اعلام سازمان امکان دسترسی به سامانه و دریافت گزارش از آن را فراهم نماید. • سامانه پایش باید با سامانه Ticketing قابلیت یکپارچگی داشته باشد و رخدادها در آن ثبت و پیگیری گردد. • سامانه پایش باید قادر به دسته‌بندی رخدادها بر اساس میزان حساسیت باشد. • سامانه پایش جهت اطلاع‌رسانی رخدادها به راهبران مربوطه باید قابلیت اطلاع‌رسانی از طریق ابزارهایی نظیر ارسال ایمیل، پیامک، هشدار صوتی و غیره را داشته باشد.
۹-۱۱	کنترل و مانیتورینگ	• کلیه پارامترهای محیطی نظیر دما و رطوبت و نشت آب توسط سیستم کنترل و مانیتورینگ، کنترل گردد • کلیه پارامترها و Log Fileهای مربوط به تمامی تجهیزات نظیر UPSها، چیلرها، Inrow Coolingها و دیزل ژنراتور می‌بایست توسط سیستم کنترل و مانیتورینگ ثبت گردند • سیستم کنترل و مانیتورینگ می‌بایست قابلیت ارسال Email و SMS را داشته باشد.

۱۰- امنیت فیزیکی		
۱۰-۱	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.
۱۰-۲	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.
۱۰-۳	شرایط فیزیکی مرکز داده	محلی که شرکت از آن به‌منظور نگهداری تجهیزات استفاده می‌کند می‌بایست دارای حداقل شرایط TIA-942-Tier2 به شرح ذیل باشد: • در برابر حوادث طبیعی و آتش‌سوزی مقاوم باشد؛ • در برابر نفوذ آبهای سطحی ایمن باشد و تمهیدات لازم جهت دفع آب پیش‌بینی گردد؛ • تمامی دیواره‌های اصلی از داخل و تمامی دیواره‌های داخلی می‌بایستی توسط مواد عایق حرارتی و توسط کناف پوشیده شوند (نباید از چوب و مشتقات آن در ساخت دیواره‌های اصلی و داخلی استفاده شود)، همچنین مرکز داده باید در برابر حملات مغناطیسی ایمن گردد؛ • هیچ‌گونه تأسیسات الکتریکی و مکانیکی غیر مرتبط نظیر لوله‌های آب و فاضلاب در این فضا وجود نداشته باشد؛ • جنس پانل‌های سقف کاذب در صورت وجود می‌بایست مناسب برای Clean Room باشد و فاقد هرگونه پرز و خاک و آلودگی باشد؛ • مستندات ساخت و نگهداری ابنیه و ساختمان شامل موارد فوق تهیه و بروزرسانی گردد.

۱۰-۴	سیستم اعلان و اطفاء حریق	در رابطه با سیستم اعلان و اطفاء حریق لازم است حداقل موارد زیر طبق ضوابط TIA-942-Tier2 در محل نگهداری تجهیزات فناوری اطلاعات رعایت گردد: • همه فضای مرکز داده/اتاق سرور می‌بایست مجهز به سیستم اعلان و اطفاء حریق اتوماتیک باشد؛ • گاز اطفاء حریق می‌بایست مورد تائید NFPA2001 و مناسب برای مراکز کامپیوتر و غیر مضر برای انسان باشد؛ • سیستم اعلان و اطفاء حریق علی الخصوص گاز و کپسول اطفاء می‌بایست دارای استاندارد FM و UL باشند؛ • سیلندر اطفاء هر اتاق خارج از اتاق مربوطه قرارگرفته باشد؛ • کپسول های گاز CO_2 دستی برای اطفاء برای هر نقطه از سایت قرار داده شود؛ • از دتکتورهایی با قابلیت تشخیص دود و آتش استفاده شود؛ • تابلو اعلان و اطفاء در محل مناسب و خارج از اتاق های برق و سرور نصب شود؛ • سیلندرها در محل نصب خود توسط بست مناسب به دیواره یا زمین متصل گردند؛ • کپسول‌های اطفاء اتوماتیک می‌بایست دارای ضامن دستی برای فعال سازی باشند؛ • سیستم اعلان و اطفاء حریق می‌بایست دارای باطری Back Up باشد؛ • مستندات ساخت و نگهداری سیستم اعلان و اطفاء حریق شامل موارد فوق تهیه و بروزرسانی گردد.
۱۰-۵	سیستم سرمایش	در رابطه با سیستم سرمایش مرکز داده حداقل الزامات TIA-942-Tier2 ذیل می‌بایست رعایت گردد: • کلیه لوله‌ها می‌بایست با عایق الاستومری[1] ایزوله و در محل‌های بدون حفاظ، پوشش کلاستر داشته باشند؛ • چیدمان رک‌ها می‌بایست به نحوی باشد که راهروهای سرد و گرم ایجاد گردد؛ • افزونگی در چیلر آبی و یا کندانسورهای گازی، حداقل به صورت n+1 رعایت گردد؛ • در کولینگ‌های هر بخش آبی و گازی، حداقل افزونگی n+1 رعایت گردد؛ • در تمامی پمپ‌های سیستم آبی، حداقل افزونگی n+1 رعایت گردد؛ • مسیر لوله‌های ورودی و خروجی در سیستم آبی از کف سایت باشد؛ • منبع آب سیستم سرمایش از نوع آبی سیلد باشد؛ • مستندات ساخت و نگهداری سیستم سرمایش شامل موارد فوق تهیه و بروزرسانی گردد.

[1] Elastomeric Insulation

۱۰-۶	برق، منبع تغذیه و ژنراتور	در رابطه با سیستم برق و توزیع حداقل الزامات TIA-942-Tier2 زیر می‌بایست رعایت گردد: • در UPSهای غیر ماژولار حداقل افزونگی n+1 می‌بایست رعایت گردد؛ • در پاور و باتری UPSهای ماژولار حداقل افزونگی n+1 می‌بایست رعایت گردد؛ • بک آپ باتری‌ها برای هر UPS می بایستی برای حداقل ۳۰ دقیقه در نظر گرفته شود؛ • از باتری‌های بدون نیاز به نگهداری (اسیدی خشک یا نیکل کادمیوم) استفاده گردد؛ • داشتن تابلو برق مخصوص به UPS (شامل محافظ برای ورودی، خروجی و کلید بای پاس) ضروری است؛ • جهت مصرف کننده‌های تک پاور، استفاده از ماژول ATS الزامی است؛ • وجود حداقل یک ژنراتور برای تغذیه UPS و سیستم سرمایش، الزامی است؛ • مخزن سوخت با حجم گازوئیل مناسب (برای ژنراتور با مصرف گازوئیل) برای حداقل مدت زمان ۴۸ ساعت می‌بایست پیش‌بینی گردد؛ • لازم است باتری ژنراتور بصورت پارالل (n+1) نصب شده باشد؛ • حتی در صورت تک بودن منبع UPS، ضروری است هر یک از رک‌ها از دو فید برق ورودی تغذیه شوند؛ • هر کابل (خروجی از تابلو و ورودی به رک) باید به کانکتور برق صنعتی مجهز گردد؛ • برای مرکز داده حداقل دو چاه ارت می‌بایست در نظر گرفته شود. همبندی چاه‌ها و تأسیسات فلزی ساختمان به منظور هم پتانسیل سازی الزامی می‌باشد؛ • مستندات ساخت و نگهداری برق، منبع تغذیه و ژنراتور شامل موارد فوق تهیه و بروزرسانی گردد.
۱۰-۷	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)
۱۰-۸	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.

۱۰-۹	کنترل دسترسی فیزیکی	ضمن مشخص و مستند کردن مکان‌های فیزیکی حساس، لازم است رویه‌ای جهت اعطاء دسترسی، ثبت و کنترل تردد تمامی پرسنل، مشاوران و پیمانکاران به این مکان ها، تدوین شده و اجرایی گردد؛ درب‌های ورودی اصلی مکان‌های فیزیکی حساس می‌بایست مجهز به سیستم کنترل تردد دارای کنترلر باشند تا امکان نفوذ به حداقل برسد؛ دستگاه‌های کنترل تردد مربوط به اتاق کامپیوتر، اتاق برق و Entrance Room می‌بایست از نوع بیومتریک باشند؛ 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. ورود و خروج رایانه‌های شخصی و تجهیزات ذخیره‌سازی قابل‌حمل به حوزه اجرا باید محدود، کنترل شده و مستند باشد. مستندات پایش و کنترل دسترسی فیزیکی شامل موارد فوق تهیه و بروزرسانی گردد.
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.
۱۰-۱۱	نظارت تصویری	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. تمامی نقاط مرکز داده باید در دید دوربین‌ها باشد. کلیه دوربین‌ها می‌بایست از انواع IP Camera و دارای کیفیت HD باشند؛ دوربین‌هایی که در فضای باز استفاده می‌شود باید از نوع Out Door باشند؛ برای ذخیره تصاویر می‌بایست از NVR و یا سرور به همراه نرم‌افزار مربوطه استفاده گردد و مقدار حافظه می‌بایست برای ذخیره حداقل یک سال محاسبه شده باشد؛ مستندات مربوط به نظارت بر ذخیره و بازیابی تصاویر شامل موارد فوق تهیه و بروزرسانی گردد.
۱۰-۱۲	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.

۱۰-۱۳	نگهداری مرکز داده	شرکت می‌بایست در رابطه با پشتیبانی و نگهداری مرکز داده/اتاق سرور موارد زیر را انجام دهد: • انجام بازدیدهای روزانه مطابق با چک لیست بازدید روزانه؛ • انجام روال‌های سرویس دوره‌ای ماهیانه، ۶ ماهه و سالیانه؛ • رعایت دستورالعمل‌ها و روال‌های تمیزکاری و نظافت مرکز داده؛ • تهیه گزارش‌های دوره‌ای و تحلیل چک لیست‌ها؛ • تأمین انبار قطعات یدکی و لوازم مصرفی؛ • دارا بودن افرادی متخصص در همه بخش‌های زیرساخت مرکز داده یا انعقاد قراردادهای پشتیبانی و سرویس و نگهداری؛ • مستندات مربوط به نگهداری مرکز داده شامل موارد فوق تهیه و بروزرسانی گردد.
۱۰-۱۴	افزونگی قطعات سخت‌افزاری	شرکت می‌بایست با توجه به اهمیت و نوع سامانه‌ها و سیستم‌ها، به ازای تجهیزات مهم مانند روتر لبه یا سوییچ‌ها، یک عدد تجهیز یدکی در انبار ذخیره داشته باشد و به ازای قطعات مصرفی و از بین رونده مانند هارد دیسک یا پاور و رم نیز، حداقل ۵٪ در انبار به عنوان یدکی داشته باشد. تمامی تجهیزات باید دارای جایگزین آماده برای نصب و راه‌اندازی در مواقع اضطراری باشند.

۱۱- پشتیبان‌گیری		
۱۱-۱	اولویت‌بندی داده‌ها برای پشتیبان‌گیری	شرکت می‌بایست تمامی اطلاعات و داده‌های موجود و مورد استفاده در حوزه اجرا را از لحاظ اهمیت و وابستگی کسب‌وکار به آنها اولویت‌بندی نموده و RTO وRPO هر یک از آنها را مشخص و مستندات آن را نگهداری و بروزرسانی نماید.
۱۱-۲	تعریف سیاست پشتیبان‌گیری	شرکت باید متناسب با RTO و RPO تعیین شده برای هر نوع از داده‌های موجود در دامنه اجرا، به صورت دوره‌ای و در بازه زمانی قابل‌قبول، از داده‌ها، بانک‌های اطلاعاتی و تنظیمات، بر اساس رویه‌ای مستند پشتیبان‌گیری نموده و در محلی امن نگهداری کند و مستندات آن را نگهداری و بروزرسانی نماید.
۱۱-۳	استراتژی پشتیبان‌گیری	در پشتیبان‌گیری از اطلاعات حساس می‌بایست از استراتژی ۳-۲-۱ (وجود ۳ نسخه پشتیبان، ۲ نسخه بروی رسانه‌های ذخیره‌سازی متفاوت و بصورت محلی و یک نسخه بصورت آفلاین در سایت پشتیبان) استفاده گردد.
۱۱-۴	نگهداری از نسخه‌های پشتیبان	کلیه نسخ پشتیبان می‌بایست بصورت امن نگهداری شوند و فرآیند دسترسی و افراد مجاز به دسترسی نیز مشخص شود.
۱۱-۵	بازه زمانی پشتیبان‌گیری	بازه زمانی پشتیبان‌گیری (Backup Window) می‌بایست بصورتی انتخاب گردد (براساس پارامترهای RTO و RPO) که کمترین احتمال از دست رفتن اطلاعات وجود داشته باشد.
۱۱-۶	آزمون اطمینان از پشتیبان‌گیری	با اجرای مانورهای دوره‌ای برای بازگرداندن داده‌های پشتیبان باید از صحت نسخ پشتیبان اطمینان حاصل گردد.
۱۱-۷	پشتیبان‌گیری از پیکربندی تجهیزات	باید رویه‌ای جهت پشتیبان‌گیری از پیکربندی تجهیزات شبکه‌ای و امنیتی به صورت مکانیزه در بازه‌های زمانی مشخص به صورت اتوماتیک و بسته به حساسیت و نقش هر تجهیز در شبکه و ارتباطات 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.
۱۱-۸	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.

۱۲- تداوم کسب‌وکار و بازیابی از بحران		
۱۲-۱	افزونگی در تجهیزات پردازشی و ذخیره‌سازی	تمامی تجهیزات پردازشی می‌بایست حداقل از طریق دو HBA به تجهیزات ذخیره‌سازی که خود حداقل داری دو Controller می‌باشد، متصل بوده و افزونگی در تمام سطوح مورد نیاز رعایت شود.
۱۲-۲	افزونگی در سرویس‌های اینترنتی	تمامی سامانه های حوزه اجرا که در مرکز داده شرکت (یا شرکت برون‌سپاری‌شده) میزبانی شده و به کاربران عمومی از طریق اینترنت سرویس‌دهی می‌شوند، می‌بایست حداقل از طریق ۲ خط ارتباط اینترنتی از ۲ تأمین‌کننده متفاوت و بر مبنای پروتکل پویای BGP یا پروتکل‌های تغییر اتوماتیک سرویس‌دهنده پهنای باند، ارائه شوند.
۱۲-۳	مرکز داده پشتیبان	ضروری است مرکز داده پشتیبان جهت جلوگیری از قطع سرویس‌دهی در زمان بروز بلایای طبیعی و اتفاقات غیرمترقبه، بر مبنای نیازمندی‌های تعریف شده در استاندارد تداوم کسب وکار (ISO 22301)، راه‌اندازی 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.
۱۲-۴	طرح تداوم کسب و کار و بازیابی از بحران	شرکت می‌بایست طرح تداوم کسب‌وکار خود را برای ادامه فعالیت کسب‌وکار و طرح بازیابی از بحران خود را مبتنی بر به‌روش‌های BCI و آخرین استانداردهای مربوطه، مستند و بروزرسانی نماید.
۱۲-۵	انتخاب سایت پشتیبان	شرکت می‌بایست محل قرارگیری فیزیکی سایت پشتیبان با کمترین تأثیرپذیری از سایت اصلی به لحاظ ریسک‌های شناسایی شده و بلایای طبیعی، مسائل جغرافیایی، سیاسی و غیره انتخاب نماید.
۱۲-۶	تطبیق سخت‌افزاری سایت پشتیبان	شرکت می‌بایست تجهیزات پردازشی، ذخیره‌سازی و شبکه‌ای منطبق بر سایت اصلی در سایت پشتیبان، پیاده‌سازی و پیکربندی نموده که در صورت بروز بحران، امکان بازیابی سریع سرویس‌ها در سایت پشتیبان فراهم باشد.
۱۲-۷	کمیته بازیابی از بحران	شرکت می‌بایست اعضای کمیته بازیابی از بحران را مشخص کرده و مسئولیت‌ها، شرح وظایف و نقش هر یک از اعضا به همراه آموزش مراحل بازیابی به هریک از افراد را انجام داده باشد.
۱۲-۸	مانور بازیابی بحران	شرکت می‌بایست تمرین بازیابی از بحران را به صورت دوره‌ای حداقل شش ماه یک بار با نظارت کمیته بازیابی از بحران انجام دهد و نتیجه مانور را مستند نماید.