تدوین ملاحظات پدافند غیر عامل در طراحی و ساخت مراکز داده

پیشگفتار

این سند شامل ملاحظات سازمان پدافند غیرعامل در طراحی و ساخت مراکز داده در کشور می‌باشد. سازمان پدافند غیر عامل کشور ۳ هدف امنیت، ایمنی و پایداری را در تمام حوزه ها از جمله حوزه فضای سایبر و فاوا (فن‌آوری اطلاعات و ارتباطات) دنبال می نماید. در این سند، این اهدف در مقوله طراحی و پیاده سازی مراکز داده کشور دنبال گردیده است. در ادامه چارچوب و محتویات سند توضیح داده می شود.

در این سند ابتدا شناخت وضعیت فعلی مراکز داده شامل تعاریف، تاریخچه و وضعیت مرکز داده در ایران و جهان آورده شده است. سپس به معماری ها و استانداردهای مراکز داده پرداخته شده و در ادامه تهدیدات امنیتی متصور برای مراکز داده کشور با رویکرد پدافند غیرعامل بررسی گردیده است. این تهدیدات در ۳ دسته ۱-تهدیدات ناشی از جنگ (سایبر و فیزیکی) و مخاصمات بین المللی ۲- تهدیدات امنیتی ۳- تهدیدات محیطی و طبیعی، مورد توجه قرار گرفته است. نهایتا در ادامه، ضمن ارائه راهکارهای فنی برای تهدیدات بیان شده، الگوی مراکز داده کشور با رویکرد پدافند غیر عامل تدوین گردیده و آورده شده است. در این الگو، ملاحظات پدافند غیر عامل به ۳ سطح بالا، میانی و پایین تقسیم بندی شده است. در ملاحظات سطح بالا، پارامترهای سطح بندی مراکز داده کشور و تعیین یکی از سطوح مهم، حساس یا حیاتی بیان گردیده است. در ملاحظات سطح میانی، کنترلهای پدافند غیر عامل و امنیتی متناسب با تهدیدات احصاء شده و به تفکیک برای هر یک از سطوح مراکز داده مهم، حساس و حیاتی بیان گردیده است. در ادامه به مصادیق ملاحظات سطح پایین مراکز داده نیز اشاره گردیده است، لیکن از آنجا که این ملاحظات وابسته به محصولات و تکنولوژی ها بوده و دائما در حال تغییر است، در

زمان طراحی و پیاده سازی هر مرکز داده، بایستی با توجه به ملاحظات سطح بالا و میانی که در این سند بیان شده، با نظارت سازمان پدافند غیر عامل تعیین و اجرا گردند.

در مجموع، هدف از تهیه این سند، ارائه راهکارهای لازم در حوزه پدافند غیر عامل در طراحی و پیاده سازی مراکز داده در کشور بمنظور استفاده توسط کلیه زیر مجموعه های کشور که نیاز به ایجاد مراکز داده دارند، می باشد. بدیهی است رعایت کنترلها و راهکارهای ذکر شده در این سند، برای کلیه بخشهای کشور الزامی است.

فهرست مطالب

فهرست شکلها

فهرست جداول

۱ فصل اول: پدافند غیر عامل

فصل اول:

پدافند غیرعامل

۱-۱ مقدمه

۱-۱-۱ پدافند غیر عامل

دفاع غیرعامل در واقع مجموعه تمهیدات، اقدامات و طرح‌هایی است که با استفاده از ابزار، شرایط و حتی‌المقدور بدون نیاز به نیروی انسانی به صورت خود اتکا صورت‌گیرد چنین اقداماتی از یک سو توان دفاعی مجموعه را در زمان بحران افزایش داده و از سوی دیگر پیامدهای بحران را کاهش و امکان بازسازی مناطق آسیب‌دیده را با کمترین هزینه فراهم می‌سازد. در حقیقت طرح‌های پدافند غیرعامل قبل از انجام مراحل تهاجم و در زمان صلح تهیه و اجرا می‌گردند. با توجه به فرصتی که در زمان صلح جهت تهیه چنین طرح‌هایی فراهم می‌گردد ضروری است این قبیل تمهیدات در متن طراحی‌ها لحاظ گردند. به‌کارگیری تمهیدات و ملاحظات پدافند غیرعامل علاوه برکاهش شدید هزینه‌ها، کارآیی دفاعی طرح‌ها، اهداف و پروژه‌ها را در زمان تهاجم دشمن بسیار افزایش خواهد داد.

۱-۲ تعاریف

۱-۲-۱ پدافند عامل [1]

عبارتست از بکارگیری مستقیم جنگ افزار، به منظور خنثی نمودن و یا کاهش اثرات عملیات خصمانه هوایی، زمینی، دریایی، نفوذی و خرابکارانه بر روی اهداف مورد نظر.

[1] Active Defence

۱-۲-۲ پدافند غیرعامل[1]

به مجموعه اقداماتی اطلاق می‌گردد که مستلزم بکارگیری جنگ افزار نبوده و با اجرای آن می‌توان از ورود خسارات مالی به تجهیزات و تأسیسات حیاتی و حساس نظامی و غیر نظامی و تلفات انسانی جلوگیری نموده و یا میزان این خسارات و تلفات را به حداقل ممکن کاهش داد.

۱-۲-۳ دفاع غیر نظامی[2]

دفاع غیرنظامی تقلیل خسارات مالی و صدمات جانی وارده بر غیر نظامیان در جنگ یا در اثر حوادث طبیعی نظیر سیل، زلزله، طوفان، آتش‌فشان، آتش‌سوزی و خشکسالی می‌باشد، در منابع خارجی، وظایف دفاع غیر نظامی شامل چهار عنوان ذیل می‌باشد:

۱- اقدامات پیشگیرانه و کاهش دهنده (Mitigation)

۲- آماده سازی و امداد رسانی (Preparation)

۳- هشدار و اخطار (Response)

۴- باز سازی مجدد (Recovery)

نکته:

ارائه تعریف دفاع غیر نظامی در این نوشتار در حوزه پدافند غیر عامل نبوده و بیشتر در جهت آگاهی مخاطبین در ممیزی بین پدافند غیرعامل و دفاع غیر نظامی می‌باشد؛ زیرا به دلیل عدم شناخت جامع در بسیاری از کتب، مقالات، و یا نوشتارهای داخلی مشاهده گردیده است که دو مفهوم یاد شده با همدیگر اشتباه گرفته می‌شوند.

---

[1] **Passive Defense**
[2] **Civil Defense**

۱-۲-۴ مراکز حیاتی و مراکز ثقل[1]

مراکز و تأسیسات حیاتی و پر اهمیت کشور می‌باشند که در صورت حمله و بمباران و انهدام آنها صدمات جدی به نظام اجتماعی، سیاسی و نظامی کشور وارد شده، آنها را در یک مخاطره و بحران جدی قرار می‌دهد.

۱-۲-۵ مراکز حیاتی[2]

مراکزی هستند که در صورت انهدام کل یا قسمتی از آنها، موجب بروز بحران، آسیب و صدمات قابل توجه در نظام سیاسی، هدایت، کنترل و فرماندهی، تولیدی و اقتصادی، پشتیبانی، ارتباطی و مواصلاتی، اجتماعی، دفاعی با سطح تأثیرگذاری در سراسر کشور گردد.

۱-۲-۶ مراکز حساس[3]

مراکزی هستند که در صورت انهدام کل یا قسمتی از آنها، موجب بروز بحران، آسیب و صدمات قابل‌توجهی در نظام سیاسی، هدایت، کنترل و فرماندهی تولیدی و اقتصادی، پشتیبانی، ارتباطی و مواصلاتی، اجتماعی، دفاعی با سطح تأثیر گذاری منطقه‌ای در بخشی از کشور گردد.

۱-۲-۷ مراکز مهم[4]

مراکزی هستند که در صورت انهدام کل یا قسمتی از آنها، آسیب و صدمات محدودی در نظام سیاسی، اجتماعی، دفاعی با سطح تأثیر گذاری محلی در کشور وارد می‌گردد.

---

[1] **Vital and Gravity Centers**

[2] **Vital Centers**

[3] **Critical Centers**

[4] **Important Centers**

۱-۲-۸ استتار و اختفاء[1]

فن و هنری است که با استفاده از وسائل طبیعی یا مصنوعی، امکان کشف و شناسائی نیروها، تجهیزات و تأسیسات را از دیده بانی، تجسس و عکسبرداری دشمن تقلیل داده و یا مخفی داشته و حفاظت نماید.

مفهوم کلی استتار، همرنگ و هم‌شکل کردن تأسیسات، تجهیزات و نیروها با محیط اطراف می‌باشد.

اختفا، حفاظت در برابر دید دشمن را تأمین می‌نماید و استتار امکان کشف یا شناسایی نیروها، تجهیزات و تأسیسات و فعالیتهای را تقلیل می‌دهد.

۱-۲-۹ پراکندگی[2]

گسترش‌باز و پخش نمودن و تمرکز زدایی نیروها، تجهیزات، تأسیسات یا فعالیت‌های خودی، به منظور تقلیل آسیب پذیری آنها در مقابل عملیات دشمن به طوری که مجموعه‌ای از آنها هدف واحدی را برای دشمن تشکیل ندهند.

۱-۲-۱۰ تفرقه و جابجایی[3]

جداسازی، گسترش افراد، تجهیزات و فعالیت‌های خودی از محل استقرار اصلی به محلی دیگر به منظور کاهش آسیب پذیری، خسارات و تلفات می‌باشد؛ مانند: انتقال هواپیماهای مسافرتی به فرودگاه‌های

---

[1] **Camouflage & Concealment**
[2] **Dispersion**
[3] **Separation and Movement**

دورتر از برد سلاح‌های دشمن و یا انتقال تجهیزات حساس قابل حمل از محل اصلی به محل موقت که به علت عدم شناسایی و حساسیت مکانی، دارای امنیت و حفاظت بیشتری می‌باشد.

۱-۲-۱۱ استتار، اختفاء و ماکت فریبنده D&CC

استفاده و بهره برداری از اقدامات تجهیزات و روش‌هایی برای پنهان نمودن، همگون سازی، تغییر شکل، شبیه سازی، ایجاد طعمه فریبنده و حذف شکل منظم هندسی اهداف در جهت ممانعت از کشف و شناسائی نیروها، تجهیزات، تأسیسات و فعالیت‌های خودی توسط سامانه‌های آشکار ساز و حساسه دشمن.

۱-۲-۱۲ فریب[1]

کلیه اقدامات طراحی شده حیله‌گرانه‌ای که موجب گمراهی دشمن در نیل به اطلاعات و محاسبه و برآورد صحیح از توان کمی و کیفی طرف مقابل گردیده و او را در تشخیص هدف و هدف گیری با شک و تردید مواجه نماید.

فریب، انحراف ذهن دشمن از اهداف حقیقی و مهم به سمت اهداف کاذب و کم اهمیت می‌باشد.

۱-۲-۱۳ مقاوم سازی و استحکامات[2]

ایجاد هر گونه حفاظتی که در مقابل اصابت مستقیم بمب، راکت، موشک، گلوله توپخانه، خمپاره و یا ترکش آنها مقاومت نموده و مانع صدمه رسیدن به نفرات، تجهیزات یا تأسیسات گردیده و اثرات ترکش و موج انفجار را به طور نسبی خنثی نماید. پناهگاه، جان پناه، سازه‌های امن و مقاوم‌سازی تأسیسات،

[1] **Deception**
[2] **Fortification**

ایجاد استحکامات صحرایی و سازه‌های موقتی، دال بتنی، کیسه شن، خاک‌ریز، بشکه شن و یا استوانه بتنی و ... جزء استحکامات محسوب می‌شوند.

۱-۲-۱۴ اعلام خبر[1]

آگاهی و هشدار به نیروهای خودی مبنی بر نزدیکی عملیات تعرض دشمن. این هشدار که برای آماده شدن می‌باشد، ممکن است چند ساعت، چند روز و یا زمانی طولانی‌تر از آغاز مخاصمات اعلام گردد.

دستگاه‌ها و وسایل اعلام خبر شامل رادار، دیده‌بانی بصری، آژیر، بلندگو، پیامها و آگهی‌های هشداردهنده می‌باشد.

۱-۲-۱۵ مکان یابی[2]

یکی از اقدامات اساسی و عمده پدافند غیر عامل، انتخاب مکان مناسب می‌باشد تا آنجا که ممکن است باید از ایجاد تأسیسات حیاتی و حساس در دشت‌های مسطح یا نسبتا هموار اجتناب کرد. زیرا تأسیسات احداث شده در چنین محل‌هایی را نمی‌توان از دید دشمن مخفی نگاه داشت.

ایجاد تأسیسات حیاتی و حساس در کنار بزرگراه‌ها، جاده‌های اصلی، کنار سواحل دریا، رودخانه‌ها و نزدیکی مرزها موجب سهولت شناسایی و هدف یابی آسان آنها توسط دشمن می‌گردد.

توضیح اینکه سه موضوع عمده که می‌بایست در مکان یابی به آن توجه خاص مبذول گردد به شرح ذیل می‌باشد:

۱- مأموریت (Mission)

---

[1] **Early warning**
[2] **Site selection**

امکان اجرای مأموریت در مکان تعیین شده موجود باشد.

۲- پراکندگی (Dispersion)

وسعت مکان انتخابی به صورتی باشد که امکان پراکندگی مناسب تأسیسات و تجهیزات را فراهم نماید.

۳- شکل عوارض و محیط (Terrain Pattern)

مکان انتخابی به گونه‌ای باید باشد که احداث تأسیسات و استقرار تجهیزات تا آنجا که ممکن است باعث بهم خوردگی شکل طبیعی زمین نگردیده، ضمنا همرنگی با عوارض محیطی (روستایی، کویری، کوهستانی، جنگلی، شهری) حفظ شود.

۱-۲-۱۶ مواد جاذب هوشمند

ترکیبی از مواد جاذب فعال و غیر فعال، حسگرهای محیطی و ماژول های الکترونیکی بوده و جهت پردازش اطلاعات جمع آوری شده طراحی گردیده به طوری که اعمال فرامین کنترلی جهت اتخاذ پاسخ مناسب را فراهم می کند.

۱-۲-۱۷ ماهواره سنجش از راه دور

سنجش از دور علم و هنر به دست آوردن اطلاعات درباره یک شیء، منطقه، یا پدیده از طریق تجزیه و تحلیل داده‌های حاصله به وسیله ابزاری است که در تماس فیزیکی با شیء، منطقه و یا پدیده تحت بررسی نباشد. توصیه می‌شود که در بدو شروع احداث تأسیسات حیاتی و حساس همیشه مراقب چشمهای بیدار سنجیده‌های سنجش از دور دشمن و ستون پنجم باشیم. ضمناً صرف هر گونه هزینه در این زمینه ها بدون لحاظ نمودن موارد حفاظتی به هدر دادن سرمایه‌های ملی منجر خواهد شد.

از آنجایی که انعطاف‌پذیری ماهواره‌ها در جمع‌آوری اطلاعات بسیار دقیق و حساس نظامی وجاسوسی دائماً در حال افزایش می‌باشد، نقش آنها در عملیات اطلاعات سری، از جمله قابلیت شناسایی و تعیین محل تأسیسات عمیق زیرزمینی به طور روزافزونی بیشتر می گردد.

ماهواره‌های اکتشافی از تعدادی حساسه و تصویربردار با وضوح فوق‌العاده مانند اسکنرهای چندطیفی لندست [1] به منظور جمع‌آوری آثار و علایم مربوط به وجود احتمالی تأسیسات زیرزمینی و فعالیت‌های آن استفاده می‌نماید که انجام این کار به تصویربرداری مادون قرمز نزدیک، مادون قرمز حرارتی و چند طیفی محیط اطراف تاسسیات بستگی دارد.

۱-۲-۱۸ منعکس کننده های زاویه ای (گوشه دار)

وقتی ردیاب به دنبال یک هدف غیرواقعی برود و از هدف واقعی غافل گردد این خود نوعی فریب است. در این روش از منعکس‌کننده‌های ویژه‌ای که دارای زوایای خاصی هستند استفاده میگردد که باعث انعکاس بیشتر امواج راداری و بالطبع افزایش سطح مقطع راداری RCS گردیده و اهداف واقعی در بین اهداف کاذب پنهان می گردند. هدف اصلی این گونه منعکس‌کننده‌ها منحرف کردن موشک‌هایی است که دارای رادارهای ردیاب موج میلی‌متری می‌باشند.

۱-۲-۱۹ فرستنده های الکترونیکی فریب (طعمه ها[2])

یکی از بهترین راهکارهای فریب موشک‌های Arm/ Harm به منظور مصون ماندن رادار، استفاده از فرستنده‌های فریب و اشباع فضا از امواج کاذب می‌باشد. این روش مقرون به صرفه بوده و از اثربخشی

[1] Handsets Multral Scanner
[2] Decoys

بالایی برخوردار است. فرستنده‌های فریب در انواع گوناگون طراحی و ساخته می‌شوند و همچنین به شیوه‌های مختلف تاکتیکی قابل بهره‌برداری می‌باشند. از انواع دیگر موشک‌های ضدتشعشع راداری می‌توان موشک‌های Alarm - Shrike را نام برد که تحت تأثیر فریب واقع می‌شوند.

۳-۱ اهداف پدافند غیرعامل

۱. ارتقاء بازدارندگی موثر و تحقق امنیت پایدار در توسعه کشور در برابر تهدیدات
۲. تحقیق و پژوهش، تولید علم و فرهنگ سازی و تبدیل آن به معارف و باور عمومی
۳. ارتقاء دانش و نظام مدیریتی کارا و اثربخش خاص شرایط بحران
٤. کاهش مجموعه آسیب‌پذیری های کشور و به حداقل رساندن تأثیر تهدیدات دشمن و افزایش هزینه تهاجم
٥. تکمیل چرخه دفاعی کشور و تعامل مثبت با پدافند عامل و غیرعامل
٦. دستیابی به زیرساختهای حیاتی امن و زیرساختهای حساس با حداقل آسیب پذیری در برابر تهدیدات
۷. دستیابی به ساختار و عملیات تداوم خدمات ملی، استانی، شهری و دستگاهی و مدیریت صحنه بحرانی و دفاع غیرنظامی در شرایط بحران ناشی از جنگ
۸. ارتقاء آستانه تحمل ملی در برابر تهدیدات و بالا بردن قابلیت بقاء و حفظ کشور در شرایط تهدید و بحران
۹. ارتقاء بهره مندی از ظرفیت‌ها و توانمندی‌های نیروهای داوطلب مردمی و بسیجی در همه حوزه‌ها و عرصه‌ها

۱۰. دستیابی به پایداری امنیت کشور و ایمن سازی زیرساختها در برابر تهدیدات نرم با استفاده از رویکردهای پدافند غیرعامل نرم

۱-۴ اصول و ملاحظات پدافند غیرعامل

۱-۴-۱ اقدامات اساسی دفاع غیر عامل

اقدامات اساسی در تأمین دفاع غیرعامل شامل موارد ذیل می‌باشد که در تهیه طرح‌ها متناسب با مأموریت، وضعیت، موقعیت و شرایط زمانی و مکانی و رده سازمانی باید مورد استفاده و بهره برداری لازم قرار گیرد. در ابتدا فهرست‌وار اصول دفاع غیر عامل و ملاحظات آن نام برده شده و سپس به تعریف هر یک از اصطلاحات پرداخته شده است.

۱. استتار (Camouflage)

۲. اختفا (Concealment)

۳. پوشش (Cover)

٤. فریب (Deception)

٥. تفرقه و پراکندگی (Separation and Dispersion)

٦. مقاوم سازی و استحکام (Hardening)

۷. اعلام خبر (Early Warning)

۸. مکان یابی (Site Selection)

۹. تحرک (Movement)

۱۰. پناهگاه (Defilade)

۱۱. جان پناه (Trench)

۱۲. انضباط استتار (Camouflage Discipline)

۱۳. حفاظت (Security)

۱٤. سیستم اطفا حریق (Extinguishing System)

۱۵. اقدامات درون سیستمی

۱٦. آموزش و ایجاد فرهنگ دفاع (Training)

۱۷. ایجاد موانع (دیوار - دکل - کابل - بالن) (Barrier)

۱۸. عملیات دود (Smoke Operation)

۱۹. اقدامات بعد از بمباران(کنترل تردد، تخلیه مجروحین، کنترل خسارت، خنثی سازی بمب و ...)

۲۰. ایمنی (Safety)

۲۱. مقابله با بمب های گرافیتی E.M.P - H.P.M

۲۲. ایجاد استحکامات صحرایی و سازه‌های موقتی (Field fortification)

۲۳. ایجاد سازه‌های امن و مقاوم سازی تأسیسات (Protective Structures)

۲٤. دفاع غیر عامل در مقابل حملات ویژه (ش.م.ه)

۱-۴-۲ ملاحظات پدافند غیرعامل

تجربیات حاصل از جنگ تحمیلی و خسارت‌های وارده ناشی از تهاجمات دشمن به تأسیسات نظامی و صنعتی از قبیل: کارخانجات تولید تسلیحات نظامی، نیروگاه‌ها، پالایشگاه‌ها، محورهای مواصلاتی، بیمارستان‌ها، پادگان‌ها و صنایع مادر، لزوم توجه به دفاع بهینه را که تلفیقی از پدافند عامل و غیرعامل می‌باشد بر همگان روشن ساخت. آنچه که در این میان و در خصوص پدافند غیرعامل و اصول مرتبط با آن

مد نظر است توجه به این نکته اساسی است که: در ساخت و راه‌اندازی پروژه‌ها و طرح‌های بزرگ و کلان اقتصادی باحجم سرمایه گذاری‌های انبوه نظیر پالایشگاه‌ها، سدها، مجتمع‌های پتروشیمی، فرودگاه‌ها و غیره به اصول و مبانی پدافند غیرعامل توجه اساسی به عمل نیامده‌است و از طرفی نیز بدون توجه به ملاحظات امنیتی و دفاعی سرمایه گذاری‌های کلانی در سطح کشور انجام‌گرفته و یا در حال انجام است. پروژه‌ها وتأسیسات اقتصادی و زیربنایی بدون رعایت و یا دخالت ملاحظات و ترتیبات دفاعی و امنیتی ساخته‌شده و یا توسعه یافته‌اند و به صورت یک هدف کاملا عریان و در عین حال قابل توجه و مورد علاقه دردسترس و یا تیررس دشمن وکشورهای مهاجم قرار گرفته‌اند.

موقعیت و موضع استقرار استحکامات و تجهیزات دفاعی کشور نظیر سایت‌های موشکی و راداری با توجه به این نکته که برخی از آنها قبل از پیروزی انقلاب اسلامی توسط نیروهای بیگانه طراحی و ساخته‌شده‌اند و یا توسط سیستم‌های جاسوسی و سیستم‌های جمع‌آوری و شناسایی دشمن کشف و شناسایی شده‌اند تغییری نکرده‌است. چنین به نظر می‌رسدکه تأسیسات و ابنیه‌های فنی در دو بخش نظامی و غیرنظامی بدون انجام مطالعات و بررسی‌های ژئوپلتیکی، طرح‌های آمایش سرزمین و طرح‌های آمایش دفاعی احداث گردیده و یا توسعه یافته‌اند. صنایع مادر و زیربنایی در کشور نیز به‌صورت یکپارچه و عظیم و در عین‌حال متمرکز طراحی و راه‌اندازی شده‌اند و به مسأله بزرگ بودن این قبیل صنایع در مقابل توجه به اصول و مبانی پدافند غیرعامل از قبیل: کوچک سازی و پراکنده‌سازی توجه بیشتری معطوف شده‌است.

۵-۱ رویکرد جامع به مقوله پدافند غیرعامل

با توجه به روند جنگ‌ها و شرایط حال حاضر دنیا (چه از لحاظ تکنولوژیکی و چه از لحاظ سیاست‌های راهبردی) رویکردهای زیر برطرح پدافند غیرعامل حاکم است:

۱. به عنوان یک فرض مسلم وقطعی، پرداختن و توجه ویژه به مقوله پدافند غیرعامل از لحاظ کمی و کیفی و بررسی سامانه‌هایی که می‌بایست مورد توجه پدافند غیرعامل قرارگیرند نقش مهم و ارزشمندی را در تعیین سرنوشت جنگ بر عهده خواهدداشت.

۲. نظر به اهمیت در خور توجه و بایسته پدافند غیرعامل و سامانه‌های آن، وحدت فرماندهی و هماهنگی در خصوص نحوه و چگونگی اجرا، هدایت و راهبرد عملیات استتاری در سطوح عمودی و افقی نیروهای مسلح کشور و سایر منابع ملی، لازمه موفقیت در عملیات‌های پدافند غیرعامل و کارآمدی مدیریت راهبردی این نوع پدافند مبتنی برشیوه‌های نوین است .

۳. بدون شک پیشرفت‌های روز افزون در حوزه‌های ارتباطات، مخابرات و سیستم‌های شناسایی و جمع‌آوری اطلاعات، تغییرات قابل توجهی را در مکانیسم‌ها و سازوکارهای حاکم بر فعالیت‌ها و چالش‌های نظامی و دفاعی بوجود آورده‌است. همچنین شرایط حاضر جهانی بسیار متغییر بوده و روند رو به رشد سیستم‌های مزبور بسیار شتاب‌آلود و سریع است.

٤. از آنجا که روش‌های طراحی، مراقبت و نگهداری، برنامه‌ریزی، دیسیپلین و توسعه میدانی در پدافند غیرعامل نوین با توجه به شرایط و نحوه رویارویی و تقابل با دشمن از نظر سیاسی و جغرافیایی متفاوت است، تنوع شرایط و راهکارها، انعطاف و پویایی مفهوم فرماندهی وکنترل عملیات پدافند غیرعامل را در پی دارد.

از عناصر و پارامترهایی که در فرآیند برنامه‌ریزی برای مدیریت، فرماندهی و کنترل مستقیم و غیرمستقیم پدافند غیرعامل مهم و تأثیرگذار هستند می‌توان موارد زیر را برشمرد:

- فرهنگ سازمانی
- ساختار سازمانی و سلسله مراتب فرماندهی
- سیاست‌های راهبردی (استراتژی راهبردی و دکترین)
- امکانات موجود رزمی و پشتیبانی
- سطح دانش و آگاهی فرماندهان

۶-۱ سیاستهای کلی سازمان پدافند غیر عامل در حوزه IT کشور

۱. سازماندهی نظام جامع و فراگیر سیاست گذاری ، مدیریت و نظارت مستمر بر امن سازی فضای سایبر کشور بر مبنای اصل ۱۷۶ قانون اساسی.

۲. امن ، ایمن و پایدارسازی فضای سایبر زیر ساختهای حیاتی حساس و مهم کشور در برابر حملات و اختلال های الکترونیکی و الکترومغناطیسی بر اساس اصول پدافند غیر عامل.

۳. رعایت توازن بین امنیت و توسعه فضای سایبر متناسب با سطح طبقه بندی امنیتی (بر مبنای سیاست های پدافند غیر عامل و معیارهای امنیتی مربوط به مراکز حیاتی، حساس و مهم).

۴. اعتمادسازی و رعایت حریم خصوصی آحاد اشخاص حقیقی و حقوقی در فضای سایبر.

۵. ساماندهی محتوا و نظارت بر آن به منظور حفظ ارزش های دینی، ملی و حقوق معنوی افراد و ملاحظات امنیت ملی در فضای سایبر.

۶. ساماندهی و توسعه زیرساختهای امنیت فن‌آوری اطلاعات با تکیه بر توانمندی های داخلی و با تأکید بر بومی سازی.

۷. ساماندهی و توسعه صنعت بومی امنیت فن‌آوری اطلاعات با تکیه بر توانمندی های داخلی اعم از بخش های دولتی و خصوصی.

۸. اقتصادی نمودن امنیت فضای سایبر برای آحاد جامعه.

۹. ساماندهی و توسعه ظرفیت های علمی، پژوهشی و آموزشی در حوزه امنیت فن‌آوری اطلاعات.

۱۰. ارتقا سطح دانش و آگاهی و مهارت های عمومی مرتبط با امنیت فن‌آوری اطلاعات.

۱۱. پیش بینی تمهیدات و ساز و کارهای لازم جهت انجام مطالعات و پایش مستمر مخاطرات امنیتی در حوزه سایبری و به روز رسانی راه کارهای مقابله (SOC-CERT).

۱۲. تعامل و همکاری منطقه ای و بین المللی در زمینه امنیت فضای سایبر با تأکید بر امنیت ملی.

۱۳. تأمین ساز و کار های حقوقی و قانونی مورد نیاز.

۱۴. تدوین و اعمال قوانین ، مقررات و استانداردهای بومی ، به روز و کارآمد.

۷-۱ جهت‌گیری کلان پدافند غیرعامل فاوای کشور

سازمان پدافند غیرعامل در حوزه تخصصی فاوا با تکیه بر فرامین و تدابیر فرمانده معظم کل قوا در چارچوب مبانی راهبردی و اصول و مقررات ابلاغی سازمان پدافند غیرعامل کشور، با هدف:

۱. حذف و یا کاهش آسیب پذیری تأسیسات و تجهیزات حیاتی، حساس و مهم و نیز زیرساخت های ارتباطات و فن آوری اطلاعات در مقابل تهدیدات دفاعی و امنیتی

۲. پایدارسازی ارتباطات بین‌المللی، ملی، منطقه ای و محلی

۳. پایدارسازی فعالیت شبکه‌های ارتباطی و الکترونیکی برای استمرار جریان اطلاع رسانی عمومی

۴. پاسداری از آرامش و امنیت روانی جامعه از طریق حفظ بستر ارتباطات مردم (مخابرات) و ظرفیت فعال اطلاع رسانی (صدا و سیما)

۵. ایجاد یأس در دشمن در تحقق اهداف خصمانه خود

به منظور بهره مندی مستمر آحاد مردم و مدیریت کشور از قابلیت ها و فعالیت‌های شبکه‌های ارتباطی، الکترونیکی و فن آوری اطلاعات، تلاش دارد با برنامه ریزی، بستر سازی، تدوین مقررات، هماهنگی، نظارت و ارزشیابی و یا برآورد تهدیدات دفاعی امنیتی و آسیب شناسی در برابر تهدیدات موثر بر این حوزه با ایجاد فرصت ها و بهره گیری از آنها و ظرفیت های قانونی و بسیج توانمندی های فنی و مدیریتی در دستگاه های مرتبط و سایر دستگاه‌های ذینفع، الزامات پیاده سازی اصول پدافند غیرعامل در این حوزه را مهیا نموده و تحقق بخشید.

۸-۱ راهبردهای اصلی پدافند غیر عامل فاوای کشور

۱. نهادینه سازی فرامین و قانونمندسازی تدابیر مقام معظم رهبری در خصوص پدافند غیرعامل در سازمان ها و دستگاه های ذیربط

۲. ساماندهی، انسجام بخشی وهدایت راهبردی مجموعه های علمی، پژوهشی، آموزشی و صنعتی مرتبط با حوزه تخصصی فاوا در راستای تولید و توسعه دانش و فن‌آوری های بومی و ملی مورد نیاز پدافند غیرعامل در حوزه فاوا

۳. توسعه امنیت، ایمنی و پایداری در شبکه‌های ارتباطی و الکترونیکی موجود با تأکید بر فن‌آوری‌های بومی

۴. نهادینه کردن اصول و ملاحظات پدافند غیرعامل در طرح‌های توسعه شبکه های ارتباطی و الکترونیکی

۵. توسعه فرهنگ پدافند غیرعامل و ارتقاء دانش و شناخت مسئولین و کارشناسان حوزه ارتباطات و الکترونیک از پدافند غیرعامل

۶. خوداتکایی از دستگاه های پشتیبان آسیب پذیر و خودکفایی از منابع خارجی فن‌آوری ها

۷. حمایت از برنامه ایجاد شبکه ملی اینترنت مبتنی بر مولفه های امنیت، ایمنی، پایداری و متکی بر فن آوری های بومی

۸. توسعه و تقویت سیستم پست کشور (بهره‌مندی از پست بسیار سریع و امین)

۹. بهره‌مندی از شبکه ارتباطی ویژه مدیریت کشور در شرایط بحران جنگ (با مولفه های امنیتی و پایداری و ایمنی بسیار بالا و دسترسی سریع)

۱۰. توسعه توان کنترل و مدیریت بحران و برنامه های حراست، حفاظت و ضد جاسوسی

نهادینه کردن ملاحظات دفاع غیرعامل و امنیت ملی در تعاملات و همکاری با کشورها و شرکت های خارجی در حوزه ICT

۹-۱ اهداف برنامه ای پدافند غیر عامل فاوای کشور

۱. به تصویب رساندن لوایح قانونی، آئین نامه ها، دستورالعمل های مورد نیاز

۲. تشکیل گروه‌های آموزشی، پژوهشی، مشاوره‌ای، تولید فن‌آوری در بخش‌های تخصصی ارتباطات و الکترونیک

۳. تأمین نقاط احتیاط[1] ایمن و پایدار برای نقاط گره ای در مراکز حیاتی و حساس

۴. تدوین برنامه تهدید شناسی و آسیب شناسی در بخش های مرتبط و اجرایی نمودن آنها

۵. تدوین برنامه تولید و توسعه فن آوری های بومی و اجرایی نمودن آنها

۶. تدوین برنامه فرهنگ سازی و آموزش پدافند غیرعامل و اجرایی نمودن آنها

۷. تعیین و تثبیت ارتباطات کابلی با تکیه بر فن آوری بومی فیبرنوری به عنوان محور توسعه شبکه های ارتباطی و الکترونیکی

۸. تدوین برنامه های ایمن و پایدارسازی شبکه ها بر مبنای نتایج برنامه ای بند۴

۹. تأمین ساختارهای سازمانی (SOC , IDC , CERT و ...) و نرم افزارهای کلیدی بومی و ملی

۱۰. تشکیل و فعال سازی کمیته پدافند غیرعامل در شرکت پست ایران

۱۱. بهره برداری از شبکه ارتباطی ویژه مدیریت کشور

۱۲. تدوین طرح مدیریت بحران و طرح تشدید اقدامات حفاظتی و ضدجاسوسی

۱۳. فعال شدن بخش حقوقی وزارت ICT در روند برنامه های پدافند غیرعامل

۱۰-۱ مراجع

[۱] اسناد بالادستی سازمان پدافند غیر عامل کشور

[1] Backup

۲ فصل دوم: کلیات و تعاریف

فصل دوم:

کلیات و تعاریف

۲-۱ مقدمه

عصر حاضر عصر اطلاعات نام گرفته است. بی تردید، این نام گذاری به دلیل ارزش بسیار و نقش تعیین کننده این عنصر در تعاملات خرد و کلان بشر امروز می‌باشد. لذا کاملاً بدیهی است هرکس تلاش کند با دستیابی به منابع بیشتری از اطلاعات، تفوق و برتری خود را به دیگران نشان دهد.

در همین راستا، طی نیم قرن اخیر، بخش مهمی از تلاش دانشمندان حوزه‌های مختلف، صرف توسعه و ارتقای علوم و فنونی بوده که بهره برداری بهینه از اطلاعات را تضمین می‌کردند که در این میان فن‌آوری اطلاعات و ارتباطات به عنوان گزینه‌ای بی رقیب، با سرعت شگفت انگیزی مراحل تکامل خود را طی کرده و اکنون به جایگاهی رسیده که به لطف ماهیت اصلی خود، یعنی اطلاعات، از نقش تعیین کننده‌ای در تمامی حوزه‌ها برخوردار شده است.

حال برای اینکه با نحوه و میزان تأثیرگذاری این فن‌آوری براطلاعات بیشتر آشنا شویم، بهتر است بحث را با سیر تعامل آنها با یکدیگر آغاز کنیم.

از ابتدای ظهور سیستم‌های رایانه‌ای تا حدود دو دهه پیش، عمدتاً از آنها به عنوان مخازن اطلاعات که توانایی پردازش محدود آنها را نیز داشتند، استفاده می‌شد. ولی در همین حد نیز آن چنان هزینه نگهداری و بهره برداری از آنها گزاف بود که تنها بعضی مراکز دولتی یا بنگاه‌های خصوصی بزرگ از عهده این هزینه‌ها بر می‌آمدند. برای مثال، در ایران برای اولین بار در سال ۱۳۴۱ شمسی بانک ملی و شرکت ملی نفت سیستم‌های رایانه‌ای را به کار گرفتند.

اما به تدریج موانع بهره برداری گسترده‌تر و متنوع‌تر از سیستم‌های رایانه‌ای برچیده شد. افراد بیشتری توانستند از آنها استفاده کنند و تنوع پردازش اطلاعات نیز بیشتر شد. ولی آنچه در این حوزه تحول شگرفی محسوب می‌شود، ظهور شبکه‌های عظیم رایانه‌ای در سراسر جهان است که به مدد ارتباطات

الکترونیکی توانسته‌اند با یکدیگر ارتباط برقرار کنند. این شبکه‌ها با قابلیت‌های برجسته‌ای که دارند، توانسته‌اند بر اطلاعات از دو جهت تأثیر عمده‌ای بگذارند:

۱- امکان ذخیره سازی نامحدود اطلاعات با هزینه بسیار مناسب در اقصی نقاط جهان

۲- دسترس پذیری جهانی اطلاعات از طریق فن‌آوری‌هایی که هر روزه در حال پیشرفت هستند، مانند پایگاه‌های اطلاع‌رسانی تحت وب که امروزه میلیاردها نمونه از آن را در شبکه جهانی اینترنت شاهد هستیم.

وجود این همه امکانات با قابلیت‌های متعدد باعث شده افراد در موقعیت‌ها وشرایط کاری مختلف به منظور افزایش کارایی فعالیت‌ها خدمات آنها را به کارگیرد. امروزه دولتمردان، دانشمندان، دانش پژوهان، تجار و اصناف و به طور کلی هرکسی که کمترین آشنایی با فضای سایبر[1] و امکانات بی‌شمار آن دارد، بدون هیچ دغدغه‌ای اصطلاحات ترکیبی با پسوند الکترونیکی را به کار می‌برد. اما کمتر کسی به این مسأله بسیار مهم می‌اندیشد که در ورای هریک از این اصطلاحات، دنیایی از اطلاعات دودویی شده با ارزش و بعضاً حساس و حیاتی وجود دارد که باید با برنامه ریزی صحیح و اساسی آنها را به این دنیای بی‌کران وارد کرد.

۲-۲ تعریف مرکز داده

در نتیجه‌گیری حاصب از بخش قبل معلوم گردید که تحول اساسی در فن‌آوری اطلاعات و ارتباطات به لطف پیدایش شبکه‌های رایانه‌ای و اتصال آنها به یکدیگر از طریق ارتباطات الکترونیک بوده است. در این بخش، زیرساخت اصلی این شبکه‌ها، یعنی مراکز داده، که در واقع زیربنای اصلی فن‌آوری اطلاعات و ارتباطات نوین را تشکیل می‌دهند مورد بررسی قرار می گیرد.

[1] Cyber Space

همان طور که اشاره شد کاربرد اولیه سیستم‌های رایانه‌ای عمدتاً در ذخیره اطلاعات و پردازش محدود آنها خلاصه می‌شد و به تدریج از قابلیت‌های دیگری بهره مند شدند. به طور کلی، می‌توان این سیر تحول را در سه مرحله مورد بررسی قرارداد:

الف) دهه ۶۰ میلادی

این دهه که مقارن با پیدایش ابررایانه‌ها بود، سیستم‌های رایانه ای، محلی برای نگهداری و پردازش اطلاعات مشتریان بودند که البته به صورت خارج از خط[1] و از طریق رسانه‌هایی چون نوار و دیسکت با آن در تعامل بودند.

ب) دهه ۸۰ میلادی

این دهه که مقارن با پیدایش رایانه‌های کوچک بود، سیستم‌ها به صورت گسترده در ذخیره‌سازی داده‌ها، پشتیبانی و پردازش داده‌ها مورد استفاده قرار می‌گرفتند. اما هنوز مشکل اصلی، یعنی ارتباط با یکدیگر برای تبادل داده‌ها یا راه اندازی یک مرکز اصلی و امکان تعامل برخط[2] با آن وجود نداشت.

ج) دهه ۹۰ میلادی تا به امروز

که مقارن با ظهور شبکه‌های رایانه‌ای و ارتباط جهانی آنها با یکدیگر از طریق ارتباطات الکترونیکی است. به این ترتیب، علاوه بر نگهداری و پردازش حجم عظیم داده‌ها، به دلیل برقراری خطوط دسترسی پرسرعت، امکان ارائه انواع خدمات میسر گشت که ملاحظه کردیم از مهم ترین آنها امکان ذخیره سازی دوردست اطلاعات و همچنین ارائه انواع خدمات شبکه‌ای تحت وب است.

با توجه به مطالب گفته شده، تأسیسات عظیم شبکه‌های الکترونیکی را که در سطوح کلان به ارائه انواع خدمات شبکه‌ای می‌پردازند و مراکز داده نامیده می‌شوند را می‌توان چنین تعریف کرد:

«مرکز داده مکانی است:

---

[1] Offline
[2] Online

الف) با امنیت فیزیکی و الکترونیکی بالا، برخوردار از پهنای باند ارتباطی وسیع، متصل به شبکه‌های رایانه‌ای ملی و جهانی، با خدمات تمام وقت و در دسترس.

ب) دارای انواع تجهیزات سخت‌افزاری(رایانه‌ها، کلیدها، مودم‌ها، و مسیر یاب‌ها[1]...) و نرم‌افزاری (پایگاه داده، سرورها، سیستم عامل، و ...) پیشرفته که از پشتیبانی و نگهداری حرفه‌ای و تمام وقت برخوردار است.

ج) به پشتیبانی و ارائه انواع خدمات مرتبط با اطلاعات و داده‌ها از قبیل خدمات ذخیره، نگهداری و بازیابی داده‌ها، ERP، میزبانی خدمات اینترنتی (ISP)، میزبانی خدمات کاربردی (ASP)، میزبانی برون‌سپاری[2] خدمات و غیره برای کلیه اشخاص حقوقی و حقیقی دولتی و غیر دولتی می‌پردازد.»

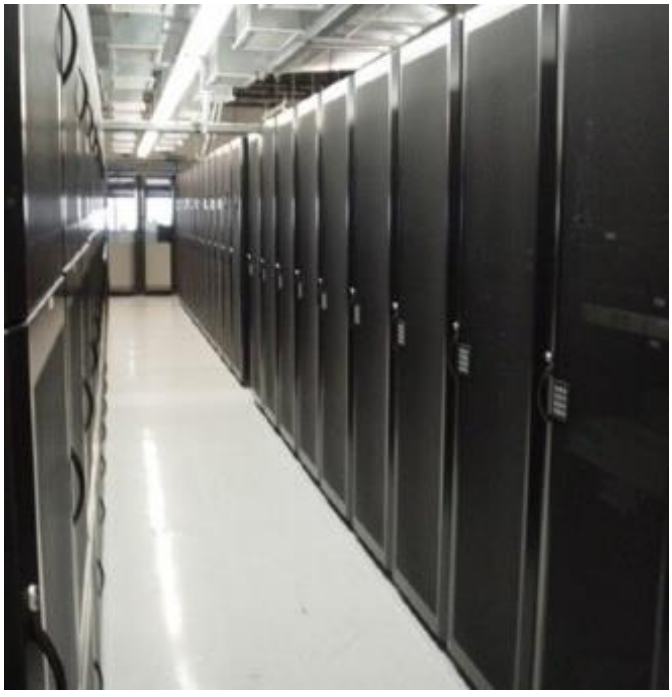
با عنایت به این تعریف در می‌یابیم مراکز داده مجموعه‌ای عظیم از سیستم‌های سخت‌افزاری و نرم‌افزاری هستند که در تأسیسات کاملاً مجهز و پیشرفته قرار دارند و در آنها تعداد زیادی پرسنل مجرب و متخصص در حوزه‌های متنوع مشغول به کارند. به طور کلی، عمده خدماتی که این مراکز می‌توانند ارائه دهند عبارتند از:

- خدمات عمومی مانند میزبانی وب، پروتکل انتقال فایل(FTP)، محیط گپ، خدمات نام دامنه (DNS)، پست الکترونیک، انباشت موقت[3]
- خدمات دسترسی باند پهن، مانند Ethernet، xDSL جهت دسترسی به مراکز داده از طریق شرکت‌های دارای مجوز PAP
- خدمات هم مکانی[4]

[1] Routers
[2] Outsourcing
[3] Caching
[4] Colocation

- خدمات دسترسی به مراکز داده از طریق شبکه‌های رایانه ای، مانند اینترنت
- خدمات شبکه خصوصی مجازی[1] در سطح برنامه کاربردی
- خدمات مدیریت شده مانند امنیت، مدیریت
- خدمات پشتیبانی مراکز داده (داده‌ها، نرم‌افزار و سخت‌افزار)
- خدمات کاربردی فن‌آوری اطلاعات (ASP)

بدیهی است این حجم از تجهیزات و تنوع خدمات از عهده یک یا چند سرور واقع در یک مکان غیر استاندارد بدون پرسنل فاقد تجربه و تخصص خارج است. شکل ۱ نمایی از یک مرکز داده است.



شکل ۱: نمایی از یک مرکز داده

[1] Virtual Private Network

۳-۲ مزایای مراکز داده

به صورت خلاصه مزایای استفاده از مراکز داده عبارتند از:

- امنیت فیزیکی بالا
- امنیت الکترونیکی بالا
- مقابله با افزونگی و تکرار اطلاعات
- ارائهٔ بالاترین سرعت پردازش در یک مکان
- ارائهٔ بالاترین سرعت انتقال اطلاعات
- خرید تنها یک نسخه از نرم‌افزارها
- پشتیبانی متمرکز

اگر از مراکز داده استفاده نشود و هر سازمانی بانک اطلاعاتی خود را در شبکه داشته باشد، به تعداد سازمانها نیاز به تیم پشتیبانی جداگانه، نرم‌افزار جداگانه، سخت‌افزار جداگانه، پهنای باند جداگانه، امنیت جداگانه و ... خواهیم داشت که سربار هزینه‌ای آن بالا خواهد بود.

به نظر می‌رسد ایدهٔ مرکز داده به دلیل تأمین کارایی و امنیت بالا و جلوگیری از افزونگی، سهولت نگهداری و مدیریت و بسیاری جنبه‌های فنی دیگر در تحقق اهدافی همچون دولت الکترونیکی، ایده‌ای کارساز باشد.

۲-۴ امنیت در مراکز داده

با توجه به این که مراکز داده محل نگهداری و پردازش انواع اطلاعات ارزشمند و بعضاً حساس و حیاتی هستند، باید از آنها در برابر انواع تهدیدها و بلایا محافظت کرد. چرا که در صورت بروز یک حادثه جزئی، ممکن است خسارات جبران ناپذیری، به ویژه به داده‌ها و اطلاعاتشان وارد آید، با توجه به اهمیت موضوع، بحث امنیت این مراکز از دو جهت مورد توجه قرار گرفته است: امنیت فیزیکی و امنیت دیجیتال که در ادامه به آنها خواهیم پرداخت.

۲-۵ امنیت فیزیکی

در این جا سعی می‌شود با بررسی کلیه جوانب از تحقق هرگونه تهدید فیزیکی یا آسیب های ناشی از بلایای طبیعی جلوگیری شود. لذا در سه مرحله تمهیدات امنیتی به اجرا در می آید:

الف) مرحله قبل از ایجاد مرکز داده (انتخاب محل مناسب)

ب) هنگام ایجاد مرکز داده (طراحی ایمن و پیش بینی کلیه شرایط)

ج) پس از ایجاد مرکز داده (مراقبت دائم) برای مثال، در خصوص انتخاب محل باید میزان خطر پذیری در برابر بلایای طبیعی مانند سیل، طوفان، ریزش کوه و زلزله، آسیب پذیری از آلودگی های خاک و هوا، میزان و نحوه رفت و آمد افراد به آن مکان و میزان و نحوه دسترسی آنها مورد توجه قرار گیرد.

تأمین برق نباید با هیچ مشکلی مواجه باشد و پرسنل امنیتی باید با برخورداری از آموزش‌های تخصصی لازم و همچنین امکانات مجهز به طور تمام وقت به مراقبت از مراکز مشغول باشند.

۶-۲ امنیت الکترونیکی

همان طور که اشاره شد، مراکز داده به عنوان مخازن بزرگ اطلاعات از طریق خطوط پر سرعت و مطمئن الکترونیکی با فضای سایبر ارتباط دارند و اغراق نیست اگر بگوییم این خطوط رگ حیات این مراکز محسوب می‌شوند. زیرا آن‌ها هستند که به این مراکز موجودیت بخشیده و امکان ارتباط آنها با دنیای خارج را فراهم می نمایند. با این حال نباید از یاد برد که این خطوط به اندازه اهمیتشان خطر ساز نیز هستند. شایان ذکر است، عمده تهدیدات علیه مرکز داده به شکل الکترونیکی و در قالب تعرضات الکترونیکی هستند و به ندرت اتفاق می افتد تعرض فیزیکی صورت گیرد. زیرا همان طور که بارها تأکید شده، ارزش واقعی این مراکز به اطلاعات ذخیره شدشان است. لذا قاعدتاً باید هدف از تهاجم به آنها نیز لطمه به اطلاعات باشد. حال وقتی می توان از دوردست ترین نقاط این کره خاکی و در آرامش خاطر این مراکز را مورد تهدید جدی قرار داد، دنبال کردن تهدیدات فیزیکی عاقلانه به نظر نمی رسد.

به این ترتیب به دلیل وجود این حساسیتها تمهیدات امنیتی الکترونیکی نیز بسیار جدی گرفته شده و حتی نسبت به تمهیدات فیزیکی نیز از تنوع و همچنین روز آمدی بسیار بیشتری برخوردارند. زیرا فن‌آوری اطلاعات و ارتباطات به طور مستمر در حال تحول و پیشرفت است و متعرضین الکترونیکی همواره به جدیدترین ابزارهای تهاجم الکترونیکی خود را مجهز می‌کنند.

در هر حال برخی مکانیزم‌های اصلی که در این راستا انجام می شود عبارتند از:

- نصب فایروال‌های سخت افزاری و نرم افزاری
- نصب سیستم های تشخیص نفوذ (IDS)
- نصب سیستم‌های شناسایی، تعیین اعتبار و حسابرسی (AAA)
- نصب سیستم های پشتیبان اطلاعات

- نصب سیستم ترمیم خرابی[1]

۲-۷ مراجع

[1]. “Internet Data Center”, http://idc.nic.in/ , [۸۶/۵/۱۷]

[2]. “Data Center & Networks”,
http://www.idcworks.com.my/data_centre_networks.htm , [۸۶/۵/۲۰]

[3]. “MyLoca Data Center”,
http://www.exabytes.com.my/about/datacenters/myloca.html , [۸۶/۵/۲۰]

[1] Disaster Recovery System

۳ فصل سوم: تاریخچه مراکز داده

فصل سوم:

تاریخچه مراکز داده

در این فصل به طور خلاصه به کارهای انجام شده درباره مراکز داده در سایر کشورها پرداخته می شود.

۳-۱ مراکز داده در آمریکا

کشور آمریکا به علت پیشرو بودن در فن‌آوری اطلاعات، و نیز به سبب حاکمیت بر بستر اصلی اینترنت، از نخستین کشورهای دارای مرکز داده بوده و در حال حاضر نیز بیشترین و بزرگترین مراکز داده در این کشور قرار دارد.

دولت امریکا به منظور ارتقای ضریب ایمنی مراکز اطلاعاتی خود بانک‌های اطلاعاتی و کارگزاران شبکه خود را در مکانهای با ضریب امنیتی بالا نگهداری می‌کند. بعضی از این اماکن محوطه‌های وسیعی در اعماق کوههای راکی، در نقاط پنهانی از اعماق صحراهای نوادا وآریزونا، در زیر یخچال‌های آلاسکا و در اعماق اقیانوس‌ها می‌باشند.

این نقاط با شدیدترین تدابیر امنیتی حفاظت می‌شوند. از طرف دیگر پیش‌بینی‌های ایمنی تهدیدات فیزیکی، از جمله آتش سوزی و بلایای طبیعی را به حداقل رسانده است. تجهیزات حفاظتی، امکان دستبرد و یا آسیب هوشمندانه فیزیکی را کاهش داده است. در این اماکن خطوط متعدد فیبرنوری با پهنای باند بالا بالاترین سرعت انتقال داده و اطلاعات را تأمین می‌کنند. تجهیزات پرسرعت مانند سوپر کامپیوترها (Main Frame) و پردازنده‌های بسیار سریع و موازی بالاترین سرعت دسترسی را در اختیار می‌گذارند. سیستم‌های پیشرفتهٔ تنظیم دما و حرارت، تنظیم رطوبت و کنترل ترکیبات هوای محیط بهینه‌ترین شرایط را برای کار تجهیزات مهیا می‌سازند و تجهیزات مانیتورینگ دقیق، لحظه به لحظه وضعیت‌های مختلف را کنترل و بازنگری می‌کنند. بناهای مستحکم در اعماق زمین نه تنها توان تحمل شدیدترین زلزله‌ها را دارند، بلکه در مقابل قویترین بمب‌های هسته‌ای موجود آسیبی نمی‌بینند. سیستم‌های پشتیبان، از اطلاعات در فواصل زمانی

مشخص بر طبق آخرین تکنیک‌های موجود نسخه‌های پشتیبان تهیه می‌کنند. ژنراتورها و مولدهای پشتیبان برق[1]، آمادهٔ تأمین نیروی برق لازم در صورت بروز اختلال می‌باشند و پوشش‌های مخصوص، تجهیزات را از تهدید امواج مختلف از قبیل امواج ماکروویو و یا میدانهای الکترومغناطیسی خارجی یا تولید شده از خود تجهیزات محافظت می‌کنند.

قسمت هواشناسی نیروی هوایی و نیروی دریایی در نیواورلئان و لس آنجلس در نوامبر ۱۹۵۱ در هم ادغام شدند و مرکز جدیدی در آشویل[2] به نام مرکز ملی مدارک هوایی[3] (NWRC) به وجود آمد. فعالیت این مرکز در ابتدا به صورت پراکنده بود. با قدرتمندتر شدن کامپیوترها کنترل کیفیت، جمع آوری و انتشار اطلاعات هواشناسی با هزینه کمتر در یک مکان واحد، مقرون به صرفه و ممکن گردید. در ژوئن ۱۹۷۰ NWRC به مرکز ملی آب و هوا[4] (NCC) تغییر نام داد تا عنوان کاری آن بهتر بتواند فعالیتهای این اداره را نشان دهد. دو سال بعد این مرکز شروع به جمع آوری داده‌ها از ماهواره‌های هواشناسی کرد و سرویس‌دهی رسمی آن آغاز شد.

پس از چند سال، اداره ثبت و بایگانی ملی این کشور، مرکز داده ملی آب و هوا[5] را به عنوان آژانس مرکزی ثبت آب و هوا طراحی کرد و بالاخره در سال ۱۹۸۴، NCC به NCDC تغییر نام داد. نام این مرکز دقیقاً مبین نقش آن بود (یعنی مرکز داده‌های آب و هوای ملی). داده‌های NCDC توسط جاهای دیگری مثل سرویس هواشناسی امریکا، سرویس نظامی، اداره هوانوردی ملی و گارد ساحلی و همچنین افراد داوطلبی که به صورت تحقیقاتی روی آب و هوا کار می‌کنند فراهم می‌شود. NCDC همچنین مقداری از داده‌های خود را از جاهای دیگری مثل ASOS و NEXRAD تأمین می‌کند.

---

[1] UPS
[2] Asheville
[3] National Weather Records Center
[4] National Climate Center
[5] National Climate Data Center

جمع‌آوری و پردازش این همه داده در زمانی معقول، کاری است که NCDC اکنون انجام می‌دهد. NCDC اکنون داده‌هایش را از تمام جهان می‌گیرد. این مرکز اکنون از بیش از ۱۵۰ سال گذشته داده در دست دارد و هم اکنون ۲۲۴ گیگابایت اطلاعات جدید هرروز دریافت می‌کند. NCDC اکنون ۳۲۰ میلیون صفحه اطلاعات کتبی، ۲/۵ میلیون میکروفیش،۱/۲ پتا بایت [1] اطلاعات دیجیتالی وعکسهای ماهواره ای از سال ۱۹۶۰ تاکنون از کره زمین را در یک محیط ذخیره‌سازی عظیم نگهداری می‌کند. همچنین NCDC ۲/۱ میلیون کپی اطلاعات آب و هوایی را نیز برای مشترکان و ۳۳۰۰۰ کاربر خود ارسال می‌کند. NCDC همچنین ۵۰۰ مجموعه دیجیتالی دارد که حدود ۲ میلیون درخواست در سال دارند و ۱۰۰ میلیون بازدید کننده در سال از وب سایتش بازدید می‌کند. NCDC همچنین با موسساتی مثل ICSU [2] و مرکز داده جهانی [3] همکاری دارد.

۲-۳ بررسی وضعیت مراکز داده در هند

در ادامه بررسی وضعیت مراکز داده در کشورها در این بخش به بررسی وضعیت کشور هند می پردازیم.

دولت هند در جهت ارائه خدمات دولتی به صورت مجتمع و با هزینه ای مناسب به شهروندانش، طرح دولت الکترونیکی ملی [4] را تهیه نموده است. این طرح شامل ۲۶ پروژه کلان مرکزی، ایالتی و مجتمع همراه با ۸ مولفه پشتیبانی برای مقدمه سازی ایجاد دولت الکـــترونیکی در هند می باشد. در طرح دولت الکترونیکی ملی هند جهت ارائه خدمات به صورت تحت وب و همچنین دسترسی به اطلاعات به صورت هر زمان و از هر کجا، از ۳ مؤلفه اصلی استفاده شده است، که شامل موارد زیر می باشد:

---

[1] براي تصور اين عدد يک ۱۰ با ۱۵ تا صفر جلوي آن در نظر بگيريد.
[2] International Council for Science Union
[3] World Data Center
[4] National E-Government Plan

الف) اتصال: شبکه های گسترده ایالتی (SWAN[1]) و شبکه سراسری NICNET[2]

ب) بانک داده ملی و مراکز داده ایالتی (SDCs[3])

ج) مراکز خدمات عمومی (CSC[4])

در ادامه هر یک از سه مورد شرح داده می‌شود.

۳-۲-۱ اتصال شبکه های گسترده ایالتی SWAN و شبکه سراسری NICNET

مرکز انفورماتیک ملی هند[5] از حوزه تکنولوژی اطلاعات، ارائه دهنده ستون فقرات شبکه و پشتیبان دولت الکترونیکی به دولت مرکزی، ایالتها، بخشها و سایر بدنه های دولت می باشد. این بخش عرضه کننده محدوده وسیعی از خدمات ICT از جمله شبکه ارتباطی سراسری می باشد که بهبود برنامه ریزیهای محلی در ارائه خدمات دولتی و شفافیت وسیعتر دولتهای محلی و ملی را باعث می شود. NIC کمک می‌کند که در اجرای پروژه‌های اطلاعات، همکاری نزدیکی بین دولت مرکزی و دولتهای محلی ایجاد شود. NICNET یک شبکه ICT سراسری است که در حوزه های دولت مرکزی و ۳۵ ایالت و ۶۰۲ بخش محلی جهت ارائه خدمات استفاده می شود.

۳-۲-۲ بانک داده ملی و مراکز داده ایالتی (SDC)

دولت هند در مورد مراکز داده عنوان کرده است که از آنجا که فرآیندهای کسب و کار و خدمات شهروندان به طور روز افزونی بر روی شبکه انجام می شود، نیاز به حفاظت از داده ها همراه با

---

[1] State Wide Area Networks

[2] Nationwide ICT Network
[3] State Data Centers
[4] Common Services Centers
[5] National Informatics Center

پشتیبانی کارآمد و وجود راه حلهای بازیابی اطلاعات بیشتر احساس می گردد و لذا تهیه یک زیر ساخت که بر پایه اصول زیر باشد، احساس می شود:

- دسترسی بالا
- قابلیت اندازه گیری سریع
- مدیریت موثر و بهره برداری مفید از منابع

جهت برآورده کردن نیازهای فوق، در NIC طرح مراکز داده اینترنت در NICHQ، دهلی نو و ۳۰ مرکز داده کوچک در ایالتهای مختلف تهیه شده است که خدمات مورد نیاز را به موجودیتهای دولت برساند.

مراکز داده اینترنت NIC متشکل از مدیریت سیستمها به صورت شبانه روزی باشد که پرسنلی که در حوزه های مختلف قرار گرفته‌اند شامل راهبران سرورها و بانکهای اطلاعاتی اینترنت و مدیریت سیستمها می‌باشند که نتیجه آن یک محیط فنی و فیزیکی است که باعث پشتیبانی قابل انعطاف و قابل اطمینان نیازهای کاربران در رابطه با سیستم های مهم یا برنامه های کاربردی خواهد شد.

مرکز داده اصلی در دهلی قراردارد که طرح آن طوری تهیه شده که ظرفیت نگهداری بیش از ۱۰۰۰ سرور و پشتیبان سطح گسترده ای از تکنولوژیها را داشته باشد. تنوع گسترده سرورها در مرکز داده باعث می شود که محدوده وسیعی از سرویس‌های پایه‌ای و مهم اینترنت به سازمانها و حوزه های دولت در سطوح مختلف از دولت مرکزی تا ایالتها ارائه گردد. نکات مهم در رابطه با این مرکز داده شامل موارد زیر است:

- شبکه حوزه ذخیره سازی[1] که شامل تقریباً ۴۰۰ سرور موجود با امکان بیش از 110 TB فضای ذخیره سازی می باشد.

[1] Storage Area Network

- زیر ساخت مبتنی بر راک
- تهیه نسخه پشتیبان و بازگردانی نسخه پشتیبان به صورت خودکار
- طرح امنیت
- شبکه فیبرنوری

اجزاء مختلف مرکز داده شامل موارد زیر است :

- استفاده از نرم افزار و سخت افزار به صورت مجتمع
- پایش (مانیتورینگ) دائم مراکز داده خدمات و سرورهای مشتریها
- مرکز داده امن از نظر فیزیکی
- اتصال به اینترنت با سرعت خیلی زیاد
- استفاده از UPS و مولد برق دیزلی پشتیبان
- سیستم تهویه هوای صنعتی قولی
- Raised Access Floor
- تجهیزات آتش نشانی
- سیستمهای تشخیص نفوذ و دیواره آتش امن
- پشتیبانی از تقسیم‌کننده بار سرور

سرویسهای که در NIC ارائه می شود شامل موارد زیر می باشد:

- سرویسهای در محل شرکت CO-location Services : که زیر ساخت کامل شامل راک،

اتصال شبکه، اتصالات فیبری، سیستمهای UPS، امنیت فیزیکی و شبکه و امکان مانیتورینگ ارائه می شود.

- خدمات میزبانی وب (Web Hosting): خدمات میزبانی وب به وزارتخانه‌ها، حوزه‌ها، سازمان‌ها و موسسات دولتی ارائه می گردد که بیش از ۳۵۰۰ وب سایت و پورتال میزبانی می‌شود. در این خدمات امکان میزبانی وب، برنامه های کاربردی و بانک اطلاعاتی به صورت میزبانی مشترک و اختصاصی وجود دارد.
- میزبانی بانک اطلاعاتی: خدمات میزبانی بانکهای اطلاعاتی اوراکل MS SQL Server و MYSQL ارائه می گردد.
- خدمات ذخیره سازی : ظرفیت فعلی ذخیره سازی 60 TB می باشد که بر روی یک RAID 5 جهت حفاظت داده ها در سطح ذخیره سازی پیکربندی شده است.
- خدمات تهیه نسخه پشتیبان : امکان تهیه نسخه های پشتیبان متنوع به طور خودکار وجود دارد.
- خدمات پخش از طریق وب[1]

۳-۲-۳ مراکز خدمات عمومی

اما طرح CSC از طرف دولت هند جهت ارائه خدمات شخصی و اجتماعی دولت به متقاضیان در هر جای کشور از جمله روستاها تهیه شده است. هدف از این طرح توسعه یک محیط است که دولت را قادر سازد خدمات شخصی و اجتماعی مورد نیاز همه اقشار جامعه را در دورترین نقاط کشور به طور مبتنی بر IT مانند سرویسهای غیر IT ارائه نماید.

[1] Web Casting

۳-۲-۴ جمع بندی

دولت هند جهت ارائه خدمات خود به شهروندانش زیرساختی متشکل از شبکه های گسترده ایالتی و یک شبکه سراسری جهت ارتباطات، بانک داده ملی و مراکز داده ایالتی و ایجاد مراکز خدمات عمومی را برنامه ریزی نموده است. از طرفی با توجه به موقعیت و بازار مناسب کشور هند در منطقه شرکتهای مهم را به سرمایه گذاری در زمینه راه اندازی مراکز داده در این کشور ترغیب نموده است که از آن جمله می توان به شرکت گوگل اشاره نمود. شرکت گوگل جهت راه اندازی یک مرکز داده در هند پروژه‌ای یک میلیارد دلاری را در نظر گرفته است.

۳-۳ بررسی وضعیت مراکز داده در مالزی

در مالزی شرکتهای خصوصی زیادی مانند IDC works, exabytes در زمینه ارائه خدمات مراکز داده فعالیت می کنند اما در رابطه با سیاست‌گذاری و استراتژی دولت مالزی در زمینه مراکز داده و وضعیت مراکز داده دولتی در مالزی، علی رقم جستجوهای بسیار، مستندات خاصی یافت نشد.

۳-۴ بررسی وضعیت مراکز داده در انگلستان

کشور انگلستان از جمله کشورهای محسوب می شود که از قدمت طولانی در راه اندازی و بکارگیری مراکز داده برای کاربردهای مختلف از هواشناسی گرفته تا انجام پردازش های پیچیده نجومی برخوردار است.

از جمله مراکز داده که به منظور انجام مطالعات بر روی وضعیت اتمسفر و شرایط جوی راه اندازی و در حال حاضر نیز مورد استفاده قرار می گیرد می توان به BADC یا British Atmospheric Data Center

اشاره نمود. این مرکز داده با ایجاد تمرکز در داده های جوی، امکان دسترسی و تفسیر آسان داده ها را برای محققین فراهم می آورد.

یکی دیگر از حوزه‌های کاربردی جالب برای مراکز داده در انگلستان و سایر کشورهای اروپایی مدرن و پیشرفته نگهداری اطلاعات پزشکی مردم کشور انگلستان می باشد. این اطلاعات شامل تصاویر مختلف رادیولوژی، سی‌تی‌اسکن، نوارهای قلب، مراجعات مختلف مردم به پزشکان و تجویزات صورت گرفته از سوی مراکز درمانی می باشد. این مراکز بر خلاف سایر مراکز که از حجم پردازشی به مراتب بالاتری برخوردار می باشند عمدتاً برای اهداف ذخیره سازی و ایجاد تمرکز در اطلاعات پزشکی افراد مورد استفاده قرار می گیرد. نباید غافل از این موضوع هم شد که نسخه‌هایی از این مراکز داده برای انجام پردازش‌های نسبتاً پیچیده از قبیل نحوه تعامل افراد با مراکز خدمات درمانی، فرآیندهای مختلف درباره کیفیت خدمات درمانی ارائه شده و میزان رضایتمندی مردم از این مراکز مورد استفاده قرار می‌گیرند. از جمله مراکز داده که برای این منظور در این کشور مورد استفاده قرار گرفته است می توان به IMPAX اشاره نمود که از جمله قابلیت ها و امکانات آن می توان به موارد زیر اشاره نمود:

- ذخیره سازی متمرکز داده های مربوط به سیستم های نامتجانس
- نگهداری اطلاعات مربوط به تصاویر پزشکی افراد
- امکان دسترسی پیوسته و یکجا به کلیه سوابق پزشکی، تصاویر پزشکی بیمار توسط متخصص

این مرکز داده استراتژی‌های مختلفی را برای ذخیره سازی اطلاعات و داده ها پشتیبانی می کند که از آن جمله می توان به TSM، GMAS، NAS، SAN و .... اشاره نمود.

۵-۳ بررسی وضعیت مرکز داده در آلمان

این کشور نیز با راه اندازی مراکز مختلف داده سعی در به خدمت گرفتن قابلیت های مراکز داده در کاربردهای مختلف بخصوص در حوزه پردازش بوده است. مراکز پردازش با بهره وری بالا که نام دیگر این مراکز داده محسوب می گردد برای طیف گسترده ای از کاربردها مورد استفاده قرار می گیرد. از جمله کاربردهای متصور برای این مراکز پردازش، ثبت وقایع مربوط به ایستگاه های زلزله نگاری توسط این مراکز و انجام پردازش های پیچیده به منظور بررسی و پیش بینی احتمال وقوع زمین لرزه در آینده نزدیک است. لازمه تحقق این مهم، برخورداری از داده های ثبت شده در گذشته و انجام پردازش بر روی مجموعه داده است.

به عنوان مثال مرکز تحلیل داده زلزله نگار، مرکز داده ای در آلمان است که توسط موسسه فدرال منابع طبیعی و زمین شناسی که برای انجام مطالعات زمین شناسی آلمان تأسیس شده، راه اندازی و در حال حاضر مورد استفاده قرار می گیرد.

داده های تهیه شده و ثبت شده توسط این مرکز داده ضمن پردازش توسط این مرکز داده مورد استفاده سایر آژانس های مطالعاتی نیز قرار می گیرد که از آن جمله می توان به آژانس های زیر اشاره نمود:

- German Catalogue
- United States Geological Survey
- International Seismological Center
- Significant Earthquake

در ادامه لیست نسبتاً جامعی از مراکز داده مهم در سطح بین الملل معرفی می گردد که می توان با مراجعه به وبگاه های این مراکز داده نسبت آنان اطلاعات جامعتری پیدا نمود.

Atmospheric Trace Gases	**Astronomy**	**Airglow**
Earth Tides	**Cosmic Rays**	**Aurora**
Glaciology	**Geomagnetism**	**Geology**

Land Cover Data	Ionosphere	Human Interactions in the Environment

۶-۳ مراجع

[1]. “Internet Data Center”, http://idc.nic.in/ , [۸۶/۵/۱۷]

[2]. “Data Center & Networks”,
http://www.idcworks.com.my/data_centre_networks.htm , [۸۶/۵/۲۰]

[3]. “MyLoca Data Center”,
http://www.exabytes.com.my/about/datacenters/myloca.html , [۸۶/۵/۲۰]

[4]. “British Atmospheric Data Center”,
http://badc.nerc.ac.uk , [۸۷/۰۴/۰۵]

[5].”United Kingdam Earthquake Data Center”,
http://www.smartbunker.com , [۸۷/۰۴/۰۵]

[6].National Geophysical Data Center,
http://www.ngdc.noaa.gov , [۸۷/۰۴/۰۵]

[7]. Word Data Center System Roster,
http://www.ngdc.noaa.gov/wdc/list.shtml , [۸۷/۰۴/۰۵]

۴ فصل چهارم: وضعیت مراکز داده در ایران

فصل چهارم:

وضعیت مراکز داده

در ایران

در این فصل به بررسی وضعیت مراکز داده در ایران پرداخته شده است. در ابتدا به سیاست‌گذاری‌های انجام شده پرداخته شده و سپس به مشکلات موجود و جایگاه ایران در غیاب مرکز داده ملی پرداخته می‌شود. در ادامه به اقدامات عملی انجام شده (یا ادعا شده) در این باره پرداخته می‌شود.

۴-۱ سیاست‌گذاریهای انجام شده در کشور

چنانچه مشخص است مراکز داده به دلیل ساختار و ماهیتی که دارند زیر بنای اصلی فن‌آوری اطلاعات و ارتباطات نوین هستند، لذا هر کشوری که می‌خواهد در این عرصه فعال باشد و نقش تعیین کننده ای داشته باشد می‌بایست برنامه منسجمی در خصوص رفع نیازمندی نسبت به این مراکز تدوین نماید.

در این راستا و بر مبنای سرفصل های مندرج در سند چشم انداز بیست ساله، ایران کشوری دست یافته به جایگاه اول اقتصادی در منطقه آسیای جنوب غربی در نظر گرفته شده و با تاکید بر جنبش نرم افزاری و تولید علم ، رشد پر شتاب و مستمر اقتصادی به همراه ارتقاء درآمد سرانه از اهداف مهم می‌باشد.

لذا قانون برنامه چهارم توسعه اقتصادی ، اجتماعی و فرهنگی کشور به عنوان اولین قانون برنامه پنج ساله اول چشم انداز ۲۰ ساله ، از ابعاد مختلف بر کاربرد فن‌آوری اطلاعات و لزوم تأمین زیر ساخت ها و امکانات مناسب برای آن تاکید کرده است .

در بند ب از ماده ۴۴ سند مذکور دولت مکلف شده تا با اتخاذ تدابیر لازم به منظور کسب سهم مناسب از بازار اطلاعات و ارتباطات بین المللی ، استفاده از فرصت منطقه ای ارتباطی ایران از طریق توسعه مراکز اطلاعات اینترنت ملی و توسعه زیر ساخت های ارتباطی با تکیه بر منابع و توان بخش های خصوصی وتعاونی و جلب مشارکت بین المللی ، اقدام نماید.

برخی اقدامات انجام شده در کشور به شرح ذیل می‌باشند :

- سال ۱۳۸۱ : ضوابط صدور مجوز ایجاد مجتمع خدمات اینترنت IDC به بخش خصوصی، که

این اقدام شامل تعریف ، مقررات مربوط به واگذاری مجوز مجتمع خدمات اینترنتی و مدارک لازم جهت ایجاد مجتمع خدمات اینترنت به بخش خصوصی می‌باشد

- سال ۱۳۸۳: دبیرخانه شورای عالی اطلاع‌رسانی با همکاری پارک فن‌آوری پردیس همایش نقش مراکز داده در توسعه فن‌آوری اطلاعات و ارتباطات را در دی ماه در تهران برگزار کرد که در پایان همایش، سند راهبردی مراکز داده کشور و همچنین آیین نامه مرکز خدمات داده اینترنتی نیز منتشر شده که خود گویای یک اقدام جدی در این حوزه بوده است.

- سال ۱۳۸۴ : اعطای مجوز تاسیس و راه اندازی مرکز داده به سه شرکت خصوصی: داده پردازی ایران ، کنسرسیوم فن آوا – پتسا و پارس آنلاین

- سال ۱۳۸۵ : در شهریور ماه این سال همایش چشم انداز مراکز داده در ایران در مرکز تحقیقات مخابرات برگزار گردید.

- سال ۱۳۸۶: برگزاری همایش بررسی فن‌آوری‌ها و روش‌های طراحی مراکز داده نوین و سایت‌های پشتیبان در سالن تلاش وزارت کار با محوریت ارائه خدمات الکترونیکی ارزش افزا، تحقق ملموس دولت الکترونیک

- سال ۱۳۸۶: مصوبه اردیبهشت‌ماه هیأت دولت مبنی بر تخصیص پنج هزار و ششصد و شصت میلیارد ریال از سوی شرکت مخابرات ایران جهت ایجاد شبکه اینترنت ملی به عنوان پیش زمینه جهت راه‌اندازی مرکز داده ملی

- سال ۱۳۸۶: برگزاری مناقصه بین شبکه علمی فاز تهران و مترو اترنت کرمان و قم به ترتیب با اعتباری حدود ۴۰ میلیارد ریال و ۱۳۵ میلیارد ریال به عنوان بخشی از پروژه شبکه ملی

- بهمن ماه ۱۳۸۶: برگزاری همایش روابط عمومی الکترونیک در حوزه مدیریت کلان ICT و مدیریت و راهبری مراکز داده

- سال ۱۳۸۶: اختصاص ۳۰۰ میلیارد ریال اعتبار از سوی وزارت ICT در فاز اول و طرح شبکه ملی دیتا به مبلغ ۳۵۰ میلیارد تومان که مقرر گردید که شرکت فن‌آوری اطلاعات به عنوان مجری طرح آنرا اجرا نماید که بعدها بنا به ایجاد تغییرات در وظایف این شرک، مجری طرح شرکت ارتباطات زیرساخت اعلام گردید.

- بهار ۱۳۸۷: مکلف شدن بانک مرکزی برای راه‌اندازی مرکز داده‌ای جهت نگهداری داده‌های تراکنش بانکی مشتریان و عملکرد کلیه پایانه‌های بانک

- خردادماه ۱۳۸۷: نشست تخصصی مرکز تحقیقات استراتژیک مجمع تشخیص مصلحت نظام با اساتید و کارشناسان دانشگاه با عنوان زیرساخت‌های فن آوری اطلاعات. در این نشست جایگاه فن آوری اطلاعات در کشور به عنوان یکی از فن آوری‌های نوین مورد تأکید سند چشم‌انداز ۲۰ ساله ایران و اقدامات انجام شده در این راستا توسط نهادهای ذی‌ربط برای توسعه نقش فن آوری اطلاعات در ابعاد مختلف اجتماعی و اقتصادی ایران، مقایسه ایران در این حوزه با سایر کشورهای حوزه آسیایی جنوب غربی، و چالش‌های پیش رو مورد بررسی قرار گرفت.

- خردادماه ۱۳۸۷: راه‌اندازی آزمایشی مرکز داده مرکز تحقیقات مخابرات

- آبان ماه ۱۳۸۷: برگزاری همایش مدیریت فن آوری اطلاعات و ارتباطات با محوریت مدیریت سرویس‌های یکپارچه در شبکه های نسل آینده در هتل المپیک تهران

۲-۴ مشکلات عمده ایجاد مرکز داده در حال حاضر

با بررسیهای انجام شده در مورد فعالیتهای انجام شده و بر مبنای استعلام نظر از مسئولین سه شرکت دارای مجوز ایجاد مراکز داده در کشور، مشکلات ایجاد مراکز داده در کشور را می‌توان به طور کلی و به شرح ذیل بیان نمود.

- **پهنای باند**: در حال حاضر مجموع پهنای باند موجود در کشور حتی به یک گیگا بایت هم نمی رسد. البته پیش از نوروز اخباری مبنی بر افزایش پهنای باند کشور به دوگیگابایت اعلام شد اما مجموع این رقم بازهم برای مراکز داده که می‌خواهند به میزبانان هزاران وب‌سایت و وب سرویس ریز و درشت ایرانی و هاب منطقه تبدیل شوند بسیار ناچیز است!
- **زیرساخت** : برای راه اندازی سرورهای استانی و ASPها به یک زیرساخت مخابراتی و ارتباطی قوی و ایمن به همراه زیرساخت ذخیره (برای استفاده در مواقع خاص) نیاز هست. باید دید آیا شبکه زیرساخت مخابراتی کشور بخصوص در بخش فیبر نوری توان جوابگویی به این هاب های استانی و منطقه ای و برقراری ارتباط بی دردسر بین سرورها را دارد یا نه ؟!
- **هزینه ها**: جز هزینه نصب و راه اندازی ، دیتاسنترها هزینه های از قبیل هزینه پهنای باند،هزینه نگهداری سرور، هزینه نیروهای متخصص و پشتیبانی شبانه روزی، هزینه نجومی برق و سوخت (برای تأمین انرژیه الکتریکی در مواقع قطع شبکه سراسری برق) و دها هزینه پنهان و آشکار دیگر را در بر دارند. باید دید آیا مدیران مراکز داده داخل کشور می‌توانند از پس هزینه های اینچنینی برآیند و به سودآوری برسند یا خیر.
- **موازی کاری** : سه شرکت خصوصی که مجوز راه اندازی مرکز داده در ایران را دریافت کردند مشکل دیگری هم پیش روی خود دارند و آن رقابت با دولت است : طبق تصمیم وزارت

ICT نصب و راه اندازی مرکز داده در ایران طبق مناقصه ای به سه شرکت "خصوصی" واگذار شد اما بخش دیگری از حاکمیت یعنی سازمان تبلیغات اسلامی (موسسه تبیان) و سازمان ثبت احوال کشور بدون توجه به تصمیم وزارت ICT و مستقلاً اقدام به برگزاری مناقصه راه اندازی IDC کرده اند که این تضاد و موازی کاری به هر صورت برای بخش خصوصی خطرناک است.

- **جذب مشتری**: جذب مشتری و قانع کردنش به مهاجرت از سرورهای فوق پرسرعت خارجی به مراکز داده ایرانی بزرگترین مشکل مدیران سرورهای داخلی بعد از فائق آمدن بر موانع بالاست!

- **امنیت شغلی** : امنیت کاری شرکتهای فعال در این حوزه اهمیت زیادی دارد. متاسفانه در ایران همه خود را متولی IT می دانند و به راحتی به خود اجازه دخالت در هر کاری را می دهد. کانالهایی بدون محدودیت قانونی همچون شرکتهای بزرگ مخابراتی و تجاری همواره برای سرویس دهندگان این دل نگرانی را در پی خواهد داشت که ممکن است یک شبه در راه فعالیتشان سنگ بزرگی انداخته شود و صبح فردایی همه کسب و کار و سرمایه شان به باد رفته باشد!

- **امنیت** : موضوع امنیت در IDCها از اهمیت و جایگاه ویژه ای برخوردار است اما متأسفانه در ایران بحث امنیت در حوزه فن‌آوری اطلاعات جدی گرفته نمی‌شود که در صورت ادامه این روند آسیب پذیری امنیتی مراکز داده ایرانی می‌تواند مشکلات و بحران‌های جدی و کمرشکنی را برایشان به ارمغان بیاورد تا جایی که این فن‌آوری در نطفه خفه شود. موضوع امنیت فن‌آوری اطلاعات و مدیریت امنیت سیستم های رایانه ای در ایران موضوع نسبتاً تازه ایست اما کم نیستند

نفوذگران ایرانی و خارجیی که از حالا برای راه اندازی IDCهای ایرانی لحظه شماری میکنند تا با نفوذ و اخلال در آنها به شهرت یا اطلاعات موردنظر برسند.

۳-۴ جایگاه کنونی ایران در غیاب مرکز داده ملی

در این بخش از گزارش ابتدا اشاره‌ای به اوضاع فعلی و فعالیتهای انجام شده در این حوزه خواهیم داشت و در بخش بعدی شرکت های فن‌آور و سپس سازمانها و ارگانهایی که بر اساس اخبار و اطلاعات موجود، بحث ایجاد مراکز داده در آنها مطرح و فعالیتهایی آغاز شده معرفی و گوشه‌ای از فعالیتهای صورت‌گرفته ارائه می‌شوند.

وضعیت حال حاضر داده‌های الکترونیکی در کشور به گونه‌ای است که لحظه به لحظه بر حجم آن افزوده می‌شود و هنوز هم اقدام اساسی در مورد ساماندهی آنها صورت نگرفته به طوریکه برون سپاری فرامرزی که از طریق تعداد زیادی از سازمانها انجام شده وضعیت خطرناک امنیتی را نشان می‌دهد.

البته بسیاری از نهادها و ارگانها چنین بیان می‌کنند که عمده خدمات مرتبط به خوبی در کشور ارائه نمی شوند لذا خود را ناگزیر از استفاده میزبانی در خارج از کشور می‌دانند که در این خصوص باید مسایل امنینی مربوطه که پیرو این میزبانی ها می‌باشد مورد توجه قرار گیرند .

با عنایت به مواردی که شرح داده شد و عدم ارائه خدمات مرتبط که به طور صد در صد مطلوب در کشور انجام نمی شود ، در حال حاضر بسیاری از سازمانها از خدمات میزبانی در داخل کشور استفاده می‌کنند که اهمیت کاری آنها در رده های بالایی قرار دارد .

لذا ضروری است که تمهیدات مناسبی اندیشیده شود تا بتوان امکانات لازم را برای سرویس دهی تهیه نمود و در اختیار سازمانها قرار داد .

۴-۴ اقدامات انجام شده در ایران

اقدامات انجام شده در کشور در راستای راه اندازی مرکز داده را می‌توان از دو جنبه کلی مورد بررسی و مطالعه قرار داد که از یک بعد به فعالیت شرکت های فن‌آور و مجری و از سوی دیگر به درخواست ها و فعالیتهای سازمانها و ارگانهای متقاضی می‌توان اشاره نمود که برخی از آنها عبارتند از :

۴-۵ شرکت داده پردازی ایران

در حال حاضر این شرکت اعلام داشته است که امکانات فیبرنوری، ارتباطات کابل‌های مخابرات، خطوط E1 آماده شده و امنیت فیزیکی و امنیت اطلاعات به‌روزرسانی شده است. همچنین سرویس‌های میزبانی وب، ایمیل، سرور اختصاصی و تخصیص فضای دیتا نیز ارایه می‌شود. ۷۰ درصد میزبانی سایت‌های این شرکت مربوط به سایت‌های غیرخصوصی است و بیش از هزار ایمیل نیز میزبانی می‌شود که از گذشته وجود داشته اما اکنون به مرکز جدید در حال انتقال است. در حال حاضر سقف ارایه سرویس داده‌پردازی ۴۰۰ سرویس اختصاصی، چهار هزار میزبانی و ۴۰ هزار پست الکترونیکی است.

بررسی کلی این طرح نشان داد که شرکت مذکور جنبه های مختلف امنیتی را در نظر گرفته و در بخش زیر ساخت به امنیت اطلاعات و سطوح دسترسی توجه داشته است. ضمناً این شرکت مجوز مربوط به ایجاد مرکز داده را از وزارت ICT دریافت نموده است.

۴-۶ کنسرسیوم فن آوا- پتسا

با عنایت به اینکه ظرفیت‌های تعیین شده از سوی وزارت ارتباطات و فن‌آوری اطلاعات که در مرحله پایلوت تعیین شده بود شامل ۵۰ هزار سایت، ۱۵۰ هزار ایمیل و ۱۰ ترابایت فضای ذخیره‌سازی است

شرکت فن‌آوا در فاز پایلوت ۷۵ هزار میزبانی سایت، ۳۰۰ هزار میزبانی ایمیل و ۱۲ ترابایت فضای ذخیره‌سازی را انجام داده است.

در حال حاضر حدود هفت هزار ایمیل و ۴۰۰ سایت در فن‌آوا میزبانی می‌شود که حدود ۹۰ درصد مشتری‌ها از بخش خصوصی هستند.

این شرکت پس از فاز پایلوت که از سوی وزارت ارتباطات تعیین شده بود سایت اصلی را راه‌اندازی نمودکه در یک برنامه چهارماهه به فاز نهایی رسید و در این فاز دو سرویس به خدمات فاز پایلوت اضافه شد که شامل "سرور اختصاصی"و"فضای اشتراکی" بود اما ً "شبکه مجازی اختصاصی" و "شبکه تلفن ثابت" نیز در فاز نهایی در حال ارایه می‌باشد.

فضای ذخیره‌سازی در این IDC به ۲۰ ترابایت رسیده که قابلیت توسعه به پنج برابر و در واقع صد برابر را نیز دارد. لیکن بر اساس نیاز و تقاضای مشتری فضای ذخیره‌سازی قابل افزایش است.

۴-۷ شرکت پارس آنلاین

خدماتی که در حال حاضر توسط این شرکت ارایه می‌شود شامل میزبانی، سرور اختصاصی و فضای اختصاصی است.

ظرفیت فعلی مرکز داده میزبانی بیش از۴۰ هزار سایت با ظرفیت متوسط ۱۰۰مگابایت به ازای هر سایت و امکان ارایه حداقل۴۰۰ هزار صندوق پستی با ظرفیت متوسط ۱۰ مگابایت به ازای هر صندوق، ۱۵۰ رک برای خدمات فضای اختصاصی، تعداد ۶۰ سرور اختصاصی، مجموع فضای ذخیره‌سازی به میزان ۹ ترابایت و توان پردازش ۴۰۰ گیگاهرتز است.

ظرفیت‌های فاز بعدی میزبانی بیش از ۳۲۰ هزار سایت با ظرفیت متوسط ۱۰۰ مگابایت به ازای هر سایت و امکان ارایه حداقل پنج میلیون صندوق پستی با ظرفیت متوسط ۱۰ مگابایت به ازای هر صندوق،

۱۵۰ راک برای خدمات فضای اختصاصی، تعداد ۸۰۰ سرور اختصاصی و مجموع فضای ذخیره‌سازی به میزان ۷۲ ترابایت خواهد بود.

خدمات ارزش افزوده برای استفاده کاربران در این مراکز داده در نظر گرفته شده است که شامل امکان برخورداری از دیواره آتش اختصاصی و اشتراکی، امکان دسترسی به فضای ذخیره‌سازی از طریق تکنولوژی های NAS و SAN است.

این در حالی است که قیمت خدمات ارایه شده به دلایل جدید بودن، تنوع و ویژگی‌های هر خدمت هم‌اکنون در کشور دارای استاندارد خاصی نیست.

تا زمان تنظیم این گزارش، این شرکت سرویس‌های پایه را با حداقل میانگین قیمت ۳۰ هزار تومان ارایه می‌کند و در حال حاضر نیز حدود ۴۰ درصد از مشتری‌ها را ارگان‌های دولتی تشکیل می‌دهند. همچنین این شرکت موفق به راه اندازی طرح پایلوت مرکز داده خود شده است و در حال ساخت یک مرکز داده استاندارد در شهرک پردیس می‌باشد که در حال حاضر و به دلیل عدم حمایت های دولتی و بر مبنای اظهارات مدیر این شرکت در همایش چشم انداز مراکز داده در ایران که در تاریخ ۱۳۸۵/۶/۲۸ در مرکز تحقیقات مخابرات ایران برگزار شد از ایجاد بزرگترین مرکز داده خاورمیانه اظهار پشیمانی نموده است.

۸-۴ مرکز تحقیقات مخابرات ایران

اخیراً در این مرکز پروژه‌ای تحقیقاتی تعریف شده است که در این رابطه ریاست مرکز ، آقای دکتر محامد پور از راه‌اندازی پایلوت مرکز داده مرکز تحقیقات مخابرات ایران خبر داده و اظهار داشت: با توجه به آن که یکی از اجزای اصلی اینترنت ملی،IDC ملی است این مرکز نسبت به راه‌اندازی IDC داخلی اقدام کرده است که مطالعات مفهومی و اولیه نرم‌افزارهای آن به پایان رسیده است و تا اواخر

اردیبهشت ماه سال ۸۶ می‌تواند مجموعه کامل از انواع سرویس‌ها را ارائه دهد. در ادامه در اواخر خرداد ۸۶ هم اعلام شد که مرکز داده به صورت پایلوت و آزمایشی راه‌اندازی شده است. با این حال تلاش ما برای کسب اطلاعات بیشتر درباره جزئیات فنی و نیز سرویس‌های ارائه شده به جایی نرسیده است.

۴-۹ ارتباطات دیتا و شرکت فن‌آوری اطلاعات

اواسط آذر ۸۳ مهندس رضا رشیدی مدیرعامل شرکت ارتباطات داده‌ها گفت: طرح میزبانی داخلی و در حقیقت همان شارع ۲ تا یک ماه آینده راه‌اندازی شده و به بهره‌برداری می‌رسد، این طرح آزمایشی است و در واقع یک پایلوت محسوب می‌شودکه بر مبنای اطلاعات واصله از آن شرکت که در جوابیه نامه مهرماه ۱۳۸۵ مرکز پژوهش های مجلس بوده است، استفاده از امکانات این مرکز داده به «آینده‌ای نزدیک» موکول شده است.

۴-۱۰ سازمان تأمین اجتماعی

در مهرماه ۱۳۸۵ مجری طرح اتوماسیون سازمان تأمین اجتماعی چنین اعلام داشته که طی هدف گذاری ۵ ساله و کسب مجوز از وزارت ارتباطات، حجم اطلاعات سازمان تأمین اجتماعی را از طریق مرکز داده پوشش می‌دهیم.

با توجه به موارد مهم امنیت، سرعت، سهولت و دسترسی وسیع‌تر مخاطبین به سازمان برای خدمات و اطلاعات، ایجاد دیتاسنتر به عنوان برنامه ای پر اهمیت قلمداد شده است.که در این رابطه فعالیتهایی دررابطه با فراهم‌سازی مقدمات و کسب مجوز از وزارت ICT انجام شده است.

۴-۱۱ شرکت سروش رسانه

رئیس کمیته انفورماتیک معاونت فنی سازمان صداوسیما در شهریور ماه سال ۱۳۸۴ چنین اعلام نموده که صدا و سیما از طریق شرکت سروش رسانه و با توجه به استاندارد بودن وضعیت مرکز داده و امنیت فوق‌العاده بالا، قابلیت میزبانی وب‌سایت‌های دولتی را دارد اما این قابلیت به معنای اجرایی شدن آنها نیست.

این مقام مسئول با اشاره به بخشنامه ریاست جمهوری مبنی بر غیرقانونی بودن میزبانی سایت‌های دولتی در خارج از کشور اظهار داشته است که اگر مسئولان سیاست‌گذار IT اقدام به انتقال میزبانی سایت‌های دولتی به داخل کنند، سازمان صدا و سیما از نظر فنی آمادگی لازم را دارد و با توجه به استاندارد بودن سیستم، با تکیه عمده خود بر روی راه‌حل‌های ایرانی از امنیت اطلاعات و پهنای باند کافی برخوردار هستیم و تا راه‌اندازی مراکز داده ملی به عنوان راه حل میانی حاضر به همکاری با مخابرات در پروژه شارع ۲ هستیم و از سوی دیگر سیستم ما به دلیل ایرانی بودن دیوار آتش و بومی‌بودن آن، از نظر امنیت کمتر دچار مشکل خواهد بود، چرا که ثبات و پایایی داخل کشور به مراتب بهتر از خارج از کشور است.

۴-۱۲ نتیجه گیری

با نگرش به موارد مطروحه در این گزارش چنین می‌نماید که اصل ضرورت ایجاد مرکز داده به صورت متمرکز و یا غیر متمرکز، ملی یا سازمانی مورد تایید مسئولان می‌باشد و فعالیتهایی هم در این زمینه صورت گرفته و لازم است خدمات مهمی مثل میزبانی سایت سازمانها و نهادهای مهم کشورکه در هر لحظه بر اهمیت امنیتی آنها افزوده می‌شود در داخل کشور انجام شود تا از وابستگی هایی که دارای مشکلات امنیتی ، عدم استفاده از نیروی انسانی و منابع داخلی و ..... می‌شود جلوگیری نماییم.

در حال حاضر چنین به نظر می رسد که کلیه شرکت هایی که در مورد راه اندازی مراکز داده توانمند و یا مدعی هستند هنوز فرصتی پیدا نکرده‌اند که در این خصوص به صورت عملیاتی پروژه ای را شروع نمایند تا میزان توانمندی آنان مشخص شودکه دلایل ذیل می توانند در این امر قابل بررسی باشند:

- حضور پرقدرت مالی، اداری و سیاسی شرکت ارتباطات دیتا
- عدم درک فنی صحیح کارفرمایان دولتی و خصوصی در مورد لزوم پیاده سازی مراکز داده در شرکت ها و ارگانهای مهم دولتی
- پرهزینه بودن پروژه های مربوط به راه اندازی مراکز داده
- طرح ادعای توانمندی راه اندازی مراکز داده توسط بعضی شرکت ها که شاید در بعضی پروژه های مرتبط تاکنون موفق عمل نکرده اند و عدم ایجاد فضای توانمندی فنی برای کارفرمایان.
- عدم واگذاری امکاناتی که وزارت ارتباطات و فن‌آوری اطلاعات به شرکت‌های مجاز راه اندازی مرکز داده قول داده بود.

۱۳-۴ مراجع

[۱] گزارش مرکز پژوهشهای مجلس – تهیه شده در گروه ارتباطات و فن‌آوریهای نوین

[۲] آرش کریم بیگی – گزارش مورخه ۱۳۸۴/۲/۳۰ منتشر شده در سایت

http://www.ICTna.ir

[۳] گزارش مورخه ۱۳۸۴/۲/۱۳ در سایت

http://www.iTanalayze.ir

[۴] بهار امیری –مرکز دادههای ایرانی – گزارش مورخه ۱۳۸۵/۷/۱ – بزرگراه فن‌آوری

[۵] گزارش مورخه شنبه، ۲۶ شهریورماه ۱۳۸۴ در سایت

http://www.ITNA.ir

[۶] سایت روزنامه توسعه – تاریخ ۱۳۸۵/۱۰/۲۰

[۷] سایت ایران-تجارت، http://www.iran-tejarat.com/News/Cat18/News10470.html،

تاریخ ۱۳۸۶/۱۲/۲۵

[۸] اخبار فن آوری اطلاعات، http://iranictnews.ir/، ۱۳۸۷/۰۴/۰۵

۵ فصل پنجم: معماری های مراکز داده

فصل پنجم:

معماری های

مراکز داده

مراکز داده جهت در بر گرفتن تجهیزات، اطلاعات و برنامه های کاربردی حساس در فضایی کاملاً مطمئن و دارای قابلیت گسترش طراحی شده‌اند. آنها تحکیم و تثبیت منابع محاسباتی بسیار مهم را در محیطهای کنترلی، تحت یک مدیریت واحد فراهم می سازند و باعث می شود که تشکیلات اقتصادی و سازمانهای مختلف مطابق نیازهای تجاری و بر طبق زمانبندی های دقیق خود عمل کنند.

۵-۱-۱ معیارهای طراحی مراکز داده

ایجاد مرکز داده به برنامه ریزی بسیار دقیق و گسترده نیاز دارد و اهداف مورد نظر از طراحی یک مرکز داده باید واضح باشد تا نیل به آن اهداف امکان پذیر شود. معیارهای طراحی برای هرکدام از سرویس های ارائه شده در مرکز داده عبارتند از:

- قابلیت دسترسی بالا
- توسعه پذیری
- امنیت
- قابلیت مدیریت

مراکز داده، هسته اصلی زیر ساخت فن‌آوری اطلاعات برای منابع مهم و حساس می باشد. ایجاد مراکز داده یک راه حل مناسب و موثر برای کاهش حدود ۵۰٪ هزینه IT و پیشرفت سریع پاسخگویی به نیازهای تجاری می باشد. بسیاری از سازمان های فن‌آوری اطلاعات مسئول برآورد نیازهای زیرساخت مراکز داده خود برای افزایش بازدهی و همزمان افزایش سطح انعطاف پذیری و مهارت در معاملات تجاری می باشد.

بررسی های انجام شده بر روی شرکت هایی که به منظور پاسخگویی سریع به نیازهای تجاری روی فن‌آوری اطلاعات مسئول برآورد نیازهای زیرساخت مراکز داده خود برای افزایش بازدهی و همزمان افزایش سطح انعطاف پذیری و مهارت در معاملات تجاری می باشد.

بررسی‌های انجام شده بر روی شرکت‌هایی که به منظور پاسخگویی سریع به نیازهای تجاری روی فن‌آوری اطلاعات سرمایه‌گذاری کردند نشان می‌دهد، که کاهش تنوع برنامه‌های کاربردی، سیستم‌ها، ساختارها و شبکه هایی که مدیریت و نظارت آنها پیچیده و پرهزینه می‌باشد، باعث کاهش هزینه‌ها می‌شود. سازمان های فن‌آوری اطلاعات به منظور تحقق بخشیدن به نیازهای بهینه سازی، تحکیم و استاندارد سازی زیر ساخت های مرکز داده و رسیدن به اهداف استراتژیک خود به وجود آمدند. تنوع و پیچیدگی نیازهای تجاری روز باعث ایجاد رقابت برای ارائه خدمات متناسب به منظور افزایش بازدهی می شود.

در مرحله اول سازمان‌های فن‌آوری اطلاعات باید امکان ایجاد یک زیر ساخت مرکز داده با این قابلیت را به منظور تعیین یک قالب ساختاری برای محیط‌های متنوع و مختلف را فراهم نمایند. این توانایی باعث کاهش از هم گسیختگی‌ها، افزایش قابلیت استفاده موثر و اطمینان از عدم وجود اشتباهات شخصی می‌شود. مراکز فن‌آوری اطلاعات مسئول آموزش و راهنمایی بخش ها و مراکز تجاری، تداوم طرح و نقشه، ارائه راه حل ها و روال های تأثیر گذار اطلاعات و سیستم‌های دور از دسترس مراکز داده برای پاسخگوئی به نیازهای تجاری و کاهش خطرات از بین رفتن اطلاعات یا زمان های تلف شده می‌باشد.

برای اطمینان از اینکه مراکز داده و برنامه های کاربردی میزبان و اطلاعات قابل اطمینان می باشد، متصدیان امنیتی باید بر روی تشخیص مخاطرات داده نظارت کامل داشته و خط مشی‌های امنیتی لازم را تعیین نمایند. بر مبنای این خط مشی‌ها، گروه‌های عملیات شبکه و امنیت می‌توانند بر روی امنیت مراکز داده، ایجاد محدوده‌های امنیتی برای نتایج ارزیابی خطر عمل می‌نمایند.

۲-۵ ساختار فیزیکی

طراحی مرکز داده نیازمند انجام مطالعات و بررسی‌های گسترده می باشد. این مطالعات در زمینه نیازهای یک سازمان، امکانات و تکنولوژی‌های موجود جهت راه اندازی مرکز داده می باشد. طراحی مرکز داده باید پاسخگوی نیازهای فعلی و آینده سازمان باشد.

به همین دلیل در طراحی آن باید قابلیت ماجولار بودن[1]، دسترس پذیری و توسعه پذیری در نظر گرفته شود. هدف اصلی طراحی مرکز داده ارائه سرویس‌ها و خدمات یک سازمان به کاربران و کارکنان آن سازمان به صورت بهینه می‌باشد. محدوده پروژه، طول عمر مرکز داده، بودجه تخصیص داده شده از طرف سازمان در نوع و تعداد تجهیزات موثر می باشد. البته تخصیص بودجه مراکز داده باید به گونه‌ای باشد که موارد ضروری و مؤلفه‌های اصلی این مراکز حذف نشوند. به عنوان مثال ایجاد سیستم برق اضطراری در راه‌اندازی مرکز داده نقش اصلی ندارد ولی از ضروریات می‌باشد زیرا قطع برق شهری حتی در مدتی کوتاه ممکن است خسارات بسیاری به سازمان وارد کند. با توجه به اینکه سیستم به صورت ۷*۲۴ و در تمامی روزهای سال حتی روزهای تعطیل باید قابل دسترس باشد تهیه تجهیزات پشتیبان، سیستم برق اضطراری و سیستم شبکه پشتیبان بسیار ضروری می باشد.

در طراحی مرکز داده، شرایط مورد نیاز مکان، کف کاذب، زیرساخت شبکه (سوئیچ ها، روترها، سرورهای ترمینال، منبع تغذیه و کنترل کننده های دما و رطوبت) بایستی تعیین شود.

نیازهای مرکز داده عبارتند از:

- مکانی امن و مطمئن برای قراردادن کامپیوترها، ذخیره سازها و ابزارهای شبکه
- ایجاد منبع تغذیه لازم برای این تجهیزات

[1] Modularity

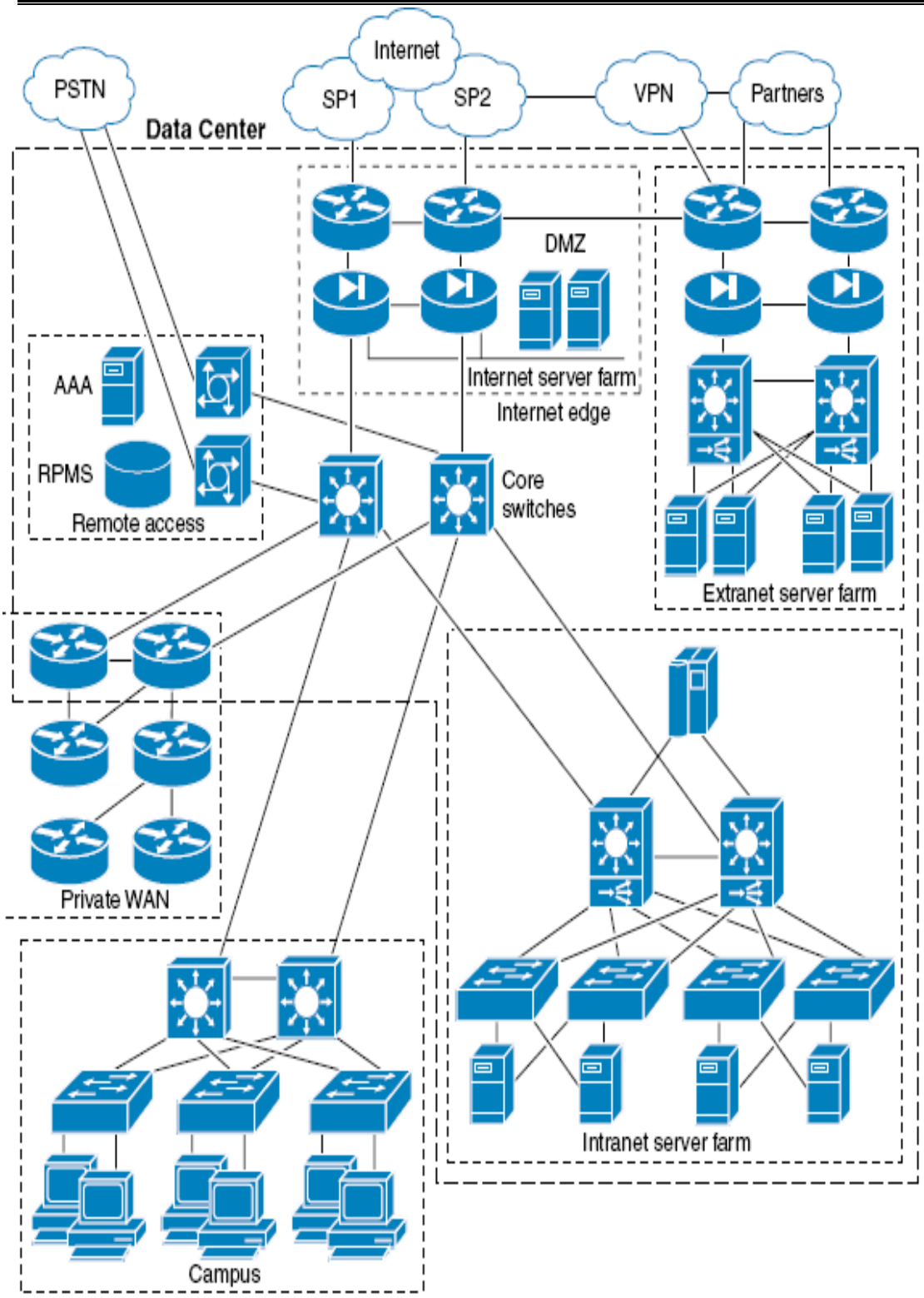
- ایجاد محیطی با قابلیت کنترل دما جهت ایجاد وضعیت بهینه برای تجهیزات
- برقراری اتصال با دیگر تجهیزات در داخل خارج مرکز داده

در طراحی یک مرکز داده جهت ارائه انواع سرویس‌ها، لازم است گذشته از ایجاد مکان مناسب جهت ارائه سرویس ها ساختاری منطقی در نظر گرفته شده باید قابلیت پوشش کلیه نیازها را داشته باشد.

۳-۵ ساختار و اجزای مرکز داده

هر مرکز داده شامل اجزایی است که هر کدام متناسب با وظایفشان از ساختار خاصی برخوردار می‌باشند. از جمله این اجزا که در یک مرکز داده متعارف قابل مشاهده است، می توان به شبکه‌های Campus، شبکه‌های گسترده خصوصی (Private WAN)، دسترسی از راه دور، انواع Server Farm ها اشاره نمود. برای ارائه خدمات به هریک از این اجزا لازم است یک زیر ساخت ارتباطی ایجاد گردد تا به واسطه آن بتوان بین این اجزا ارتباط برقرار نمود.

شکل ۲ زیرساخت شبکه فراگیر و جایگاه مرکز داده را به همراه مولفه‌های آن نشان می‌دهد.



شکل ۲: زیرساخت شبکه فراگیر و جایگاه مرکز داده

شکل ۳: لایه‌های مختلف دسترسی در شبکه مرکز داده

تعیین ساختار مرکز داده وابستگی شدیدی به نوع برنامه های کاربردی و بار ترافیک آن دارد. اما نکته مهم در تعیین ساختار تبدیل نیازها به اهداف تعریف شده ای است که به واسطه آن بتوان طرح تفصیلی یک مرکز داده را تعیین نمود. با توجه به اهمیت یک مرکز داده لازم است ساختار آن به صورت لایه ای در نظر گرفته شود. در هریک از لایه ها مدل های مختلفی برای طراحی مطرح می‌باشد. در طراحی بهینه مرکز داده باید از امکانات هر مدل نهایت استفاده را نمود. به طور مثال در طراحی قسمت هایی از آن استفاده از مدل‌های چندلایه‌ای بهینه می‌باشد.

شکل ۳ نشان دهنده لایه‌های مختلف دسترسی در شبکه مرکز داده می باشد که لایه های این طراحی عبارتند از:

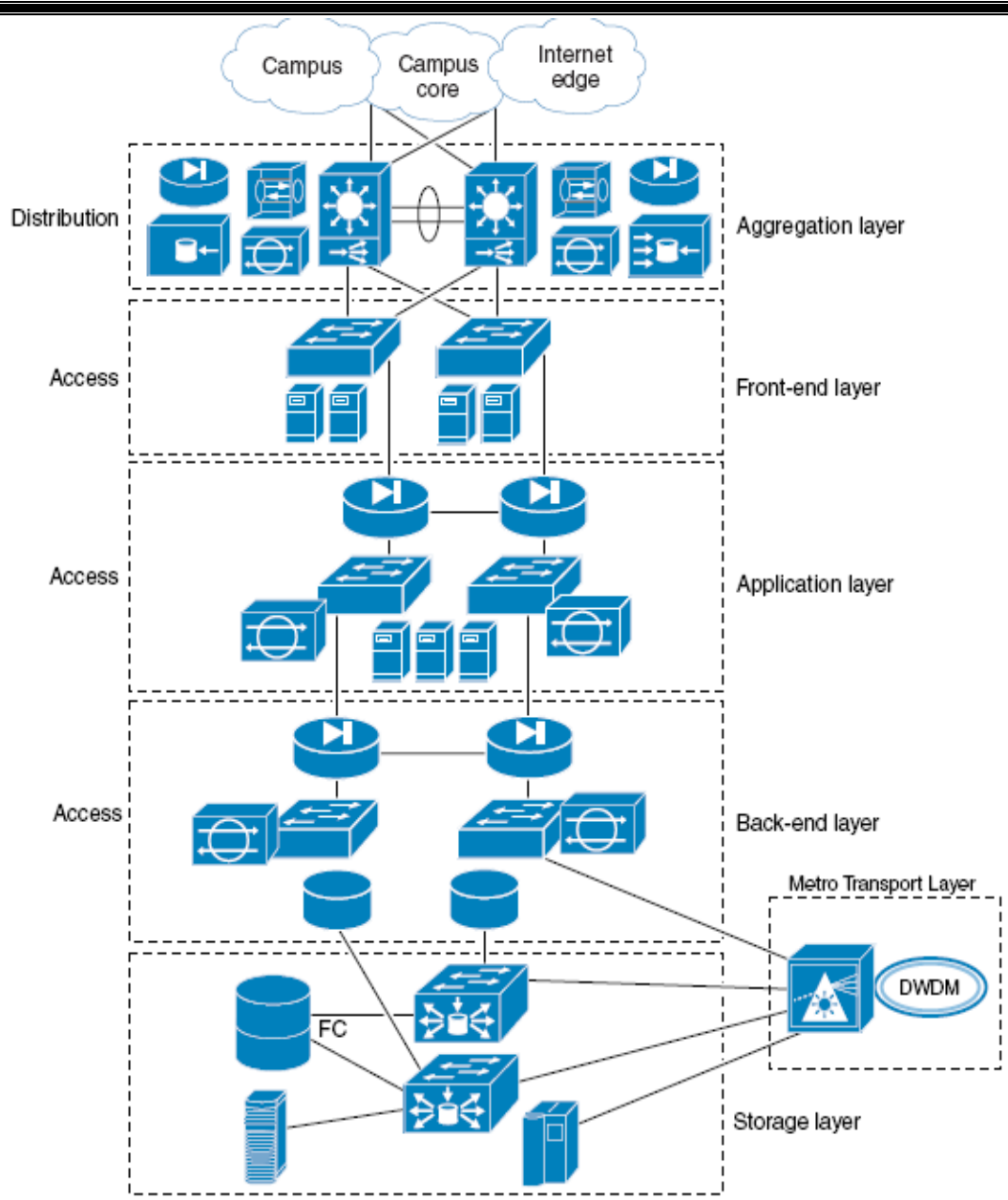
- لایه تجمیع[1]
- لایه خط مقدم[2]
- لایه کاربرد

[1] Back end
[2] Storage

- لایه عقبه[1]
- لایه ذخیره سازی[2]
- لایه انتقال شهری[3]

اهداف طراحی و سرویسهایی که توسط مرکز داده ارائه می‌شوند ملزومات ساختمان شبکه مرکز را تعیین می‌کنند که در این خصوص شکل ۴ معماری مرجع مرکز داده را به عنوان مدلی برای استفاده مشخص می‌کند.

[1] Back end
[2] Storage
[3] Metro Transport



شکل ۴: معماری مرکز داده

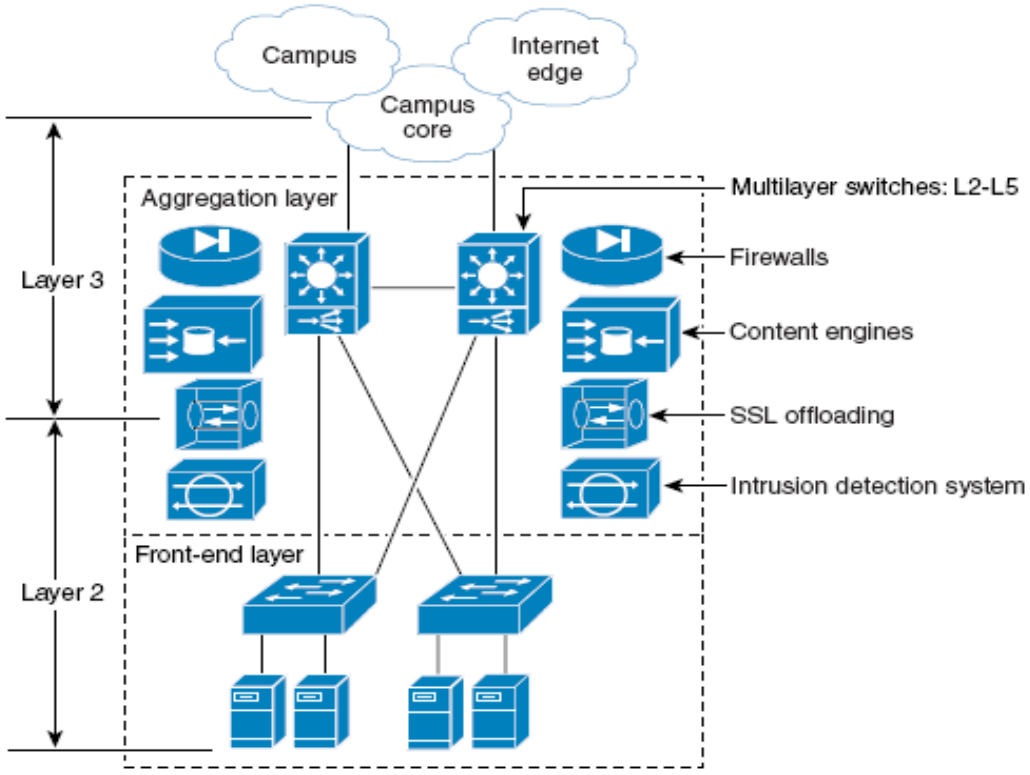
۴-۵ معرفی لایه‌های دسترسی شبکه

در ادامه هر یک از لایه‌های دسترسی شبکه که در شکل ۳ به آن اشاره شد شرح داده می‌شوند.

۵-۵ لایه تجمیع

وظیفه مهم این لایه برقرای ارتباط بین حوزه سرویس دهنده‌ها و بقیه شبکه مرکز داده بر مبنای مدل ارائه شده می‌باشد. همچنین ایجاد ارتباط بین تجهیزات مرکز داده و پشتیبانی از فعالیتهای لایه ۲ و ۳ از دیگر وظایف این لایه می‌باشد و در مجموع، فعالیتهای این لایه از مدل معماری ارائه شده شامل موارد ذیل می‌باشد که در شکل ۵ نشان شده است:

- سوییچهای اصلی
- دیوارهای آتش
- سیستم‌های تشخیص تهاجم
- موتورهای اصلی سیستم
- ارتباطات SSL



شکل ۵: لایهٔ تجمیع

۵-۶ لایه خط مقدم

این لایه ارتباط با رده اول سرویس دهنده‌ها در بخش سرویس دهنده‌ها را برقرار نموده و سرویس دهنده مربوطه در این لایه شامل سرویس‌های ذیل می‌باشد:

- FTP
- Telnet
- SMTP
- Web Servers
- و دیگر سرویس‌های مربوط به برنامه‌های کاربردی

موارد دیگر مثل QoS بستگی به سرویس دهنده‌ها و نوع عملکردهای آنها دارد. به طور مثال اگر Voice Over IP فعال گردد سرویس QoS نیز برقرار می‌شود.

۵-۷ لایه کاربرد

فعالیت‌های این لایه گذشته از سرویس دهی در خصوص برنامه‌های کاربردی ،ارتباط منطقی بین لایه خط مقدم و عقبه را نیز شامل می‌شود .سرویس دهنده‌های این لایه درخواستهای کاربران را برای اعمال فرامین مربوطه به سرویس دهنده‌های لایه عقبه ترجمه می‌کنند.

لایه‌های خط مقدم، کاربرد و عقبه

نشان دهنده ارتباط بین سه لایه خط مقدم، کاربرد و عقبه می‌باشد و وضعیت عملکرد این سه لایه را مشخص می‌کند که در ادامه به تشریح آن می‌پردازیم .

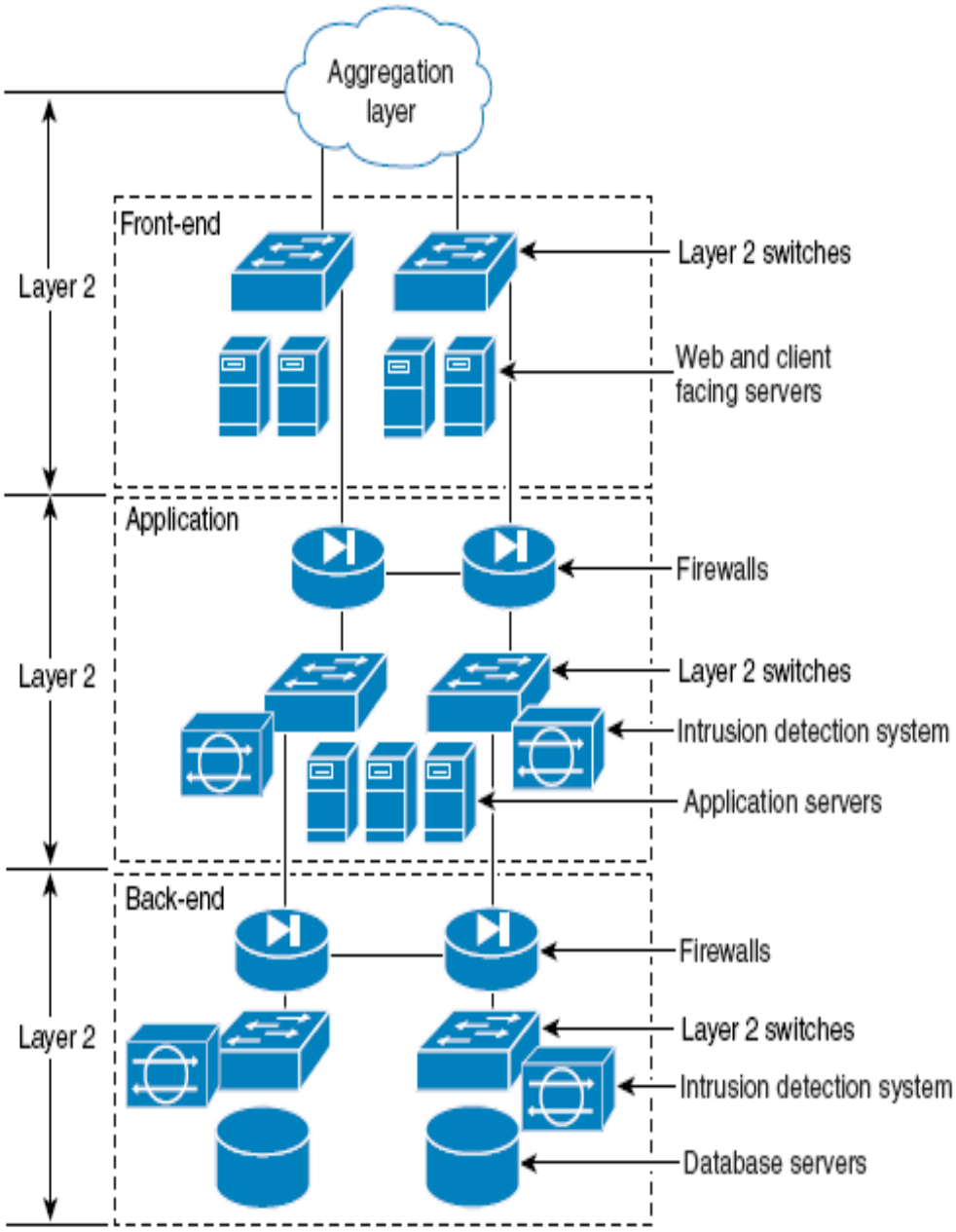
موارد درخواستی در این لایه شباهت زیادی به چنین مواردی در لایه Front-end دارند.

بر مبنای لزوم اعمال تدابیر امنیتی، سیستم‌های دیوار آتش ارتباط امن بین یک سری از کاربران و سرویس دهنده‌ها را با سرویس دهنده‌های لایه کاربردی برقرار می‌سازند .همچنین سیستم‌های تشخیص تهاجم انواع دیگر ترافیک‌های موجود را مورد ارزیابی قرار می‌دهند .

۵-۸ لایه عقبه

وظیفه اصلی این لایه برقراری ارتباط با سرویس‌های بانک اطلاعاتی می‌باشد و تا حدودی همانند لایه کاربردی عمل می‌کند و ارتباط خود با لایه بالاتر (سرویس دهنده‌های لایه کاربردی) را با استفاده از سیستم‌های مثل دیوار آتش تحت کنترل امنیتی دارد.

همچنین سرویس دهنده‌های بانک‌های اطلاعاتی در این لایه می‌توانند از طریق سوییچهای لایه ۲ با تجهیزات لایه بالاتر تبادل اطلاعات نمایند.



شکل ۶: لایه‌های خط مقدم، کاربرد و عقبه

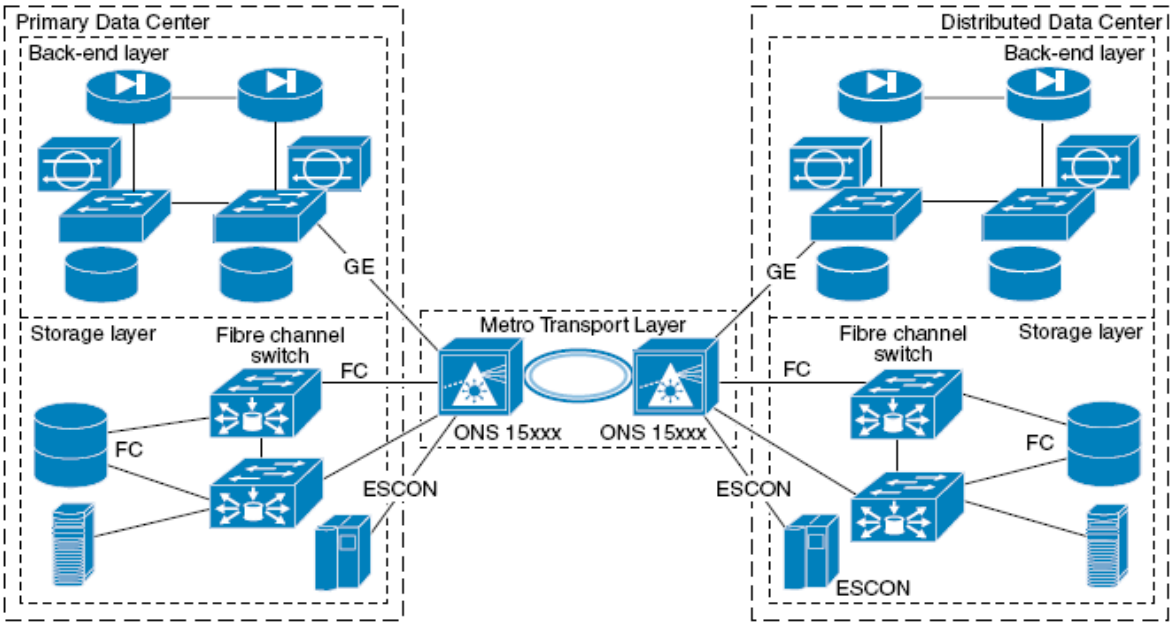
۵-۹ لایه ذخیره سازی

در این لایه عملیات مربوط به ارتباطات سیستم‌ها در شبکه ذخیره سازی توسط کانال‌هایی مثل فیبر نوری به عمل می‌آید و این ارتباطات به کمک سوییچهایی که دارای اتصال‌های فیبر نوری هستند از سرویس دهنده‌های دارای امکانات فیبر نوری به سیستم‌های ذخیره ساز مثل واحدهای نوارمغناطیسی برقرار می‌شود.

۵-۱۰ لایه انتقال شهری

وظیفه اصلی این لایه انجام عملیات در خصوص برقراری ارتباط پر سرعت بین مراکز داده توزیع شده می‌باشد و به عبارتی این لایه ارتباط سریع campus-to-campus را برقرار می‌نماید. این مراکز داده توزیع شده از تکنولوژی Metro-Optical برای ارتباط بین بانکهای اطلاعاتی و سیستم‌های ذخیره سازی استفاده می‌کنند. اتصالات پرسرعت برای ارتباطات همزمان و غیر همزمان استفاده می‌شوند.

در شکل ۷ وضعیت منطقی بین لایه عقبه و این لایه نشان داده شده است.



شکل ۷: همبندی انتقال شهری

۵-۱۱ سرورها در مراکز داده

Farm ها قلب مراکز داده می باشند. در حقیقت مراکز داده ای جهت پشتیبانی از server farm ها بوجود آمدند. اگرچه هر یک از این server farm ها برنامه های کاربردی و سرویس های خاصی را ارائه می دهند اما دارای ساختاری شبیه به یکدیگر می باشند. هر یک از این server farmها ارائه می شوند می توان آنها را به انواع زیر تقسیم نمود:

- Interanet Server Farm

کاربرانی که می توانند به این سرورها دسترسی پیدا کنند تنها کاربرانی هستند که در شبکه اینترانت قرار دارند. کاربران خارج از اینترانت عموماً به شبکه و سرورها دسترسی ندارند گرچه کاربران داخلی از شبکه اینترنت جهت انتقال اطلاعات استفاده می کنند.

- Internet Server Farm

این سرورها همانطور که از نامشان پیداست مستقیماً با اینترنت مرتبط می باشند. این نکته مشخص کننده این موضوع است که کاربران internet server farmها در مکانهای مختلفی در اینترنت واقع شده اند و برای اتصال به این سرورها از بستر ارتباطی اینترنت استفاده می‌نمایند. کاربران داخلی نیز به این سرورها دسترسی دارند. برای اتصال به این سرورها از واسط های web یا مرورگرهایweb استفاده می شود.

- Extranet server farm

این server farm درحقیقت در مکانی مابین server farm های اینترنت و اینترانت قرار گرفته اند. Extranet server farm نیز از برنامه های کاربردی web-based استفاده می‌نمایند ولی بر خلاف اینترنت و اینترانت، آنها تنها اجازه دسترسی به گروه‌های خاصی از کاربران را می دهند که به هیچ کدام از کاربران اینترنت و یا اینترانت وابسته نمی باشند. مهمترین هدف از ایجاد این server farm فراهم نمودن ارتباطات business-to-business با استفاده از واسط های User Friendly می باشد که باعث سرعت بخشیدن به تبادلات تجاری می گردد.

۱۲-۵ مراکز داده توزیع شده

مراکز داده توزیع شده Distributed Data Center (DDC) جهت فراهم آوردن قابلیتهای در دسترس بودن، گسترش، افزونگی و پاسخگویی به سوال بالا ایجاد شدند.

DDCها عموماً کوچکتر از مرکز داده اصلی می باشند و وظیفه مرکز داده اصلی را بعد از خرابی[1] آن به عهده می‌گیرند. بازیابی اطلاعات به هنگام وقوع یک حادثه ناگوار و امکان ارائه خدمات یکی از مهمترین مسائلی می باشد که در DDC ها مطرح می شود. DDC زمان توقف برنامه های کاربردی را

[1] Fail

برای برنامه های بسیار حساس کاهش می دهند و میزان از بین رفتن اطلاعات را به حداقل می رسانند. با استفاده از DDCها، اطلاعات بین DDC بر روی لایه انتقال انتقال شهری، تکرار می شود.

۱۳-۵ سرویس های مرکز داده

مراکز داده از سیستمهای متعددی پشتیبانی می نماید که در مجموع کلیه نیازهای برنامه های کاربردی موجود در مرکز داده توسط این سرویسها برآورده می شود که شامل سرویسهای زیرساخت، سرویس های server farm، سرویس ذخیره سازی، سرویس های عمومی و اختصاصی سازمان، سروسی های امنیتی و مدیریتی می باشد.

سرویس های زیرساخت شامل تمامی مشخصات هسته‌ای است که جهت زیر ساخت یک مرکز داده و نیز عملیاتی شدن کلیه سرویس های آن مورد نیاز است که سرویسهای این بخش به سرویسهای لایه ۱ یا سرویس های لایه ۲، سرویس های لایه ۳ و سرویس های هوشمند شبکه ای تقسیم می شوند.

سرویس های server farm شامل ویژگی هایی می باشند که باعث هوشمندی server farm ها می گردد. این مشخصات به منظور بالا بردن کارایی server farm و کنترل بسته ها (Packet Inspection) در لایه ۴ یا ۵ می باشد. به منظور ایجاد امکان در شبکه بایستی از امکاناتی از جمله امکان سوئیچینگ محتوا، SSL Termination,Caching و Content Transformation استفاده نمود.

سرویس ذخیره سازی در مرکز داده یکی از اصلی ترین و هزینه برترین سرویس ها می باشد. این سرویس از طریق دو سیستم ذخیره سازی NAS (Network attached storage) و SAN (Storage Area networks) ارائه می گردند. مبنای کار این دو سیستم متناسب با ساختارشان می باشد.

با توجه به ماهیت مرکز داده، می توان یک سری سرویس های عمومی نظیر پست الکترونیکی، میزبانی وب، سرویس های عمومی نظیر پست الکترونیکی، میزبانی وب، سرویس خبرگزاری، FTP، و

تالار گفتمان را نیز از طریق این مرکز ارائه نمود. مرکز داده به طور کلی با هدف ارائه خدمات ایجاد می گردد و به این منظور لازم است امکانات مربوط به سرویس های مختلف را متناسب با نیازهای سازمان تأمین نماید. همچنین در این مرکز سرویسهای امنیتی و مدیریتی لحاظ می گردد.

۱۴-۵ امنیت مرکز داده

سرویس های امنیتی شامل مشخصات و تکنولوژیهایی می باشند که باعث امنیت زیر ساخت مرکز داده و برنامه های کاربردی می گردند. هدف از به کارگیری سرویس های امنیتی حفاظت مرکز داده در برابر موارد زیر می باشد:

- دسترسی غیرمجاز
- ممانعت از سرویس
- کرم‌ها و ویروس‌ها
- حملات لایه پیوند داده
- شناسایی شبکه
- IP Spoofing

جهت رسیدن به اهداف ذکر شده لزوم به پیاده سازی سرویس‌های متعددی در مرکز داده می‌باشد که در زیر به پاره ای از آنها اشاره شده است:

۵-۱۵ لیست های کنترلی دسترسی[1] (ACL)

ACL ها از دسترسی‌های غیر مجاز به شبکه جلوگیری می کنند به این ترتیب از سرویس های server farm حفاظت می شود. ACLها می توانند در نقاط مختلف مرکز داده و در انواع متفاوت ارائه شوند. از جمله ACL ها می توان به QoS ACLs, VLAN ACLs, Router ACLs اشاره نمود. هریک از این انواع برای منظور خاصی مورد استفاده قرار می گیرد. از نکات مهم قابل اشاره در استفاده از ACL ها این است که می توان بدون ایجاد گلوگاه در شبکه با استفاده از آنها عملیات کلاسه بندی و کنترل بسته‌ها را انجام داد.

۵-۱۶ فایروال‌ها

استقرار دقیق فایروال‌ها در شبکه یکی از مهمترین پارامترها در طراحی مرکز داده می‌باشد. زیرا به واسطه جایگزاری مناسب مرکز داده بسیار امن یا بر خلاف آن نا امن خواهد شد. به طور کلی مناسب‌ترین مکان برای قراردادن یک فایروال در مرز اتصال به اینترنت می باشد. اما برای ایمنی بیشتر معمولاً در server Farm هایی که به صورت چندلایه‌ای طراحی می‌گردند نیز از فایروال در حد واسط بین لایه‌ها استفاده می‌گردد.

۵-۱۷ سیستم‌های تشخیص نفوذ

کشف نفوذ و اخطار پس از تشخیص آنها یکی از پایه های اولیه برقراری امنیت در مرکز داده می باشد. IDS ها به طور کلی به دو دسته تقسیم می شوند. دسته اول IDS هایی است که روی تجهیزات شبکه

[1] Access control Lists

نظیر راهگزین‌ها قرار می‌گیرند و از آنها در برابر حملات محافظت می نمایند. دسته دوم IDS هایی است که بر روی سرورها نصب شده و از حملات هکرها به سرورها جلوگیری می نمایند.

۵-۱۸ Authentication, Authorization, and Accounting

با استفاده از AAA یک لایه دیگر امنیتی به شبکه اضافه می‌گردد. با ایجاد یک سری پروفایلهای از پیش تعیین شده فقط به کاربرانی اجازه دسترسی به شبکه و بهره‌مندی از سرویس‌های آن داده می‌شود، که پروفایلشان موجود باشد. کلیه تراکنش‌های کاربرانی که مجوز ورود به شبکه را کسب می نماید در یک سرور به نام سرور سابقه جهت آنالیزهای accounting ذخیره می شود.

۵-۱۹ مدیریت مرکز داده

سرویسهای مدیریتی در مرکز داده در راس کلیه سرویس ها قرار دارند. هریک از سرویس ها نیازمند مدیریت می باشند به همین جهت این سرویس از اهمیت بالیی در مرکز داده برخوردار می باشد. با توجه به اینکه تجهیزات موجود در مرکز داده توسط یک سازمان خاص و یا یک سازنده ارائه نمی شود لازم است سرویس مدیریت با واسط های استاندارد در گروه های مختلف برای مانیتورینگ و رفع عیب ارائه گردد. پروتکل های استانداردی نظیر SNMP جهت فرستادن خطا و بدست آوردن اطلاعات کلی می تواند مورد استفاده قرار گیرد. برای مدیریت تجهیزاتی که در Internet Edge قرار دارند همچنین مدیریت روترها و سوییچ ها باید از قابلیت SSH استفاده گردد. برای مدیریت مرکز داده استفاده از پروتکل هایی نظیر HTTP و Telnet توصیه نمی‌گردد. گروه های مدیریتی که در یک مرکز داده باید همواره مد نظر قرار گیرد عبارتند از:

- مدیریت خطا

- مدیریت پیکربندی
- مدیریت حسابداری
- مدیریت کارآیی
- مدیریت امنیت

۲۰-۵ مراجع

[1]. Sufia Tippu, “Google likely to set up $1 billion datacenter in India”, **http://www.itwire.com.au/content/view/5254/945/** , [۸۶/۵/۲۲]

[2]. “Data Center & Networks”, **http://www.idcworks.com.my/data_centre_networks.htm** , [۸۶/۵/۲۰]

[3]. “MyLoca Data Center”, **http://www.exabytes.com.my/about/datacenters/myloca.html** , [۸٦/٥/۲۰]

۶ فصل ششم: استاندارد های مراکز داده

فصل ششم:

استاندارد های

مراکز داده

در این فصل استانداردهای فنی مطرح برای طراحی یا پیاده‌سازی مراکز داده مرور می‌شوند.

۶-۱ موارد مطرح در استانداردها

قبل از اینکه به معرفی استانداردهای مربوط به مراکز داده بپردازیم مهمترین مشخصات عمومی یک دیتاسنتر به عنوان سر فصل‌های مهم برگرفته از استانداردهای مختلف را به شرح ذیل معرفی می شوند:

۶-۲ اتصالات مختلف به اینترنت

در اختیار داشتن لینک‌های مختلف جهت اتصال از طریق ISP و ICPهای مختلف- به طور معمول یک دیتاسنتر برای اتصال به اینترنت از چندین اتصال مختلف استفاده می کند تا در صورتی که هر یک از اتصال‌ها به دلیلی از کار افتادند، در سرویس دهی مرکز وقفه‌ای پیش نیاید.

۶-۳ وجود سیستم قدرت پشتیبان

یکی از مهمترین مسائل در مرکز داده سرویس دهی بدون وقفه به مشتریان است. با توجه به امکان قطع برق به دلایل مختلف مثل حوادث غیرمترقبه یا جنگ، نیاز به سیستم برق پشتیبان ضروری است. معمولاً مرکز داده‌های بزرگ از UPSهای مخصوصی استفاده می کنند که امکان سرویس دهی به بیش از ۱۰۰ کامپیوتر را دارند. علاوه بر سیستم UPS ژنراتورهای قوی نیز در مرکز داده‌ای وجود دارد تا در صورت قطع بلندمدت برق، سرویس دهی بدون وقفه انجام شود.

۶-۴ وجود سرورهای متعدد

هدف اصلی یک مرکز داده در اختیار گذاشتن سرورهای وب برای مشتریان است. سرورهای مورد استفاده با توجه به نیاز و امکانات دیتاسنتر تعیین می شود. تنها تفاوت مهم، نوع سرورهای مورد استفاده توسط مرکز داده است. در این مراکز داده‌ای از دو نوع سرور استفاده می شود: سرورهای Rack mount یا سرورهایDesktop .

۶-۵ مشخصات فیزیکی

ساختمان‌های مراکز داده‌ای اکثراً با سقف‌های بلند ساخته می شوند که علاوه بر تهویه هوا، امکان قراردادن سرورهای بیشتر را فراهم می کنند. همچنین در تمامی مراکز داده، مسیرهایی برای گذراندن کابل‌های شبکه و همچنین کابل‌های برق وجود دارد. علاوه بر اینها، وجود سیستم تهویه قوی برای پایین نگاه داشتن دمای سرورها ضروری است. البته مشخصاتی چون وجود سقف کاذب، کف کاذب و همچنین سیستم اطفای حریق در برخی موارد توصیه شده است [۱].

۶-۶ استاندارد TIA/TR 942

اولین استاندارد مطرح که موارد زیادی از ملزومات مرکز داده را تحت پوشش قرار می‌داد در اکتبر سال ۲۰۰۴ میلادی منتشر شد.این استاندارد با نام TIA/TR 942 نام گرفت .نسخه بعدی این استانداردکه تکمیل شده آن بود بعدها به نام استاندارد TIP ارائه شد.

این استاندارد که نام کامل آن ANSI/TIA/EIA-942 می‌باشد به عنوان یک استاندارد ارتباطی برای مراکز داده مطرح می‌باشد که همیشه در حال تکمیل و به روز شدن است به طوریکه موارد مهم

طراحی را در مراکز داده کوچک تا مراکز داده بزرگ شامل می‌شود و به طور کلی این استاندارد شامل توصیه‌هایی در خصوص عملیات کابل کشی، طراحی شبکه و دیگر ملزومات می‌باشد[۲].

عناوین کلی این استاندارد عبارتند از :

- تجهیزات مکانی (زمین و سیستم‌های تهویه و ...)
- پیکر بندی مسیرهای ارتباطی شبکه داده
- پیکر بندی مسیرهای خطوط برق
- سیستم‌های پشتیبان اطلاعات
- سیستم‌های پشتیبان تغذیه برق
- سیستم‌های سخت‌افزار

در این استاندارد چهار مدل زیر ساخت برای طراحی و پیکر بندی مراکز داده در خصوص سیستم توزیع برق و تهویه پیشنهاد می گردد که عبارتند از[۳] :

- لایه ۱: در این لایه تنها یک مسیر برای توزیع برق و تهویه در نظر گرفته می‌شود و شامل تجهیزات پشتیبان نمی شود که در این حالت درصد دسترس پذیری به میزان ۹۹.۶۷۱٪ می‌باشد.
- لایه ۲: در این لایه تنها یک مسیر برای توزیع برق و تهویه در نظر گرفته می‌شود و شامل تجهیزات پشتیبان می‌شود که در این حالت درصد دسترس پذیری به میزان ۹۹.۷۴۱٪ می‌باشد.
- لایه ۳: در این لایه چندین مسیر برای توزیع برق و تهویه در نظر گرفته می‌شود و شامل تجهیزات پشتیبان و یک مسیر پشتیبان انتقال داده می‌شود که در این حالت درصد دسترس پذیری به میزان ۹۹.۹۸۲٪ می‌باشد.

- لایه ۴: در این لایه چندین مسیر برای توزیع برق و تهویه در نظر گرفته می‌شود و شامل تجهیزات پشتیبان و چند مسیر پشتیبان انتقال داده می‌شود که در این حالت درصد دسترس پذیری به میزان ٪۹۹.۹۹۵ می‌باشد.

۶-۷ استاندارد EN 50173-4

در این استاندارد تغییرات اساسی در حوزه زیر ساخت فیزیکی مرکز داده با توجه به موارد ذیل در نظر گرفته می‌شوند.[۳] .

۶-۸ ملزومات در طراحی مرکز داده

- مدیریت صحیح بر زیر ساخت لایه فیزیکی مرکز داده می‌تواند تأثیر مستقیم بر راهبری شبکه مرکز و ارائه خدمات آن داشته باشد.
- با به اجرا درآوردن راهکارهای فنی و درست کابل کشی می‌توان زیرساخت لایه فیزیکی را به عنوان کلید موفقیت در راهبری مرکز داده در نظر گرفت.
- تفکراتی که بتواند راه کارهای قابل انعطاف ایجاد کند به تداوم عمر سیستم کابل کشی کمک می‌کند .

۶-۹ ایجاد یک مرکز داده

موارد مورد نیاز در ایجاد یک مرکز داده از نقطه نظر این استاندارد و در حوزه سیستم‌های زیرساخت عبارتند از:

- تجهیزات پشتیبان با دسترسی راه دور
- ترسیم راه کارفنی مرکز
- سیستم اعلام و اطفاء حریق
- سیستم‌های پشتیبان تجهیزات برق، آب و ...
- در نظر داشتن لایه‌های امنیتی مختلف

۱۰-۶ استاندارد EN 50173-5

این استاندارد که در حقیقت بخش اتصالات از استاندارد TIA 942 را شامل می‌شود به طور عمده در مورد ملزومات طراحی مرکز داده در حوزه اتصال کابلها، سیستم‌ها، منابع تغذیه و .... می‌باشد. (شکل ۸)

همچنین در مورد سیستم‌های پشتیبان، امنیت لایه‌ای، کابل کشی استاندارد، انعطاف پذیری در طراحی و دیگر موارد مرتبط راهنمایی‌های لازم را ارائه می‌نماید .

شکل ۸: حوزه استانداردهای EN 50173

۶-۱۱ استاندارد NFPA (National Fire Protection Association)

این استاندارد به طور کلی در مورد طراحی سیستم‌های اعلام و اطفاء حریق در مراکز داده، توصیه‌هایی را ارائه می‌نماید و در خصوص جنبه‌های مختلف این حوزه دارای بخش‌های مختلف به ذکر عناوین ذیل می‌باشد [۲] .

- NFPA 13 – سیستم‌های آب پاشی و تهویه هوا
- NFPA 90A - در حوزه سیستم‌های تهویه

۶-۱۲ دیگر استانداردها

تا کنون برخی از استانداردها در این گزارش معرفی شده اند و هر روز بر مبنای نوع نیاز ارگانها و سازمانها که با تکنولوژیهای جدید آغاز به کار می‌کنند استانداردها و توصیه نامه‌هایی تدوین می‌شوند که

در این بخش نیز توصیه نامه‌ها و شبه استانداردهای دیگری نیز وجود دارند که بر مبنای موضوعات مطرح در طراحی مراکز داده به ذکر آنها می‌پردازیم[۳]:

۶-۱۳ سیستم‌های تغذیه

- RMI – توصیه در مورد اعمال تدابیر مهندسی در خصوص جلوگیری از اتلاف کار سیستم‌های تغذیه برق
- EPA – جلوگیری از اتلاف انرژی برق در مرکز داده

۶-۱۴ طراحی مرکز داده

- EPA – نحوه توزیع انرژی برای سرویس دهنده‌ها در مرکز داده
- محاسبات مربوط به هزینه زیرساخت سیستم کابل کشی

۶-۱۵ مراجع

[1] . “GUIDELINES FOR IMPLEMENTATION OF THE COMMON SERVICES CENTERS (CSC) SCHEME IN STATES “, http://www.mit.gov.in/ ,DEPARTMENT OF INFORMATION TECHNOLOGY GOVERNMENT OF INDIA, 2006

[2] . “Department of Information Technology”, http://www.mit.gov.in/ , [۸۶/۵/۱۷]

[3]. “Internet Data Center”, http://idc.nic.in/ , [۸٦/٥/١٧]

۷ فصل هفتم: مفاهیم امنیت و پدافند غیر عامل در مراکز داده

فصل هفتم:

مفاهیم امنیت و پدافند غیر عامل در مراکز داده

۷-۱ مقدمه

اساساً امنیت رایانه‌ای مجموعه ای از راه حلهای فنی برای مشکلات غیر فنی است. زمان، پول و تلاش زیادی را می توان برای ایمن کردن سیستم‌ها صرف کرد. اما هرگز نمی توان از نگرانی در مورد پاک شدن تصادفی داده ها یا تخریب عمدی اطلاعات راحت شد. با در نظر گرفتن مجموعه شرایط – اشکالات نرم افزاری، حوادث، اشتباهات، بداقبالی، آب و هوای بد یا یک مهاجم مجهز و با انگیزه – مشاهده می شود که هر رایانه ممکن است مورد سوء استفاده قرار بگیرد، از فعالیت بیفتد، یا حتی کاملاً منهدم شود.

برنامه ریزی امنیتی را می‌توان به پنج مرحله مجزا تقسیم کرد:

۱. برنامه ریزی برای تعیین نیازهای امنیتی
۲. ارزیابی مخاطره و انتخاب بهترین شیوه ها
۳. ایجاد سیاستهایی برای انعکاس نیازها
۴. پیاده سازی امنیت
۵. بررسی و واکنش به وقایع

بنابراین اولین گام فراهم کردن امنیت برای هر سیستم تعیین نیازهای امنیتی آن سیستم می‌باشد. در این گزارش با توجه به ماهیت مراکز داده، ابتدا معماری ها و استانداردهای مهم مرکز داده بیان، سپس نیازمندی‌های امنیتی کلی و سطح بالای مراکز داده برشمرده شده است و نیز راهکارها و نکاتی که باید برای تعیین نیازهای امنیتی جزئی یک مرکز داده خاص رعایت شوند آورده شده است.

به طور کلی مفاهیم امنیتی و پدافند غیر عامل مراکز داده مجموعا حول سه محور امنیت، ایمنی و پایداری و عامل امنیت حول ۳ محور محرمانگی، تمامیت (صحت) و دسترس‌پذیری هستند. عوامل

پایداری(ثبات و سازگاری) و دسترس پذیری بسیار به هم نزدیک بوده و عامل ایمنی با مفهوم امنیت فیزیکی و محیطی تطابق دارد. با این حال در عمل بهتر است نیازمندی‌های دیگری را نیز به طور صریح در کنار این‌ها قرار داد. در ادامه به مفاهیم پایه و نیازمندی‌های امنیتی و پدافند غیر عامل مراکز داده با رویکرد علمی پرداخته می شود.

۷-۲ نیازمندیهای امنیتی (با رویکرد علمی)

۷-۲-۱ محرمانگی

محرمانگی [1] عبارتست از حفاظت از اطلاعات در مقابل خوانده شدن یا نسخه برداری توسط اشخاصی که از جانب مالک آن اطلاعات مجوز دسترسی به آن را ندارند. این بُعد امنیت نه تنها حفاظت کلی از اطلاعات را در بر می‌گیرد، بلکه حفاظت از داده‌های منفرد که ممکن است به خودی خود آسیبی در پی نداشته باشند ولی از طریق تعدادی از آنها بتوان به اطلاعات محرمانه پی برد را نیز شامل می‌شود.

۷-۲-۲ صحت (تمامیت)

صحت یا تمامیت [2] عبارتست از محافظت از اطلاعات (منجمله برنامه‌ها) در مقابل هرگونه حذف و تغییر غیر مجاز یا توسط افراد غیر مجاز.

[1] Confidentiality
[2] Integrity

۷-۲-۳ دسترس‌پذیری

دسترس‌پذیری[1] عبارتست از این که منابع سیستم مانند سرویس‌ها، برنامه‌های کاربردی و داده‌ها در دسترس افراد مجاز با کیفیت قابل قبول باشند. برای این کار باید از برنامه‌های خدماتی به گونه‌ای که بدون احراز هویت تنزل پیدا نکنند و تخریب نشوند حفاظت کرد. اگر هنگامی که یک کاربر مجاز به اطلاعات نیاز دارد سیستم و داده‌ها در دسترس نباشند نتیجه می‌تواند به اندازه زمانی که اطلاعات از روی سیستم حذف شده اند ناخوشایند باشد.

۷-۲-۴ ثبات و سازگاری (پایداری)

ثبات و سازگاری[2] عبارتست از حصول اطمینان از این که سیستم به گونه‌ای که مورد انتظار کاربران است رفتار می‌کند. اگر نرم افزار یا سخت افزار ناگهان به گونه‌ای بسیار متفاوت از قبل عمل کند – خصوصاً بعد از یک ارتقاء یا رفع اشکال – مشکلات زیادی ممکن است رخ دهد. این گونه امنیت را می‌توان اطمینان از صحت داده‌ها و نرم افزارهایی که مورد استفاده قرار دارند نامید.

۷-۲-۵ کنترل

کنترل عبارتست از ضابطه‌مند کردن دسترسی به سیستم. اگر افراد (یا نرم افزارهایی) ناشناخته و غیر مجاز در سیستم وجود داشته باشند می‌توانند دردسرهای زیادی بیافرینند. جبران چنین مشکلاتی می‌تواند بسیار وقت‌گیر و پرهزینه باشد. شاید راهبر سیستم مجبور شود سیستم خود را از ابتدا نصب و راه اندازی کند.

---

[1] Availability
[2] Consistency

۷-۲-۶ بازبینی

به همان میزان که باید نگران دسترسی افراد غیر مجاز به سیستم بود، باید به امکان وقوع اشتباهات یا انجام اعمال بدخواهانه توسط کاربران مجاز نیز توجه کرد. در چنین شرایطی باید آنچه که انجام شده، فرد انجام دهنده و تأثیرات آن را مشخص نمود. تنها راه مطمئن برای دستیابی به این نتایج، داشتن سوابق و ثبت‌های غیر قابل مخدوش از فعالیتها در سیستم است که می‌تواند افراد و عملکرد آنها را شناسایی کند. در برخی از نرم افزارهای بسیار حساس، شیوه بازبینی ممکن است آنقدر گسترده باشد که بتواند بعد از تنظیم وضعیت سیستم به یک حالت جدید، اجازه بازگشت به وضعیت اولیه را نیز بدهد.

۷-۲-۷ تفاوت نیازمندی امنیتی سازمان‌های مختلف

اگر چه کلیه این وجوه امنیتی اهمیت دارند، اما سازمانهای مختلف به هر یک با درجه اهمیت متفاوتی می‌نگرند. این اختلاف بدلیل این است که هر سازمان ملاحظات امنیتی خاص خود را دارد و باید اولویتها و سیاستهای خود را بر حسب آن ملاحظات تعیین کند. بعنوان مثال:

- محیط بانکداری

در چنین محیطی، یکپارچگی، کنترل و بازبینی از اصول بسیار مهم و حیاتی هستند، و محرمانگی و در دسترس بودن در درجه بعدی قرار دارند.

- محیط نظامی

در یک سیستم دفاعی ملی که حاوی اطلاعات طبقه بندی شده است، محرمانگی در اولین درجه اهمیت قرار دارد و در دسترس بودن در درجه آخر. در برخی از محیطهای بسیار طبقه بندی شده ممکن

است مقامات رسمی ترجیح دهند که یک ساختمان را منفجر کنند تا اجازه نداده باشند اطلاعات بدست مهاجمین بیفتد.

- محیط دانشگاهی

در چنین محیطی، یکپارچگی و در دسترس بودن اطلاعات مهمترین نیازمندیها هستند. حصول اطمینان از در دسترس بودن اطلاعات در زمانیکه دانشجویان به آنها نیاز دارند به مراتب مهمتر از این است که راهبران بتوانند زمان استفاده دانشجویان از حسابهای کاربری خود را تشخیص دهند.

یک راهبر امنیت باید نیازهای محیط عملیاتی و کاربران را بشناسید و سپس بر مبنای آن روالهای خود را تعریف کند. ناگفته پیداست که نیازمندی‌های گفته شده کلی بوده و لزوماً برای تمامی محیطها مناسب نیستند.

۷-۳ نکات کلی در برآورده کردن نیازمندیهای امنیتی وپدافند غیر عامل

مشخص کردن جزئیات نیازمندیهای امنیتی یک سیستم، نرم افزار و به طور خاص در اینجا یک مرکز داده تقریباً امکان پذیر نیست. ولی به طور کلی می‌توان نیازمندیهای یک مرکز داده عام را تشریح کرد. در این راستا اهداف زیر باید مد نظر قرار گیرند:

۷-۳-۱ خط مشی‌های امنیتی

خط مشی‌های امنیتی در واقع تبیین کننده نیازهای امنیتی به صورت جزئی هستند و یک نیازمندی امنیتی به طور نوعی یک نیازمندی جزئی است که بخشی از خط مشی‌های امنیتی سطح بالا را پیاده سازی می کند.

۷-۳-۲ نیازمندیهای صحت و درستی

نیازمندیهای امنیتی بر پایه نیازهای درستی و صحت هستند، زیرا اشکالهای پیاده سازی اغلب باگهایی هستند که آسیب پذیری‌های امنیتی را به وجود می‌آورند. بنابراین باید نیازهای صحت و درستی سیستم‌ها در یک مرکز داده مشخص شوند.

۷-۳-۳ امکان پذیری

امن کردن صد در صد سیستمها، برنامه‌های کاربردی، مولفه‌ها یا سایر موارد غیر ممکن است. افزایش امنیت معمولاً منجر به موارد زیر می‌گردد:

- افزایش هزینه
- افزایش زمان
- کاهش کاربرد پذیری

۷-۳-۴ موارد سوء استفاده

برای مشخص شدن نیازمندیهای امنیتی می‌توان سناریوهای سوء استفاده شناخته شده را احصاء کرده و مطابق با آنها نیازمندیهای امنیتی برای مقابله در نظر گرفت.

۷-۳-۵ تهدیدها در برابر اهداف

در حالی که بیشتر نیازمندیها بر حسب آنچه که باید باشد و انجام شود بیان می‌شوند، نیازمندیهای امنیتی اغلب بر حسب آنچه که نباید باشد و نباید روی دهد بیان می‌شوند. از این رو باید تهدیدها برآورده شده و بر اساس آنها نیازهای جزئی امنیتی مشخص شوند. بر این اساس قبل و پس از شروع به کار هر مرکز

داده لازم است ارزیابی ریسک انجام شده و تهدیدها و ریسکها با تخمین میزان ضربه و احتمال وقوع به طور خاص برای آن مرکز داده مشخص شوند. در این صورت تیم امنیت می‌تواند مطمئن شود که نیازمندیهای امنیت از لحاظ هزینه به صرفه هستند.

۷-۴ نیازمندیهای تعیین هویت

یک نیازمندی تعیین هویت، نیازمندی امنیتی است که بیان می‌کند یک مولفه از سیستم مانند برنامه کاربردی باید قبل از هر تعاملی با نهادهای خارجی، مانند کاربران، برنامه‌های کاربردی دیگر، هویت وی را تعیین کنند.

۷-۴-۱ مثالها

- «برنامه کاربردی باید هویت تمام کاربران انسانی خود را قبل از اجازه استفاده از امکانات خود مشخص نماید.»
- « برنامه کاربردی باید هویت تمام برنامه‌های کاربردی مشتری خود را قبل از اجازه استفاده از امکانات خود، مشخص نماید.»
- « مرکز داده باید هویت تمام کارکنان را قبل از ورود تعیین نماید »
- (احراز هویت یکباره Single Sign – on) « برنامه کاربردی در طول یک نشست نباید بیش از یکبار هویت وی را پرسیده و ارزیابی کند »

۷-۴-۲ خطوط راهنما

- نیازمندیهای تعیین هویت اغلب ناکافی هستند و نوعاً پیش نیاز نیازمندیها احراز هویت[1] هستند.
- نیازمندیهای تعیین هویت نباید بر حسب انواع مکانیزمهای معماری امنیت که به طور نوعی برای پیاده سازی آنها استفاده می‌شود، بیان شوند.
- نیازمندیهای تعیین هویت باید با نیازمندیهای گمنامی[2] سازگار باشند. در نیازمندیهای گمنامی باید کاربر کمنام باقی بماند.

۷-۵ احراز هویت

نیازمندی احراز هویت، یک نیازمندی امنیتی است که بیان می‌کند یک مولفه سیستم مانند برنامه کاربردی، باید هویت طرفهای خارجی خود (مانند کاربران، برنامه‌های کاربردی دیگر) را قبل از تعامل با آنها بررسی و احراز کنند.

بنابراین نیازمندی احراز هویت، اطمینان از هویت طرف و این که وی واقعاً همان است که ادعا می‌کند، می‌باشد.

۷-۵-۱ مثالها

- «برنامه کاربردی باید هویت تمام کاربران و طرفهای خود را قبل از اجازه استفاده از امکانات، احراز نماید.»
- « مرکز داده باید هویت تمام کارکنان را قبل از ورود احراز نماید »

---

[1] Authentication
[2] Anonymity

۷-۵-۲ خطوط راهنما

- نیازمندیهای احراز هویت نوعاً کافی نیستند، اما پیش نیاز نیازمندیهای مجاز سنجی[1] هستند
- نیازمندیهای احراز هویت نباید بر حسب انواع مکانیزمهای امنیتی معماری که نوعاً برای پیاده سازی آنها به کار می‌رود بیان شود. توجه داشته باشید که اغلب مکانیزمهای معماری امنیت برای پیاده سازی همزمان نیازمندیهای تعیین و احراز هویت به کار می‌روند.
- به علت ارتباط نزدیک نیازمندیهای تعیین و احراز هویت، اغلب با هم بیان می‌شوند.

۷-۶ نیازمندیهای مجازسنجی

نیازمندی مجاز سنجی، یک نیاز امنیتی است که مجوزهای دسترسی و استفاده کاربران احراز هویت شده و برنامه‌های آنان را تعیین می کنند.

اهداف نوعی در نیازمندی مجاز سنجی عبارتند از :

- اطمینان از اینکه طرفهای احراز هویت شده می‌توانند به امکانات یک برنامه خاص یا یک مولفه دسترسی پیدا کنند. اگر و فقط اگر صریحاً توسط افراد تعیین صلاحیت شده، به آنها مجوز آن دسترسی داده شده باشد.
- اطمینان از اینکه تنها یک یا چند نفر که از طرف سازمان تعیین شده اند، می‌توانند دسترسی‌های افراد دیگر را تعیین و کنترل نمایند.
- جلوگیری از:
  - دسترسی کاربران غیر مجاز به داده‌های محرمانه

[1] Authorization

- دستکاری غیرمجاز داده توسط کاربران مجاز
- دستکاری داده‌ها توسط کاربران غیر مجاز

۷-۶-۱ خطوط راهنما

- مجاز شناسی به تعیین و احراز هویت، هردو، بستگی دارد.
- و احراز هویت، هردو، بستگی دارد.
- دسترسی‌ها باید بر اساس وظایف کاربری و نیازهای وی اعطا شود و اصل « دسترسی حداقل برای انجام وظیفه » رعایت شود.
- تنها تعداد کمی از افراد مجاز به اعطا یا تغییر مجوزها باشند.
- یک تهدید شایع علیه امنیت برنامه کاربردی، حمله منع سرویس است که برنامه با تعداد زیادی درخواست مجاز روبهرو می‌شود. بهتر است صریحاً به عنوان نیازمندی ذکر شود که کسی نباید با تعداد زیادی درخواست در زمان کوتاه، کیفیت مجاز سنجی را پایین آورد.

۷-۷ نیازمندیهای صحت

نیازمندیهای صحت، یک نیازمندی امنیتی است که بیان می‌کند داده‌ها و ارتباطات یک برنامه کاربردی یا یک مولفه نباید به طور عمدی، به صورت غیر مجاز تغییر داده شده یا حذف شود یا به طور غیر مجاز ایجاد شود.

اهداف نوعی در نیازمندیهای صحت عبارتست از اطمینان از این که می‌توان به داده‌ها یا ارتباطات اعتماد کرد.

۷-۸ نیازمندیهای تشخیص نفوذ

یک نیازمندی کشف نفوذ، نیاز امنیتی است که بیان می‌کند یک برنامه کاربردی یا یک مولفه باید دسترسی‌های غیرمجاز یا تلاش برای دسترسی غیر مجاز را کشف و ثبت نماید.

اهداف نوعی نیازمندی کشف نفوذ عبارتند از:

- کشف کاربران و برنامه‌های غیرمجاز که سعی دردسترسی به برنامه‌ها یا مولفه‌ها دارند.
- ثبت اطلاعات درباره دسترسی‌های غیر مجاز یا تلاش برای دسترسی غیرمجاز
- گزارش دهی به راهبران سیستم

۷-۸-۱ مثال‌ها

- سیستم‌ها باید تمام تلاشهای ناموفق برای تعیین و احراز هویت و یا مجاز سنجی را کشف و ثبت نمایند.
- سیستم‌ها باید به طور روزانه به راهبر امنیت مرکز داده درباره تلاش‌های ناموفق دسترسی در طول ۲۴ ساعت قبل گزارش دهند.
- سیستم‌ها باید حداکثر طی ۵ دقیقه پس از کشف تلاش‌های مکرر برای نفوذ یا دسترسی غیرمجاز به راهبر امنیت مرکز داده گزارش دهند.

۷-۸-۲ خطوط راهنما

- نیازمندی‌های کشف نفوذ نیازمندیهای تعیین و احراز هویت و مجازسنجی بستگی دارند.

- نیازمندی‌های کشف نفوذ نباید بر حسب مکانیزمهای معماری امنیت که به طور نوعی برای پیاده سازی آنها به کار می‌روند بیان شوند.

۹-۷ نیازمندیهای عدم انکار

یک نیازمندی عدم انکار[1]، یک نیاز امنیتی است که بیان می‌کند برنامه کاربردی یا مولفه سیستم باید از انکار انجام یا دخالت در عمل انجام شده توسط یک نهاد یا شیء جلوگیری کند.

اهداف نوعی یک نیازمندی عدم انکار عبارتند از:

- اطمینان از ثبت رکوردهای اطلاعاتی به اندازه کافی، برای جلوگیری از انکار توسط عاملان
- به حداقل رساندن هرگونه مشکل قانونی احتمالی که در آینده ممکن است به علت تخطی یکی از کاربران به وجود آید.

۱-۹-۷ خطوط راهنما

- نیازمندیهای امنیتی عدم انکار اصولاً درباره کافی بودن و عدم امکان مخدوش نمودن رکوردها هستند. ثبت رکوردها خود به خود کافی نیست. این رکوردها باید کافی و غیر قابل خدشه باشند.
- نیازمندیهای عدم انکار نوعاً شامل ذخیره حجم زیادی از اطلاعات درباره تعاملات است که شامل موارد زیر می‌باشد:
  - هویت احراز شده هریک از طرفهای درگیر

[1] Non repudiation

- تاریخ و زمان ارسال، دریافت و تصدیق دریافت
- اطلاعات ارسالی

- نیازمندیهای عدم انکار اغلب مرتبط با نیازمندیهای قابلیت ممیزی هستند ولی از آن محدودتر هستند.
- نیازمندیهای عدم انکار نباید بر حسب مکانیزمهای امنیتی که نوعاً برای پیاده سازی آنها استفاده می‌شوند، بیان شوند (مانند امضاء رقمی، رمز نگاری، توابع درهم سازی).

۷-۱۰ نیازمندیهای محرمانگی

یک نیازمندی محرمانگی، یک نیاز امنیتی است که بیان می‌کند برنامه کاربردی یا مولفه سیستم باید داده‌های حساس خود را از دسترس افراد و برنامه‌های غیر مجاز حفظ کند.

اهداف نوعی محرمانگی عبارتند از:

- اطمینان از اینکه افراد و برنامه‌های غیرمجاز دسترسی به داده‌های حساس ندارند
- فراهم کردن دسترسی به داده‌ها را بر اساس اصل « نیاز به دانستن »

۷-۱۰-۱ مثال

- «برنامه کاربردی نباید اجازه دسترسی افراد غیر مجاز به داده‌های ذخیره شده یا در حال انتقال بدهد.»

۷-۱۰-۲ خطوط راهنما

- نیازمندی‌های محرمانگی باید دقیقاً حیطه خود را مشخص نمایند:
  - سطوح طبقه بندی داده‌ها مشخص شده و مشخص شود که چگونه داده‌ها طبقه بندی شوند (معیارهای طبقه‌بندی)
  - محل‌هایی که داده ذخیره می‌شوند یا عبور داده می‌شوند (مانند اینترنت، خارج محل امن).
- محرمانگی ممکن است با برخی قوانین تضاد داشته باشند. به عنوان مثال برخی الزامات قانونی لازم دارد که برخی اطلاعات به طرفهای دیگر داده شود.
- نیازمندی‌های امنیتی نباید بر حسب مکانیزمهای معماری امنیت مانند رویدادنگاری که نوعاً از آنها برای پیاده سازی نیازمندیها استفاده می‌شود، بیان شوند (مانند رمزنگاری متقارن یا نامتقارن، ابزارهای موجود رمزنگاری).
- نیازمندی‌های امنیتی باید با نیازمندی‌های ممیزی، تعیین هویت، و عدم انکار که لازمه آنها ارائه اطلاعات از طرف کاربر یا ثبت آنها می‌باشد، سازگار باشند.

۱۱-۷ نیازمندیهای ممیزی امنیت

یک نیازمندی ممیزی امنیت[1]، یک نیاز امنیتی است که بیان می کند برنامه کاربردی یا مولفه سیستم باید امکان بررسی و ممیزی وضعیت و نحوه استفاده از مکانیزمهای امنیتی را فراهم کنند.

اهداف نوعی یک نیازمندی ممیزی عبارتند از اطمینان از اینکه برنامه کاربردی یا مولفه سیستم اطلاعات درباره :

[1] Security auditing

- وضعیت (مانند فعال و غیر فعال بودن، نسخه به روز) مکانیزمهای امنیتی
- استفاده از مکانیزمهای امنیتی (مانند دسترسی یا تغییر)

را جمع آوری، تحلیل و گزارش می‌نامند.

۷-۱۱-۱ مثال

برنامه کاربردی باید به طور دائم وضعیت مکانیزم‌های امنیتی خود شامل:

- تعیین و احراز هویت، مجازشناسی
- مصونیت[1]
- محرمانگی
- تشخیص نفوذ

را جمع‌آوری، سازمان‌دهی، خلاصه کرده و به طور منظم گزارش دهد.

۷-۱۱-۲ خطوط راهنما

- باید توجه داشت که بین نیازمندیهای ممیزی امنیت و کشف نفوذ، افزونگی و روهم افتادگی نباشد.
- نیازمندیهای ممیزی امنیت نباید بر حسب مکانیزمهای معماری امنیت مانند رویدادنگاری که نوعاً از آنها برای پیاده سازی نیازمندیها استفاده می‌شود، بیان شوند.

[1] Immunity

۷-۱۲ نیازمندیهای حفاظت فیزیکی

یک نیازمندی حفاظت فیزیکی، یک نیاز امنیتی است که بیان می‌کند یک مرکز یا سایت باید خود در برابر صدمات فیزیکی محافظت کند.

۷-۱۲-۱ مثال ها

- « مرکز داده باید مولفه‌های سخت افزاری را در برابر خرابی فیزیکی، سرقت، یا جایگزینی غیر مجاز حفاظت نماید».
- «مرکز داده باید از کارکنان خود در برابر مرگ، جرح و آدم ربایی محافظت نماید.»

۷-۱۲-۲ خطوط راهنما

- نیازمندی‌های حفاظت فیزیکی نباید با مکانیزم‌های معماری امنیت که برای پیاده‌سازی آن استفاده می‌شود، اشتباه شود، مانند: قفل درها، محافظ‌های امنیتی، دسترسی سریع به پلیس.

۷-۱۳ نیازمندیهای امنیت نگهداری سیستم

نیازمندی امنیت نگهداری سیستم، یک نیاز امنیتی است که بیانگر لزوم جلوگیری از شکست اتفاقی مکانیزمهای امنیتی در طی عملیات نگهداری سیستم (مانند به‌روز رسانی، پیکربندی و بهبود) می‌باشد.

هدف اصلی نیازمندی امنیت نگهداری سیستم، حفظ سطح امنیت در طی مدت استفاده از سیستم است.

۷-۱۳-۱ مثال ها

- «برنامه کاربردی نباید نیازمندی‌های امنیتی خود را در نتیجه ارتقای مولفه‌های سخت‌افزار، نرم‌افزار یا داده نقض نماید.»
- «برنامه کاربردی نباید نیازمندی‌های امنیتی خود را در نتیجه جایگزینی مولفه‌های سخت‌افزار، نرم‌افزار یا داده نقض نماید.»

۷-۱۳-۲ خطوط راهنما

- نیازمندی‌های امنیت نگهداری سیستم ممکن است با نیازمندی‌های دسترس‌پذیری سیستم تضاد داشته باشند. در نیازمندی دسترس‌پذیری ممکن است اجازه داده نشود که در طی نگهداری سیستم از مدار خارج شود.
- نیازمندی‌های امنیت نگهداری سیستم نباید با با مکانیزم‌های معماری امنیت که برای پیاده‌سازی آن استفاده می‌شود، اشتباه شود، مانند: روال‌های نگهداری و بهبود، آزمون عدم نقض امنیت.

۷-۱۴ مراجع

[1] . “GUIDELINES FOR IMPLEMENTATION OF THE COMMON SERVICES CENTERS (CSC) SCHEME IN STATES “, http://www.mit.gov.in/ ,DEPARTMENT OF INFORMATION TECHNOLOGY GOVERNMENT OF INDIA, 2006

[2]. Sufia Tippu, “Google likely to set up $1 billion datacenter in India”, http://www.itwire.com.au/content/view/5254/945/ , [۸۶/۵/۲۲]

[3]. “Internet Data Center”, http://idc.nic.in/ , [۸۶/۵/۱۷]

[4]. “Data Center & Networks”, http://www.idcworks.com.my/data_centre_networks.htm , [۸۶/۵/۲۰]

۸ فصل هشتم: ملاحظات پدافند غیر عامل سطح بالای مراکز داده

فصل هشتم:

ملاحظات پدافند غیر عامل

سطح بالای

مراکز داده

۸-۱ مقدمه

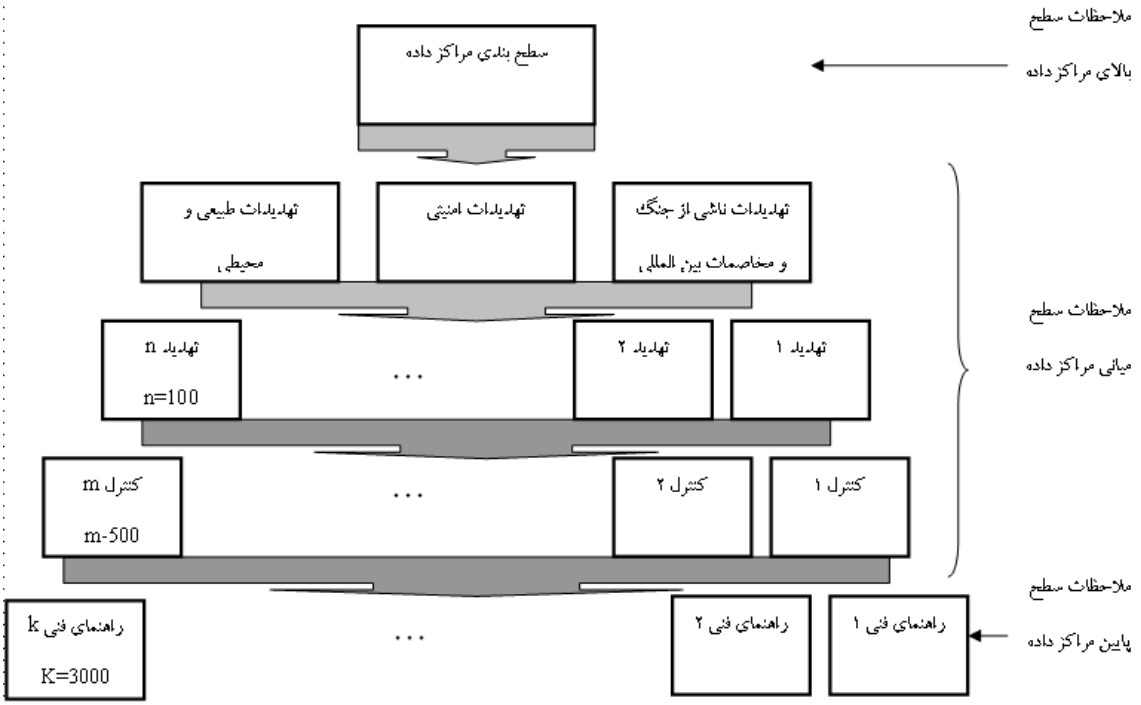
مراکز داده به عنوان قلب تپنده در زیرساخت‌های فن‌آوری اطلاعات یک کشور هستند و از این رو نقش مهمی در امنیت یک کشور می‌توانند داشته باشند. با به خطر افتادن امنیت یک مرکز داده سرویس‌های حیاتی مبتنی بر آن به مخاطره می‌افتند. اما همه مراکز داده در یک درجه از اهمیت قرار ندارند، و بسته به نقش آنها، خدمات ارائه شده و گستره آنها و دیگر پارامترها در رده‌های گوناگون اهمیت قرار دارند که ملزومات امنیتی هر یک نیز متفاوت از دیگری است. از طرف دیگر همیشه برقراری امنیت هزینه بالایی می‌طلبد. از این رو لازم است مطابق نیازمندی‌های واقعی امنیتی یک مرکز داده، تدابیر امنیتی لازم اتخاذ شده و صرف هزینه زیادی جلوگیری شود.

از همین رو باید مراکز داده را از نظر حساسیت امنیتی طبقه‌بندی نمود. این طبقه‌بندی باید حتی‌الامکان نزدیک به سطح واقعی امنیت مورد نیاز باشد تا از یک طرف از نقض احتمالی امنیت به علت مسامحه در برقرار امنیت مورد نیاز جلوگیری شود و هم از صرف هزینه‌های گزاف به علت افراط در تعیین سطح امنیتی پیشگیری شود.

با توجه به لزوم توسعه مراکز داده در کشور، از سویی اهمیت و حساسیت این مراکز، تهیه سند بالادستی در حوزه ملاحظات پدافند غیر عامل در این مراکز بسیار ضروری بوده است. لذا با توجه به اهداف و رویکردهای سازمان پدافند غیر عامل که تکیه بر ۳ اصل امنیت، ایمنی و پایداری، تهدیدات مصور برای این مراکز را در ۳ دسته تهدیدات ناشی از جنگ و مخاصمات بین المللی، تهدیدات امنیتی و تهدیدات محیطی و طبیعی برای مکانهای مهم، حساس و حیاتی دارد، سعی گردیده است که این موارد متناسب با موضوع مراکز داده کشور بیان گردد. برای این منظور ابتدا مراکز داده به ۳ دسته مهم، حساس و حیاتی تقسیم بندی شده است. در ادامه مصادیق رده بندی یک مرکز داده بمنظور تعیین طبقه بندی آن نیز بیان شده

است. لذا با استفاده از این مصادیق، می توان در زمان تصمیم گیری برای طراحی و پیاده سازی یک مرکز داده خاص، سطح آن مرکز داده (مهم، حساس یا حیاتی) را مشخص نمود. نهایتا در بخش انتهایی و اصلی این سند، ملاحظات پدافند غیر عامل در خصوص هر سطح مرکز داده به تفکیک بصورت کنترلهای سطح میانی در حوزه های مختلف بیان شده است. لذا پس از تعیین سطح و مشخص شدن سطح مرکز داده، کافیست کنترلهای تعیین شده برای آن سطح، مورد توجه قرار گرفته و لحاظ گردند. طبیعی است جنس این کنترلها از نوع کنترلهای فنی سطح بالا و سطح میانی بوده و لذا به موارد فنی سطح پایین که عموما مرتبط با محصولات مختلف و تکنولوژیهای سطح پایین بوده و وابسته به زمان طراحی و پیاده سازی و متناسب با ابزارهای در دسترس پیاده ساز در زمان پیاده سازی می باشد و از سویی دائما در حال تغییر است، نمی توانست در این سند اشاره گردد. لازم به ذکر است که کنترلهای سطح بالا و میانی به گونه ای انتخاب گردیده است که در صورت رعایت نمودن و لحاظ نمودن این موارد، تمامی موارد مورد نظر پدافند غیر عامل در سطح پایین نیز لحاظ خواهد گردید.

لذا روش بکار گرفته شده برای تدوین این سند که روشی منحصر به فرد در کشور می باشد، دارای ۵ لایه می باشد (شکل ۹).



شکل ۹: روش ۵ لایه تدوین ملاحظات پدافند غیر عامل در مراکزداده

در لایه اول، ملاحظات پدافند غیر عامل در مراکز داده در سطح بالا، در لایه های دوم، سوم و چهارم، این ملاحظات در سطح میانی و نهایتا در لایه پنجم، این ملاحظات در سطح پایین بیان گردیده است.

در سطح بالا، مطالب مربوط به رده بندی مراکز داده و مصادیق این رده بندی و چگونگی تعیین سطح یک مرکز داده و مشخص کردن نوع آن (مهم، حساس یا حیاتی) بیان گردیده است (لایه اول).

در سطح میانی، بدلیل گستردگی سطحی و عمقی مراکز داده (به عنوان قلب تپنده IT) و کاربرد اکثر مقوله های مطرح امروزی در حوزه IT در این مراکز، و بمنظور پرداختن به تمامی کنترلهای مربوط به این مقوله ها در مراکز داده، ابتدا ۳ حوزه اصلی تهدید مشخص، سپس کلیه تهدیدات متصور برای مراکز

داده برای این ۳ حوزه که مرتبط با مراکز داده بوده است (لایه دوم)، در حدود ۱۰۰ مقوله احصاء (لایه سوم) و در نهایت کنترلهای مربوط به این تهدیدات در قالب حدود ۵۰۰ کنترل (لایه چهارم) مشخص گردیده است.

در سطح پایین نیز همانگونه که اشاره شد، از آنجا که این کنترل ها وابسته به محصولات و تکنولوژیهای مرتبط با زمان پیاده سازی مرکز داده می باشد، لذا این موارد بایستی در زمان پیاده سازی و با توجه به کنترل های سطح میانی توسط کارشناسان خبره طراح مراکز داده در حوزه های مختلف، استخراج شده و لحاظ گردند. این حوزه ها حدودا ۵۰۰ تا ۱۰۰۰ موضوع مختلف را شامل می شوند.

در این روش شرح داده شده اولین سطح، ملاحظات سطح بالای پدافند غیر عامل می باشد که در این فصل به آن پرداخته می شود.

هدف از ملاحظات پدافند غیر عامل سطح بالای مراکز داده، ارائه انواع و مصادیق طبقه بندی مراکز داده با رویکرد پدافند غیر عامل می باشد. بنابراین در ملاحظات سطح بالای مراکز داده کشور، دسته بندی این مراکز با توجه به ملاحظات پدافند غیر عامل کشور و همچنین مصادیق تعیین جایگاه یک مرکز داده خاص در این دسته بندی بررسی می شود. توضیح اینکه، پس از بیان دسته بندی مراکز داده، مصادیقی ارائه گردیده است که هر سازمانی که بخواهد اقدام به ایجاد مرکز داده نماید، با توجه به این مصادیق بتواند سطح مرکز داده مورد نیاز خود را احصاء نماید، سپس ملاحظات پدافندی ذکر شده در این سند (ملاحظات سطح میانی) متناسب با آن سطح مرکز داده را اعمال نماید.

۲-۸ دسته بندی مراکز داده با رویکرد پدافند غیر عامل

با توجه به سطوح دسته بندی مراکز از دیدگاه سازمان پدافند غیر عامل، رده‌های زیر برای یک مرکز داده وجود خواهد داشت:

- **سطح III مرکز داده حیاتی**
- **سطح II مرکز داده حساس**
- **سطح II مرکز داده مهم**

در ادامه، مصادیق رده بندی مراکز داده بیان شده و نهایتا در بخشهای بعدی، ملاحظات پدافند غیر عامل متناسب با هر رده از این مراکز بیان می شود.

با توجه به اصول پدافند غیر عامل یعنی ۳ اصل امنیت، ایمنی و پایداری، ساختار مراکز داده بایستی به گونه‌ای طراحی و پیاده سازی گردد که این سه اصل همواره مورد توجه قرار گرفته شده باشد. مقوله اول یعنی امنیت در ادامه شرح داده خواهد شد، مقوله دوم نیز در بخش امنیت محیطی و طبیعی مفصلا مورد توجه و تاکید قرار گرفته شده است و مقوله سوم یعنی پایداری نیز به عنوان یکی از اصول مهم پدافند غیرعامل، هم در موضوعات مرتبط به امنیت و هم در موضوعات مرتبط به تهدیدات ناشی از جنگ و مخاصمات بین المللی به آن پرداخته شده است، بدین مفهوم که در دسترس بودن و پایداری مورد توجه قرار گرفته است. لازم به ذکر است که مقوله هایی نظیر کنترل و بازبینی، زیر مجموعه موارد گفته شده قرار می گیرند و پوشش داده می شوند.

۸-۲-۱ مصادیق طبقه‌بندی و رده بندی مراکز داده کشور

در ادامه مصادیق تعیین سطح یا رده یک مرکز داده بیان می شود. برای این منظور لازم است تا در زمان طراحی یک مرکز داده، با عنایت به این مصادیق و توسط کارشناسان خبره و با نظارت سازمان پدافند غیر عامل، این تعیین سطح انجام گیرد. طبیعی است پس از تعیین سطح یک مرکز داده، کلیه ملاحظات پدافند غیر عامل مربوط به آن سطح که در بخشهای بعدی سند آورده شده است، می بایست برای آن مرکز داده لحاظ گردند.

۱-۱-۲-۸ طبقه‌بندی داده ها و اطلاعات و تعیین سطح ضربه بالقوه

یکی از مصادیق تعیین سطح و رده مرکز داده یک سازمان، سطح طبقه بندی داده ها و اطلاعات آن سازمان می باشد. این طبقه‌بندی بر اساس ضربه احتمالی در اثر عدم امنیت آنها در هر یک از ابعاد امنیتی انجام می‌شود. در ابتدا ابعاد و اهداف امنیتی بیان شده، سپس سطوح ضربه تعریف و سپس بر مبنای آنها تعریف طبقه‌بندی داده‌ها ارائه می‌شود.

در این بخش ضربه بالقوه به سازمان یا کشور را در اثر عدم امنیت اطلاعات یا امنیت به سه رده تقسیم می شود:

- **سطح ضربه پایین (low) است اگر**: عدم محرمانگی، عدم صحت یا عدم دسترس‌پذیری ضربه محدودی بر عملیات یا دارایی‌های سازمان بگذارد.
- **سطح ضربه متوسط (moderate) است اگر**: عدم محرمانگی، عدم صحت یا عدم دسترس‌پذیری ضربه شدیدی بر بخشی از منابع کشور وارد کند.
- **سطح ضربه، بالا (high) است اگر**: عدم محرمانگی، عدم صحت یا عدم دسترس‌پذیری به امنیت ملی کشور لطمه وارد نماید.

لازم به ذکر است که مطابق با دستورالعمل‌های حفاظتی، سطوح محرمانگی داده‌ها و اطلاعات عبارتند از: عادی، محرمانه، خیلی محرمانه، سری و بکلی سری.

از این منظر، با توجه به ضربه بالقوه که عدم وجود هر یک از ابعاد امنیت ممکن است به سیستم وارد نمایند، داده‌ها و اطلاعات طبقه‌بندی می‌شود. سپس از این طبقه‌بندی برای تعیین سطح مرکز داده برای یک سازمانها استفاده خواهد شد. بدیهی است این تعیین سطح در زمان طراحی و پیاده سازی مراکز داده و با توجه به پارامترهای سازمان بهره برداری کننده انجام خواهد گردید.

۸-۲-۱-۲ تجمیع داده‌ها

یکی دیگر از مصادیق تعیین سطح و رده مرکز داده یک سازمان، میزان تجمیع داده ها و اطلاعات آن سازمان می باشد. برخی داده‌ها ممکن است به تنهایی حساسیت کمی داشته باشند ولی هنگامی که تجمیع شوند و حجم زیادی از آنها کنار هم جمع شود، حساسیت بالایی پیدا کنند. معمولا داده‌ها هنگامی که تجمیع شوند طبقه‌بندی بالاتری از طبقه‌بندی داده منفرد پیدا می‌کنند. با توجه به پیشرفت ابزارهای استنتاج و داده‌کاوی، ممکن از داده‌های انبوه اطلاعات مختلف و گوناگونی بتوان استخراج نمود. بنابراین لازم است بر حسب مورد، مالک داده‌ها درباره طبقه‌بندی تجمیع داده‌ها تصمیم بگیرد.

۸-۲-۱-۳ کاربرد مراکز داده

یکی دیگر از مصادیق تعیین سطح و رده مرکز داده یک سازمان، نوع کاربرد آن مرکز داده می باشد. مراکز داده ممکن است کاربرد نظامی داشته باشند که در این صورت حساسیت بالاتری خواهند داشت. یا اینکه غیر نظامی باشند. به عنوان مثال یک مرکز داده ممکن است در سطح یک وزارتخانه مورد استفاده قرار گیرد؛ یا یک مرکز داده برای ستاد کل مشترک نیروهای مسلح تاسیس شود. بنابراین کاربرد یک مرکز داده به عنوان نظامی یا غیر نظامی بودن یک مرکز داده، در تعیین سطح آن تأثیر دارد.

۸-۲-۱-۴ گستره کاربرد مراکز داده

مراکز داده در کشور ممکن است گستره‌های مختلفی از سطح کشور تا مراکز داده‌ای کوچک در سطح شهر داشته باشند. از این رو سطوح مختلف گسترهٔ مراکز داده به شرح زیر پیشنهاد می‌گردد:

۱. **مرکز داده کشوری (ملـی):** مرکـز داده‌ای اسـت کـه داده‌هـای موجـود در آن در سـطح کشوری بوده و یا استفاده کنندگان آن در سطح کشور پراکنده می‌باشند.

۲. **مرکز داده استانی:** مرکز داده‌ای است که داده‌های موجود در آن در سطح استانی بوده و یا استفاده کنندگان آن در سطح یک استان پراکنده می‌باشند.

۳. **مرکز داده شهری:** مرکز داده‌ای است که داده‌های موجود در آن در سطح شهری بوده و یا استفاده کنندگان آن در سطح یک شهر پراکنده می‌باشند.

در این راستا نکات زیر قابل توجه می‌باشد:

- در صورت خسارت دیدن یک مرکز داده کشـوری، ممکـن اسـت امنیـت ملـی یـک کشـور بـه مخاطره بیفتد و یا حتی در صورت نظامی بودن ضرر جبران‌ناپذیری به کشـور وارد شـود. از ایـن رو این مراکز داده را در سطح حیاتی دسته‌بندی می‌کنیم.
- در صورت خسارت دیدن یک مرکز داده با گستره استانی و با کاربرد غیر نظامی، ممکـن اسـت بخشی از منابع کشور لطمه بخـورد. از ایـن رو ایـن مراکـز داده را در سـطح حسـاس دسـته‌بندی می‌کنیم.
- در صورت خسارت دیدن یک مرکز داده با گستره شهری و با کاربرد غیر نظامی، ممکـن اسـت بخشی از منابع یک یا چند سـازمان لطمـه بخـورد. از ایـن رو ایـن مراکـز داده را در سـطح مهـم دسته‌بندی می‌کنیم.
- مراکز داده نظامی از نظر اهمیت یک سطح بالاتر از مرکز داده غیرنظامی با گسترهٔ مشابه دارند.

۸-۲-۱-۵ جمع بندی

با وجود آنکه نمی توان فرمولی واحد و جامع را برای تعیین سطح یک مرکز داده ارائه نمود، لذا بدیهی است این موضوع، در زمان ایجاد آن مرکز داده و با توجه به مصادیق بیان شده، توسط کارشناسان خبره این حوزه تعیین خواهد شد.

۸-۳ مراجع

[۱] اسناد بالادستی سازمان پدافند غیر عامل کشور

۹ فصل نهم: تهدیدات مراکز داده و ملاحظات پدافند غیر عامل سطح میانی

فصل نهم:

تهدیدات مراکز داده و

ملاحظات پدافند

غیر عامل سطح میانی

۹-۱ مقدمه

در این بخش کنترلهای لازم در خصوص ملاحظات پدافند غیر عامل مراکز داده متناسب با سطح مراکز داده (مهم، حساس و حیاتی) بیان گردیده است. همان طور که گفته شد، روش کار بدین صورت بوده است که با برشمردن تهدیدهای مراکز داده، با بررسی و انتخاب راهکارهای مناسب در قالب کنترل‌های فنی پیشنهادی با توجه به شرایط ملی و بومی کشور، موارد لازم بیان گردیده است. این کنترلها برای تهدیدات مربوط به مراکز داده که در ۳ دسته کلی "تهدیدات جنگ و مخاصمات بین الملل"، "تهدیدات امنیتی" و "تهدیدات محیطی و طبیعی" دسته بندی شده اند، بیان گردیده است.

در ادامه به طور مفصل به این تهدیدات و همچنین راهکارهای متناسب با آنها برای سطوح مختلف مراکز داده پرداخته می شود:

۹-۲ تهدیدات مراکز داده با رویکرد پدافند غیر عامل

در این بخش لیست تهدیدات شناسایی شده که مراکز داده امروزی را مورد هدف قرار داده را مورد توجه قرار داده و در ادامه در بخش‌های بعدی بسته به نوع مرکز داده (مهم، حساس و حیاتی) به ارائه کنترل‌های لازم در جهت کاهش مخاطرات ناشی تهدیدات به مراکز داده می‌پردازیم.

جدول ۱. تهدیدات مراکز داده با رویکرد پدافند غیر عامل

ردیف	تهدید	نوع مرکز داده
۱	اختلال الکترونیکی و الکتریکی	تهدیدات ناشی از جنگ (اطلاعات و فیزیکی) و مخاصمات بین المللی
۲	کدهای مخرب و بدافزارها(Malwares)	تهدیدات ناشی از جنگ (اطلاعات و فیزیکی) و مخاصمات بین المللی
۳	دسترسی غیرمجاز از راه دور	تهدیدات ناشی از جنگ (اطلاعات و فیزیکی) و مخاصمات بین المللی
۴	وقفه در کار	تهدیدات ناشی از جنگ (اطلاعات و فیزیکی) و مخاصمات بین المللی
۵	جاسوسی	تهدیدات ناشی از جنگ (اطلاعات و فیزیکی) و مخاصمات بین المللی
۶	حملات تروریستی سایبری(هکرها)	تهدیدات ناشی از جنگ (اطلاعات و فیزیکی) و مخاصمات بین المللی

۷	دسترسی غیرمجاز به اطلاعات	تهدیدات ناشی از جنگ (اطلاعات و فیزیکی) و مخاصمات بین المللی
۸	دسترسی غیرمجاز به شبکه	تهدیدات ناشی از جنگ (اطلاعات و فیزیکی) و مخاصمات بین المللی
۹	دسترسی غیرمجاز به سیستم‌عامل	تهدیدات ناشی از جنگ (اطلاعات و فیزیکی) و مخاصمات بین المللی
۱۰	دسترسی غیرمجاز به برنامه‌های کاربردی	تهدیدات ناشی از جنگ (اطلاعات و فیزیکی) و مخاصمات بین المللی
۱۱	دسترسی غیر مجاز به اطلاعات یا سیستم‌های حین مبادله با نهادهای خارج از مرکز داده	تهدیدات ناشی از جنگ (اطلاعات و فیزیکی) و مخاصمات بین المللی
۱۲	پردازش‌های اطلاعاتی غیر مجاز	تهدیدات ناشی از جنگ (اطلاعات و فیزیکی) و مخاصمات بین المللی
۱۳	تغییر غیرمجاز، از دست دادن یا سوءاستفاده از اطلاعات در برنامه‌های کاربردی	تهدیدات ناشی از جنگ (اطلاعات و فیزیکی) و مخاصمات بین المللی
۱۴	حمله فیزیکی، هسته‌ای و اتمی	تهدیدات ناشی از جنگ (اطلاعات و فیزیکی) و مخاصمات بین المللی
۱۵	بمب گذاری یا انفجار	تهدیدات ناشی از جنگ (اطلاعات و فیزیکی) و مخاصمات بین المللی
۱۶	حوادث شیمیایی	تهدیدات ناشی از جنگ (اطلاعات و فیزیکی) و مخاصمات بین المللی
۱۷	جنگ الکترومغناطیسی	تهدیدات ناشی از جنگ (اطلاعات و فیزیکی) و مخاصمات بین المللی
۱۸	ارگانیزم ها (ویروس، باکتری و...)	تهدیدات ناشی از جنگ (اطلاعات و فیزیکی) و مخاصمات بین المللی
۱۹	دسترسی غیر مجاز به سیستم ها، تجهیزات و منطقه فیزیکی	تهدیدات ناشی از جنگ (اطلاعات و فیزیکی) و مخاصمات بین المللی
۲۰	دسترسی غیر مجاز به رسانه‌های ذخیره‌سازی اطلاعات	تهدیدات ناشی از جنگ (اطلاعات و فیزیکی) و مخاصمات بین المللی
۲۱	دسترسی فیزیکی غیرمجاز به بستر انتقال داده‌ها	تهدیدات ناشی از جنگ (اطلاعات و فیزیکی) و مخاصمات بین المللی
۲۲	عدم سازگاری با فن‌آوری‌های مدرن جنگ الکترونیک	تهدیدات ناشی از جنگ (اطلاعات و فیزیکی) و مخاصمات بین المللی
۲۳	تهدید ناشی از عدم سازگاری با سیستم‌های مدرن اطلاعات عملیات	تهدیدات ناشی از جنگ (اطلاعات و فیزیکی) و مخاصمات بین المللی
۲۴	تهدید ناشی از عدم سازگاری با فن آوری‌های مدرن جنگ متحرک	تهدیدات ناشی از جنگ (اطلاعات و فیزیکی) و مخاصمات بین المللی
۲۵	آسیب یا سرقت (الکترونیکی)	تهدیدات ناشی از جنگ (اطلاعات و فیزیکی) و مخاصمات بین المللی
۲۶	آسیب یا سرقت (فیزیکی)	تهدیدات ناشی از جنگ (اطلاعات و فیزیکی) و مخاصمات بین المللی
۲۷	اختلال در ارتباطات شبکه	تهدیدات ناشی از جنگ (اطلاعات و فیزیکی) و مخاصمات بین المللی
۲۸	اختلال در سیستم برق	تهدیدات ناشی از جنگ (اطلاعات و فیزیکی) و مخاصمات بین المللی
۲۹	قرار دادن کشور در موقعیت جنگ تمام عیار اطلاعاتی	تهدیدات ناشی از جنگ (اطلاعات و فیزیکی) و مخاصمات بین المللی
۳۰	تهدید ناشی از تحریم فن آوری های پیشرفته خارجی	تهدیدات ناشی از جنگ (اطلاعات و فیزیکی) و مخاصمات بین المللی
۳۱	وابستگی به خارج از کشور در بخش تعمیر و نگهداری	تهدیدات ناشی از جنگ (اطلاعات و فیزیکی) و مخاصمات بین المللی
۳۲	وابستگی به تولیدات سخت افزاری و نرم افزاری خارجی	تهدیدات ناشی از جنگ (اطلاعات و فیزیکی) و مخاصمات بین المللی
۳۳	تغییر سریع فن آوری (در حوزه جنگ سایبر)	تهدیدات ناشی از جنگ (اطلاعات و فیزیکی) و مخاصمات بین المللی
۳۴	جهانی شدن	تهدیدات ناشی از جنگ (اطلاعات و فیزیکی) و مخاصمات بین المللی

۳۵	زیرساخت‌های عمده جهانی نظیر اینترنت	تهدیدات ناشی از جنگ (اطلاعات و فیزیکی) و مخاصمات بین المللی
۳۶	حملات مختل کننده خدمات	تهدیدات ناشی از جنگ (اطلاعات و فیزیکی) و مخاصمات بین المللی
۳۷	جنگ روانی دشمن	تهدیدات ناشی از جنگ (اطلاعات و فیزیکی) و مخاصمات بین المللی
۳۸	تغییر هویت اطلاعات درحال گذر	تهدیدات ناشی از جنگ (اطلاعات و فیزیکی) و مخاصمات بین المللی
۳۹	دسترسی غیرمجاز به اطلاعات	تهدیدات ناشی از جنگ (اطلاعات و فیزیکی) و مخاصمات بین المللی
۴۰	ناآرامی‌های اجتماعی	تهدیدات ناشی از جنگ (اطلاعات و فیزیکی) و مخاصمات بین المللی
۴۱	ورود و خروج غیر مجاز افراد	تهدیدات امنیتی
۴۲	عدم رویکرد مداوم برای مدیریت حوادث امنیتی	تهدیدات امنیتی
۴۳	عدم اصلاح و بازیابی پس از حوادث امنیتی	تهدیدات امنیتی
۴۴	ناامنی یا نادرستی در عملیات پردازش اطلاعات	تهدیدات امنیتی
۴۵	عدم امنیت در تعامل با طرفهای ثالث	تهدیدات امنیتی
۴۶	خطاهای سیستم	تهدیدات امنیتی
۴۷	برون‌سپاری خدمات و پردازش اطلاعات	تهدیدات امنیتی
۴۸	عدم بکارگیری نرم‌افزارهای کدباز	تهدیدات امنیتی
۴۹	نقض صحت[1] و دسترس‌پذیری اطلاعات و سیستم‌های پردازش اطلاعات	تهدیدات امنیتی
۵۰	عدم حفاظت اطلاعات در شبکه‌ها	تهدیدات امنیتی
۵۱	دسترسی غیر مجاز کاربر	تهدیدات امنیتی
۵۲	عدم در نظر گرفتن امنیت در سیستم‌های اطلاعاتی به عنوان یک بخش اصلی	تهدیدات امنیتی
۵۳	نقض محرمانگی یا صحت اطلاعات در اثر عدم استفاده یا استفاده نادرست از رمزنگاری	تهدیدات امنیتی
۵۴	عدم اطمینان از امنیت فایل سیستم ها	تهدیدات امنیتی
۵۵	نقض امنیت اطلاعات و نرم‌افزارهای کاربردی سیستم‌عامل	تهدیدات امنیتی
۵۶	عدم مدیریت آسیب‌پذیری‌های فنی	تهدیدات امنیتی
۵۷	عدم رعایت قوانین	تهدیدات امنیتی
۵۸	عدم وجود مدیریت یکپارچه امنیت اطلاعات	تهدیدات امنیتی
۵۹	عدم سازگاری با خط مشی‌ها	تهدیدات امنیتی
۶۰	فقدان نظام مدیریت امنیت اطلاعات	تهدیدات امنیتی
۶۱	استخدام یا به کارگماری افراد نامناسب	تهدیدات امنیتی
۶۲	عدم آگاهی نیروهای انسانی از مسوولیتها و تعهدات	تهدیدات امنیتی

[1] Integrity

۶۳	تهدیدهای مربوط به تغییر شغل یا انفصال از خدمت کارکنان و پیمانکاران	تهدیدات امنیتی
۶۴	دسترسی‌های غیرمجاز طرفهای خارج مرکز داده	تهدیدات امنیتی
۶۵	عدم تجهیز به سیستم مدیریت بحران و شرایط اضطرار	تهدیدات امنیتی
۶۶	فقدان یک سیستم هشداردهنده سریع و به موقع	تهدیدات امنیتی
۶۷	عدم بکارگیری سازه‌های امن و پایدار	تهدیدات امنیتی
۶۸	تولید اطلاعات غلط و نامطمئن	تهدیدات امنیتی
۶۹	عدم بهره مندی از مراکز احتیاط (Backup) امن، ایمن و پایدار	تهدیدات امنیتی
۷۰	عدم بکارگیری خطوط ارتباطی مطمئن و پایدار	تهدیدات امنیتی
۷۱	اتصالات ناامن به شبکه‌های اینترنت و اینترانت و فیبر نوری	تهدیدات امنیتی
۷۲	عدم پیش‌بینی برق پشتیبان	تهدیدات امنیتی
۷۳	عدم وجود نیروی انسانی متخصص لازم	تهدیدات امنیتی
۷۴	عدم وجود آموزش امنیتی کافی	تهدیدات امنیتی
۷۵	اشتباهات و غفلت‌ها مانند عدم بکارگیری صحیح تجهیزات، عدم نصب صحیح نرم‌افزارها و برنامه‌های کاربردی، سهل انگاری	تهدیدات امنیتی
۷۶	عدم وجود کنترل روی قوانین	تهدیدات امنیتی
۷۷	اتکا قابل ملاحظه به سیستم‌های ارتباطی بی‌سیم و ماهواره غیر امن	تهدیدات امنیتی
۷۸	عدم سازگاری با سیستم اطلاعات جغرافیایی (GIS)	تهدیدات امنیتی
۷۹	زلزله	تهدیدات محیطی و طبیعی
۸۰	آتش	تهدیدات محیطی و طبیعی
۸۱	طوفان و صاعقه	تهدیدات محیطی و طبیعی
۸۲	سیل	تهدیدات محیطی و طبیعی
۸۳	رطوبت و دما	تهدیدات محیطی و طبیعی
۸۴	دود	تهدیدات محیطی و طبیعی
۸۵	سقوط اجسام	تهدیدات محیطی و طبیعی
۸۶	تداخل الکترومغناطیسی امواج	تهدیدات محیطی و طبیعی
۸۷	مشکلات تأسیساتی (آب ،گاز، برق، تلفن)	تهدیدات محیطی و طبیعی
۸۸	مواد پرخطر	تهدیدات محیطی و طبیعی
۸۹	تشعشعات رادیواکتیو	تهدیدات محیطی و طبیعی
۹۰	گرد وغبار و مه	تهدیدات محیطی و طبیعی

۳-۹ ملاحظات پدافند غیر عامل برای تهدیدات مختلف

در این بخش، ملاحظات پدافند غیر عامل به تفکیک هر تهدید برای مراکز داده مهم، حساس و حیاتی بیان شده است. لازم به ذکر است که مراکز داده حساس، علاوه بر کنترلهای مراکز داده مهم می بایست کنترلهای ذکر شده برای مراکز داده حساس را نیز لحاظ نمایند. به همین ترتیب، مراکز داده حیاتی، علاوه بر کنترلهای ذکر شده برای مراکز داده مهم و حساس، می بایست کنترلهای ذکر شده برای مراکز داده حیاتی را نیز لحاظ نمایند.

جدول ۲. ملاحظات پدافند غیرعامل[1] برای تهدیدات مختلف

ردیف	تهدید	نوع مرکز داده	شرح کنترل
۱	اختلال الکترونیکی و الکتریکی	مهم	• ایجاد اتصال زمین برای تجهیزات به منظور انتقال بار الکتریکی اضافی • تجهیزات باید از افت جریان برق یا هر اختلالی که بر اثر عدم پشتیبانی تأسیسات بوجود می‌آید، حفاظت شوند. (A.9.2.2) • تجهیزات محافظ جهت جلوگیری از عملکرد اعوجاج و امواج الکترونیکی و الکتریکی • تجهیزات محافظ ولتاژ به منظور جلوگیری از تغییرات و ضربه های ولتاژ برق • بکارگیری سیستم برق اضطراری مجهز به مانیتور جهت مشاهده وضعیت برق تغذیه کننده سیستم ها • محافظت در مقابل نقایص منبع تغذیه • آموزش کارکنان شاغل در مرکز جهت رفع اشکالات مربوط به اختلال های الکترونیکی و الکتریکی
		حساس	• بکارگیری ژنراتور برق جهت تولید برق در زمان وقوع اختلال • استفاده از تجهیزات جلوگیری کننده از اختلال الکترونیکی

[1] شماره های انتهای هر کنترل امنیتی، ارجاع به شماره کنترل در استاندارد ISO/IEC 27001:2005 می باشد. در برخی موارد از کنترلهای استاندارد NIST SP-800-30 نیز استفاده شده است که دراین صورت شماره مربوطه ذکر شده است.

		حیاتی	• ایجاد یک مسیر برق غیر فعال برای زمان بوجود آمدن اختلال الکتریکی و استفاده از آن
۲	کدهای مخرب و بدافزارها (Malwares)	مهم	• کنترل‌های کشف، جلوگیری، و ترمیم به منظور محافظت در برابر کدهای مخرب، به همراه روال‌های مناسب آگاهی کاربران باید پیاده‌سازی شوند. (A.10.4.1) • جایی که استفاده از کد سیار مجاز است، پیکربندی آنها باید به گونه‌ای باشد که اطمینان از تطابق کدهای سیار مجاز با خط مشی های امنیتی تعریف شده، حاصل شود و باید از اجرای کد سیار غیر مجاز جلوگیری شود. (A.10.4.2)
		حساس و حیاتی	• استفاده از نرم‌افزارهای بومی جهت کشف بدافزارها • ایجاد محدودیت‌هایی در جهت ممانعت از دریافت کدهای اجرایی از سوی افراد • مسدود کردن درگاه‌های غیرضروری سیستم به منظور جلوگیری از امکان سوء استفاده به عنوان درهای پشتی
۳	دسترسی غیرمجاز از راه دور	مهم، حساس و حیاتی	• باید یک خط مشی رسمی اِعمال شده و روشهای مناسب امنیتی جهت محافظت در برابر ریسکهای استفاده از کامپیوترهای سیار و امکانات ارتباطات باید به کار گرفته شوند. (A.11.7.1) • باید یک خط مشی، برنامه های عملیاتی و روش های اجرایی توسعه یافته برای فعالیتهای کاری از راه دور اجرا شوند.(A.11.7.2)
۴	وقفه در کار	مهم و حساس	• فرآیند تنظیم شده باید توسعه یافته و باید جهت استمرار کسب و کار در کل سازمان نگهداری شود که اشاره به الزامات امنیتی اطلاعات مورد نیاز برای استمرار کسب و کار سازمان را دارد. (A.14.1.1) • رخدادهایی که ممکن است باعث وقفه در کار مرکز داده شوند باید به همراه احتمال و خسارت ناشی از وقفه و دیگر پیامدهای امنیتی مشخص شوند. • باید برای نگهداری یا بازیابی عملیات و اطمینان از دسترس‌پذیری در سطح مورد نظر و در زمان مورد نظر برنامه‌ریزی شود. • باید یک چارچوب کلی برای طرح‌های استمرار کسب و کار تدوین شود تا طرح‌ها سازگار بوده و نیازمندیهای امنیتی را به درستی مشخص کنند. همچنین اولویت‌های آزمون و ارزیابی را مشخص نماید. • طرحهای تداوم کسب و کار باید آزمایش شده و به طور منظم ارتقاء یابند تا از به روز بودن و اثر بخشی آنها اطمینان حاصل شود.

			(A.14.1.5)
		حیاتی	• هر طرحی که احتمال ایجاد وقفه در کسب و کار را تقویت می کند می‌بایستی برکنار و راه‌کار جایگزینی ارائه گردد. • عوامل ایجاد وقفه شناسایی گردند و ریسک حضور این عوامل در طراحی مرکز داده در نظر گرفته شود.
۵	جاسوسی	مهم	• هر مورد از تجهیزات که شامل ذخیره رسانه است، قبل از کنار گذاری باید به منظور حصول اطمینان از عدم وجود اطلاعات خاص بررسی شود. اینگونه اطلاعات و نرم افزارهای ثبت شده کنار گذاشته شده باید قبل از کنار گذاری در صورت نیاز بر روی رسانه ای دیگر ثبت گردد. • بکارگیری سیستم تشخیص هویت و شناسایی افراد به صورت جامع • جلوگیری از عکاسی ، فیلمبرداری و ضبط صدا • ثبت تمام ورود و خروج ها • آموزش ضد جاسوسی به کارکنان • تهیه نقشه تأسیسات و قابلیت دسترسی آنها برای افراد مجاز • تهیه لیست تجهیزات و قابلیت دسترسی آنها برای افراد مجاز
		حساس	• جداسازی مکانهای فعالیت افراد
		حیاتی	• محرمانگی مسیرهای فیزیکی انتقال اطلاعات و انرژی
۶	حملات تروریستی سایبری(هکرها)	مهم، حساس و حیاتی	• تهیه داده‌های پشتیبان در فواصل زمانی مناسب به منظور جلوگیری از احتمال بروز خرابی در تمامیت و صحت داده‌ها • ردگیری و تهیه سوابق دقیق از عملیات صورت گرفته از سوی هر کاربر به منظور مطالعه و شناسایی رفتار و اقدامات مشکوک صورت گرفته • کاهش سطح تماس سرویس‌های مرکز داده به متقاضیان • پرهیز از افشاء ماهیت و رفتار درونی سیستم، نرم افزار/ سخت‌افزار و مولفه‌های نرم‌افزاری به کار رفته در آن به سایرین • اتخاذ سیاست امنیتی مثبت به عنوان یک سیاست امنیتی بازدارنده • استفاده از مولفه‌های امنیتی فعال چون دروازه‌های آتش در محل ورودی ترافیک به شبکه داخلی مرکز داده • به کارگیری سیستم های تشخیص نفوذ مبتنی بر رفتار و امضاء جهت تشخیص به موقع ناهنجاری‌های رفتاری کاربران • آموزش پرسنل به استفاده از کلمات عبور طولانی و پیچیده و تغییر کلمات عبور به طور ادواری

			• به کارگیری تیمی از متخصیص نفوذ به منظوری شناسایی حفره‌های امنیتی موجود بخصوص در سطح نرم‌افزار و اتخاذ راه‌کارهایی جهت انسداد این حفره‌ها • غیرفعال کردن سرویس‌ها و مولفه‌های عمومی غیر قابل استفاده در سطح مرکز داده • استفاده از مولفه‌های نرم‌افزاری اختصاصی (in-house) به جای استفاده از مولفه‌های عمومی؛ بسیاری ازاین مولفه‌های به دلیل قابل دسترس بودن ضعف‌های امنیتی آنان برای همگان شناخته شده است.
۷	دسترسی غیرمجاز به اطلاعات	مهم، حساس و حیاتی	• خط مشی کنترل دسترسی باید پایه‌ریزی و مستند سازی شده و بر اساس کسب و کار و الزامات امنیتی برای دسترسی بازنگری شود. (A.11.1.1)
۸	دسترسی غیرمجاز به شبکه	مهم و حساس	• برای کاربران فقط دسترسی به سرویس هایی باید مهیا شوند که بطور مشخص اجازه استفاده از آنها را دارند.(A.11.4.1) • روشهای مناسب باید برای کنترل دسترسی توسط کاربران بیرونی مورد استفاده قرار بگیرد. • دسترسی فیزیکی و منطقی به درگاهها (پورت‌ها) باید تحت کنترل باشد. • برای شبکه های مشترک به خصوص آنهایی که به خارج از مرزهای سازمانی کشیده شدند ظرفیت کاربران محدود شود. • برای حصول اطمینان از اینکه ارتباطات کامپیوتری و جریان اطلاعات، خط مشی کنترل دسترسی را نقض نکند باید کنترل مسیریابی برای شبکه ها اجرا شود.(A.11.4.7)
		حیاتی	• حداکثر تعداد اتصال یا نشست‌های همزمان به یک سیستم باید کنترل و محدود شود. این محدودیت توسط مدیر سیستم تعیین می‌شود. (NIST-AC-10) • مرکز داده باید از مکانیزم‌های خودکار برای تسهیل در پایش و کنترل روشهای دسترسی از راه دور استفاده نماید. (NIST-AC-17(1)) • مرکز داده باید از رمزنگاری برای فراهم کردن محرمانگی نشست‌های از راه دور استفاده نماید. (NIST-AC-27(2)) • مرکز داده همه دسترسی‌های از راه دور را از طریق یک نقطه کنترل دسترسی مدیریت شده، کنترل می‌نماید. (NIST-AC-27(3))
۹	دسترسی غیرمجاز به سیستم‌عامل	مهم، حساس و	• دسترسی به سیستم های عامل باید توسط فرآیند اجرایی امن

		حیاتی	(Logon) کنترل شوند.(A.11.5.1) • همه کاربران باید ID انحصاری برای استفاده شخصی خود داشته باشند و باید یک تکنیک مناسب تأیید، جهت اثبات ادعای ID کاربر انتخاب شود. • سیستم های تنظیم کلمه عبور باید دو سویه بوده و کیفیت کلمه عبور را اطمینان دهد. • استفاده از برنامه های کاربردی که توانایی کنترل کاربردها را داشته باشند به شدت تحت کنترل قرارداده شده و محدود شوند. • برای فراهم نمودن امنیت بیشتر برای کاربردهای دارای ریسک بالا، باید محدودیت هایی در زمان برقراری اتصال اعمال شود. (A.11.5.6)
۱۰	دسترسی غیرمجاز به برنامه‌های کاربردی	مهم، حساس و حیاتی	• دسترسی به اطلاعات و عملیات سیستمهای کاربردی توسط کاربران و کارکنان پشتیبانی باید طبق خط مشی کنترل دسترسی مشخص محدود گردد.(A.11.6.1) • سیستمهای حساس باید محیط کامپیوتری(محاسباتی) اختصاصی(مجزا) داشته باشند.(A.11.6.2)
۱۱	دسترسی غیر مجاز به اطلاعات یا سیستم‌های حین مبادله با نهادهای خارج از مرکز داده	مهم، حساس و حیاتی	• خط مشی تبادل رسمی، روش های اجرایی و کنترل ها جهت حفاظت از تبادل اطلاعات با استفاده از همه انواع امکانات ارتباطی باید در محل وجود داشته باشد.(A.10.8.1) • توافقات جهت مبادله اطلاعات و نرم افزار بین سازمان و طرفهای خارج از سازمان باید پایه ریزی و تدوین شوند. • رسانه های حاوی اطلاعات باید در مقابل دسترسی غیرمجاز، سوء استفاده یا انحراف در زمان انتقال به خارج از مرزهای فیزیکی سازمان، حفاظت شود. • خط مشی ها و روش های اجرایی جهت حفاظت از اطلاعات همراه با ارتباطات داخلی سیستمهای اطلاعاتی کسب و کار باید تدوین شده و دائما ارتقاء یابند.(A.10.8.5)
۱۲	پردازش‌های اطلاعاتی غیر مجاز	مهم	• الزامات ممیزی و فعالیتهای که شامل بررسی سیستم‌های عملیاتی است، برای کمینه کردن مخاطرات اختلال در فرایند کسب و کار، باید با دقت طرح‌ریزی و تصویب شوند.(A.15.3.1) • رکوردهای ممیزی مربوط به فعالیت‌های کاربران، وقایع استثنایی، و رویدادهای امنیتی باید تولید و نگهداری شوند. این رکوردها برای کمک به تفحصهای آتی و نظارت بر کنترل دسترسی کاربرد دارند. (A.10.10.1)

			• فرایند اجرایی برای استفاده از مراقبت امکانات پردازش اطلاعات باید پایه ریزی شده و نتایج نظارت فعالیتها باید به طور منظم بازنگری شوند. • امکانات ثبت کردن و ثبت اطلاعات باید در برابر دسترسی بدون مجوز و پنهانی حفاظت شود. • فعالیتهای مدیر و اپراتور سیستم باید ثبت شوند. • خطاها باید ثبت و تحلیل شده و اقدامات مناسب صورت بگیرد. • ساعت سیستمهای پردازش اطلاعات در سازمان یا حوزه امنیتی باید با زمان دقیق مرجع هماهنگ باشند.(A.10.10.6) • در صورت بروز خطا در ثبت رکوردهای ممیزی یا پر شدن ظرفیت محل ذخیره، باید هشدار مناسب به مدیر فنی مربوط داده شده و اقدام مقتضی (توقف ثبت، خاموش کردن سیستم، یا بازنویسی روی رکوردهای قدیمی) انجام شود. (NIST AU-5) • سیستم‌های اطلاعاتی باید مهر زمانی (timestamp) هر رویداد را مشخص نمایند. (NIST AU-8) • سیستم‌های اطلاعاتی باید از اطلاعات ممیزی و ابزارهای ممیزی در مقابل دسترسی غیرمجاز، تغییر یا حذف محافظت کنند. (NIST AU-9) (A.15.3.2)
		حساس	• هر سیستم اطلاعاتی باید امکان ثبت وقایع بیشتر و جزئی‌تر در رکوردهای ممیزی به همراه نوع، محل، و عامل آن فراهم کنند. (NIST AU-3(1)) • در صورتی که حجم رکوردهای ممیزی به ۷۵٪ ظرفیت محل ذخیره رسید، باید سیستم اطلاعاتی هشداری به مدیر سیستم بدهد. (NIST AU-5(1)) • سیستم‌های اطلاعاتی باید قابلیت تحلیل و خلاصه‌سازی رکوردهای ممیزی و تولید گزارش‌های مفید و قابل پیکربندی بر اساس انتخاب رویدادهای خاص را داشته باشند. (NIST AU-7, AU-7(1))
		حیاتی	• هر سیستم اطلاعاتی باید قابلیت مدیریت مرکزی محتوای رکوردهای ممیزی تولید شده توسط مولفه‌های مختلف سیستم را داشته باشد. (NIST AU-3(2)) • مرکز داده باید از مکانیزم‌های خودکار برای هشدار فوری به پرسنل امنیتی درباره فعالیت‌های غیرمعمول، استفاده نماید (NIST AU-6(2)) • سیستم‌های اطلاعاتی باید اطلاعات ممیزی خود را روی رسانه‌های سخت‌افزاری با قابلیت یکبار-نوشتن (write-once_) ثبت نمایند

			(مانند نوشتن روی CD یا چاپ روی کاغذ) (NIST AU-9(1))
۱۳	تغییر غیرمجاز، از دست دادن یا سوءاستفاده از اطلاعات در برنامه‌های کاربردی	مهم، حساس و حیاتی	• داده های ورودی برای سیستم کاربردی باید برای حصول اطمینان از صحت و مناسب بودن آنها، اعتبار سنجی شوند. (A.12.2.1) • باید در سیستم‌های کاربردی از وارسی‌های اعتبارسنجی به منظور کشف هر گونه خرابی داده استفاده شود. • الزامات برای اطمینان از درستی و حفاظت از صحت پیام در کاربردها باید مشخص شده و کنترل های مناسب باید مشخص و اجرا شوند. • داده های خروجی یک سیستم کاربردی باید به منظور اطمینان از درستی و مناسب بودن پردازش اطلاعات ذخیره شده با شرایط مربوطه مورد تعیین اعتبار قرار گیرد.(A.12.2.4)
۱۴	حمله فیزیکی، هسته‌ای و اتمی	مهم	• استفاده از تکنیکهای استتار بمنظور عدم تشخیص مکان مرکز داده توسط دشمن • استفاده از تکنیکهای اختفا بمنظور عدم تشخیص مکان مرکز داده توسط دشمن • استفاده از تکنیک‌های فریب دشمن بمنظور عدم تشخیص مکان واقعی مرکز داده • تهیه اطلاعات پشتیبان و ارسال آنان به نقطه‌ای خارج از فضای فیزیکی مرکز داده بمنظور حفظ داده ها و اطلاعات • ایجاد یک مرکز داده پشتیبان Offline در محل فیزیکی دیگر بمنظور سرویس دهی در صورت عدم امکان سرویس دهی توسط مرکز اصلی • تربیت تیم های تخصصی بمنظور استفاده جهت ترمیم آسیب ها در شرایط اضطرار
		حساس	• مکان یابی محل فیزیکی مناسب بمنظور ایجاد مرکز داده و استفاده از منابع طبیعی نظیر کوه برای این منظور • ایجاد یک مرکز داده پشتیبان فعال (Active) در محل فیزیکی دیگر بمنظور سرویس دهی در صورت عدم امکان سرویس دهی توسط مرکز اصلی • ایجاد سازه مرکز داده بصورت زیر زمینی و در عمق زمین
		حیاتی	• ایجاد یک مرکز داده پشتیبان فعال (Active)و یک مرکز داده Offline در محل های فیزیکی دیگر بمنظور سرویس دهی در صورت عدم امکان سرویس دهی توسط مرکز اصلی

			• پیش بینی تجهیزات لازم بمنظور معدوم ساختن اطلاعات حیاتی در صورت دسترسی دشمن به تأسیسات داخلی مراکز داده • استفاده از نیروهای نظامی و انتظامی به منظور حفاظت فیزیکی از مرکز داده
۱۵	بمب گذاری یا انفجار	مهم	• کنترل تردد تجهیزات و بسته ها • طراحی و بکارگیری برنامه حفاظت فیزیکی در برابر آسیبهای ناشی از انفجار (A.9.1.4) • آموزش کارکنان شاغل در مرکز جهت رفع اشکالات و ایرادات بوجود آمده پس از انفجار • ارتباط مستقیم با متخصصان مربوط به خنثی سازی موارد منفجره
		حساس	• وجود تجهیزات و افراد خنثی کننده بمب
		حیاتی	• طراحی و ایجاد ساختمان مرکز داده بصورت ضد انفجار (حداقل برای بخش بسیار حیاتی مرکز داده)
۱۶	حوادث شیمیایی	مهم، حساس و حیاتی	• شیلد نمودن و عایق بندی جداره‌های و منافذ ورودی تأسیسات مراکز داده به منظور جلوگیری از نفوذ گازهای شیمیایی به داخل مراکز • استقرار تجهیزات ایمنی از قبیل ماسک و سایر تجهیزات موجود جهت جلوگیری از آسیب پرسنل • نگهداری پادزهرهای مختلف مربوط به انواع گازهای شیمیایی در جعبه کمک‌های اولیه به منظور انجام اقدامات اولیه به مصدومین
۱۷	جنگ الکترومغناطیسی	مهم	• مکان یابی نصب تجهیزات به منظور دوری از تجهیزات منشا تداخل مثل خطوط برق فشار قوی و خطوط با جریان بالا • آموزش کارکنان شاغل در مرکز جهت رفع اشکالات مربوط به اختلال های الکترومغناطیسی • رعایت استانداردهای مربوط به کابل کشی و فواصل مربوط به نصب کابل های انتقال داده ، برق و تلفن • استفاده از سیستم برق اضطراری برای مواقع خاص
		حساس	• بکارگیری حفاظهای امواج الکترومغناطیس بر روی بسترهای انتقال
		حیاتی	• پیش بینی شبکه طیف گسترده جهت جلوگیری از تداخل الکترومغناطیسی
۱۸	ارگانیزم ها (ویروس، باکتری و...)	مهم	• کنترل مواد خوراکی • کنترل محیط مرکز داده در خصوص گسترش موارد ارگانیزمی و اقدامات پیشگیرانه

			• آموزش کارکنان شاغل در مرکز جهت مقابله با موارد ارگانیزمی • ایجاد مرکز بهداشت و درمان به منظور رفع مشکلات با گستردگی محدود در مورد افراد شاغل
		حساس	• نمونه گیری و آزمایش مرتب موارد خوراکی و محیط
		حیاتی	• آزمایش طبی پرسنل به صورت شش ماهه
۱۹	دسترسی غیر مجاز به سیستم ها، تجهیزات و منطقه فیزیکی	مهم	• نقاط دسترسی نظیر نواحی بارگیری یا تحویل و دیگر نقاطی که احتمال ورود اشخاص فاقد صلاحیت وجود دارد کنترل شده و در صورت امکان از سایر بخش‌ها و تأسیسات منفک گردد. • تجهیزات باید به منظور کاهش ریسک های حاصل از تهدیدات و آسیبهای محیط و فرصتهای دسترسی غیرمجاز، حفاظت شوند.(A.9.2.1) • تجهیزات باید جهت حصول اطمینان از تداوم دسترسی و صحت بطور مناسب نگهداری شوند.(A.9.2.4) • تجهیزات، اطلاعات یا نرم افزار نباید بدون مجوز قبلی از محل خارج شوند.(A.9.2.7) • از سامانه های امنیتی (موانعی نظیر دیوارها، گیت های ورودی که با کارت کنترل می شود یا میزهای پذیرش آماده) بمنظور محافظت ناحیه هایی که شامل اطلاعات و سامانه های پردازش اطلاعات باشد، استفاده شود. (A.9.1.1) • نواحی امن بوسیله کنترل های ورودی مناسب جهت اطمینان از اینکه فقط پرسنل مجوز دار اجازه دسترسی داشته باشند محافظت شود. (A.9.1.2) • امنیت فیزیکی لازم برای دفاتر، اتاق ها و تاسیسات، طراحی و بکار گرفته شود.(A.9.1.3) • آموزش های لازم به کابران ارائه گردد.
		حساس و حیاتی	• بکارگیری سیستم حفاظت فیزیکی هوشمند پیرامونی (دوربین های مدار بسته) و هشدار دهنده
۲۰	دسترسی غیر مجاز به رسانه‌های ذخیره‌سازی اطلاعات	مهم	• باید دستورالعمل اجرایی برای مدیریت رسانه متحرک تدوین گردد. (A.10.7.1) • در صورت عدم نیاز به یک رسانه، باید به صورت امن و ایمن و طی یک فرآیند رسمی امحاء شود. (A.10.7.2) • مستند سازی سیستم باید در برابر دسترسی غیر مجاز حفاظت شود.(A.10.7.4)

			• رسانه های ذخیره سازی اطلاعات در محل امن نگهداری شوند. • اطلاعات رسانه قبل از تعویض ثبت گردد. (A.9.2.6)
		حساس و حیاتی	• وجود روش های اجرایی در محل برای مدیریت رسانه متحرک. (A.10.7.1) • در صورت عدم نیاز به یک رسانه، باید به صورت امن و ایمن و طی یک فرآیند رسمی امحاء شود. (A.10.7.2) • شبکه ها باید به منظور حفاظت در برابر تهدیدها و حفظ امنیت سیستمها و برنامه های کاربردی شبکه و داده های در حال انتقال، به طور مناسب مدیریت شوند.(A.10.6.1)
۲۱	دسترسی فیزیکی غیرمجاز به بستر انتقال داده‌ها	مهم	• لزوم حفاظت از بسترهای انتقال داده با تدوین سیاست نامه ای در خصوص نحوه دسترسی به آنها، مسئولیتهای افراد در این ارتباط و کد گذاری بسترها ی انتقال (NIST-MP-1) ، (NIST-MP-2) و (NIST-MP-3) • نحوه دسترسی، افراد مجاز و نحوه دریافت اطلاعات ورودی به بسترهای انتقال از هر نوع (اطلاعات الکترونیکی ، کاغذی و ...) بایستی مورد کنترل قرار گیرد. (NIST-MP-5) • حفاظت فیزیکی مناسب از کابلها و بکارگیری داکت • قرار دادن کانال انتقال داده‌ها در محیط غیرقابل دسترسی • کنترل بسترهای انتقال داده در زمان کنارگذاری و یا استفاده مجدد آنها.(NIST-MP-7)
		حساس	• استفاده از مکانیزم‌های بازدارنده روی کانال‌های انتقال داده به منظور کاهش احتمال دسترسی فیزیکی غیرمجاز
		حیاتی	• استفاده از چند کانال‌های ارتباطی به جای یک کانال ارتباطی و انتقال داده‌ها به صورت تصادفی از این کانال‌ها
۲۲	عدم سازگاری با فن‌آوری‌های مدرن جنگ الکترونیک	مهم، حساس و حیاتی	• جایگزینی فن‌آوری موجود با فن آوری قابل انطباق • استفاده از فن‌آوری‌های مبدل به منظور انطباق فن‌آوری موجود با فن‌آوری مدرن • تلاش برای بروزسازی فن‌آوری جدید با افزودن قابلیت‌های موجود در فن‌آوری‌های مدرن
۲۳	تهدید ناشی از عدم سازگاری با سیستم‌های مدرن اطلاعات عملیات	مهم، حساس و حیاتی	• استفاده از مولفه‌های مبدل به منظور ایجاد ارتباط و هماهنگی بین سیستم‌های کنونی اطلاعات عملیات و سیستم‌های نوین اطلاعات عملیات

۲۴	تهدید ناشی از عدم سازگاری با فن آوری‌های مدرن جنگ متحرک	مهم، حساس و حیاتی	• اتخاذ ملاحظاتی برای امکان جابجایی تجهیزات ذخیره سازی داده ها و اطلاعات در زمان بحران بمنظور استفاده در مرکز داده دیگر
۲۵	آسیب یا سرقت (الکترونیکی)	مهم	• آموزش کارکنان شاغل در مرکز جهت جلوگیری از سرقت الکترونیکی شناسه‌های هویت آنها • ملزم کردن کارکنان به تغییر کلمات عبور به صورت ادواری • استفاده از کلمات عبور پیچیده، طولانی غیرقابل حدس زدن
		حساس	• دسترسی به اطلاعات طبقه‌بندی شده باید لزوماً با عبور از مکانیسم‌های احراز هویت چندگانه امکان‌پذیر گردد. • کاهش کانال‌های الکترونیکی جهت دسترسی کاربران به منابع داده‌ای و سرویس‌های ارائه شده از سوی مرکز داده
		حیاتی	• قبل از دسترسی کاربر به اطلاعات و سرویس حیاتی حتماً شناسه هویت کاربر بار دیگر از وی درخواست گردد. • دسترسی به اطلاعات حیاتی مبتنی بر احراز هویت کاربران بر مبنای مشخصه‌های بیومتریک چون مشخصه عنبیه افراد، اثر انگشت، DNA و ... باشد. برای این منظور لازم است که دستگاه‌هایی با امکان تشخیص و دریافت این اطلاعات بر روی سیستم های کامپیوتری مستقر باشد.
۲۶	آسیب یا سرقت (فیزیکی)	مهم	• از تجهیزات باید به منظور کاهش ریسک های حاصل از تهدیدات و آسیبهای محیط و فرصتهای دسترسی غیرمجاز، متناسب با ماهیت هر یک حفاظت شود. • آموزش کارکنان شاغل در مرکز جهت جلوگیری از آسیب یا سرقت • از نقشه تأسیسات و موارد زیر بنایی در مکان مناسب (گاوصندوق یا محل مطمئن) حفاظت گردد. • ثبت ورود و خروج افراد • حفاظت از لیست تجهیزات • حفاظت از تجهیزات در زمان انتقال به تعمیرگاه و یا به هنگام تعمیر و رعایت تمهیدات مربوطه
		حساس	• جداسازی مکانهای فعالیت افراد دارای دسترسی های مختلف • رعایت اصول و سطوح طبقه بندی
		حیاتی	• رعایت محرمانگی مسیرهای فیزیکی انتقال اطلاعات و انرژی
۲۷	اختلال در ارتباطات شبکه	مهم	• استفاده از کانال‌های ارتباطی فاقد امکان اختلال • شیلد کردن کانال‌ها و تجهیزات ارتباطی و مکانهای قرار گرفتن این

			تجهیزات
		حساس و حیاتی	• استفاده از ارتباطات پشتیبان ناهمگون
۲۸	اختلال در سیستم برق	مهم، حساس و حیاتی	• بکارگیری سیستم توان پشتیبان • استخدام نیروهای متخصص برق به منظور انجام سرویس بلادرنگ در زمان بروز اختلال در سیستم برق • نگهداری سوخت کافی برای ژنراتورهای مولد برق برای شرایط خاص که امکان دسترسی به سوخت تا مدت‌ها وجود ندارد
۲۹	قرار دادن کشور در موقعیت جنگ تمام عیار اطلاعاتی	مهم، حساس و حیاتی	• الزام به قرار گرفتن در شرایط آماده باش کامل به منظور نظارت بر حسن اجرای تمامی کنترل‌های پیشنهادی (پدافند غیرعامل و امنیت)
۳۰	تهدید ناشی از تحریم فن آوری های پیشرفته خارجی	مهم، حساس و حیاتی	• تلاش جهت تسلط بر دانش و فناوری ها بمنظور بومی‌سازی فن‌آوری به منظور کاهش دغدغه‌های ناشی از تحریم فن‌آوری • تعامل با بخش های تحقیقاتی و پژوهشی کشور بمنظور بکرگیری حداکثری توان داخلی جهت تولید فناوری های لازم در داخل کشور داخل کشور
۳۱	وابستگی به خارج از کشور در بخش تعمیر و نگهداری	مهم و حساس	• انتقال دانش تعمیر و نگهداری به متخصصین بومی • استفاده از تکنولوژی‌های بومی موجود • جلوگیری از امکان دسترسی به داده‌های طبقه‌بندی شده و سوابق ذخیره شده بر روی سخت‌افزار و رسانه‌های ذخیره سازی مربوطه با تهیه نسخه پشتیبان و امحاء داده‌های موجود بر روی سیستم‌ها قبل از ارسال به مراکز تعمیر
		حیاتی	• قطع وابستگی به تعمیر و نگهداری با بومی سازی تکنولوژی مربوطه و انتقال دانش تعمیر و نگهداری به داخل کشور
۳۲	وابستگی به تولیدات سخت افزاری و نرم افزاری خارجی	مهم و حساس	• انتقال دانش تولید سخت افزارها و نرم افزارها به متخصصین بومی
		حیاتی	• استفاده حداکثری از محصولات بومی موجود • رعایت ملاحظات امنیتی در استفاده از محصولاتی که نمونه داخلی آنها وجود ندارد
۳۳	تغییر سریع فن آوری (در حوزه جنگ سایبر)	مهم	• تلاش جهت تسلط بر دانش و فناوری ها بمنظور بومی‌سازی فن‌آوری به منظور کاهش دغدغه‌های ناشی از تغییرات در فن‌آوری • آموزش نیروی متخصص و کارآمد جهت بهره گیری و انتقال فن‌آوری به داخل کشور
		حساس و حیاتی	• رعایت ملاحظات امنیتی در صورت لزوم استفاده از فناوریهای جدید و مشاوره با بخشهای متخصص آگاه و امین در کشور • تعامل با سازمانهای داخلی مرتبط با دانش و فناوریها بمنظور تسریع

			در روند بومی سازی فن آوری
۳۴	جهانی شدن	مهم، حساس و حیاتی	• تعامل با سازمانها و نهادهای مربوطه در داخل کشور بمنظور توجه به چالش‌های پیش روی جهانی شدن جهت ارائه راه‌کارهایی به منظور تطبیق با شرایط جدید • اتخاذ سیاست‌هایی در راستای تغییرات و تمهیدات ایجاد شده بمنظور اعمال در سازمان
۳۵	زیرساخت‌های عمده جهانی نظیر اینترنت	مهم	• استفاده کنترل شده از زیرساخت‌های جهانی با رعایت مسائل امنیتی و حفاظتی
		حساس و حیاتی	• استفاده از زیرساخت های بومی و قابل اتکاء و اعتماد • استفاده از این زیرساخت‌ها تنها برای اهداف خاص • استفاده از این زیرساخت‌های بصورت جداگانه (ایزوله) از زیرساختهای اصلی مرکز داده
۳۶	حملات مختل کننده خدمات	مهم، حساس و حیاتی	• بکارگیری سیستم‌هایی به منظور جلوگیری از نفوذ و شناسایی حملات مختل کتنده خدمات در صورت نفوذ، نظیر IDSها و فایروالهای بومی • شناسایی و ثبت الگوهای رفتاری حمله‌کنندگان داخلی به منظور جلوگیری از الگوهای رفتاری مشابه توسط سایر کاربران • پیش بینی و بکارگیری مراکز احتیاط وتشکیل تیمهای CERT در شرایط وقوع وقفه سرویس • تعیین حدمجاز بهره‌مندی کاربران از سرویس‌های ارائه شده • قرار دادن کاربران خاطی و غیرقابل اعتماد در لیست سیاه و ممانعت از سرویس‌دهی به آنان
۳۷	جنگ روانی دشمن	مهم	• برگزاری دوره های آگاهسازی برای کارکنان و کاربران در این خصوص
		حساس و حیاتی	• انتشار مستنداتی از اهداف خرابکارانه دشمن در تضعیف روحیه افراد که حاکی از بی‌پایه بودن گفته‌های دشمن دارد
۳۸	تغییر هویت اطلاعات درحال گذر	مهم، حساس و حیاتی	• استفاده از الگوریتم‌های رمزنگاری بومی، امضاهای دیجیتال در رمزنگاری اطلاعات متناسب با ماهیت و نوع سرویسها به منظور جلوگیری از افشا و امکان دستکاری اطلاعات در حال گذر • عدم استفاده از الگوریتم های رمزنگاری غیرمطمئن بمنظور رمزنگاری اطلاعات در حال گذر • استفاده از مکانیزمهای پنهان نگاری اطلاعات در شرایط لازم بمنظور انتقال اطلاعات مهم • عدم استفاده از کانال‌های ارتباطی بی‌سیم بدون در نظر گرفتن

			مکانیزمهای امنیتی مطمئن
۳۹	دسترسی غیرمجاز به اطلاعات	مهم	• استفاده از مکانیزمهای رمزنگاری اطلاعات و الگوریتم‌های رمزنگاری بومی بمنظور نگهداری اطلاعات بر روی رسانه های ذخیره سازی اطلاعات • عدم استفاده از الگوریتم های رمزنگاری غیرمطمئن بمنظور رمزنگاری اطلاعات • استفاده از مکانیزم‌های احراز هویت برای دسترسی به سرویسها و اطلاعات به منظور جلوگیری از دسترسی غیر مجاز به اطلاعات • پیش بینی تمهیدات امنیتی متناسب با سطح اهمیت و میزان تجمیع اطلاعات
		حساس و حیاتی	• استفاده از کانالهای ارتباطی خاص و غیر مشترک جهت تبادل اطلاعات با پیش بینی تمهیدات امنیتی • استفاده از مکانیزم‌های احراز هویت حداقل ۲ عاملی برای دسترسی به سرویسها و اطلاعات به منظور جلوگیری از دسترسی غیر مجاز به اطلاعات
۴۰	ناآرامی‌های اجتماعی	مهم	• محافظت بمنظور عدم افشای محل مرکز داده • حفاظت فیزیکی در برابر آسیبهای ناشی از آشوب های شهری بمنظور جلوگیری از ورود افراد متفرقه • محافظت بمنظور ذکر نشدن محل مرکز داده در نقشه های جغرافیایی
		حساس و حیاتی	• احداث مرکز داده در مکانهای فیزیکی غیر قابل دسترس مردم عادی
۴۱	ورود و خروج غیر مجاز افراد	مهم	• محیط های امنیتی (موانعی نظیر دیوارها، گیت های ورودی که با کارت کنترل می شود یا میزهای پذیرش آماده) باید بمنظور محافظت ناحیه هایی را که شامل اطلاعات و سامانه های پردازش اطلاعات باشد، استفاده شود. (A.9.1.1) • از سامانه های امنیتی (موانعی نظیر دیوارها، گیت های ورودی که با کارت کنترل می شود، دستگاههای X-Ray یا میزهای پذیرش آماده) بمنظور کنترل ورود و خروج افراد و تجهیزات همراه آنها استفاده شود. (A.9.1.1)

			• بکارگیری دوربین های کنترل تردد و سیستم حفاظت پیرامونی • اجبار در استفاده ازکارت شناسایی توسط افراد و کنترل آن توسط مبادی ذیربط • ثبت زمان ورود و خروج افراد • آموزش کارکنان
		حساس	• جداسازی مکانهای فعالیت افراد دارای طبقه بندی مختلف و رعایت اصول حیطه بندی
		حیاتی	• بازدید مرتب کارت شناسایی • استفاده از یونیفورم برای کارکنان • تعبیه یک محل ورود و خروج • بازدید کنندگان به همراه افراد مجوز دار تردد نمایند.
۴۲	عدم رویکرد مداوم برای مدیریت حوادث امنیتی	مهم	• باید مسئولیتهای مدیریت و فرآیندهای اجرایی جهت حصول اطمینان از پاسخ، سریع، موثر و مرتب به حوادث امنیتی اطلاعات پایه ریزی شود. (A.13.2.1) • باید مکانیزمهایی برای سنجش و پایش نوع، حجم، و هزینه حوادث امنیتی وجود داشته باشند. (A.13.2.2) • هر مرکز داده بایستی دارای مرکز عملیات امنیتی (SOC) بمنظور مانیتور و کنترل حوادث امنیتی باشد. • بعد از حادثه امنیتی اطلاعات، پی گیری در برابر فرد یا سازمانی صورت می گیرد که شامل اقدام قانونی (چه مدنی ، جزایی) است، شواهد باید جمع آوری و نگهداری شده و برای مطابقت با قوانین جهت مطرح شدن شواهد در یک دادرسی مربوطه ارائه شوند. (A.13.2.3)
		حساس	• سازمان بایستی میزان سرعت واکنش و کارآیی مکانیزمها در شرایط مورد نیاز را، آزمایش نماید. (NIST-IR-3)
		حیاتی	• سازمان بایستی با طراحی مکانیزمهای اتوماتیک، میزان سرعت واکنش و کارآیی آنرا در شرایط مورد نیاز، بهتر و موثرتر آزمایش نماید. ((NIST-IR-3 (1))
۴۳	عدم اصلاح و بازیابی پس از حوادث امنیتی	مهم، حساس و حیاتی	• رویدادهای امنیتی اطلاعات باید توسط مدیریت کانالهای مناسب تا حد امکان به سرعت گزارش شوند.(A.13.1.1) • مرکز داده بایستی دارای تیم CERT بمنظور ترمیم حوادث احتمالی در صورت وقوع، باشد. • تمام کارکنان پیمانکاران و مصرف کنندگان ثالث مصرف کننده سیستمها و خدمات اطلاعات باید ملزم شوند تا هرگونه ضعف

			امنیتی مشاهده شده و مشکوک در سیستمها و خدمات را به آن توجه کرده و گزارش دهند.(A.13.1.2)
۴۴	ناامنی یا نادرستی در عملیات پردازش اطلاعات	مهم، حساس و حیاتی	• روش های اجرایی عملیاتی باید مستند سازی و نگهداری شده، و برای همه کاربران که به آن نیاز دارند در دسترس باشد.(A.10.1.1) • تغییرات در امکانات پردازش اطلاعات و سیستمها باید کنترل شده باشند. • وظایف و حوزه های مسئولیت باید در راستای کاهش فرصت برای افراد غیرمجاز یا تغییرات ناخواسته یا سوء استفاده از دارایی های سازمان تفکیک شوند. • پیشرفت، آزمایش و امکانات عملیاتی باید تفکیک شوند تا دسترسی های غیرمجاز یا تغییرات سیستم عملیاتی را کاهش دهد.(A.10.1.4)
۴۵	عدم امنیت در تعامل با طرفهای ثالث	مهم، حساس و حیاتی	• استفاده از منابع باید مراقبت و تنظیم گردد. پیش بینی های لازم طبق الزامات ظرفیت آینده جهت حصول اطمینان از عملکرد سیستم ضروری است.(A.10.3.1) • باید معیار پذیرش سیستم های اطلاعاتی جدید، ارتقاء و نسخه های جدید پایه ریزی شده و آزمونهای مناسب سیستم ها در طی پیشرفت و قبل پذیرش انجام شوند.(A.10.3.2)
۴۶	خطاهای سیستم	مهم، حساس و حیاتی	• در استفاده از منابع باید مراقبت گردد. پیش بینی های لازم طبق الزامات ظرفیت آینده جهت حصول اطمینان از عملکرد سیستم ضروری است.(A.10.3.1) • باید معیار پذیرش سیستم های اطلاعاتی جدید، ارتقاء و نسخه های جدید باید پایه ریزی شده و آزمونهای مناسب سیستم ها در طی پیشرفت و قبل از پذیرش انجام شوند.(A.10.3.2)
۴۷	برون‌سپاری خدمات و پردازش اطلاعات	مهم و حساس	• الزامات امنیتی یک مرکز داده که مدیریت و کنترل تمامی یا بخشی از سیستم‌های امنیتی، شبکه‌ها و محیط‌های کاری آن به سازمانی دیگر واگذار می‌شود، باید در یک قرارداد که بین مرکز داده و طرف دیگر توافق شده است، دقیقا مشخص شود. • افراد و مراکز مجاز در حوزه های مرتبط با مراکز داده استعلام گردد.
		حیاتی	• برون‌سپاری خدمات مدیریتی، نگهداری و هرگونه خدمات دیگر در این مراکز داده به افراد و مراکز غیر مجاز ممنوع است.

۴۸	عدم بکارگیری نرم‌افزارهای کدباز	مهم، حساس و حیاتی	• استفاده از نرم‌افزارهای کدباز بجای استفاده از نرم‌افزارهای کدبسته در صورت وجود و پس از بررسی های امنیتی لازم بر روی آن • اتخاذ سیاست تولید کد بجای بکارگیری نرم‌افزارهای بین‌المللی موجود حتی از نوع کد باز و تعامل با مراکز و سازمانهای مجاز در این رابطه
۴۹	نقض صحت[1] و دسترس‌پذیری اطلاعات و سیستم‌های پردازش اطلاعات	مهم، حساس و حیاتی	• تهیه نسخه پشتیبان از اطلاعات و نرم افزار به طور مرتب و مطابق با خط مشی پشتیبان گیری • استفاده از مکانیزمهای جلوگیری از نقض صحت اطلاعات متناسب با نوع سرویسها و پردازشها • استفاده از مکانیزمهای جلوگیری از نقض دسترس پذیری اطلاعات متناسب با نوع سرویسها و پردازشها
۵۰	عدم حفاظت اطلاعات در شبکه‌ها	مهم، حساس و حیاتی	• شبکه ها باید به منظور حفاظت در برابر تهدیدها و حفظ امنیت سیستمها و برنامه های کاربردی شبکه و داده های در حال انتقال، به طور مناسب مدیریت شوند. • ویژگی امنیت، سطوح خدمات و الزامات مدیریت همه خدمات شبکه باید مشخص شده و لحاظ گردند. • امنیت شبکه در چند لایه مطابق مدلهای دفاع از عمق طراحی و پیاده سازی گردد.
۵۱	دسترسی غیر مجاز کاربر	مهم	• باید یک روش اجرایی رسمی ثبت و حذف کاربر در محل برای اعطا و لغو حق دسترسی به همه سیستم ها و سرویس های اطلاعاتی وجود داشته باشد.(A.11.2.1) • تخصیص و استفاده از مجوزها محدود و کنترل شود. • تخصیص کلمات عبور از طریق یک فرآیند مدیریتی رسمی کنترل شود. • مدیریت، حقوق دسترسی کاربران را در فواصل منظم، در راستای استفاده فرآیندهای اصلی، بازنگری کند. (A.11.2.4) • کاربران باید ملزم به رعایت نکات ایمنی در انتخاب و استفاده از کلمات عبور باشند.(A.11.3.1) • کاربران باید مطمئن باشند که تجهیزات بدون مراقبت از حفاظت مناسب برخوردارند. • سیاست میز مرتب برای کاغذها و رسانه ذخیره متحرک و سیاست صحنه نمایش واضح برای امکانات پردازش اطلاعات باید پذیرفته

[1] Integrity

			شود.(A.10.3.3) • هر سیستم اطلاعاتی باید محدودیت حداکثر ۳ ورود ناموفق را در طی ۳۰ دقیقه اعمال کند. پس از رسیدن تعداد ورودهای ناموفق به حد نصاب، سیستم باید قفل شده و به طور خودکار پس از یک ساعت به حالت عادی برگردد. (NIST-AC-7) • مرکز داده باید مطابق خط مشی‌های استفاده و اعمال کنترل‌های دسترسی، فعالیت‌های کاربران را مرور کرده و بر آنها نظارت داشته باشد. (NIST-AC-13)
		حساس	• سیستمها باید حسابهای کاربری موقتی و اضطراری را بلافاصله پس از اتمام کار غیرفعال نمایند.((NIST-AC-2(2) • هر سیستم اطلاعاتی باید پس از ۵ دقیقه عدم فعالیت کاربر، نشست وی را قفل نماید و دسترسی مجدد کاربر را منوط به طی مراحل احراز هویت و مجاز شناسی نماید. (NIST-AC-11) • هر سیستم اطلاعاتی باید پس از ۱۵ دقیقه عدم فعالیت کاربر، به طور کامل به نشست خاتمه دهد (log off نماید). (NIST-AC-12)
		حیاتی	• مرکز داده باید از مکانیزمهای خودکار مدیریت حسابهای کاربری سیستم‌ها استفاده نماید. ((NIST-AC-2(1) • همه سیستم‌های اطلاعاتی باید حساب کاربری بلااستفاده را [پس از مدت زمان مشخص شده در سیاست امنیت سازمان مربوط به مرکز داده] غیر فعال نمایند. ((NIST-AC-2(3) • سیستم اطلاعاتی باید پس از رسیدن تعداد ورودهای ناموفق به حد نصاب، به طور خودکار قفل شده و تنها توسط مدیر سیستم به حالت عادی برگردد. ((NIST-AC-7(1) • مرکز داده باید از مکانیزم‌های خودکار برای اطمینان از این که همه اعمال ایجاد، تغییر، غیرفعال‌سازی، و حذف بازرسی و به کاربران مقتضی اطلاع داده می‌شود، بهره بگیرند. ((NIST-AC-2 (4)
۵۲	عدم در نظر گرفتن امنیت در سیستم‌های اطلاعاتی به عنوان یک بخش اصلی	مهم، حساس و حیاتی	• هر گونه درخواست برای تهیه، خرید، یا تولید سیستم‌های اطلاعاتی باید صریحا نیازمندیها و الزامات امنیتی را نیز مشخص کند. • در تمامی بخشهای یک سیستم اطلاعاتی از تولید تا بهره برداری، امنیت بعنوان یک جزء انکار ناپذیر در نظر گرفته شود. • تشکیلات امنیتی و ساختار سازمانی لازم برای امنیت پیش بینی گردد.
۵۳	نقض محرمانگی یا صحت اطلاعات در اثر عدم استفاده یا	مهم، حساس و حیاتی	• برای حفاظت از اطلاعات باید یک خط مشی استفاده از کنترل های رمز نگاری توسعه پیدا کرده و اجرا شود.(A.12.3.1)

	استفاده نادرست از رمزنگاری		• مدیریت کلید باید جهت پشتیبانی از استفاده سازمان از تکنیکهای رمز نگاری تعبیه شود.(A.12.3.2)
۵۴	عدم اطمینان از امنیت فایل سیستم ها	مهم، حساس و حیاتی	• از سیستم فایلهای مطمئن استفاده گردد و در این راستا از مشاوره مجموعه های متخصص و مورد اعتماد بهره گرفته شود. • باید روش های اجرایی جهت کنترل نصب نرم افزار بر روی سیستمهای عامل تعبیه شوند.(A.12.4.1)
۵۵	نقض امنیت اطلاعات و نرم‌افزارهای کاربردی سیستم‌عامل	مهم و حساس	• هر گونه تغییر با استفاده از روش های اجرایی رسمی کنترل تغییرات کنترل شود.(A.12.5.1) • تغییرات در بسته های نرم افزار باید کم شده، به تغییرات لازم محدود شود و همه تغییرات باید شدیداً تحت کنترل باشند.(A.12.5.3) • از هر گونه نشست اطلاعات باید جلوگیری شود.(A.12.5.4) • توسعه و تغییر نرم افزار برون سپاری شده باید توسط مرکز داده نظارت شود.(A.12.5.5) • مرکز داده باید پیکربندی پایه و اولیه هر سیستم اطلاعاتی را تهیه و مستند ساخته و فهرستی از مولفه‌های سازگار سیستم تهیه نماید. • مرکز داده باید هر گونه تغییر در سیستم‌های اطلاعاتی را مستندسازی و کنترل نماید. این تغییرات باید ابتدا توسط مقام مسوول تایید شود. • مرکز داده باید تغییر دادن سیستم‌های اطلاعاتی را محدود به افراد مجاز نماید. • باید پیکربندی امنیتی سیستم‌های اطلاعاتی به نحوی باشد که بیشترین محدودیت را اعمال نماید و سازگار با نیازمندیهای عملیاتی و امنیتی سیستم‌ها شود.(NIST CM-6)
		حیاتی	• مرکز داده باید از روشهای خودکار برای اعمال محدودیت دسترسی در تغییر سیستم‌های اطلاعاتی استفاده نماید. • مرکز داده باید از روشهای خودکار برای مدیریت، اعمال و بررسی پیکربندی سیستم‌های اطلاعاتی بهره بگیرد.
۵۶	عدم مدیریت آسیب‌پذیری‌های فنی	مهم، حساس و حیاتی	• اطلاعات به موقع در مورد آسیب پذیری‌های فنی سیستمهای اطلاعاتی مورد استفاده باید کسب شده و اثر آنها بر مرکز داده بررسی شده و تدابیر مناسبی برای مقابله با آنها اتخاذ شود.(A.12.6.1)
۵۷	عدم رعایت قوانین	مهم، حساس و	• تمام الزامات مقرراتی، حقوقی و قراردادی و همه رویکرد سازمان

		حیاتی	برای تأمین این الزامات باید صریحاً مشخص، مستندسازی شده و برای هر سیستم اطلاعاتی سازمان ارتقاء داده شود.(A.15.1.1) • برای حصول اطمینان از انطباق با الزامات قانون گذاری، مقرراتی و قراردادی در استفاده مادی با توجه به ارتباط با حقوق مالکیت فکری یا استفاده اختصاصی محصولات نرم افزاری، روشهای اجرایی تدوین و اجرا شود.(A.15.1.2) • سوابق مهم باید در برابر مفقود شدن، تخریب و تحریف طبق قوانین قانونی، مقرراتی و قراردادی الزامات کسب و کار، محافظت شوند.(A.15.1.3) • از استفاده کاربران از امکانات پردازش اطلاعات بدون مجوز ممانعت به عمل آید.(A.15.1.5)
۵۸	عدم وجود مدیریت یکپارچه امنیت اطلاعات	مهم، حساس و حیاتی	• یک سند سیاست امنیتی توسط مدیریت مرکز داده تدوین و تصویب گردیده و منتشر گردد و بر حسب اقتضاء مورد تبادل نظر با تمام کارکنان قرار گیرد. • خط‌مشی های ذکر شده در سند سیاست امنیتی باید به طور منظم و نیز در مواردی که تغییرات مؤثری وجود داشته باشد، مورد بازنگری قرار گیرند تا از تداوم مناسب بودن خط‌مشی اطمینان حاصل شود. • فرم ها، اسناد و سیاست واکنش سریع مرکز داده شامل اهداف، محدوده، قوانین، مسؤلیتها و هماهنگی، همچنین مکانیزمهای کنترلی پیاده سازی، تولید و مرتبا مرور و به روز گردند.(NIST-IR-1)
۵۹	عدم سازگاری با خط مشی‌ها	مهم، حساس و حیاتی	• مدیران باید از اجرای صحیح تمام روش های اجرایی امنیت در حیطه مسئولیتشان برای دستیابی به تطابق با سند سیاست امنیتی و استانداردها، مطمئن شوند.(A.15.2.1) • سیستم های اطلاعاتی باید به طور منظم از نظر تطابق فنی با استانداردهای اجرایی امنیت مورد بررسی قرار گیرند.(A.15.2.2)
۶۰	فقدان نظام مدیریت امنیت اطلاعات	مهم،حساس و حیاتی	• مدیریت باید فعالانه از امنیت در سازمان با ساختار شفاف، تعهد آشکار، وظیفه صریح و قبول مسئولیتهای امنیت اطلاعات پشتیبانی کند. (A.6.1.1) • تشکیلات لازم و نیروی انسانی متخصص در زمینه امنی اطلاعات جذب یا تربیت گردند. • مسئولیت‌های حفاظت از هریک از دارایی‌های منفرد و انجام فرآیندهای امنیتی مشخص باید به طور شفاف تعریف شوند.(A.6.1.3) • برای استفاده از امکانات پردازش اطلاعات جدید، باید یک فرآیند

			صدور مجوز از طرف مدیریت پایه ریزی شود.(A.6.1.4) • باید همکاری مناسبی تحت مجوزهای قانونی، بین سازمانهای تنظیم کننده مقررات، تأمین‌کنندگان سرویسهای اطلاعاتی و اپراتورهای مخابراتی ایجاد و حفظ گردد.(A.4.1.7) • رویکرد سازمان برای مدیریت امنیت اطلاعات و اجرای آن (مثال: اهداف کنترل، کنترل ها، سیاستها، فرآیندها، روش های اجرایی امنیت اطلاعات) بصورت مستقل با طرح ریزی دوره ای یا هنگامی که تغییرات مهم در اجرای امنیت رخ می دهد، بازنگری شود.(A.6.1.8)
۶۱	استخدام یا به کارگماری افراد نامناسب	مهم، حساس و حیاتی	• نقشهای امنیتی و مسوولیتهای کارکنان، پیمانکاران و کاربران ثالث باید طبق سند سیاست امنیت اطلاعات مرکز داده مشخص و مستند سازی گردند. • بررسی سوابق همه افراد آماده استخدام، پیمانکاران و کاربران ثالث، باید طبق قوانین، اصول و قوانین مربوط و متناسب با الزامات کسب و کار طبقه‌بندی اطلاعات در دسترس باشد. • به عنوان بخشی از تعهد قراردادی افراد، کارکنان، پیمانکاران و کاربران ثالث باید طبق قوانین، اصول و مقررات مربوطه و متناسب با الزامات کسب و کار طبقه بندی اطلاعات در دسترسی را مدنظر داشته و به ریسک‌های ناشی از افشاء اطلاعات و دسترسی غیرمجاز دیگران واقف باشند.
۶۲	عدم آگاهی نیروهای انسانی از مسوولیتها و تعهدات	مهم	• مدیریت باید از کارکنان و پیمانکاران و کاربران ثالث بخواهد تا امنیت را طبق خط‌مشی‌های تدوین شده و رویه‌های مرکز داده بکار برند. • همه کارکنان سازمان (مرتبط با مرکز داده)، پیمانکاران و کاربران ثالث، باید آگاهی و آموزش مناسب و خط مشی های به روز شده و روشهای اجرایی که به عملکرد شغلی آنها مربوط می شود، را دریافت کنند. • باید فرآیند انضباطی رسمی برای کارکنانی که تعهدات امنیتی را نقض کردند وجود داشته باشد.
		حساس	• سازمان بایستی آموزشهای لازم در خصوص مسولیتهای آنها و قوانین واکنش سریع در مواقع لازم را به همه کارکنان (مرتبط با مرکز داده) داده و مرتبا به روز نماید. (NIST-IR-2)
		حیاتی	• سازمان بایستی با ارایه اتفاقات و حوادث شبیه سازی شده در قالب آموزش، میزان کارآیی آموزشهای ارایه شده به پرسنل را در شرایط

			حیاتی ارزیابی نماید.((NIST-IR-2 (1)
۶۳	تهدیدهای مربوط به تغییر شغل یا انفصال از خدمت کارکنان و پیمانکاران	مهم، حساس و حیاتی	• مسئولیتها برای آن افرادی که دوره استخدامشان پایان یافته یا تغییر پیدا کرده باید بصورت روشن و واضح بوده و تعیین شود.(A.8.3.1) • همه کارکنان، پیمانکاران و کاربران ثالث باید همه دارایی های سازمان را (آنچه در تصرف دارند) به محض خاتمه استخدام ، قرارداد و توافق بازگردانند.(A.8.3.2) • مجوزهای دسترسی به اطلاعات و امکانات پردازش اطلاعات برای کل کارکنان ، پیمانکاران و کاربران ثالث باید به محض اتمام استخدامشان، قرارداد و توافقشان حذف شده یا به محض تغییر، تنظیم شود.(A.8.3.3)
۶۴	دسترسی‌های غیرمجاز طرفهای خارج مرکز داده	مهم، حساس و حیاتی	• ریسکهای مرتبط با دسترسی به امکانات پردازش اطلاعات سازمان توسط طرف خارج مرکز داده (منظور طرفهای داخل کشور می باشد نه خارج کشور) باید برآورد شده و کنترل‌های امنیتی مناسب پیاده‌سازی گردد.(A.6.2.1) • در قراردادهای با طرفهای خارج مرکز داده شامل دسترسی، پردازش، ارتباط، مدیریت اطلاعات یا تجهیزات، خرید تجهیزات، نصب و غیره باید تمام ملزومات امنیتی مربوط مشخص شوند.(A.6.2.3)
۶۵	عدم تجهیز به سیستم مدیریت بحران و شرایط اضطرار	مهم، حساس و حیاتی	• نصب سیستم‌های مدیریت بحران • اتخاذ سیاست‌ها و مکانیزم‌های اجرایی جهت جلوگیری از وقوع شرایط اضطرار • آموزش پرسنل برای رویارویی با شرایط اضطرار • تهیه دستورالعمل‌های لازم و ابلاغ آن به زیر مجموعه ها
۶۶	فقدان یک سیستم هشداردهنده سریع و به موقع	مهم، حساس و حیاتی	• بکارگیری سیستم‌های هشداردهنده سریع در حوزه های مختلف • بکارگیری سیستم‌های هوشمند اعلام خطر در خصوص حملات سایبری (نظیر DIDS) • بکارگیری سیستم‌های اعلام حریق هوشمند • آموزش پرسنل برای استفاده از این سیستم‌ها
۶۷	عدم بکارگیری سازه‌های امن و پایدار	مهم	• استفاده از سازه‌های امن و پایدار در طراحی مرکز داده • قرار دادن تجهیزات حساس و آسیب‌پذیر در فضای مطمئن
		حساس و حیاتی	• استفاده از موانع طبیعی علاوه بر سازه‌های مصنوعی (پوشش سازه های مصنوعی در درون موانع طبیعی نظیر عمق زمین یا زیر کوه)

۶۸	تولید اطلاعات غلط و نامطمئن	مهم، حساس و حیاتی	• شناسایی علل ناشی از تولید اطلاعات غلط اعم از نرم افزاری، سخت افزاری و نیروی انسانی و رفع این موارد
۶۹	عدم بهره مندی از مراکز احتیاط (Backup) امن، ایمن و پایدار	مهم	• ایجاد یک مرکز داده پشتیبان Offline در محل فیزیکی دیگر بمنظور سرویس دهی در صورت عدم امکان سرویس دهی توسط مرکز اصلی
		حساس	• ایجاد یک مرکز داده پشتیبان فعال (Active) در محل فیزیکی دیگر بمنظور سرویس دهی در صورت عدم امکان سرویس دهی توسط مرکز اصلی
		حیاتی	• ایجاد یک مرکز داده پشتیبان فعال (Active)و یک مرکز داده Offline در محل های فیزیکی دیگر بمنظور سرویس دهی در صورت عدم امکان سرویس دهی توسط مرکز اصلی
۷۰	عدم بکارگیری خطوط ارتباطی مطمئن و پایدار	مهم، حساس و حیاتی	• بکارگیری چندین خطوط ارتباط مطمئن و پشتیبان در کنار همدیگر به منظور پشتیبان ارتباطی یکدیگر • استفاده از تکنولوژی‌های ارتباطی ناهمگون
۷۱	اتصالات ناامن به شبکه‌های اینترنت و اینترانت و فیبر نوری	مهم	• طراحی صحیح اتصالات در زمان طراحی مراکز داده بمنظور عدم وجود اتصال ناامن • نظارت و کنترل دوره ای در این خصوص و شناسایی تمامی اتصالات احتمالی ناامن و حذف آنها • ایزوله بودن سرویسهای بین المللی مورد نیاز در مراکز داده از سرویسهای داخلی
		حساس و حیاتی	• ایزوله بودن کامل در بالاترین حد ممکن در خصوص سرویسهای بین المللی مورد نیاز در مراکز داده از سرویسهای داخلی
۷۲	عدم پیش‌بینی برق پشتیبان	مهم، حساس و حیاتی	• پیش بینی برق UPS برای مرکز داده بمنظور استفاده در صورت قطع برق عادی متناسب با گستردگی، سطح و اهمیت مرکز داده • استفاده از مولدهای تولید برق پشتیبان، بمنظور پشتیبانی از برق UPS متناسب با سطح و اهمیت مرکز داده • نگهداری سوخت کافی برای مولدهای برق بمنظور استفاده در شرایط لازم
۷۳	عدم وجود نیروی انسانی متخصص لازم	مهم، حساس و حیاتی	• تربیت یا جذب نیروی انسانی متخصص لازم در حوزه های تخصصی مورد نیاز • ارائه آموزشهای عرضی تخصص‌های لازم به کارکنان • اولویت به استفاده از فن‌آوری‌هایی که نیروی متخصص آن در اختیار است.

			• تشویق کارکنان به فراگیری تخصص‌های متنوع و جدید • برگزاری آزمون‌های دوره‌ای جهت ارزیابی وضعیت آموزشی و کنترل کیفی مهارت‌های فنی آنان • برگزاری مانورهای آموزشی و مدیریت بحران به طور ادواری جهت ارزیابی سرعت عمل و انتقال در کارکنان جهت رویارویی با شرایط واقعی بحران
۷۴	عدم وجود آموزش امنیتی کافی	مهم	• برگزاری کلاسهای آگاهسازی و توجیه کارکنان در خصوص خسارات گزاف ناشی از عدم رعایت مسائل امنیتی • برگزاری دوره های آموزشی تخصصی عرضی امنیت برای متخصصین شبکه و امنیت • ارائه آموزشهای عمومی امنیت در سطوح مختلف به مدیران و کارکنان
		حساس و حیاتی	• ابلاغ سیاست‌های امنیتی و موظف نمودن کارکنان به تبعیت از سیاست‌ها با استفاده از مکانیزمهای مدیریتی
۷۵	اشتباهات و غفلت‌ها مانند عدم بکارگیری صحیح تجهیزات، عدم نصب صحیح نرم‌افزارها و برنامه‌های کاربردی، سهل انگاری	مهم، حساس و حیاتی	• آموزش کارکنان در خصوص نحوه صحیح نصب تجهیزات، نرم‌افزارها، برنامه‌های کاربردی و همچنین کاربری صحیح سیستم ها و تجهیزات • تدوین برنامه‌های ادواری جهت کنترل و شناسایی اشتباهات احتمالی کارکنان • نصب سیستم‌های هشداردهنده که در صورت فراموشی و یا غفلت کاربران هشدار دهد.
۷۶	عدم وجود کنترل روی قوانین	مهم، حساس و حیاتی	• تدوین سیاست کاری به منظور اجرای کنترل‌های لازم بمنظور اجرای قوانین تدوینی • بازبینی دوره ای قوانین و شناسایی قوانین ضعیف و متناقض و انجام تصحیحات لازم • تشویق و تنبیه کارکنان فعال و خاطی
۷۷	اتکا قابل ملاحظه به سیستم‌های ارتباطی بی‌سیم و ماهواره غیر امن	مهم	• رمزنگاری داده‌های ارسالی جهت کاهش مخاطرات ناشی از دسترسی غیرمجاز به داده‌ها در شرایط اضطرار به استفاده از این ارتباطات
		حساس و حیاتی	• عدم استفاده از سیستم‌های ارتباطی بی‌سیم بعلت عدم وجود امنیت کافی در این نوع از ارتباطات • استفاده از ارتباطات ماهواره ای داخلی در صورت راه اندازی در آینده در صورت نیاز

۷۸	عدم سازگاری با سیستم اطلاعات جغرافیایی (GIS)	مهم، حساس و حیاتی	• استفاده از سامانه های مبدل جهت ایجاد سازگاری با سیستم اطلاعات جغرافیایی در صورت نیاز
۷۹	زلزله	مهم	• عملیات مکان یابی صحیح و اصولی ساختمان باید در زمان انتخاب مکان مرکز داده انجام شود. • حفاظت فیزیکی در برابر آسیبهای ناشی از سیل، زلزله بایستی طراحی و بکارگرفته شود. (A.9.1.4) • طراحی و مقاومت ساختمان متناسب با کاربری مرکز داده در نظر گرفته شود. • عملیات مقاوم سازی ساختمان انجام گیرد. • آموزش افراد برای مقابله با حوادث (زلزله) • تدوین دستورالعملهای مرتبط با حوادث (زلزله) • تهیه و بکارگیری تجهیزات کمکهای اولیه • چیدمان مناسب تجهیزات جهت مقابله با لرزش های زلزله • تهیه و در دسترس بودن نقشه کلیه تأسیسات فنی و ابنیه ها • تهیه لیست تجهیزات موجود در مرکز داده • آموزش و بکارگیری گروه تعمیر، امداد و نجات
		حساس	• پیش بینی و بکارگیری سیستم روشنایی و برق اضطراری متحرک • پیش بینی سیستم های ارتباط داده پشتیبان بمنظور استفاده در شرایط اضطراری (NIST-CP-8(4)) • پیش بینی ارتباط مستقیم با مرکز زلزله نگاری (Hot line Connection) • پیش بینی تجهیزات جابجایی اشیاء (جرثقیل و ...)
		حیاتی	• پیش بینی و نصب تجهیزات هشدار وقوع زلزله در ساختمان • ایجاد سایت پشتیبان Active با ارتباط مستقیم و برخط (NIST-CP-6) و (NIST-CP-7) و و یک سایت پشتیبان Active دور • ایجاد و بکارگیری سیستم هوشمند قطع و وصل منابع (برق، آب، گاز) • پیش بینی رایانه های قابل حمل بی سیم جهت بکارگیری در زمان زلزله • پیش بینی ژنراتور برای تولید برق در شرایط قطع برق قبل و بعد از زلزله
۸۰	آتش	مهم	• استفاده حداکثری از مصالح و تجهیزات مقاوم در برابر آتش در زمان ساخت مرکز داده.

			• طراحی حفاظت فیزیکی در برابر آسیبهای ناشی از آتش سوزی • اعمال محدودیتها در مورد ممنوعیت ورود مواد آتش زا و پرخطر • تهیه و بکارگیری سیستم های هشداردهنده و اعلام حریق • تهیه و بکارگیری تجهیزات اطفاء حریق • آموزش دوره ای افراد شاغل در مرکز در مورد پیشگیری و مهار آتش • آموزش و بکارگیری گروه اطفاء حریق
		حساس	• ارتباط Online با مرکز آتش نشانی
		حیاتی	• پیش بینی ارتباط بی سیم با مرکز آتش نشانی • پیش بینی ارتباط مستقیم با مرکز زلزله نگاری (Hot line Connection)
۸۱	طوفان و صاعقه	مهم	• پیش بینی سیستم برق گیر و Earth جهت انتقال بار الکتریکی اضافی به زمین • ارائه آموزش پیشگیری و مقابله با حوادث برای افراد شاغل در مرکز داده • آموزش و بکارگیری گروه حوادث غیر مترقبه
		حساس	• پیش بینی تجهیزات جابجایی اشیاء (جرثقیل و ...) • ارتباط Online با مراکز امداد و نجات
		حیاتی	• پیش بینی ارتباط مستقیم با مراکز امداد و نجات (Hot line Connection)
۸۲	سیل	مهم	• تجهیز مرکز به سیستم جمع آوری آبهای سطحی • طراحی حفاظت فیزیکی در برابر آسیبهای ناشی از سیل • آموزش و بکارگیری گروه حوادث غیر مترقبه
		حساس	• ارتباط Online با مراکز امداد و نجات
		حیاتی	• پیش بینی ارتباط مستقیم با مراکز هواشناسی (Hot line Connection) • وجود امکانات ارتباط بی سیم با مراکز امداد و نجات
۸۳	رطوبت و دما	مهم	• تهیه و بکارگیری تجهیزات تهویه مطبوع در ساختمان مرکز داده • استفاده از مصالح مناسب در ساخت مرکز داده • استفاده از دماسنج و رطوبت سنج بخصوص در نقاطی که از تجهیزات حساس به دما استفاده می شود
		حساس	• الزام در خصوص عایق بندی کلیه سیستم های حساس به رطوبت و دمای نامناسب

		حیاتی	• تهیه و بکارگیری سیستم های تهویه اضطراری منظور استفاده در زمان از کارافتادگی سیستم های اصلی
۸۴	دود	مهم، حساس و حیاتی	• تهیه و بکارگیری نورافکن و مه شکن در نقاط مختلف مرکز داده و پیرامون آن • بکارگیری تجهیزات کم کننده اثرات دود • پیش بینی ارتباط با مرکز هواشناسی
۸۵	سقوط اجسام	مهم، حساس و حیاتی	• رعایت استحکام مناسب در طراحی سازه مراکز داده متناسب با نوع آنها
۸۶	تداخل الکترومغناطیسی امواج	مهم	• مکان یابی نصب تجهیزات به منظور دوری از تجهیزات تداخل کننده مثل خطوط برق فشار قوی و خطوط با جریان بالا • رعایت استانداردهای مربوط به کابل کشی و فواصل مربوط به نصب کابل های انتقال داده ، برق و تلفن در زمان طراحی مرکز داده • آموزش و بکارگیری گروه متخصص در خصوص اختلال های الکترومغناطیسی
		حساس	• بکارگیری حفاظهای امواج الکترومغناطیس بر روی بسترهای انتقال
		حیاتی	• پیش بینی شبکه طیف گسترده جهت جلوگیری از تداخل الکترومغناطیسی
۸۷	مشکلات تأسیساتی (آب ،گاز، برق، تلفن)	مهم، حساس و حیاتی	• طراحی مناسب تأسیسات و رعایت استانداردهای نصب مسیرهای انتقال در زمان طراحی مرکز داده • استفاده از سیستم های هوشمند هشدار دهنده و کنترل کننده تاسیسات • حفاظت تجهیزات از افت جریان برق یا هر اختلالی که بر اثر عدم پشتیبانی تأسیسات بوجود می آید • استفاده از سیستم های پشتیبان برای آب، گاز، برق و تلفن بمنظور استفاده در صورت اختلال در مسیر اصلی • آموزش و بکارگیری گروه تاسیسات
۸۸	مواد پرخطر	مهم، حساس و حیاتی	• کنترل و نظارت بمنظور عدم انتقال مواد پرخطر و حساس • بازرسی افراد و تجهیزات به هنگام ورود و خروج • پیش بینی تجهیزات لازم بمنظور مقابله با حوادث احتمالی پیش آمده از طریق این مواد • آموزش و بکارگیری گروه متخصص جهت انجام عکس العمل مناسب

۸۹	تشعشعات رادیواکتیو	مهم، حساس و حیاتی	• نصب تجهیزات هشدار دهنده جهت اعلام خطر نشت مواد رادیواکتیو در محیط • قرار دادن لباس‌های مخصوص کار در محیط‌های آلوده به تشعشعات رادیواکتیو جهت استفاده پرسنل در صورت نیاز • استفاده از گیت‌های ورودی حساس به تشعشعات رادیواکتیو در تمامی ورودی‌های مراکز داده • تجهیز دیواره‌های داخلی مراکز داده به مواد شیمیایی مخصوص جذب موارد رادیواکتیو • آموزش و بکارگیری گروه متخصص جهت انجام عکس العمل مناسب
۹۰	گرد وغبار و مه	مهم، حساس و حیاتی	• بکارگیری فیلترهای جلوگیری کننده از ورود گرد و غبار • استفاده از حسگرهای گرد و غبار بمنظور اعلام هشدار در مواقع لازم • آموزش کارکنان در مورد نحوه رفع مشکل • آموزش و بکارگیری گروهی جهت انجام عکس العمل مناسب

۹-۴ ملاحظات پدافند غیر عامل برای مراکز داده مهم

جدول ۳. ملاحظات پدافند غیرعامل برای مراکز داده مهم

ردیف	تهدید	شرح کنترل
۱	اختلال الکترونیکی و الکتریکی	• ایجاد اتصال زمین برای تجهیزات به منظور انتقال بار الکتریکی اضافی • تجهیزات باید از افت جریان برق یا هر اختلالی که بر اثر عدم پشتیبانی تأسیسات بوجود می‌آید، حفاظت شوند. (A.9.2.2) • تجهیزات محافظ جهت جلوگیری از عملکرد اعوجاج و امواج الکترونیکی و الکتریکی • تجهیزات محافظ ولتاژ به منظور جلوگیری از تغییرات و ضربه های ولتاژ برق • بکارگیری سیستم برق اضطراری مجهز به مانیتور جهت مشاهده وضعیت برق تغذیه کننده سیستم ها • محافظت در مقابل نقایص منبع تغذیه • آموزش کارکنان شاغل در مرکز جهت رفع اشکالات مربوط به اختلال های الکترونیکی و الکتریکی
۲	کدهای مخرب و بدافزارها (Malwares)	• کنترل‌های کشف، جلوگیری، و ترمیم به منظور محافظت در برابر کدهای مخرب، به همراه روال‌های مناسب آگاهی کاربران باید پیاده‌سازی شوند. (A.10.4.1) • جایی که استفاده از کد سیار مجاز است، پیکربندی آنها باید به گونه‌ای باشد که اطمینان از تطابق کدهای سیار مجاز با خط مشی های امنیتی تعریف شده، حاصل شود و باید از اجرای کد سیار غیر مجاز جلوگیری شود. (A.10.4.2)
۳	دسترسی غیرمجاز از راه دور	• باید یک خط مشی رسمی اِعمال شده و روشهای مناسب امنیتی جهت محافظت در برابر ریسکهای استفاده از کامپیوترهای سیار و امکانات ارتباطات باید به کار گرفته شوند. (A.11.7.1) • باید یک خط مشی، برنامه های عملیاتی و روش های اجرایی توسعه یافته برای فعالیتهای کاری از راه دور اجرا شوند.(A.11.7.2)
۴	وقفه در کار	• فرآیند تنظیم شده باید توسعه یافته و باید جهت استمرار کسب و کار در کل سازمان نگهداری شود که اشاره به الزامات امنیتی اطلاعات مورد نیاز برای استمرار کسب و کار سازمان را دارد. (A.14.1.1) • رخدادهایی که ممکن است باعث وقفه در کار مرکز داده شوند باید به همراه احتمال و خسارت ناشی از وقفه و دیگر پیامدهای امنیتی مشخص شوند. • باید برای نگهداری یا بازیابی عملیات و اطمینان از دسترس‌پذیری در سطح مورد نظر و در زمان مورد نظر برنامه‌ریزی شود. • باید یک چارچوب کلی برای طرح‌های استمرار کسب و کار تدوین شود تا طرح‌ها سازگار بوده و نیازمندیهای امنیتی را به درستی مشخص کنند. همچنین اولویت‌های

		آزمون و ارزیابی را مشخص نماید. • طرحهای تداوم کسب و کار باید آزمایش شده و به طور منظم ارتقاء یابند تا از به روز بودن و اثر بخشی آنها اطمینان حاصل شود. (A.14.1.5)
۵	جاسوسی	• هر مورد از تجهیزات که شامل ذخیره رسانه است، قبل از کنار گذاری باید به منظور حصول اطمینان از عدم وجود اطلاعات خاص بررسی شود. اینگونه اطلاعات و نرم افزارهای ثبت شده کنار گذاشته شده باید قبل از کنار گذاری در صورت نیاز بر روی رسانه ای دیگر ثبت گردد. • بکارگیری سیستم تشخیص هویت و شناسایی افراد به صورت جامع • جلوگیری از عکاسی ، فیلمبرداری و ضبط صدا • ثبت تمام ورود و خروج ها • آموزش ضد جاسوسی به کارکنان • تهیه نقشه تأسیسات و قابلیت دسترسی آنها برای افراد مجاز • تهیه لیست تجهیزات و قابلیت دسترسی آنها برای افراد مجاز
۶	حملات تروریستی سایبری(هکرها)	• تهیه داده‌های پشتیبان در فواصل زمانی مناسب به منظور جلوگیری از احتمال بروز خرابی در تمامیت و صحت داده‌ها • ردگیری و تهیه سوابق دقیق از عملیات صورت گرفته از سوی هر کاربر به منظور مطالعه و شناسایی رفتار و اقدامات مشکوک صورت گرفته • کاهش سطح تماس سرویس‌های مرکز داده به متقاضیان • پرهیز از افشاء ماهیت و رفتار درونی سیستم، نرم افزار/ سخت‌افزار و مولفه‌های نرم‌افزاری به کار رفته در آن به سایرین • اتخاذ سیاست امنیتی مثبت به عنوان یک سیاست امنیتی بازدارنده • استفاده از مولفه‌های امنیتی فعال چون دروازه‌های آتش در محل ورودی ترافیک به شبکه داخلی مرکز داده • به کارگیری سیستم های تشخیص نفوذ مبتنی بر رفتار و امضاء جهت تشخیص به موقع ناهنجاری‌های رفتاری کاربران • آموزش پرسنل به استفاده از کلمات عبور طولانی و پیچیده و تغییر کلمات عبور به طور ادواری

		• به کارگیری تیمی از متخصیص نفوذ به منظوری شناسایی حفره‌های امنیتی موجود بخصوص در سطح نرم‌افزار و اتخاذ راه‌کارهایی جهت انسداد این حفره‌ها • غیرفعال کردن سرویس‌ها و مولفه‌های عمومی غیر قابل استفاده در سطح مرکز داده • استفاده از مولفه‌های نرم‌افزاری اختصاصی (in-house) به جای استفاده از مولفه‌های عمومی؛ بسیاری ازاین مولفه‌های به دلیل قابل دسترس بودن ضعف‌های امنیتی آنان برای همگان شناخته شده است.
۷	دسترسی غیرمجاز به اطلاعات	• خط مشی کنترل دسترسی باید پایه‌ریزی و مستند سازی شده و بر اساس کسب و کار و الزامات امنیتی برای دسترسی بازنگری شود. (A.11.1.1)
۸	دسترسی غیرمجاز به شبکه	• برای کاربران فقط دسترسی به سرویس هایی باید مهیا شوند که بطور مشخص اجازه استفاده از آنها را دارند.(A.11.4.1) • روشهای مناسب باید برای کنترل دسترسی توسط کاربران بیرونی مورد استفاده قرار بگیرد. • دسترسی فیزیکی و منطقی به درگاهها (پورت‌ها) باید تحت کنترل باشد. • برای شبکه های مشترک به خصوص آنهایی که به خارج از مرزهای سازمانی کشیده شدند ظرفیت کاربران محدود شود. • برای حصول اطمینان از اینکه ارتباطات کامپیوتری و جریان اطلاعات، خط مشی کنترل دسترسی را نقض نکند باید کنترل مسیریابی برای شبکه ها اجرا شود.(A.11.4.7)
۹	دسترسی غیرمجاز به سیستم‌عامل	• دسترسی به سیستم های عامل باید توسط فرآیند اجرایی امن (Logon) کنترل شوند.(A.11.5.1) • همه کاربران باید ID انحصاری برای استفاده شخصی خود داشته باشند و باید یک تکنیک مناسب تأیید، جهت اثبات ادعای ID کاربر انتخاب شود. • سیستم های تنظیم کلمه عبور باید دو سویه بوده و کیفیت کلمه عبور را اطمینان دهد. • استفاده از برنامه های کاربردی که توانایی کنترل کاربردها را داشته باشند به شدت تحت کنترل قرارداده شده و محدود شوند. • برای فراهم نمودن امنیت بیشتر برای کاربردهای دارای ریسک بالا، باید محدودیت هایی در زمان برقراری اتصال اعمال شود.(A.11.5.6)
۱۰	دسترسی غیرمجاز به برنامه‌های کاربردی	• دسترسی به اطلاعات و عملیات سیستمهای کاربردی توسط کاربران و کارکنان پشتیبانی باید طبق خط مشی کنترل دسترسی مشخص محدود گردد.(A.11.6.1) • سیستمهای حساس باید محیط کامپیوتری(محاسباتی) اختصاصی(مجزا) داشته باشند.(A.11.6.2)
۱۱	دسترسی غیر مجاز به اطلاعات یا سیستم‌های حین مبادله با نهادهای خارج از مرکز داده	• خط مشی تبادل رسمی، روش های اجرایی و کنترل ها جهت حفاظت از تبادل اطلاعات با استفاده از همه انواع امکانات ارتباطی باید در محل وجود داشته باشد.(A.10.8.1) • توافقات جهت مبادله اطلاعات و نرم افزار بین سازمان و طرفهای خارج از سازمان باید پایه ریزی و تدوین شوند.

		• رسانه های حاوی اطلاعات باید در مقابل دسترسی غیرمجاز، سوء استفاده یا انحراف در زمان انتقال به خارج از مرزهای فیزیکی سازمان، حفاظت شود. • خط مشی ها و روش های اجرایی جهت حفاظت از اطلاعات همراه با ارتباطات داخلی سیستمهای اطلاعاتی کسب و کار باید تدوین شده و دائما ارتقاء یابند.(A.10.8.5)
۱۲	پردازش‌های اطلاعاتی غیر مجاز	• الزامات ممیزی و فعالیتهای که شامل بررسی سیستم‌های عملیاتی است، برای کمینه کردن مخاطرات اختلال در فرایند کسب و کار، باید با دقت طرح‌ریزی و تصویب شوند.(A.15.3.1) • رکوردهای ممیزی مربوط به فعالیت‌های کاربران، وقایع استثنایی، و رویدادهای امنیتی باید تولید و نگهداری شوند. این رکوردها برای کمک به تفحصهای آتی و نظارت بر کنترل دسترسی کاربرد دارند. (A.10.10.1) • فرایند اجرایی برای استفاده از مراقبت امکانات پردازش اطلاعات باید پایه ریزی شده و نتایج نظارت فعالیتها باید به طور منظم بازنگری شوند. • امکانات ثبت کردن و ثبت اطلاعات باید در برابر دسترسی بدون مجوز و پنهانی حفاظت شود. • فعالیتهای مدیر و اپراتور سیستم باید ثبت شوند. • خطاها باید ثبت و تحلیل شده و اقدامات مناسب صورت بگیرد. • ساعت سیستمهای پردازش اطلاعات در سازمان یا حوزه امنیتی باید با زمان دقیق مرجع هماهنگ باشند.(A.10.10.6) • در صورت بروز خطا در ثبت رکوردهای ممیزی یا پر شدن ظرفیت محل ذخیره، باید هشدار مناسب به مدیر فنی مربوط داده شده و اقدام مقتضی (توقف ثبت، خاموش کردن سیستم، یا بازنویسی روی رکوردهای قدیمی) انجام شود. (NIST AU-5) • سیستم‌های اطلاعاتی باید مهر زمانی (timestamp) هر رویداد را مشخص نمایند. (NIST AU-8) • سیستم‌های اطلاعاتی باید از اطلاعات ممیزی و ابزارهای ممیزی در مقابل دسترسی غیرمجاز، تغییر یا حذف محافظت کنند. (NIST AU-9) (A.15.3.2)
۱۳	تغییر غیرمجاز، از دست دادن یا سوءاستفاده از اطلاعات در برنامه‌های کاربردی	• داده های ورودی برای سیستم کاربردی باید برای حصول اطمینان از صحت و مناسب بودن آنها، اعتبار سنجی شوند. (A.12.2.1) • باید در سیستم‌های کاربردی از وارسی‌های اعتبارسنجی به منظور کشف هر گونه خرابی داده استفاده شود. • الزامات برای اطمینان از درستی و حفاظت از صحت پیام در کاربردها باید مشخص شده و کنترل های مناسب باید مشخص و اجرا شوند. • داده های خروجی یک سیستم کاربردی باید به منظور اطمینان از درستی و مناسب بودن پردازش اطلاعات ذخیره شده با شرایط مربوطه مورد تعیین اعتبار قرار گیرد.(A.12.2.4)

۱۴	حمله فیزیکی، هسته‌ای و اتمی	• استفاده از تکنیکهای استتار بمنظور عدم تشخیص مکان مرکز داده توسط دشمن • استفاده از تکنیکهای اختفا بمنظور عدم تشخیص مکان مرکز داده توسط دشمن • استفاده از تکنیک‌های فریب دشمن بمنظور عدم تشخیص مکان واقعی مرکز داده • تهیه اطلاعات پشتیبان و ارسال آنان به نقطه‌ای خارج از فضای فیزیکی مرکز داده بمنظور حفظ داده ها و اطلاعات • ایجاد یک مرکز داده پشتیبان Offline در محل فیزیکی دیگر بمنظور سرویس دهی در صورت عدم امکان سرویس دهی توسط مرکز اصلی • تربیت تیم های تخصصی بمنظور استفاده جهت ترمیم آسیب ها در شرایط اضطرار
۱۵	بمب گذاری یا انفجار	• کنترل تردد تجهیزات و بسته ها • طراحی و بکارگیری برنامه حفاظت فیزیکی در برابر آسیبهای ناشی از انفجار (A.9.1.4) • آموزش کارکنان شاغل در مرکز جهت رفع اشکالات و ایرادات بوجود آمده پس از انفجار • ارتباط مستقیم با متخصصان مربوط به خنثی سازی موارد منفجره
۱۶	حوادث شیمیایی	• شیلد نمودن و عایق بندی جداره‌های و منافذ ورودی تأسیسات مراکز داده به منظور جلوگیری از نفوذ گازهای شیمیایی به داخل مراکز • استقرار تجهیزات ایمنی از قبیل ماسک و سایر تجهیزات موجود جهت جلوگیری از آسیب پرسنل • نگهداری پادزهرهای مختلف مربوط به انواع گازهای شیمیایی در جعبه کمک‌های اولیه به منظور انجام اقدامات اولیه به مصدومین
۱۷	جنگ الکترومغناطیسی	• مکان یابی نصب تجهیزات به منظور دوری از تجهیزات منشا تداخل مثل خطوط برق فشار قوی و خطوط با جریان بالا • آموزش کارکنان شاغل در مرکز جهت رفع اشکالات مربوط به اختلال های الکترومغناطیسی • رعایت استانداردهای مربوط به کابل کشی و فواصل مربوط به نصب کابل های انتقال داده ، برق و تلفن • استفاده از سیستم برق اضطراری برای مواقع خاص
۱۸	ارگانیزم ها (ویروس، باکتری و...)	• کنترل مواد خوراکی • کنترل محیط مرکز داده در خصوص گسترش موارد ارگانیزمی و اقدامات پیشگیرانه • آموزش کارکنان شاغل در مرکز جهت مقابله با موارد ارگانیزمی • ایجاد مرکز بهداشت و درمان به منظور رفع مشکلات با گستردگی محدود در مورد افراد شاغل

۱۹	دسترسی غیر مجاز به سیستم ها، تجهیزات و منطقه فیزیکی	• نقاط دسترسی نظیر نواحی بارگیری یا تحویل و دیگر نقاطی که احتمال ورود اشخاص فاقد صلاحیت وجود دارد کنترل شده و در صورت امکان از سایر بخش‌ها و تأسیسات منفک گردد. • تجهیزات باید به منظور کاهش ریسک های حاصل از تهدیدات و آسیبهای محیط و فرصتهای دسترسی غیرمجاز، حفاظت شوند.(A.9.2.1) • تجهیزات باید جهت حصول اطمینان از تداوم دسترسی و صحت بطور مناسب نگهداری شوند.(A.9.2.4) • تجهیزات، اطلاعات یا نرم افزار نباید بدون مجوز قبلی از محل خارج شوند. (A.9.2.7) • از سامانه های امنیتی (موانعی نظیر دیوارها، گیت های ورودی که با کارت کنترل می شود یا میزهای پذیرش آماده) بمنظور محافظت ناحیه هایی که شامل اطلاعات و سامانه های پردازش اطلاعات باشد، استفاده شود. (A.9.1.1) • نواحی امن بوسیله کنترل های ورودی مناسب جهت اطمینان از اینکه فقط پرسنل مجوز دار اجازه دسترسی داشته باشند محافظت شود. (A.9.1.2) • امنیت فیزیکی لازم برای دفاتر، اتاق ها و تاسیسات، طراحی و بکار گرفته شود.(A.9.1.3) • آموزش های لازم به کابران ارائه گردد.
۲۰	دسترسی غیر مجاز به رسانه‌های ذخیره‌سازی اطلاعات	• باید دستورالعمل اجرایی برای مدیریت رسانه متحرک تدوین گردد. (A.10.7.1) • در صورت عدم نیاز به یک رسانه، باید به صورت امن و ایمن و طی یک فرآیند رسمی امحاء شود. (A.10.7.2) • مستند سازی سیستم باید در برابر دسترسی غیر مجاز حفاظت شود.(A.10.7.4) • رسانه های ذخیره سازی اطلاعات در محل امن نگهداری شوند. • اطلاعات رسانه قبل از تعویض ثبت گردد. (A.9.2.6)
۲۱	دسترسی فیزیکی غیرمجاز به بستر انتقال داده‌ها	• لزوم حفاظت از بسترهای انتقال داده با تدوین سیاست نامه ای در خصوص نحوه دسترسی به آنها، مسئولیتهای افراد در این ارتباط و کد گذاری بسترها ی انتقال (NIST-MP-1) ، (NIST-MP-2) و (NIST-MP-3) • نحوه دسترسی، افراد مجاز و نحوه دریافت اطلاعات ورودی به بسترهای انتقال از هر نوع (اطلاعات الکترونیکی ، کاغذی و ...) بایستی مورد کنترل قرار گیرد. (NIST-MP-5) • حفاظت فیزیکی مناسب از کابلها و بکارگیری داکت • قرار دادن کانال انتقال داده‌ها در محیط غیرقابل دسترسی • کنترل بسترهای انتقال داده در زمان کنارگذاری و یا استفاده مجدد آنها.(NIST-MP-7)

۲۲	عدم سازگاری با فن‌آوری‌های مدرن جنگ الکترونیک	• جایگزینی فن‌آوری موجود با فن آوری قابل انطباق • استفاده از فن‌آوری‌های مبدل به منظور انطباق فن‌آوری موجود با فن‌آوری مدرن • تلاش برای بروزسازی فن‌آوری جدید با افزودن قابلیت‌های موجود در فن‌آوری‌های مدرن
۲۳	تهدید ناشی از عدم سازگاری با سیستم‌های مدرن اطلاعات عملیات	• استفاده از مولفه‌های مبدل به منظور ایجاد ارتباط و هماهنگی بین سیستم‌های کنونی اطلاعات عملیات و سیستم‌های نوین اطلاعات عملیات
۲۴	تهدید ناشی از عدم سازگاری با فن آوری‌های مدرن جنگ متحرک	• اتخاذ ملاحظاتی برای امکان جابجایی تجهیزات ذخیره سازی داده ها و اطلاعات در زمان بحران بمنظور استفاده در مرکز داده دیگر
۲۵	آسیب یا سرقت (الکترونیکی)	• آموزش کارکنان شاغل در مرکز جهت جلوگیری از سرقت الکترونیکی شناسه‌های هویت آنها • ملزم کردن کارکنان به تغییر کلمات عبور به صورت ادواری • استفاده از کلمات عبور پیچیده، طولانی غیرقابل حدس زدن
۲۶	آسیب یا سرقت (فیزیکی)	• از تجهیزات باید به منظور کاهش ریسک های حاصل از تهدیدات و آسیبهای محیط و فرصتهای دسترسی غیرمجاز، متناسب با ماهیت هر یک حفاظت شود. • آموزش کارکنان شاغل در مرکز جهت جلوگیری از آسیب یا سرقت • از نقشه تأسیسات و موارد زیر بنایی در مکان مناسب (گاوصندوق یا محل مطمئن) حفاظت گردد. • ثبت ورود و خروج افراد • حفاظت از لیست تجهیزات • حفاظت از تجهیزات در زمان انتقال به تعمیرگاه و یا به هنگام تعمیر و رعایت تمهیدات مربوطه
۲۷	اختلال در ارتباطات شبکه	• استفاده از کانال‌های ارتباطی فاقد امکان اختلال • شیلد کردن کانال‌ها و تجهیزات ارتباطی و مکانهای قرار گرفتن این تجهیزات
۲۸	اختلال در سیستم برق	• بکارگیری سیستم توان پشتیبان • استخدام نیروهای متخصص برق به منظور انجام سرویس بلادرنگ در زمان بروز اختلال در سیستم برق • نگهداری سوخت کافی برای ژنراتورهای مولد برق برای شرایط خاص که امکان دسترسی به سوخت تا مدت‌ها وجود ندارد
۲۹	قرار دادن کشور در موقعیت جنگ تمام عیار اطلاعاتی	• الزام به قرار گرفتن در شرایط آماده باش کامل به منظور نظارت بر حسن اجرای تمامی کنترل‌های پیشنهادی (پدافند غیرعامل و امنیت)
۳۰	تهدید ناشی از تحریم فن آوری های پیشرفته خارجی	• تلاش جهت تسلط بر دانش و فناوری ها بمنظور بومی‌سازی فن‌آوری به منظور کاهش دغدغه‌های ناشی از تحریم فن‌آوری

		• تعامل با بخش های تحقیقاتی و پژوهشی کشور بمنظور بکرگیری حداکثری توان داخلی جهت تولید فناوری های لازم در داخل کشور داخل کشور
۳۱	وابستگی به خارج از کشور در بخش تعمیر و نگهداری	• انتقال دانش تعمیر و نگهداری به متخصصین بومی • استفاده از تکنولوژی‌های بومی موجود • جلوگیری از امکان دسترسی به داده‌های طبقه‌بندی شده و سوابق ذخیره شده بر روی سخت‌افزار و رسانه‌های ذخیره سازی مربوطه با تهیه نسخه پشتیبان و امحاء داده‌های موجود بر روی سیستم‌ها قبل از ارسال به مراکز تعمیر
۳۲	وابستگی به تولیدات سخت افزاری و نرم افزاری خارجی	• انتقال دانش تولید سخت افزارها و نرم افزارها به متخصصین بومی
۳۳	تغییر سریع فن آوری (در حوزه جنگ سایبر)	• تلاش جهت تسلط بر دانش و فناوری ها بمنظور بومی‌سازی فن‌آوری به منظور کاهش دغدغه‌های ناشی از تغییرات در فن‌آوری • آموزش نیروی متخصص و کارآمد جهت بهره گیری و انتقال فن‌آوری به داخل کشور
۳۴	جهانی شدن	• تعامل با سازمانها و نهادهای مربوطه در داخل کشور بمنظور توجه به چالش‌های پیش روی جهانی شدن جهت ارائه راه‌کارهایی به منظور تطبیق با شرایط جدید • اتخاذ سیاست‌هایی در راستای تغییرات و تمهیدات ایجاد شده بمنظور اعمال در سازمان
۳۵	زیرساخت‌های عمده جهانی نظیر اینترنت	• استفاده از زیرساخت های بومی و قابل اتکاء و اعتماد در صورت وجود
۳۶	حملات مختل کننده خدمات	• بکارگیری سیستم‌هایی به منظور جلوگیری از نفوذ و شناسایی حملات مختل کننده خدمات در صورت نفوذ، نظیر IDSها و فایروالهای بومی • شناسایی و ثبت الگوهای رفتاری حمله‌کنندگان داخلی به منظور جلوگیری از الگوهای رفتاری مشابه توسط سایر کاربران • پیش بینی و بکارگیری مراکز احتیاط وتشکیل تیمهای CERT در شرایط وقوع وقفه سرویس • تعیین حدمجاز بهره‌مندی کاربران از سرویس‌های ارائه شده • قرار دادن کاربران خاطی و غیرقابل اعتماد در لیست سیاه و ممانعت از سرویس‌دهی به آنان
۳۷	جنگ روانی دشمن	• برگزاری دوره های آگاهسازی برای کارکنان و کاربران در این خصوص
۳۸	تغییر هویت اطلاعات درحال گذر	• استفاده از الگوریتم‌های رمزنگاری بومی، امضاهای دیجیتال در رمزنگاری اطلاعات متناسب با ماهیت و نوع سرویسها به منظور جلوگیری از افشا و امکان دستکاری اطلاعات در حال گذر • عدم استفاده از الگوریتم های رمزنگاری غیرمطمئن بمنظور رمزنگاری اطلاعات در حال گذر • استفاده از مکانیزمهای پنهان نگاری اطلاعات در شرایط لازم بمنظور انتقال اطلاعات مهم

		• عدم استفاده از کانال‌های ارتباطی بی‌سیم بدون در نظر گرفتن مکانیزمهای امنیتی مطمئن
۳۹	دسترسی غیرمجاز به اطلاعات	• استفاده از مکانیزمهای رمزنگاری اطلاعات و الگوریتم‌های رمزنگاری بومی بمنظور نگهداری اطلاعات بر روی رسانه های ذخیره سازی اطلاعات • عدم استفاده از الگوریتم های رمزنگاری غیرمطمئن بمنظور رمزنگاری اطلاعات • استفاده از مکانیزم‌های احراز هویت برای دسترسی به سرویسها و اطلاعات به منظور جلوگیری از دسترسی غیر مجاز به اطلاعات • پیش بینی تمهیدات امنیتی متناسب با سطح اهمیت و میزان تجمیع اطلاعات
۴۰	ناآرامی‌های اجتماعی	• محافظت بمنظور عدم افشای محل مرکز داده • حفاظت فیزیکی در برابر آسیبهای ناشی از آشوب های شهری بمنظور جلوگیری از ورود افراد متفرقه • محافظت بمنظور ذکر نشدن محل مرکز داده در نقشه های جغرافیایی
۴۱	ورود و خروج غیر مجاز افراد	• محیط های امنیتی (موانعی نظیر دیوارها، گیت های ورودی که با کارت کنترل می شود یا میزهای پذیرش آماده) باید بمنظور محافظت ناحیه هایی را که شامل اطلاعات و سامانه های پردازش اطلاعات باشد، استفاده شود. (A.9.1.1) • از سامانه های امنیتی (موانعی نظیر دیوارها، گیت های ورودی که با کارت کنترل می شود، دستگاههای X-Ray یا میزهای پذیرش آماده) بمنظور کنترل ورود و خروج افراد و تجهیزات همراه آنها استفاده شود. (A.9.1.1) • بکارگیری دوربین های کنترل تردد و سیستم حفاظت پیرامونی • اجبار در استفاده ازکارت شناسایی توسط افراد و کنترل آن توسط مبادی ذیربط • ثبت زمان ورود و خروج افراد • آموزش کارکنان
۴۲	عدم رویکرد مداوم برای مدیریت حوادث امنیتی	• باید مسئولیتهای مدیریت و فرآیندهای اجرایی جهت حصول اطمینان از پاسخ، سریع، موثر و مرتب به حوادث امنیتی اطلاعات پایه ریزی شود. (A.13.2.1) • باید مکانیزمهایی برای سنجش و پایش نوع، حجم، و هزینه حوادث امنیتی وجود داشته باشند. (A.13.2.2) • هر مرکز داده بایستی دارای مرکز عملیات امنیتی (SOC) بمنظور مانیتور و کنترل حوادث امنیتی باشد. • بعد از حادثه امنیتی اطلاعات، پی گیری در برابر فرد یا سازمانی صورت می گیرد که شامل اقدام قانونی (چه مدنی ، جزایی) است، شواهد باید جمع آوری و نگهداری شده و برای مطابقت با قوانین جهت مطرح شدن شواهد در یک دادرسی مربوطه ارائه شوند.

		(A.13.2.3)
۴۳	عدم اصلاح و بازیابی پس از حوادث امنیتی	• رویدادهای امنیتی اطلاعات باید توسط مدیریت کانالهای مناسب تا حد امکان به سرعت گزارش شوند.(A.13.1.1) • مرکز داده بایستی دارای تیم CERT بمنظور ترمیم حوادث احتمالی در صورت وقوع، باشد. • تمام کارکنان پیمانکاران و مصرف کنندگان ثالث مصرف کننده سیستمها و خدمات اطلاعات باید ملزم شوند تا هرگونه ضعف امنیتی مشاهده شده و مشکوک در سیستمها و خدمات را به آن توجه کرده و گزارش دهند.(A.13.1.2)
۴۴	ناامنی یا نادرستی در عملیات پردازش اطلاعات	• روش های اجرایی عملیاتی باید مستند سازی و نگهداری شده، و برای همه کاربران که به آن نیاز دارند در دسترس باشد.(A.10.1.1) • تغییرات در امکانات پردازش اطلاعات و سیستمها باید کنترل شده باشند. • وظایف و حوزه های مسئولیت باید در راستای کاهش فرصت برای افراد غیرمجاز یا تغییرات ناخواسته یا سوء استفاده از دارایی های سازمان تفکیک شوند. • پیشرفت، آزمایش و امکانات عملیاتی باید تفکیک شوند تا دسترسی های غیرمجاز یا تغییرات سیستم عملیاتی را کاهش دهد.(A.10.1.4)
۴۵	عدم امنیت در تعامل با طرفهای ثالث	• استفاده از منابع باید مراقبت و تنظیم گردد. پیش بینی های لازم طبق الزامات ظرفیت آینده جهت حصول اطمینان از عملکرد سیستم ضروری است.(A.10.3.1) • باید معیار پذیرش سیستم های اطلاعاتی جدید، ارتقاء و نسخه های جدید پایه ریزی شده و آزمونهای مناسب سیستم ها در طی پیشرفت و قبل پذیرش انجام شوند. (A.10.3.2)
۴۶	خطاهای سیستم	• در استفاده از منابع باید مراقبت گردد. پیش بینی های لازم طبق الزامات ظرفیت آینده جهت حصول اطمینان از عملکرد سیستم ضروری است.(A.10.3.1) • باید معیار پذیرش سیستم های اطلاعاتی جدید، ارتقاء و نسخه های جدید باید پایه ریزی شده و آزمونهای مناسب سیستم ها در طی پیشرفت و قبل از پذیرش انجام شوند. (A.10.3.2)

۴۷	برون‌سپاری خدمات و پردازش اطلاعات	• الزامات امنیتی یک مرکز داده که مدیریت و کنترل تمامی یا بخشی از سیستم‌های امنیتی، شبکه‌ها و محیط‌های کاری آن به سازمانی دیگر واگذار می‌شود، باید در یک قرارداد که بین مرکز داده و طرف دیگر توافق شده است، دقیقا مشخص شود. • افراد و مراکز مجاز در حوزه های مرتبط با مراکز داده استعلام گردد.
۴۸	عدم بکارگیری نرم‌افزارهای کدباز	• استفاده از نرم‌افزارهای کدباز بجای استفاده از نرم‌افزارهای کدبسته در صورت وجود و پس از بررسی های امنیتی لازم بر روی آن • اتخاذ سیاست تولید کد بجای بکارگیری نرم‌افزارهای بین‌المللی موجود حتی از نوع کد باز و تعامل با مراکز و سازمانهای مجاز در این رابطه
۴۹	نقض صحت[1] و دسترس‌پذیری اطلاعات و سیستم‌های پردازش اطلاعات	• تهیه نسخه پشتیبان از اطلاعات و نرم افزار به طور مرتب و مطابق با خط مشی پشتیبان گیری • استفاده از مکانیزمهای جلوگیری از نقض صحت اطلاعات متناسب با نوع سرویسها و پردازشها • استفاده از مکانیزمهای جلوگیری از نقض دسترس پذیری اطلاعات متناسب با نوع سرویسها و پردازشها
۵۰	عدم حفاظت اطلاعات در شبکه‌ها	• شبکه ها باید به منظور حفاظت در برابر تهدیدها و حفظ امنیت سیستمها و برنامه های کاربردی شبکه و داده های در حال انتقال، به طور مناسب مدیریت شوند. • ویژگی امنیت، سطوح خدمات و الزامات مدیریت همه خدمات شبکه باید مشخص شده و لحاظ گردند. • امنیت شبکه در چند لایه مطابق مدلهای دفاع از عمق طراحی و پیاده سازی گردد.

[1] Integrity

۵۱	دسترسی غیر مجاز کاربر	• باید یک روش اجرایی رسمی ثبت و حذف کاربر در محل برای اعطا و لغو حق دسترسی به همه سیستم ها و سرویس های اطلاعاتی وجود داشته باشد.(A.11.2.1) • تخصیص و استفاده از مجوزها محدود و کنترل شود. • تخصیص کلمات عبور از طریق یک فرآیند مدیریتی رسمی کنترل شود. • مدیریت، حقوق دسترسی کاربران را در فواصل منظم، در راستای استفاده فرآیندهای اصلی، بازنگری کند. (A.11.2.4) • کاربران باید ملزم به رعایت نکات ایمنی در انتخاب و استفاده از کلمات عبور باشند.(A.11.3.1) • کاربران باید مطمئن باشند که تجهیزات بدون مراقبت از حفاظت مناسب برخوردارند. • سیاست میز مرتب برای کاغذها و رسانه ذخیره متحرک و سیاست صحنه نمایش واضح برای امکانات پردازش اطلاعات باید پذیرفته شود.(A.10.3.3) • هر سیستم اطلاعاتی باید محدودیت حداکثر ۳ ورود ناموفق را در طی ۳۰ دقیقه اعمال کند. پس از رسیدن تعداد ورودهای ناموفق به حد نصاب، سیستم باید قفل شده و به طور خودکار پس از یک ساعت به حالت عادی برگردد. (NIST-AC-7) • مرکز داده باید مطابق خط مشی‌های استفاده و اِعمال کنترل‌های دسترسی، فعالیت‌های کاربران را مرور کرده و بر آنها نظارت داشته باشد. (NIST-AC-13)
۵۲	عدم در نظر گرفتن امنیت در سیستم‌های اطلاعاتی به عنوان یک بخش اصلی	• هر گونه درخواست برای تهیه، خرید، یا تولید سیستم‌های اطلاعاتی باید صریحا نیازمندیها و الزامات امنیتی را نیز مشخص کند. • در تمامی بخشهای یک سیستم اطلاعاتی از تولید تا بهره برداری، امنیت بعنوان یک جزء انکار ناپذیر در نظر گرفته شود. • تشکیلات امنیتی و ساختار سازمانی لازم برای امنیت پیش بینی گردد.
۵۳	نقض محرمانگی یا صحت اطلاعات در اثر عدم استفاده یا استفاده نادرست از رمزنگاری	• برای حفاظت از اطلاعات باید یک خط مشی استفاده از کنترل های رمز نگاری توسعه پیدا کرده و اجرا شود.(A.12.3.1) • مدیریت کلید باید جهت پشتیبانی از استفاده سازمان از تکنیکهای رمز نگاری تعبیه شود. (A.12.3.2)
۵۴	عدم اطمینان از امنیت فایل سیستم ها	• از سیستم فایلهای مطمئن استفاده گردد و در این راستا از مشاوره مجموعه های متخصص و مورد اعتماد بهره گرفته شود. • باید روش های اجرایی جهت کنترل نصب نرم افزار بر روی سیستمهای عامل تعبیه شوند.(A.12.4.1)

۵۵	نقض امنیت اطلاعات و نرم‌افزارهای کاربردی سیستم‌عامل	• هر گونه تغییر با استفاده از روش های اجرایی رسمی کنترل تغییرات کنترل شود.(A.12.5.1) • تغییرات در بسته های نرم افزار باید کم شده، به تغییرات لازم محدود شود و همه تغییرات باید شدیداً تحت کنترل باشند.(A.12.5.3) • از هر گونه نشست اطلاعات باید جلوگیری شود.(A.12.5.4) • توسعه و تغییر نرم افزار برون سپاری شده باید توسط مرکز داده نظارت شود.(A.12.5.5) • مرکز داده باید پیکربندی پایه و اولیه هر سیستم اطلاعاتی را تهیه و مستند ساخته و فهرستی از مولفه‌های سازگار سیستم تهیه نماید. • مرکز داده باید هر گونه تغییر در سیستم‌های اطلاعاتی را مستندسازی و کنترل نماید. این تغییرات باید ابتدا توسط مقام مسوول تایید شود. • مرکز داده باید تغییر دادن سیستم‌های اطلاعاتی را محدود به افراد مجاز نماید. • باید پیکربندی امنیتی سیستم‌های اطلاعاتی به نحوی باشد که بیشترین محدودیت را اعمال نماید و سازگار با نیازمندیهای عملیاتی و امنیتی سیستم‌ها شود.(NIST CM-6)
۵۶	عدم مدیریت آسیب‌پذیری‌های فنی	• اطلاعات به موقع در مورد آسیب پذیری‌های فنی سیستمهای اطلاعاتی مورد استفاده باید کسب شده و اثر آنها بر مرکز داده بررسی شده و تدابیر مناسبی برای مقابله با آنها اتخاذ شود.(A.12.6.1)
۵۷	عدم رعایت قوانین	• تمام الزامات مقرراتی، حقوقی و قراردادی و همه رویکرد سازمان برای تأمین این الزامات باید صریحاً مشخص، مستندسازی شده و برای هر سیستم اطلاعاتی سازمان ارتقاء داده شود.(A.15.1.1) • برای حصول اطمینان از انطباق با الزامات قانون گذاری، مقرراتی و قراردادی در استفاده مادی با توجه به ارتباط با حقوق مالکیت فکری یا استفاده اختصاصی محصولات نرم افزاری، روشهای اجرایی تدوین و اجرا شود.(A.15.1.2) • سوابق مهم باید در برابر مفقود شدن، تخریب و تحریف طبق قوانین قانونی، مقرراتی و قراردادی الزامات کسب و کار، محافظت شوند.(A.15.1.3) • از استفاده کاربران از امکانات پردازش اطلاعات بدون مجوز ممانعت به عمل آید.(A.15.1.5)
۵۸	عدم وجود مدیریت یکپارچه امنیت اطلاعات	• یک سند سیاست امنیتی توسط مدیریت مرکز داده تدوین و تصویب گردیده و منتشر گردد و بر حسب اقتضاء مورد تبادل نظر با تمام کارکنان قرار گیرد. • خط‌مشی های ذکر شده در سند سیاست امنیتی باید به طور منظم و نیز در مواردی که تغییرات مؤثری وجود داشته باشد، مورد بازنگری قرار گیرند تا از تداوم مناسب بودن خط‌مشی اطمینان حاصل شود. • فرم ها، اسناد و سیاست واکنش سریع مرکز داده شامل اهداف، محدوده، قوانین، مسؤلیتها و هماهنگی، همچنین مکانیزمهای کنترلی پیاده سازی، تولید و مرتبا مرور و به

		روز گردند.(NIST-IR-1)
۵۹	عدم سازگاری با خط مشی‌ها	• مدیران باید از اجرای صحیح تمام روش های اجرایی امنیت در حیطه مسئولیتشان برای دستیابی به تطابق با سند سیاست امنیتی و استانداردها، مطمئن شوند.(A.15.2.1) • سیستم های اطلاعاتی باید به طور منظم از نظر تطابق فنی با استانداردهای اجرایی امنیت مورد بررسی قرار گیرند.(A.15.2.2)
۶۰	فقدان نظام مدیریت امنیت اطلاعات	• مدیریت باید فعالانه از امنیت در سازمان با ساختار شفاف، تعهد آشکار، وظیفه صریح و قبول مسئولیتهای امنیت اطلاعات پشتیبانی کند. (A.6.1.1) • تشکیلات لازم و نیروی انسانی متخصص در زمینه امنی اطلاعات جذب یا تربیت گردند. • مسئولیت‌های حفاظت از هریک از دارایی‌های منفرد و انجام فرآیندهای امنیتی مشخص باید به طور شفاف تعریف شوند.(A.6.1.3) • برای استفاده از امکانات پردازش اطلاعات جدید، باید یک فرآیند صدور مجوز از طرف مدیریت پایه ریزی شود.(A.6.1.4) • باید همکاری مناسبی تحت مجوزهای قانونی، بین سازمانهای تنظیم کننده مقررات، تأمین‌کنندگان سرویسهای اطلاعاتی و اپراتورهای مخابراتی ایجاد و حفظ گردد.(A.4.1.7) • رویکرد سازمان برای مدیریت امنیت اطلاعات و اجرای آن (مثال: اهداف کنترل، کنترل ها، سیاستها، فرآیندها، روش های اجرایی امنیت اطلاعات) بصورت مستقل با طرح ریزی دوره ای یا هنگامی که تغییرات مهم در اجرای امنیت رخ می دهد، بازنگری شود.(A.6.1.8)
۶۱	استخدام یا به کارگماری افراد نامناسب	• نقشهای امنیتی و مسوولیتهای کارکنان، پیمانکاران و کاربران ثالث باید طبق سند سیاست امنیت اطلاعات مرکز داده مشخص و مستند سازی گردند. • بررسی سوابق همه افراد آماده استخدام، پیمانکاران و کاربران ثالث، باید طبق قوانین، اصول و قوانین مربوط و متناسب با الزامات کسب و کار طبقه‌بندی اطلاعات در دسترس باشد. • به عنوان بخشی از تعهد قراردادی افراد، کارکنان، پیمانکاران و کاربران ثالث باید طبق قوانین، اصول و مقررات مربوطه و متناسب با الزامات کسب و کار طبقه بندی اطلاعات در دسترسی را مدنظر داشته و به ریسک‌های ناشی از افشاء اطلاعات و دسترسی غیرمجاز دیگران واقف باشند.

۶۲	عدم آگاهی نیروهای انسانی از مسوولیتها و تعهدات	• مدیریت باید از کارکنان و پیمانکاران و کاربران ثالث بخواهد تا امنیت را طبق خط‌مشی‌های تدوین شده و رویه‌های مرکز داده بکار برند. • همه کارکنان سازمان (مرتبط با مرکز داده)، پیمانکاران و کاربران ثالث، باید آگاهی و آموزش مناسب و خط مشی های به روز شده و روشهای اجرایی که به عملکرد شغلی آنها مربوط می شود، را دریافت کنند. • باید فرآیند انضباطی رسمی برای کارکنانی که تعهدات امنیتی را نقض کردند وجود داشته باشد.
۶۳	تهدیدهای مربوط به تغییر شغل یا انفصال از خدمت کارکنان و پیمانکاران	• مسئولیتها برای آن افرادی که دوره استخدامشان پایان یافته یا تغییر پیدا کرده باید بصورت روشن و واضح بوده و تعیین شود.(A.8.3.1) • همه کارکنان، پیمانکاران و کاربران ثالث باید همه دارایی های سازمان را (آنچه در تصرف دارند) به محض خاتمه استخدام ، قرارداد و توافق بازگردانند.(A.8.3.2) • مجوزهای دسترسی به اطلاعات و امکانات پردازش اطلاعات برای کل کارکنان ، پیمانکاران و کاربران ثالث باید به محض اتمام استخدامشان، قرارداد و توافقشان حذف شده یا به محض تغییر، تنظیم شود.(A.8.3.3)
۶۴	دسترسی‌های غیرمجاز طرفهای خارج مرکز داده	• ریسکهای مرتبط با دسترسی به امکانات پردازش اطلاعات سازمان توسط طرف خارج مرکز داده (منظور طرفهای داخل کشور می باشد نه خارج کشور) باید برآورد شده و کنترل‌های امنیتی مناسب پیاده‌سازی گردد.(A.6.2.1) • در قراردادهای با طرفهای خارج مرکز داده شامل دسترسی، پردازش، ارتباط، مدیریت اطلاعات یا تجهیزات، خرید تجهیزات، نصب و غیره باید تمام ملزومات امنیتی مربوط مشخص شوند.(A.6.2.3)
۶۵	عدم تجهیز به سیستم مدیریت بحران و شرایط اضطرار	• نصب سیستم‌های مدیریت بحران • اتخاذ سیاست‌ها و مکانیزم‌های اجرایی جهت جلوگیری از وقوع شرایط اضطرار • آموزش پرسنل برای رویارویی با شرایط اضطرار • تهیه دستورالعمل‌های لازم و ابلاغ آن به زیر مجموعه ها
۶۶	فقدان یک سیستم هشداردهنده سریع و به موقع	• بکارگیری سیستم‌های هشداردهنده سریع در حوزه های مختلف • بکارگیری سیستم‌های هوشمند اعلام خطر در خصوص حملات سایبری (نظیر DIDS) • بکارگیری سیستم‌های اعلام حریق هوشمند • آموزش پرسنل برای استفاده از این سیستم‌ها
۶۷	عدم بکارگیری سازه‌های امن و پایدار	• استفاده از سازه‌های امن و پایدار در طراحی مرکز داده • قرار دادن تجهیزات حساس و آسیب‌پذیر در فضای مطمئن
۶۸	تولید اطلاعات غلط و نامطمئن	• شناسایی علل ناشی از تولید اطلاعات غلط اعم از نرم افزاری، سخت افزاری و نیروی انسانی و رفع این موارد
۶۹	عدم بهره مندی از مراکز احتیاط (Backup) امن، ایمن و پایدار	• ایجاد یک مرکز داده پشتیبان Offline در محل فیزیکی دیگر بمنظور سرویس دهی در صورت عدم امکان سرویس دهی توسط مرکز اصلی

۷۰	عدم بکارگیری خطوط ارتباطی مطمئن و پایدار	• بکارگیری چندین خطوط ارتباط مطمئن و پشتیبان در کنار همدیگر به منظور پشتیبان ارتباطی یکدیگر • استفاده از تکنولوژی‌های ارتباطی ناهمگون
۷۱	اتصالات ناامن به شبکه‌های اینترنت و اینترانت و فیبر نوری	• طراحی صحیح اتصالات در زمان طراحی مراکز داده بمنظور عدم وجود اتصال ناامن • نظارت و کنترل دوره ای در این خصوص و شناسایی تمامی اتصالات احتمالی ناامن و حذف آنها • ایزوله بودن سرویسهای بین المللی مورد نیاز در مراکز داده از سرویسهای داخلی
۷۲	عدم پیش‌بینی برق پشتیبان	• پیش بینی برق UPS برای مرکز داده بمنظور استفاده در صورت قطع برق عادی متناسب با گستردگی، سطح و اهمیت مرکز داده • استفاده از مولدهای تولید برق پشتیبان، بمنظور پشتیبانی از برق UPS متناسب با سطح و اهمیت مرکز داده • نگهداری سوخت کافی برای مولدهای برق بمنظور استفاده در شرایط لازم
۷۳	عدم وجود نیروی انسانی متخصص لازم	• تربیت یا جذب نیروی انسانی متخصص لازم در حوزه های تخصصی مورد نیاز • ارائه آموزشهای عرضی تخصص‌های لازم به کارکنان • اولویت به استفاده از فن‌آوری‌هایی که نیروی متخصص آن در اختیار است. • تشویق کارکنان به فراگیری تخصص‌های متنوع و جدید • برگزاری آزمون‌های دوره‌ای جهت ارزیابی وضعیت آموزشی و کنترل کیفی مهارت‌های فنی آنان • برگزاری مانورهای آموزشی و مدیریت بحران به طور ادواری جهت ارزیابی سرعت عمل و انتقال در کارکنان جهت رویارویی با شرایط واقعی بحران
۷۴	عدم وجود آموزش امنیتی کافی	• برگزاری کلاسهای آگاهسازی و توجیه کارکنان در خصوص خسارات گزاف ناشی از عدم رعایت مسائل امنیتی • برگزاری دوره های آموزشی تخصصی عرضی امنیت برای متخصصین شبکه و امنیت • ارائه آموزشهای عمومی امنیت در سطوح مختلف به مدیران و کارکنان
۷۵	اشتباهات و غفلت‌ها مانند عدم بکارگیری صحیح تجهیزات، عدم نصب صحیح نرم‌افزارها و برنامه‌های کاربردی، سهل انگاری	• آموزش کارکنان در خصوص نحوه صحیح نصب تجهیزات، نرم‌افزارها، برنامه‌های کاربردی و همچنین کاربری صحیح سیستم ها و تجهیزات • تدوین برنامه‌های ادواری جهت کنترل و شناسایی اشتباهات احتمالی کارکنان • نصب سیستم‌های هشداردهنده که در صورت فراموشی و یا غفلت کاربران هشدار دهد.
۷۶	عدم وجود کنترل روی قوانین	• تدوین سیاست کاری به منظور اجرای کنترل‌های لازم بمنظور اجرای قوانین تدوینی • بازبینی دوره ای قوانین و شناسایی قوانین ضعیف و متناقض و انجام تصحیحات لازم • تشویق و تنبیه کارکنان فعال و خاطی
۷۷	اتکا قابل ملاحظه به سیستم‌های ارتباطی بی‌سیم و ماهواره غیر	• رمزنگاری داده‌های ارسالی جهت کاهش مخاطرات ناشی از دسترسی غیرمجاز به داده‌ها در شرایط اضطرار به استفاده از این ارتباطات

	امن	• عدم استفاده از سیستم‌های ارتباطی بی‌سیم بعلت عدم وجود امنیت کافی در این نوع از ارتباطات • استفاده از ارتباطات ماهواره ای داخلی در صورت راه اندازی در آینده در صورت نیاز
۷۸	عدم سازگاری با سیستم اطلاعات جغرافیایی (GIS)	• استفاده از سامانه های مبدل جهت ایجاد سازگاری با سیستم اطلاعات جغرافیایی در صورت نیاز
۷۹	زلزله	• عملیات مکان یابی صحیح و اصولی ساختمان باید در زمان انتخاب مکان مرکز داده انجام شود. • حفاظت فیزیکی در برابر آسیبهای ناشی از سیل، زلزله بایستی طراحی و بکارگرفته شود. (A.9.1.4) • طراحی و مقاومت ساختمان متناسب با کاربری مرکز داده در نظر گرفته شود. • عملیات مقاوم سازی ساختمان انجام گیرد. • آموزش افراد برای مقابله با حوادث (زلزله) • تدوین دستورالعملهای مرتبط با حوادث (زلزله) • تهیه و بکارگیری تجهیزات کمکهای اولیه • چیدمان مناسب تجهیزات جهت مقابله با لرزش های زلزله • تهیه و در دسترس بودن نقشه کلیه تأسیسات فنی و ابنیه ها • تهیه لیست تجهیزات موجود در مرکز داده • آموزش و بکارگیری گروه تعمیر، امداد و نجات
۸۰	آتش	• استفاده حداکثری از مصالح و تجهیزات مقاوم در برابر آتش در زمان ساخت مرکز داده. • طراحی حفاظت فیزیکی در برابر آسیبهای ناشی از آتش سوزی • اعمال محدودیتها در مورد ممنوعیت ورود مواد آتش زا و پرخطر • تهیه و بکارگیری سیستم های هشداردهنده و اعلام حریق • تهیه و بکارگیری تجهیزات اطفاء حریق • آموزش دوره ای افراد شاغل در مرکز در مورد پیشگیری و مهار آتش • آموزش و بکارگیری گروه اطفاء حریق
۸۱	طوفان و صاعقه	• پیش بینی سیستم برق گیر و Earth جهت انتقال بار الکتریکی اضافی به زمین • ارائه آموزش پیشگیری و مقابله با حوادث برای افراد شاغل در مرکز داده • آموزش و بکارگیری گروه حوادث غیر مترقبه
۸۲	سیل	• تجهیز مرکز به سیستم جمع آوری آبهای سطحی • طراحی حفاظت فیزیکی در برابر آسیبهای ناشی از سیل • آموزش و بکارگیری گروه حوادث غیر مترقبه
۸۳	رطوبت و دما	• تهیه و بکارگیری تجهیزات تهویه مطبوع در ساختمان مرکز داده • استفاده از مصالح مناسب در ساخت مرکز داده

		• استفاده از دماسنج و رطوبت سنج بخصوص در نقاطی که از تجهیزات حساس به دما استفاده می شود
۸۴	دود	• تهیه و بکارگیری نورافکن و مه شکن در نقاط مختلف مرکز داده و پیرامون آن • بکارگیری تجهیزات کم کننده اثرات دود • پیش بینی ارتباط با مرکز هواشناسی
۸۵	سقوط اجسام	• رعایت استحکام مناسب در طراحی سازه مراکز داده متناسب با نوع آنها
۸۶	تداخل الکترومغناطیسی امواج	• مکان یابی نصب تجهیزات به منظور دوری از تجهیزات تداخل کننده مثل خطوط برق فشار قوی و خطوط با جریان بالا • رعایت استانداردهای مربوط به کابل کشی و فواصل مربوط به نصب کابل های انتقال داده ، برق و تلفن در زمان طراحی مرکز داده • آموزش و بکارگیری گروه متخصص در خصوص اختلال های الکترومغناطیسی
۸۷	مشکلات تأسیساتی (آب ،گاز، برق، تلفن)	• طراحی مناسب تأسیسات و رعایت استانداردهای نصب مسیرهای انتقال در زمان طراحی مرکز داده • استفاده از سیستم های هوشمند هشدار دهنده و کنترل کننده تاسیسات • حفاظت تجهیزات از افت جریان برق یا هر اختلالی که بر اثر عدم پشتیبانی تأسیسات بوجود می آید • استفاده از سیستم های پشتیبان برای آب، گاز، برق و تلفن بمنظور استفاده در صورت اختلال در مسیر اصلی • آموزش و بکارگیری گروه تاسیسات
۸۸	مواد پرخطر	• کنترل و نظارت بمنظور عدم انتقال مواد پرخطر و حساس • بازرسی افراد و تجهیزات به هنگام ورود و خروج • پیش بینی تجهیزات لازم بمنظور مقابله با حوادث احتمالی پیش آمده از طریق این مواد • آموزش و بکارگیری گروه متخصص جهت انجام عکس العمل مناسب
۸۹	تشعشعات رادیواکتیو	• نصب تجهیزات هشدار دهنده جهت اعلام خطر نشت مواد رادیواکتیو در محیط • قرار دادن لباس‌های مخصوص کار در محیط‌های آلوده به تشعشعات رادیواکتیو جهت استفاده پرسنل در صورت نیاز • استفاده از گیت‌های ورودی حساس به تشعشعات رادیواکتیو در تمامی ورودی‌های مراکز داده • تجهیز دیواره‌های داخلی مراکز داده به مواد شیمیایی مخصوص جذب موارد رادیواکتیو • آموزش و بکارگیری گروه متخصص جهت انجام عکس العمل مناسب
۹۰	گرد وغبار و مه	• بکارگیری فیلترهای جلوگیری کننده از ورود گرد و غبار • استفاده از حسگرهای گرد و غبار بمنظور اعلام هشدار در مواقع لازم • آموزش کارکنان در مورد نحوه رفع مشکل • آموزش و بکارگیری گروهی جهت انجام عکس العمل مناسب

۹-۵ ملاحظات پدافند غیر عامل برای مراکز داده حساس

جدول ۴. ملاحظات پدافند غیرعامل برای مراکز داده حساس

ردیف	تهدید	شرح کنترل
۱	اختلال الکترونیکی و الکتریکی	• ایجاد اتصال زمین برای تجهیزات به منظور انتقال بار الکتریکی اضافی • تجهیزات باید از افت جریان برق یا هر اختلالی که بر اثر عدم پشتیبانی تأسیسات بوجود می‌آید، حفاظت شوند. (A.9.2.2) • تجهیزات محافظ جهت جلوگیری از عملکرد اعوجاج و امواج الکترونیکی و الکتریکی • تجهیزات محافظ ولتاژ به منظور جلوگیری از تغییرات و ضربه های ولتاژ برق • بکارگیری سیستم برق اضطراری مجهز به مانیتور جهت مشاهده وضعیت برق تغذیه کننده سیستم ها • محافظت در مقابل نقایص منبع تغذیه • آموزش کارکنان شاغل در مرکز جهت رفع اشکالات مربوط به اختلال های الکترونیکی و الکتریکی • بکارگیری ژنراتور برق جهت تولید برق در زمان وقوع اختلال • استفاده از تجهیزات جلوگیری کننده از اختلال الکترونیکی
۲	کدهای مخرب و بدافزارها (Malwares)	• کنترل‌های کشف، جلوگیری، و ترمیم به منظور محافظت در برابر کدهای مخرب، به همراه روال‌های مناسب آگاهی کاربران باید پیاده‌سازی شوند. (A.10.4.1) • جایی که استفاده از کد سیار مجاز است، پیکربندی آنها باید به گونه‌ای باشد که اطمینان از تطابق کدهای سیار مجاز با خط مشی های امنیتی تعریف شده، حاصل شود و باید از اجرای کد سیار غیر مجاز جلوگیری شود. (A.10.4.2) • استفاده از نرم‌افزارهای بومی جهت کشف بدافزارها • ایجاد محدودیت‌هایی در جهت ممانعت از دریافت کدهای اجرایی از سوی افراد • مسدود کردن درگاه‌های غیرضروری سیستم به منظور جلوگیری از امکان سوء استفاده به عنوان درهای پشتی
۳	دسترسی غیرمجاز از راه دور	• باید یک خط مشی رسمی اِعمال شده و روشهای مناسب امنیتی جهت محافظت در برابر ریسکهای استفاده از کامپیوترهای سیار و امکانات ارتباطات باید به کار گرفته شوند. (A.11.7.1) • باید یک خط مشی، برنامه های عملیاتی و روش های اجرایی توسعه یافته برای فعالیتهای کاری از راه دور اجرا شوند.(A.11.7.2)

۴	وقفه در کار	• فرآیند تنظیم شده باید توسعه یافته و باید جهت استمرار کسب و کار در کل سازمان نگهداری شود که اشاره به الزامات امنیتی اطلاعات مورد نیاز برای استمرار کسب و کار سازمان را دارد. (A.14.1.1) • رخدادهایی که ممکن است باعث وقفه در کار مرکز داده شوند باید به همراه احتمال و خسارت ناشی از وقفه و دیگر پیامدهای امنیتی مشخص شوند. • باید برای نگهداری یا بازیابی عملیات و اطمینان از دسترس‌پذیری در سطح مورد نظر و در زمان مورد نظر برنامه‌ریزی شود. • باید یک چارچوب کلی برای طرح‌های استمرار کسب و کار تدوین شود تا طرح‌ها سازگار بوده و نیازمندیهای امنیتی را به درستی مشخص کنند. همچنین اولویت‌های آزمون و ارزیابی را مشخص نماید. • طرحهای تداوم کسب و کار باید آزمایش شده و به طور منظم ارتقاء یابند تا از به روز بودن و اثر بخشی آنها اطمینان حاصل شود. (A.14.1.5) • هر طرحی که احتمال ایجاد وقفه در کسب و کار را تقویت می‌کند می‌بایستی برکنار و راه‌کار جایگزینی ارائه گردد. • عوامل ایجاد وقفه شناسایی گردند و ریسک حضور این عوامل در طراحی مرکز داده در نظر گرفته شود.
۵	جاسوسی	• هر مورد از تجهیزات که شامل ذخیره رسانه است، قبل از کنار گذاری باید به منظور حصول اطمینان از عدم وجود اطلاعات خاص بررسی شود. اینگونه اطلاعات و نرم افزارهای ثبت شده کنار گذاشته شده باید قبل از کنار گذاری در صورت نیاز بر روی رسانه ای دیگر ثبت گردد. • بکارگیری سیستم تشخیص هویت و شناسایی افراد به صورت جامع • جلوگیری از عکاسی ، فیلمبرداری و ضبط صدا • ثبت تمام ورود و خروج ها • آموزش ضد جاسوسی به کارکنان • تهیه نقشه تأسیسات و قابلیت دسترسی آنها برای افراد مجاز • تهیه لیست تجهیزات و قابلیت دسترسی آنها برای افراد مجاز • جداسازی مکانهای فعالیت افراد
۶	حملات تروریستی سایبری(هکرها)	• تهیه داده‌های پشتیبان در فواصل زمانی مناسب به منظور جلوگیری از احتمال بروز خرابی در تمامیت و صحت داده‌ها • ردگیری و تهیه سوابق دقیق از عملیات صورت گرفته از سوی هر کاربر به منظور مطالعه و شناسایی رفتار و اقدامات مشکوک صورت گرفته • کاهش سطح تماس سرویس‌های مرکز داده به متقاضیان • پرهیز از افشاء ماهیت و رفتار درونی سیستم، نرم افزار/ سخت‌افزار و مولفه‌های نرم‌افزاری به کار رفته در آن به سایرین

		• اتخاذ سیاست امنیتی مثبت به عنوان یک سیاست امنیتی بازدارنده • استفاده از مولفه‌های امنیتی فعال چون دروازه‌های آتش در محل ورودی ترافیک به شبکه داخلی مرکز داده • به کارگیری سیستم های تشخیص نفوذ مبتنی بر رفتار و امضاء جهت تشخیص به موقع ناهنجاری‌های رفتاری کاربران • آموزش پرسنل به استفاده از کلمات عبور طولانی و پیچیده و تغییر کلمات عبور به طور ادواری • به کارگیری تیمی از متخصیص نفوذ به منظوری شناسایی حفره‌های امنیتی موجود بخصوص در سطح نرم‌افزار و اتخاذ راه‌کارهایی جهت انسداد این حفره‌ها • غیرفعال کردن سرویس‌ها و مولفه‌های عمومی غیر قابل استفاده در سطح مرکز داده • استفاده از مولفه‌های نرم‌افزاری اختصاصی (in-house) به جای استفاده از مولفه‌های عمومی؛ بسیاری ازاین مولفه‌های به دلیل قابل دسترس بودن ضعف‌های امنیتی آنان برای همگان شناخته شده است.
۷	دسترسی غیرمجاز به اطلاعات	• خط مشی کنترل دسترسی باید پایه‌ریزی و مستند سازی شده و بر اساس کسب و کار و الزامات امنیتی برای دسترسی بازنگری شود. (A.11.1.1)
۸	دسترسی غیرمجاز به شبکه	• برای کاربران فقط دسترسی به سرویس هایی باید مهیا شوند که بطور مشخص اجازه استفاده از آنها را دارند.(A.11.4.1) • روشهای مناسب باید برای کنترل دسترسی توسط کاربران بیرونی مورد استفاده قرار بگیرد. • دسترسی فیزیکی و منطقی به درگاهها (پورت‌ها) باید تحت کنترل باشد. • برای شبکه های مشترک به خصوص آنهایی که به خارج از مرزهای سازمانی کشیده شدند ظرفیت کاربران محدود شود. • برای حصول اطمینان از اینکه ارتباطات کامپیوتری و جریان اطلاعات، خط مشی کنترل دسترسی را نقض نکند باید کنترل مسیریابی برای شبکه ها اجرا شود. (A.11.4.7) • حداکثر تعداد اتصال یا نشست‌های همزمان به یک سیستم باید کنترل و محدود شود. این محدودیت توسط مدیر سیستم تعیین می‌شود. (NIST-AC-10) • مرکز داده باید از مکانیزم‌های خودکار برای تسهیل در پایش و کنترل روشهای دسترسی از راه دور استفاده نماید. (NIST-AC-17(1)) • مرکز داده باید از رمزنگاری برای فراهم کردن محرمانگی نشست‌های از راه دور استفاده نماید. ((NIST-AC-27(2) • مرکز داده همه دسترسی‌های از راه دور را از طریق یک نقطه کنترل دسترسی مدیریت شده، کنترل می‌نماید. ((NIST-AC-27(3)

۹	دسترسی غیرمجاز به سیستم‌عامل	• دسترسی به سیستم های عامل باید توسط فرآیند اجرایی امن (Logon) کنترل شوند.(A.11.5.1) • همه کاربران باید ID انحصاری برای استفاده شخصی خود داشته باشند و باید یک تکنیک مناسب تأیید، جهت اثبات ادعای ID کاربر انتخاب شود. • سیستم های تنظیم کلمه عبور باید دو سویه بوده و کیفیت کلمه عبور را اطمینان دهد. • استفاده از برنامه های کاربردی که توانایی کنترل کاربردها را داشته باشند به شدت تحت کنترل قرارداده شده و محدود شوند. • برای فراهم نمودن امنیت بیشتر برای کاربردهای دارای ریسک بالا، باید محدودیت هایی در زمان برقراری اتصال اعمال شود.(A.11.5.6)
۱۰	دسترسی غیرمجاز به برنامه‌های کاربردی	• دسترسی به اطلاعات و عملیات سیستمهای کاربردی توسط کاربران و کارکنان پشتیبانی باید طبق خط مشی کنترل دسترسی مشخص محدود گردد.(A.11.6.1) • سیستمهای حساس باید محیط کامپیوتری(محاسباتی) اختصاصی(مجزا) داشته باشند.(A.11.6.2)
۱۱	دسترسی غیر مجاز به اطلاعات یا سیستم‌های حین مبادله با نهادهای خارج از مرکز داده	• خط مشی تبادل رسمی، روش های اجرایی و کنترل ها جهت حفاظت از تبادل اطلاعات با استفاده از همه انواع امکانات ارتباطی باید در محل وجود داشته باشد.(A.10.8.1) • توافقات جهت مبادله اطلاعات و نرم افزار بین سازمان و طرفهای خارج از سازمان باید پایه ریزی و تدوین شوند. • رسانه های حاوی اطلاعات باید در مقابل دسترسی غیرمجاز، سوء استفاده یا انحراف در زمان انتقال به خارج از مرزهای فیزیکی سازمان، حفاظت شود. • خط مشی ها و روش های اجرایی جهت حفاظت از اطلاعات همراه با ارتباطات داخلی سیستمهای اطلاعاتی کسب و کار باید تدوین شده و دائما ارتقاء یابند.(A.10.8.5)

۱۲	پردازش‌های اطلاعاتی غیر مجاز	• الزامات ممیزی و فعالیتهای که شامل بررسی سیستم‌های عملیاتی است، برای کمینه کردن مخاطرات اختلال در فرایند کسب و کار، باید با دقت طرح‌ریزی و تصویب شوند.(A.15.3.1) • رکوردهای ممیزی مربوط به فعالیت‌های کاربران، وقایع استثنایی، و رویدادهای امنیتی باید تولید و نگهداری شوند. این رکوردها برای کمک به تفحصهای آتی و نظارت بر کنترل دسترسی کاربرد دارند. (A.10.10.1) • فرایند اجرایی برای استفاده از مراقبت امکانات پردازش اطلاعات باید پایه ریزی شده و نتایج نظارت فعالیتها باید به طور منظم بازنگری شوند. • امکانات ثبت کردن و ثبت اطلاعات باید در برابر دسترسی بدون مجوز و پنهانی حفاظت شود. • فعالیتهای مدیر و اپراتور سیستم باید ثبت شوند. • خطاها باید ثبت و تحلیل شده و اقدامات مناسب صورت بگیرد. • ساعت سیستمهای پردازش اطلاعات در سازمان یا حوزه امنیتی باید با زمان دقیق مرجع هماهنگ باشند.(A.10.10.6) • در صورت بروز خطا در ثبت رکوردهای ممیزی یا پر شدن ظرفیت محل ذخیره، باید هشدار مناسب به مدیر فنی مربوط داده شده و اقدام مقتضی (توقف ثبت، خاموش کردن سیستم، یا بازنویسی روی رکوردهای قدیمی) انجام شود. (NIST AU-5) • سیستم‌های اطلاعاتی باید مهر زمانی (timestamp) هر رویداد را مشخص نمایند. (NIST AU-8) • سیستم‌های اطلاعاتی باید از اطلاعات ممیزی و ابزارهای ممیزی در مقابل دسترسی غیرمجاز، تغییر یا حذف محافظت کنند. (NIST AU-9) (A.15.3.2) • هر سیستم اطلاعاتی باید امکان ثبت وقایع بیشتر و جزئی‌تر در رکوردهای ممیزی به همراه نوع، محل، و عامل آن فراهم کنند. (NIST AU-3(1)) • در صورتی که حجم رکوردهای ممیزی به ۷۵٪ ظرفیت محل ذخیره رسید، باید سیستم اطلاعاتی هشداری به مدیر سیستم بدهد. (NIST AU-5(1)) • سیستم‌های اطلاعاتی باید قابلیت تحلیل و خلاصه‌سازی رکوردهای ممیزی و تولید گزارش‌های مفید و قابل پیکربندی بر اساس انتخاب رویدادهای خاص را داشته باشند. (NIST AU-7, AU-7(1))
۱۳	تغییر غیرمجاز، از دست دادن یا سوءاستفاده از اطلاعات در برنامه‌های کاربردی	• داده های ورودی برای سیستم کاربردی باید برای حصول اطمینان از صحت و مناسب بودن آنها، اعتبار سنجی شوند. (A.12.2.1) • باید در سیستم‌های کاربردی از وارسی‌های اعتبارسنجی به منظور کشف هر گونه خرابی داده استفاده شود. • الزامات برای اطمینان از درستی و حفاظت از صحت پیام در کاربردها باید مشخص شده و کنترل های مناسب باید مشخص و اجرا شوند.

		• داده های خروجی یک سیستم کاربردی باید به منظور اطمینان از درستی و مناسب بودن پردازش اطلاعات ذخیره شده با شرایط مربوطه مورد تعیین اعتبار قرار گیرد.(A.12.2.4)
۱۴	حمله فیزیکی، هسته‌ای و اتمی	• استفاده از تکنیکهای استتار بمنظور عدم تشخیص مکان مرکز داده توسط دشمن • استفاده از تکنیکهای اختفا بمنظور عدم تشخیص مکان مرکز داده توسط دشمن • استفاده از تکنیک‌های فریب دشمن بمنظور عدم تشخیص مکان واقعی مرکز داده • تهیه اطلاعات پشتیبان و ارسال آنان به نقطه‌ای خارج از فضای فیزیکی مرکز داده بمنظور حفظ داده ها و اطلاعات • ایجاد یک مرکز داده پشتیبان Offline در محل فیزیکی دیگر بمنظور سرویس دهی در صورت عدم امکان سرویس دهی توسط مرکز اصلی • تربیت تیم های تخصصی بمنظور استفاده جهت ترمیم آسیب ها در شرایط اضطرار • مکان یابی محل فیزیکی مناسب بمنظور ایجاد مرکز داده و استفاده از منابع طبیعی نظیر کوه برای این منظور • ایجاد یک مرکز داده پشتیبان فعال (Active) در محل فیزیکی دیگر بمنظور سرویس دهی در صورت عدم امکان سرویس دهی توسط مرکز اصلی • ایجاد سازه مرکز داده بصورت زیر زمینی و در عمق زمین
۱۵	بمب گذاری یا انفجار	• کنترل تردد تجهیزات و بسته ها • طراحی و بکارگیری برنامه حفاظت فیزیکی در برابر آسیبهای ناشی از انفجار (A.9.1.4) • آموزش کارکنان شاغل در مرکز جهت رفع اشکالات و ایرادات بوجود آمده پس از انفجار • ارتباط مستقیم با متخصصان مربوط به خنثی سازی موارد منفجره • وجود تجهیزات و افراد خنثی کننده بمب
۱۶	حوادث شیمیایی	• شیلد نمودن و عایق بندی جداره‌های و منافذ ورودی تأسیسات مراکز داده به منظور جلوگیری از نفوذ گازهای شیمیایی به داخل مراکز • استقرار تجهیزات ایمنی از قبیل ماسک و سایر تجهیزات موجود جهت جلوگیری از آسیب پرسنل • نگهداری پادزهرهای مختلف مربوط به انواع گازهای شیمیایی در جعبه کمک‌های اولیه به منظور انجام اقدامات اولیه به مصدومین

۱۷	جنگ الکترومغناطیسی	• مکان یابی نصب تجهیزات به منظور دوری از تجهیزات منشا تداخل مثل خطوط برق فشار قوی و خطوط با جریان بالا • آموزش کارکنان شاغل در مرکز جهت رفع اشکالات مربوط به اختلال های الکترومغناطیسی • رعایت استانداردهای مربوط به کابل کشی و فواصل مربوط به نصب کابل های انتقال داده ، برق و تلفن • استفاده از سیستم برق اضطراری برای مواقع خاص • بکارگیری حفاظهای امواج الکترومغناطیس بر روی بسترهای انتقال
۱۸	ارگانیزم ها (ویروس، باکتری و...)	• کنترل مواد خوراکی • کنترل محیط مرکز داده در خصوص گسترش موارد ارگانیزمی و اقدامات پیشگیرانه • آموزش کارکنان شاغل در مرکز جهت مقابله با موارد ارگانیزمی • ایجاد مرکز بهداشت و درمان به منظور رفع مشکلات با گستردگی محدود در مورد افراد شاغل • نمونه گیری و آزمایش مرتب موارد خوراکی و محیط
۱۹	دسترسی غیر مجاز به سیستم ها، تجهیزات و منطقه فیزیکی	• نقاط دسترسی نظیر نواحی بارگیری یا تحویل و دیگر نقاطی که احتمال ورود اشخاص فاقد صلاحیت وجود دارد کنترل شده و در صورت امکان از سایر بخش‌ها و تأسیسات منفک گردد. • تجهیزات باید به منظور کاهش ریسک های حاصل از تهدیدات و آسیبهای محیط و فرصتهای دسترسی غیرمجاز، حفاظت شوند.(A.9.2.1) • تجهیزات باید جهت حصول اطمینان از تداوم دسترسی و صحت بطور مناسب نگهداری شوند.(A.9.2.4) • تجهیزات، اطلاعات یا نرم افزار نباید بدون مجوز قبلی از محل خارج شوند. (A.9.2.7) • از سامانه های امنیتی (موانعی نظیر دیوارها، گیت های ورودی که با کارت کنترل می شود یا میزهای پذیرش آماده) بمنظور محافظت ناحیه هایی که شامل اطلاعات و سامانه های پردازش اطلاعات باشد، استفاده شود. (A.9.1.1) • نواحی امن بوسیله کنترل های ورودی مناسب جهت اطمینان از اینکه فقط پرسنل مجوز دار اجازه دسترسی داشته باشند محافظت شود. (A.9.1.2) • امنیت فیزیکی لازم برای دفاتر، اتاق ها و تاسیسات، طراحی و بکار گرفته شود.(A.9.1.3) • آموزش های لازم به کابران ارائه گردد. • بکارگیری سیستم حفاظت فیزیکی هوشمند پیرامونی (دوربین های مدار بسته) و هشدار دهنده

۲۰	دسترسی غیر مجاز به رسانه‌های ذخیره‌سازی اطلاعات	• باید دستورالعمل اجرایی برای مدیریت رسانه متحرک تدوین گردد. (A.10.7.1) • در صورت عدم نیاز به یک رسانه، باید به صورت امن و ایمن و طی یک فرآیند رسمی امحاء شود. (A.10.7.2) • مستند سازی سیستم باید در برابر دسترسی غیر مجاز حفاظت شود.(A.10.7.4) • رسانه های ذخیره سازی اطلاعات در محل امن نگهداری شوند. • اطلاعات رسانه قبل از تعویض ثبت گردد. (A.9.2.6) • وجود روش های اجرایی در محل برای مدیریت رسانه متحرک. (A.10.7.1) • در صورت عدم نیاز به یک رسانه، باید به صورت امن و ایمن و طی یک فرآیند رسمی امحاء شود. (A.10.7.2) • شبکه ها باید به منظور حفاظت در برابر تهدیدها و حفظ امنیت سیستمها و برنامه های کاربردی شبکه و داده های در حال انتقال، به طور مناسب مدیریت شوند.(A.10.6.1)
۲۱	دسترسی فیزیکی غیرمجاز به بستر انتقال داده‌ها	• لزوم حفاظت از بسترهای انتقال داده با تدوین سیاست نامه ای در خصوص نحوه دسترسی به آنها، مسئولیتهای افراد در این ارتباط و کد گذاری بسترها ی انتقال (NIST-MP-1)، (NIST-MP-2) و (NIST-MP-3) • نحوه دسترسی، افراد مجاز و نحوه دریافت اطلاعات ورودی به بسترهای انتقال از هر نوع (اطلاعات الکترونیکی ، کاغذی و ...) بایستی مورد کنترل قرار گیرد. (NIST-MP-5) • حفاظت فیزیکی مناسب از کابلها و بکارگیری داکت • قرار دادن کانال انتقال داده‌ها در محیط غیرقابل دسترسی • کنترل بسترهای انتقال داده در زمان کنارگذاری و یا استفاده مجدد آنها.(NIST-MP-7) • استفاده از مکانیزم‌های بازدارنده روی کانال‌های انتقال داده به منظور کاهش احتمال دسترسی فیزیکی غیرمجاز
۲۲	عدم سازگاری با فن‌آوری‌های مدرن جنگ الکترونیک	• جایگزینی فن‌آوری موجود با فن آوری قابل انطباق • استفاده از فن‌آوری‌های مبدل به منظور انطباق فن‌آوری موجود با فن‌آوری مدرن • تلاش برای بروزسازی فن‌آوری جدید با افزودن قابلیت‌های موجود در فن‌آوری‌های مدرن
۲۳	تهدید ناشی از عدم سازگاری با سیستم‌های مدرن اطلاعات عملیات	• استفاده از مولفه‌های مبدل به منظور ایجاد ارتباط و هماهنگی بین سیستم‌های کنونی اطلاعات عملیات و سیستم‌های نوین اطلاعات عملیات
۲۴	تهدید ناشی از عدم سازگاری با فن آوری‌های مدرن جنگ متحرک	• اتخاذ ملاحظاتی برای امکان جابجایی تجهیزات ذخیره سازی داده ها و اطلاعات در زمان بحران بمنظور استفاده در مرکز داده دیگر

۲۵	آسیب یا سرقت (الکترونیکی)	• آموزش کارکنان شاغل در مرکز جهت جلوگیری از سرقت الکترونیکی شناسه‌های هویت آنها • ملزم کردن کارکنان به تغییر کلمات عبور به صورت ادواری • استفاده از کلمات عبور پیچیده، طولانی غیرقابل حدس زدن • دسترسی به اطلاعات طبقه‌بندی شده باید لزوماً با عبور از مکانیسم‌های احراز هویت چندگانه امکان‌پذیر گردد. • کاهش کانال‌های الکترونیکی جهت دسترسی کاربران به منابع داده‌ای و سرویس‌های ارائه شده از سوی مرکز داده
۲۶	آسیب یا سرقت (فیزیکی)	• از تجهیزات باید به منظور کاهش ریسک های حاصل از تهدیدات و آسیبهای محیط و فرصتهای دسترسی غیرمجاز، متناسب با ماهیت هر یک حفاظت شود. • آموزش کارکنان شاغل در مرکز جهت جلوگیری از آسیب یا سرقت • از نقشه تأسیسات و موارد زیر بنایی در مکان مناسب (گاوصندوق یا محل مطمئن) حفاظت گردد. • ثبت ورود و خروج افراد • حفاظت از لیست تجهیزات • حفاظت از تجهیزات در زمان انتقال به تعمیرگاه و یا به هنگام تعمیر و رعایت تمهیدات مربوطه • جداسازی مکانهای فعالیت افراد دارای دسترسی های مختلف • رعایت اصول و سطوح طبقه بندی
۲۷	اختلال در ارتباطات شبکه	• استفاده از کانال‌های ارتباطی فاقد امکان اختلال • شیلد کردن کانال‌ها و تجهیزات ارتباطی و مکانهای قرار گرفتن این تجهیزات • استفاده از ارتباطات پشتیبان ناهمگون
۲۸	اختلال در سیستم برق	• بکارگیری سیستم توان پشتیبان • استخدام نیروهای متخصص برق به منظور انجام سرویس بلادرنگ در زمان بروز اختلال در سیستم برق • نگهداری سوخت کافی برای ژنراتورهای مولد برق برای شرایط خاص که امکان دسترسی به سوخت تا مدت‌ها وجود ندارد
۲۹	قرار دادن کشور در موقعیت جنگ تمام عیار اطلاعاتی	• الزام به قرار گرفتن در شرایط آماده باش کامل به منظور نظارت بر حسن اجرای تمامی کنترل‌های پیشنهادی (پدافند غیرعامل و امنیت)
۳۰	تهدید ناشی از تحریم فن آوری های پیشرفته خارجی	• تلاش جهت تسلط بر دانش و فناوری ها بمنظور بومی‌سازی فن‌آوری به منظور کاهش دغدغه‌های ناشی از تحریم فن‌آوری • تعامل با بخش های تحقیقاتی و پژوهشی کشور بمنظور بکرگیری حداکثری توان داخلی جهت تولید فناوری های لازم در داخل کشور داخل کشور

۳۱	وابستگی به خارج از کشور در بخش تعمیر و نگهداری	• انتقال دانش تعمیر و نگهداری به متخصصین بومی • استفاده از تکنولوژی‌های بومی موجود • جلوگیری از امکان دسترسی به داده‌های طبقه‌بندی شده و سوابق ذخیره شده بر روی سخت‌افزار و رسانه‌های ذخیره سازی مربوطه با تهیه نسخه پشتیبان و امحاء داده‌های موجود بر روی سیستم‌ها قبل از ارسال به مراکز تعمیر • قطع وابستگی به تعمیر و نگهداری با بومی سازی تکنولوژی مربوطه و انتقال دانش تعمیر و نگهداری به داخل کشور
۳۲	وابستگی به تولیدات سخت افزاری و نرم افزاری خارجی	• انتقال دانش تولید سخت افزارها و نرم افزارها به متخصصین بومی • استفاده حداکثری از محصولات بومی موجود • رعایت ملاحظات امنیتی در استفاده از محصولاتی که نمونه داخلی آنها وجود ندارد
۳۳	تغییر سریع فن آوری (در حوزه جنگ سایبر)	• تلاش جهت تسلط بر دانش و فناوری ها بمنظور بومی‌سازی فن‌آوری به منظور کاهش دغدغه‌های ناشی از تغییرات در فن‌آوری • آموزش نیروی متخصص و کارآمد جهت بهره گیری و انتقال فن‌آوری به داخل کشور • رعایت ملاحظات امنیتی در صورت لزوم استفاده از فناوریهای جدید و مشاوره با بخشهای متخصص آگاه و امین در کشور • تعامل با سازمانهای داخلی مرتبط با دانش و فناوریها بمنظور تسریع در روند بومی سازی فن آوری
۳۴	جهانی شدن	• تعامل با سازمانها و نهادهای مربوطه در داخل کشور بمنظور توجه به چالش‌های پیش روی جهانی شدن جهت ارائه راه‌کارهایی به منظور تطبیق با شرایط جدید • اتخاذ سیاست‌هایی در راستای تغییرات و تمهیدات ایجاد شده بمنظور اعمال در سازمان
۳۵	زیرساخت‌های عمده جهانی نظیر اینترنت	• استفاده از زیرساخت های بومی و قابل اتکاء و اعتماد در صورت وجود • استفاده کنترل شده از زیرساخت‌های جهانی با رعایت مسائل امنیتی و حفاظتی • استفاده از این زیرساخت‌های تنها برای اهداف خاص • استفاده از این زیرساخت‌های بصورت جداگانه (ایزوله) از زیرساختهای اصلی مرکز داده
۳۶	حملات مختل کننده خدمات	• بکارگیری سیستم‌هایی به منظور جلوگیری از نفوذ و شناسایی حملات مختل کتنده خدمات در صورت نفوذ، نظیر IDSها و فایروالهای بومی • شناسایی و ثبت الگوهای رفتاری حمله‌کنندگان داخلی به منظور جلوگیری از الگوهای رفتاری مشابه توسط سایر کاربران • پیش بینی و بکارگیری مراکز احتیاط وتشکیل تیمهای CERT در شرایط وقوع وقفه سرویس • تعیین حدمجاز بهره‌مندی کاربران از سرویس‌های ارائه شده

		• قرار دادن کاربران خاطی و غیرقابل اعتماد در لیست سیاه و ممانعت از سرویس‌دهی به آنان
۳۷	جنگ روانی دشمن	• برگزاری دوره های آگاهسازی برای کارکنان و کاربران در این خصوص • انتشار مستنداتی از اهداف خرابکارانه دشمن در تضعیف روحیه افراد که حاکی از بی‌پایه بودن گفته‌های دشمن دارد
۳۸	تغییر هویت اطلاعات درحال گذر	• استفاده از الگوریتم‌های رمزنگاری بومی، امضاهای دیجیتال در رمزنگاری اطلاعات متناسب با ماهیت و نوع سرویسها به منظور جلوگیری از افشا و امکان دستکاری اطلاعات در حال گذر • عدم استفاده از الگوریتم های رمزنگاری غیرمطمئن بمنظور رمزنگاری اطلاعات در حال گذر • استفاده از مکانیزمهای پنهان نگاری اطلاعات در شرایط لازم بمنظور انتقال اطلاعات مهم • عدم استفاده از کانال‌های ارتباطی بی‌سیم بدون در نظر گرفتن مکانیزمهای امنیتی مطمئن
۳۹	دسترسی غیرمجاز به اطلاعات	• استفاده از مکانیزمهای رمزنگاری اطلاعات و الگوریتم‌های رمزنگاری بومی بمنظور نگهداری اطلاعات بر روی رسانه های ذخیره سازی اطلاعات • عدم استفاده از الگوریتم های رمزنگاری غیرمطمئن بمنظور رمزنگاری اطلاعات • استفاده از مکانیزم‌های احراز هویت برای دسترسی به سرویسها و اطلاعات به منظور جلوگیری از دسترسی غیر مجاز به اطلاعات • پیش بینی تمهیدات امنیتی متناسب با سطح اهمیت و میزان تجمیع اطلاعات • استفاده از کانالهای ارتباطی خاص و غیر مشترک جهت تبادل اطلاعات با پیش بینی تمهیدات امنیتی • استفاده از مکانیزم‌های احراز هویت حداقل ۲ عاملی برای دسترسی به سرویسها و اطلاعات به منظور جلوگیری از دسترسی غیر مجاز به اطلاعات
۴۰	ناآرامی‌های اجتماعی	• محافظت بمنظور عدم افشای محل مرکز داده • حفاظت فیزیکی در برابر آسیبهای ناشی از آشوب های شهری بمنظور جلوگیری از ورود افراد متفرقه • محافظت بمنظور ذکر نشدن محل مرکز داده در نقشه های جغرافیایی • احداث مرکز داده در مکانهای فیزیکی غیر قابل دسترس مردم عادی

۴۱	ورود و خروج غیر مجاز افراد	• محیط های امنیتی (موانعی نظیر دیوارها، گیت های ورودی که با کارت کنترل می شود یا میزهای پذیرش آماده) باید بمنظور محافظت ناحیه هایی را که شامل اطلاعات و سامانه های پردازش اطلاعات باشد، استفاده شود. (A.9.1.1) • از سامانه های امنیتی (موانعی نظیر دیوارها، گیت های ورودی که با کارت کنترل می شود، دستگاههای X-Ray یا میزهای پذیرش آماده) بمنظور کنترل ورود و خروج افراد و تجهیزات همراه آنها استفاده شود. (A.9.1.1) • بکارگیری دوربین های کنترل تردد و سیستم حفاظت پیرامونی • اجبار در استفاده ازکارت شناسایی توسط افراد و کنترل آن توسط مبادی ذیربط • ثبت زمان ورود و خروج افراد • آموزش کارکنان • جداسازی مکانهای فعالیت افراد دارای طبقه بندی مختلف و رعایت اصول حیطه بندی
۴۲	عدم رویکرد مداوم برای مدیریت حوادث امنیتی	• باید مسئولیتهای مدیریت و فرآیندهای اجرایی جهت حصول اطمینان از پاسخ، سریع، موثر و مرتب به حوادث امنیتی اطلاعات پایه ریزی شود. (A.13.2.1) • باید مکانیزمهایی برای سنجش و پایش نوع، حجم، و هزینه حوادث امنیتی وجود داشته باشند. (A.13.2.2) • هر مرکز داده بایستی دارای مرکز عملیات امنیتی (SOC) بمنظور مانیتور و کنترل حوادث امنیتی باشد. • بعد از حادثه امنیتی اطلاعات، پی گیری در برابر فرد یا سازمانی صورت می گیرد که شامل اقدام قانونی (چه مدنی ، جزایی) است، شواهد باید جمع آوری و نگهداری شده و برای مطابقت با قوانین جهت مطرح شدن شواهد در یک دادرسی مربوطه ارائه شوند. (A.13.2.3) • سازمان بایستی میزان سرعت واکنش و کارآیی مکانیزمها در شرایط مورد نیاز را، آزمایش نماید. (NIST-IR-3)
۴۳	عدم اصلاح و بازیابی پس از حوادث امنیتی	• رویدادهای امنیتی اطلاعات باید توسط مدیریت کانالهای مناسب تا حد امکان به سرعت گزارش شوند.(A.13.1.1) • مرکز داده بایستی دارای تیم CERT بمنظور ترمیم حوادث احتمالی در صورت وقوع، باشد. • تمام کارکنان پیمانکاران و مصرف کنندگان ثالث مصرف کننده سیستمها و خدمات اطلاعات باید ملزم شوند تا هرگونه ضعف امنیتی مشاهده شده و مشکوک در سیستمها و خدمات را به آن توجه کرده و گزارش دهند.(A.13.1.2)
۴۴	ناامنی یا نادرستی در عملیات پردازش اطلاعات	• روش های اجرایی عملیاتی باید مستند سازی و نگهداری شده، و برای همه کاربران که به آن نیاز دارند در دسترس باشد.(A.10.1.1) • تغییرات در امکانات پردازش اطلاعات و سیستمها باید کنترل شده باشند.

		• وظایف و حوزه های مسئولیت باید در راستای کاهش فرصت برای افراد غیرمجاز یا تغییرات ناخواسته یا سوء استفاده از دارایی های سازمان تفکیک شوند. • پیشرفت، آزمایش و امکانات عملیاتی باید تفکیک شوند تا دسترسی های غیرمجاز یا تغییرات سیستم عملیاتی را کاهش دهد.(A.10.1.4)
۴۵	عدم امنیت در تعامل با طرفهای ثالث	• استفاده از منابع باید مراقبت و تنظیم گردد. پیش بینی های لازم طبق الزامات ظرفیت آینده جهت حصول اطمینان از عملکرد سیستم ضروری است.(A.10.3.1) • باید معیار پذیرش سیستم های اطلاعاتی جدید، ارتقاء و نسخه های جدید پایه ریزی شده و آزمونهای مناسب سیستم ها در طی پیشرفت و قبل پذیرش انجام شوند. (A.10.3.2)
۴۶	خطاهای سیستم	• در استفاده از منابع باید مراقبت گردد. پیش بینی های لازم طبق الزامات ظرفیت آینده جهت حصول اطمینان از عملکرد سیستم ضروری است.(A.10.3.1) • باید معیار پذیرش سیستم های اطلاعاتی جدید، ارتقاء و نسخه های جدید باید پایه ریزی شده و آزمونهای مناسب سیستم ها در طی پیشرفت و قبل از پذیرش انجام شوند.(A.10.3.2)
۴۷	برون‌سپاری خدمات و پردازش اطلاعات	• الزامات امنیتی یک مرکز داده که مدیریت و کنترل تمامی یا بخشی از سیستم‌های امنیتی، شبکه‌ها و محیط‌های کاری آن به سازمانی دیگر واگذار می‌شود، باید در یک قرارداد که بین مرکز داده و طرف دیگر توافق شده است، دقیقا مشخص شود. • افراد و مراکز مجاز در حوزه های مرتبط با مراکز داده استعلام گردد. • برون‌سپاری خدمات مدیریتی، نگهداری و هرگونه خدمات دیگر در این مراکز داده به افراد و مراکز غیر مجاز ممنوع است.
۴۸	عدم بکارگیری نرم‌افزارهای کدباز	• استفاده از نرم‌افزارهای کدباز بجای استفاده از نرم‌افزارهای کدبسته در صورت وجود و پس از بررسی های امنیتی لازم بر روی آن • اتخاذ سیاست تولید کد بجای بکارگیری نرم‌افزارهای بین‌المللی موجود حتی از نوع کد باز و تعامل با مراکز و سازمانهای مجاز در این رابطه
۴۹	نقض صحت[1] و دسترس‌پذیری اطلاعات و سیستم‌های پردازش اطلاعات	• تهیه نسخه پشتیبان از اطلاعات و نرم افزار به طور مرتب و مطابق با خط مشی پشتیبان گیری • استفاده از مکانیزمهای جلوگیری از نقض صحت اطلاعات متناسب با نوع سرویسها و پردازشها • استفاده از مکانیزمهای جلوگیری از نقض دسترس پذیری اطلاعات متناسب با نوع سرویسها و پردازشها
۵۰	عدم حفاظت اطلاعات در شبکه‌ها	• شبکه ها باید به منظور حفاظت در برابر تهدیدها و حفظ امنیت سیستمها و برنامه های کاربردی شبکه و داده های در حال انتقال، به طور مناسب مدیریت شوند.

[1] Integrity

		• ویژگی امنیت، سطوح خدمات و الزامات مدیریت همه خدمات شبکه باید مشخص شده و لحاظ گردند. • امنیت شبکه در چند لایه مطابق مدلهای دفاع از عمق طراحی و پیاده سازی گردد.
۵۱	دسترسی غیر مجاز کاربر	• باید یک روش اجرایی رسمی ثبت و حذف کاربر در محل برای اعطا و لغو حق دسترسی به همه سیستم ها و سرویس های اطلاعاتی وجود داشته باشد.(A.11.2.1) • تخصیص و استفاده از مجوزها محدود و کنترل شود. • تخصیص کلمات عبور از طریق یک فرآیند مدیریتی رسمی کنترل شود. • مدیریت، حقوق دسترسی کاربران را در فواصل منظم، در راستای استفاده فرآیندهای اصلی، بازنگری کند. (A.11.2.4) • کاربران باید ملزم به رعایت نکات ایمنی در انتخاب و استفاده از کلمات عبور باشند.(A.11.3.1) • کاربران باید مطمئن باشند که تجهیزات بدون مراقبت از حفاظت مناسب برخوردارند. • سیاست میز مرتب برای کاغذها و رسانه ذخیره متحرک و سیاست صحنه نمایش واضح برای امکانات پردازش اطلاعات باید پذیرفته شود.(A.10.3.3) • هر سیستم اطلاعاتی باید محدودیت حداکثر ۳ ورود ناموفق را در طی ۳۰ دقیقه اعمال کند. پس از رسیدن تعداد ورودهای ناموفق به حد نصاب، سیستم باید قفل شده و به طور خودکار پس از یک ساعت به حالت عادی برگردد. (NIST-AC-7) • مرکز داده باید مطابق خط مشی‌های استفاده و اعمال کنترل‌های دسترسی، فعالیت‌های کاربران را مرور کرده و بر آنها نظارت داشته باشد. (NIST-AC-13) • سیستمها باید حسابهای کاربری موقتی و اضطراری را بلافاصله پس از اتمام کار غیرفعال نمایند.((NIST-AC-2(2) • هر سیستم اطلاعاتی باید پس از ۵ دقیقه عدم فعالیت کاربر، نشست وی را قفل نماید و دسترسی مجدد کاربر را منوط به طی مراحل احراز هویت و مجاز شناسی نماید. (NIST-AC-11) • هر سیستم اطلاعاتی باید پس از ۱۵ دقیقه عدم فعالیت کاربر، به طور کامل به نشست خاتمه دهد (log off نماید). (NIST-AC-12)
۵۲	عدم در نظر گرفتن امنیت در سیستم‌های اطلاعاتی به عنوان یک بخش اصلی	• هر گونه درخواست برای تهیه، خرید، یا تولید سیستم‌های اطلاعاتی باید صریحا نیازمندیها و الزامات امنیتی را نیز مشخص کند. • در تمامی بخشهای یک سیستم اطلاعاتی از تولید تا بهره برداری، امنیت بعنوان یک جزء انکار ناپذیر در نظر گرفته شود. • تشکیلات امنیتی و ساختار سازمانی لازم برای امنیت پیش بینی گردد.
۵۳	نقض محرمانگی یا صحت اطلاعات در اثر عدم استفاده یا استفاده نادرست از رمزنگاری	• برای حفاظت از اطلاعات باید یک خط مشی استفاده از کنترل های رمز نگاری توسعه پیدا کرده و اجرا شود.(A.12.3.1) • مدیریت کلید باید جهت پشتیبانی از استفاده سازمان از تکنیکهای رمز نگاری تعبیه

		شود.(A.12.3.2)
۵۴	عدم اطمینان از امنیت فایل سیستم ها	• از سیستم فایلهای مطمئن استفاده گردد و در این راستا از مشاوره مجموعه های متخصص و مورد اعتماد بهره گرفته شود. • باید روش های اجرایی جهت کنترل نصب نرم افزار بر روی سیستمهای عامل تعبیه شوند.(A.12.4.1)
۵۵	نقض امنیت اطلاعات و نرم‌افزارهای کاربردی سیستم‌عامل	• هر گونه تغییر با استفاده از روش های اجرایی رسمی کنترل تغییرات کنترل شود.(A.12.5.1) • تغییرات در بسته های نرم افزار باید کم شده، به تغییرات لازم محدود شود و همه تغییرات باید شدیداً تحت کنترل باشند.(A.12.5.3) • از هر گونه نشست اطلاعات باید جلوگیری شود.(A.12.5.4) • توسعه و تغییر نرم افزار برون سپاری شده باید توسط مرکز داده نظارت شود.(A.12.5.5) • مرکز داده باید پیکربندی پایه و اولیه هر سیستم اطلاعاتی را تهیه و مستند ساخته و فهرستی از مولفه‌های سازگار سیستم تهیه نماید. • مرکز داده باید هر گونه تغییر در سیستم‌های اطلاعاتی را مستندسازی و کنترل نماید. این تغییرات باید ابتدا توسط مقام مسوول تایید شود. • مرکز داده باید تغییر دادن سیستم‌های اطلاعاتی را محدود به افراد مجاز نماید. • باید پیکربندی امنیتی سیستم‌های اطلاعاتی به نحوی باشد که بیشترین محدودیت را اعمال نماید و سازگار با نیازمندیهای عملیاتی و امنیتی سیستم‌ها شود.(NIST CM-6) • مرکز داده باید از روشهای خودکار برای اعمال محدودیت دسترسی در تغییر سیستم‌های اطلاعاتی استفاده نماید. • مرکز داده باید از روشهای خودکار برای مدیریت، اعمال و بررسی پیکربندی سیستم‌های اطلاعاتی بهره بگیرد.
۵۶	عدم مدیریت آسیب‌پذیری‌های فنی	• اطلاعات به موقع در مورد آسیب پذیری‌های فنی سیستمهای اطلاعاتی مورد استفاده باید کسب شده و اثر آنها بر مرکز داده بررسی شده و تدابیر مناسبی برای مقابله با آنها اتخاذ شود.(A.12.6.1)
۵۷	عدم رعایت قوانین	• تمام الزامات مقرراتی، حقوقی و قراردادی و همه رویکرد سازمان برای تأمین این الزامات باید صریحاً مشخص، مستندسازی شده و برای هر سیستم اطلاعاتی سازمان ارتقاء داده شود.(A.15.1.1) • برای حصول اطمینان از انطباق با الزامات قانون گذاری، مقرراتی و قراردادی در استفاده مادی با توجه به ارتباط با حقوق مالکیت فکری یا استفاده اختصاصی محصولات نرم افزاری، روشهای اجرایی تدوین و اجرا شود.(A.15.1.2) • سوابق مهم باید در برابر مفقود شدن، تخریب و تحریف طبق قوانین قانونی، مقرراتی

		و قراردادی الزامات کسب و کار، محافظت شوند.(A.15.1.3) • از استفاده کاربران از امکانات پردازش اطلاعات بدون مجوز ممانعت به عمل آید.(A.15.1.5)
۵۸	عدم وجود مدیریت یکپارچه امنیت اطلاعات	• یک سند سیاست امنیتی توسط مدیریت مرکز داده تدوین و تصویب گردیده و منتشر گردد و بر حسب اقتضاء مورد تبادل نظر با تمام کارکنان قرار گیرد. • خط‌مشی های ذکر شده در سند سیاست امنیتی باید به طور منظم و نیز در مواردی که تغییرات مؤثری وجود داشته باشد، مورد بازنگری قرار گیرند تا از تداوم مناسب بودن خط‌مشی اطمینان حاصل شود. • فرم ها، اسناد و سیاست واکنش سریع مرکز داده شامل اهداف، محدوده، قوانین، مسؤلیتها و هماهنگی، همچنین مکانیزمهای کنترلی پیاده سازی، تولید و مرتبا مرور و به روز گردند.(NIST-IR-1)
۵۹	عدم سازگاری با خط مشی‌ها	• مدیران باید از اجرای صحیح تمام روش های اجرایی امنیت در حیطه مسئولیتشان برای دستیابی به تطابق با سند سیاست امنیتی و استانداردها، مطمئن شوند.(A.15.2.1) • سیستم های اطلاعاتی باید به طور منظم از نظر تطابق فنی با استانداردهای اجرایی امنیت مورد بررسی قرار گیرند.(A.15.2.2)
۶۰	فقدان نظام مدیریت امنیت اطلاعات	• مدیریت باید فعالانه از امنیت در سازمان با ساختار شفاف، تعهد آشکار، وظیفه صریح و قبول مسئولیتهای امنیت اطلاعات پشتیبانی کند. (A.6.1.1) • تشکیلات لازم و نیروی انسانی متخصص در زمینه امنی اطلاعات جذب یا تربیت گردند. • مسئولیت‌های حفاظت از هریک از دارایی‌های منفرد و انجام فرآیندهای امنیتی مشخص باید به طور شفاف تعریف شوند.(A.6.1.3) • برای استفاده از امکانات پردازش اطلاعات جدید، باید یک فرآیند صدور مجوز از طرف مدیریت پایه ریزی شود.(A.6.1.4) • باید همکاری مناسبی تحت مجوزهای قانونی، بین سازمانهای تنظیم کننده مقررات، تأمین‌کنندگان سرویسهای اطلاعاتی و اپراتورهای مخابراتی ایجاد و حفظ گردد.(A.4.1.7) • رویکرد سازمان برای مدیریت امنیت اطلاعات و اجرای آن (مثال: اهداف کنترل، کنترل ها، سیاستها، فرآیندها، روش های اجرایی امنیت اطلاعات) بصورت مستقل با طرح ریزی دوره ای یا هنگامی که تغییرات مهم در اجرای امنیت رخ می دهد، بازنگری شود.(A.6.1.8)
۶۱	استخدام یا به کارگماری افراد نامناسب	• نقشهای امنیتی و مسوولیتهای کارکنان، پیمانکاران و کاربران ثالث باید طبق سند سیاست امنیت اطلاعات مرکز داده مشخص و مستند سازی گردند. • بررسی سوابق همه افراد آماده استخدام، پیمانکاران و کاربران ثالث، باید طبق قوانین،

		اصول و قوانین مربوط و متناسب با الزامات کسب و کار طبقه‌بندی اطلاعات در دسترس باشد. • به عنوان بخشی از تعهد قراردادی افراد، کارکنان، پیمانکاران و کاربران ثالث باید طبق قوانین، اصول و مقررات مربوطه و متناسب با الزامات کسب و کار طبقه بندی اطلاعات در دسترسی را مدنظر داشته و به ریسک‌های ناشی از افشاء اطلاعات و دسترسی غیرمجاز دیگران واقف باشند.
۶۲	عدم آگاهی نیروهای انسانی از مسوولیتها و تعهدات	• مدیریت باید از کارکنان و پیمانکاران و کاربران ثالث بخواهد تا امنیت را طبق خط‌مشی‌های تدوین شده و رویه‌های مرکز داده بکار برند. • همه کارکنان سازمان (مرتبط با مرکز داده)، پیمانکاران و کاربران ثالث، باید آگاهی و آموزش مناسب و خط مشی های به روز شده و روشهای اجرایی که به عملکرد شغلی آنها مربوط می شود، را دریافت کنند. • باید فرآیند انضباطی رسمی برای کارکنانی که تعهدات امنیتی را نقض کردند وجود داشته باشد. • سازمان بایستی آموزشهای لازم در خصوص مسولیتهای آنها و قوانین واکنش سریع در مواقع لازم را به همه کارکنان (مرتبط با مرکز داده) داده و مرتبا به روز نماید. (NIST-IR-2)
۶۳	تهدیدهای مربوط به تغییر شغل یا انفصال از خدمت کارکنان و پیمانکاران	• مسئولیتها برای آن افرادی که دوره استخدامشان پایان یافته یا تغییر پیدا کرده باید بصورت روشن و واضح بوده و تعیین شود.(A.8.3.1) • همه کارکنان، پیمانکاران و کاربران ثالث باید همه دارایی های سازمان را (آنچه در تصرف دارند) به محض خاتمه استخدام ، قرارداد و توافق بازگردانند.(A.8.3.2) • مجوزهای دسترسی به اطلاعات و امکانات پردازش اطلاعات برای کل کارکنان ، پیمانکاران و کاربران ثالث باید به محض اتمام استخدامشان، قرارداد و توافقشان حذف شده یا به محض تغییر، تنظیم شود.(A.8.3.3)
۶۴	دسترسی‌های غیرمجاز طرفهای خارج مرکز داده	• ریسکهای مرتبط با دسترسی به امکانات پردازش اطلاعات سازمان توسط طرف خارج مرکز داده (منظور طرفهای داخل کشور می باشد نه خارج کشور) باید برآورد شده و کنترل‌های امنیتی مناسب پیاده‌سازی گردد.(A.6.2.1) • در قراردادهای با طرفهای خارج مرکز داده شامل دسترسی، پردازش، ارتباط، مدیریت اطلاعات یا تجهیزات، خرید تجهیزات، نصب و غیره باید تمام ملزومات امنیتی مربوط مشخص شوند.(A.6.2.3)
۶۵	عدم تجهیز به سیستم مدیریت بحران و شرایط اضطرار	• نصب سیستم‌های مدیریت بحران • اتخاذ سیاست‌ها و مکانیزم‌های اجرایی جهت جلوگیری از وقوع شرایط اضطرار • آموزش پرسنل برای رویارویی با شرایط اضطرار • تهیه دستورالعمل‌های لازم و ابلاغ آن به زیر مجموعه ها

۶۶	فقدان یک سیستم هشداردهنده سریع و به موقع	• بکارگیری سیستم‌های هشداردهنده سریع در حوزه های مختلف • بکارگیری سیستم‌های هوشمند اعلام خطر در خصوص حملات سایبری (نظیر DIDS) • بکارگیری سیستم‌های اعلام حریق هوشمند • آموزش پرسنل برای استفاده از این سیستم‌ها
۶۷	عدم بکارگیری سازه‌های امن و پایدار	• استفاده از سازه‌های امن و پایدار در طراحی مرکز داده • قرار دادن تجهیزات حساس و آسیب‌پذیر در فضای مطمئن • استفاده از موانع طبیعی علاوه بر سازه‌های مصنوعی (پوشش سازه های مصنوعی در درون موانع طبیعی نظیر عمق زمین یا زیر کوه)
۶۸	تولید اطلاعات غلط و نامطمئن	• شناسایی علل ناشی از تولید اطلاعات غلط اعم از نرم افزاری، سخت افزاری و نیروی انسانی و رفع این موارد
۶۹	عدم بهره مندی از مراکز احتیاط (Backup) امن، ایمن و پایدار	• ایجاد یک مرکز داده پشتیبان فعال (Active) در محل فیزیکی دیگر بمنظور سرویس دهی در صورت عدم امکان سرویس دهی توسط مرکز اصلی
۷۰	عدم بکارگیری خطوط ارتباطی مطمئن و پایدار	• بکارگیری چندین خطوط ارتباط مطمئن و پشتیبان در کنار همدیگر به منظور پشتیبان ارتباطی یکدیگر • استفاده از تکنولوژی‌های ارتباطی ناهمگون
۷۱	اتصالات ناامن به شبکه‌های اینترنت و اینترانت و فیبر نوری	• طراحی صحیح اتصالات در زمان طراحی مراکز داده بمنظور عدم وجود اتصال ناامن • نظارت و کنترل دوره ای در این خصوص و شناسایی تمامی اتصالات احتمالی ناامن و حذف آنها • ایزوله بودن سرویسهای بین المللی مورد نیاز در مراکز داده از سرویسهای داخلی • ایزوله بودن کامل در بالاترین حد ممکن در خصوص سرویسهای بین المللی مورد نیاز در مراکز داده از سرویسهای داخلی
۷۲	عدم پیش‌بینی برق پشتیبان	• پیش بینی برق UPS برای مرکز داده بمنظور استفاده در صورت قطع برق عادی متناسب با گستردگی، سطح و اهمیت مرکز داده • استفاده از مولدهای تولید برق پشتیبان، بمنظور پشتیبانی از برق UPS متناسب با سطح و اهمیت مرکز داده • نگهداری سوخت کافی برای مولدهای برق بمنظور استفاده در شرایط لازم
۷۳	عدم وجود نیروی انسانی متخصص لازم	• تربیت یا جذب نیروی انسانی متخصص لازم در حوزه های تخصصی مورد نیاز • ارائه آموزشهای عرضی تخصص‌های لازم به کارکنان • اولویت به استفاده از فن‌آوری‌هایی که نیروی متخصص آن در اختیار است. • تشویق کارکنان به فراگیری تخصص‌های متنوع و جدید • برگزاری آزمون‌های دوره‌ای جهت ارزیابی وضعیت آموزشی و کنترل کیفی مهارت‌های فنی آنان • برگزاری مانورهای آموزشی و مدیریت بحران به طور ادواری جهت ارزیابی سرعت

		عمل و انتقال در کارکنان جهت رویارویی با شرایط واقعی بحران
۷۴	عدم وجود آموزش امنیتی کافی	• برگزاری کلاسهای آگاهسازی و توجیه کارکنان در خصوص خسارات گزاف ناشی از عدم رعایت مسائل امنیتی • برگزاری دوره های آموزشی تخصصی عرضی امنیت برای متخصصین شبکه و امنیت • ارائه آموزشهای عمومی امنیت در سطوح مختلف به مدیران و کارکنان • ابلاغ سیاست‌های امنیتی و موظف نمودن کارکنان به تبعیت از سیاست‌ها با استفاده از مکانیزمهای مدیریتی
۷۵	اشتباهات و غفلت‌ها مانند عدم بکارگیری صحیح تجهیزات، عدم نصب صحیح نرم‌افزارها و برنامه‌های کاربردی، سهل انگاری	• آموزش کارکنان در خصوص نحوه صحیح نصب تجهیزات، نرم‌افزارها، برنامه‌های کاربردی و همچنین کاربری صحیح سیستم ها و تجهیزات • تدوین برنامه‌های ادواری جهت کنترل و شناسایی اشتباهات احتمالی کارکنان • نصب سیستم‌های هشداردهنده که در صورت فراموشی و یا غفلت کاربران هشدار دهد.
۷۶	عدم وجود کنترل روی قوانین	• تدوین سیاست کاری به منظور اجرای کنترل‌های لازم بمنظور اجرای قوانین تدوینی • بازبینی دوره ای قوانین و شناسایی قوانین ضعیف و متناقض و انجام تصحیحات لازم • تشویق و تنبیه کارکنان فعال و خاطی
۷۷	اتکا قابل ملاحظه به سیستم‌های ارتباطی بی‌سیم و ماهواره غیر امن	• رمزنگاری داده‌های ارسالی جهت کاهش مخاطرات ناشی از دسترسی غیرمجاز به داده‌ها در شرایط اضطرار به استفاده از این ارتباطات • عدم استفاده از سیستم‌های ارتباطی بی‌سیم بعلت عدم وجود امنیت کافی در این نوع از ارتباطات • استفاده از ارتباطات ماهواره ای داخلی در صورت راه اندازی در آینده در صورت نیاز
۷۸	عدم سازگاری با سیستم اطلاعات جغرافیایی (GIS)	• استفاده از سامانه های مبدل جهت ایجاد سازگاری با سیستم اطلاعات جغرافیایی در صورت نیاز

۷۹	زلزله	• عملیات مکان یابی صحیح و اصولی ساختمان باید در زمان انتخاب مکان مرکز داده انجام شود. • حفاظت فیزیکی در برابر آسیبهای ناشی از سیل، زلزله بایستی طراحی و بکارگرفته شود. (A.9.1.4) • طراحی و مقاومت ساختمان متناسب با کاربری مرکز داده در نظر گرفته شود. • عملیات مقاوم سازی ساختمان انجام گیرد. • آموزش افراد برای مقابله با حوادث (زلزله) • تدوین دستورالعملهای مرتبط با حوادث (زلزله) • تهیه و بکارگیری تجهیزات کمکهای اولیه • چیدمان مناسب تجهیزات جهت مقابله با لرزش های زلزله • تهیه و در دسترس بودن نقشه کلیه تأسیسات فنی و ابنیه ها • تهیه لیست تجهیزات موجود در مرکز داده • آموزش و بکارگیری گروه تعمیر، امداد و نجات • پیش بینی و بکارگیری سیستم روشنایی و برق اضطراری متحرک • پیش بینی سیستم های ارتباط داده پشتیبان بمنظور استفاده در شرایط اضطراری (NIST-CP-8(4)) • پیش بینی ارتباط مستقیم با مرکز زلزله نگاری (Hot line Connection) • پیش بینی تجهیزات جابجایی اشیاء (جرثقیل و ...)
۸۰	آتش	• استفاده حداکثری از مصالح و تجهیزات مقاوم در برابر آتش در زمان ساخت مرکز داده. • طراحی حفاظت فیزیکی در برابر آسیبهای ناشی از آتش سوزی • اعمال محدودیتها در مورد ممنوعیت ورود مواد آتش زا و پرخطر • تهیه و بکارگیری سیستم های هشداردهنده و اعلام حریق • تهیه و بکارگیری تجهیزات اطفاء حریق • آموزش دوره ای افراد شاغل در مرکز در مورد پیشگیری و مهار آتش • آموزش و بکارگیری گروه اطفاء حریق • ارتباط Online با مرکز آتش نشانی
۸۱	طوفان و صاعقه	• پیش بینی سیستم برق گیر و Earth جهت انتقال بار الکتریکی اضافی به زمین • ارائه آموزش پیشگیری و مقابله با حوادث برای افراد شاغل در مرکز داده • آموزش و بکارگیری گروه حوادث غیر مترقبه • پیش بینی تجهیزات جابجایی اشیاء (جرثقیل و ...) • ارتباط Online با مراکز امداد و نجات

۸۲	سیل	• تجهیز مرکز به سیستم جمع آوری آبهای سطحی • طراحی حفاظت فیزیکی در برابر آسیبهای ناشی از سیل • آموزش و بکارگیری گروه حوادث غیر مترقبه • ارتباط Online با مراکز امداد و نجات
۸۳	رطوبت و دما	• تهیه و بکارگیری تجهیزات تهویه مطبوع در ساختمان مرکز داده • استفاده از مصالح مناسب در ساخت مرکز داده • استفاده از دماسنج و رطوبت سنج بخصوص در نقاطی که از تجهیزات حساس به دما استفاده می شود • الزام در خصوص عایق بندی کلیه سیستم های حساس به رطوبت و دمای نامناسب
۸۴	دود	• تهیه و بکارگیری نورافکن و مه شکن در نقاط مختلف مرکز داده و پیرامون آن • بکارگیری تجهیزات کم کننده اثرات دود • پیش بینی ارتباط با مرکز هواشناسی
۸۵	سقوط اجسام	• رعایت استحکام مناسب در طراحی سازه مراکز داده متناسب با نوع آنها
۸۶	تداخل الکترومغناطیسی امواج	• مکان یابی نصب تجهیزات به منظور دوری از تجهیزات تداخل کننده مثل خطوط برق فشار قوی و خطوط با جریان بالا • رعایت استانداردهای مربوط به کابل کشی و فواصل مربوط به نصب کابل های انتقال داده ، برق و تلفن در زمان طراحی مرکز داده • آموزش و بکارگیری گروه متخصص در خصوص اختلال های الکترومغناطیسی • بکارگیری حفاظهای امواج الکترومغناطیس بر روی بسترهای انتقال
۸۷	مشکلات تأسیساتی (آب ،گاز، برق، تلفن)	• طراحی مناسب تأسیسات و رعایت استانداردهای نصب مسیرهای انتقال در زمان طراحی مرکز داده • استفاده از سیستم های هوشمند هشدار دهنده و کنترل کننده تاسیسات • حفاظت تجهیزات از افت جریان برق یا هر اختلالی که بر اثر عدم پشتیبانی تأسیسات بوجود می آید • استفاده از سیستم های پشتیبان برای آب، گاز، برق و تلفن بمنظور استفاده در صورت اختلال در مسیر اصلی • آموزش و بکارگیری گروه تاسیسات
۸۸	مواد پرخطر	• کنترل و نظارت بمنظور عدم انتقال مواد پرخطر و حساس • بازرسی افراد و تجهیزات به هنگام ورود و خروج • پیش بینی تجهیزات لازم بمنظور مقابله با حوادث احتمالی پیش آمده از طریق این مواد • آموزش و بکارگیری گروه متخصص جهت انجام عکس العمل مناسب

۸۹	تشعشعات رادیواکتیو	• نصب تجهیزات هشدار دهنده جهت اعلام خطر نشت مواد رادیواکتیو در محیط • قرار دادن لباس‌های مخصوص کار در محیط‌های آلوده به تشعشعات رادیواکتیو جهت استفاده پرسنل در صورت نیاز • استفاده از گیت‌های ورودی حساس به تشعشعات رادیواکتیو در تمامی ورودی‌های مراکز داده • تجهیز دیواره‌های داخلی مراکز داده به مواد شیمیایی مخصوص جذب موارد رادیواکتیو • آموزش و بکارگیری گروه متخصص جهت انجام عکس العمل مناسب
۹۰	گرد وغبار و مه	• بکارگیری فیلترهای جلوگیری کننده از ورود گرد و غبار • استفاده از حسگرهای گرد و غبار بمنظور اعلام هشدار در مواقع لازم • آموزش کارکنان در مورد نحوه رفع مشکل • آموزش و بکارگیری گروهی جهت انجام عکس العمل مناسب

۹-۶ ملاحظات پدافند غیر عامل مراکز داده حیاتی

جدول ۵. ملاحظات پدافند غیرعامل مراکز داده حیاتی

ردیف	تهدید	شرح کنترل
۱	اختلال الکترونیکی و الکتریکی	• ایجاد اتصال زمین برای تجهیزات به منظور انتقال بار الکتریکی اضافی • تجهیزات باید از افت جریان برق یا هر اختلالی که بر اثر عدم پشتیبانی تأسیسات بوجود می‌آید، حفاظت شوند. (A.9.2.2) • تجهیزات محافظ جهت جلوگیری از عملکرد اعوجاج و امواج الکترونیکی و الکتریکی • تجهیزات محافظ ولتاژ به منظور جلوگیری از تغییرات و ضربه های ولتاژ برق • بکارگیری سیستم برق اضطراری مجهز به مانیتور جهت مشاهده وضعیت برق تغذیه کننده سیستم ها • محافظت در مقابل نقایص منبع تغذیه • آموزش کارکنان شاغل در مرکز جهت رفع اشکالات مربوط به اختلال های الکترونیکی و الکتریکی • بکارگیری ژنراتور برق جهت تولید برق در زمان وقوع اختلال • استفاده از تجهیزات جلوگیری کننده از اختلال الکترونیکی • ایجاد یک مسیر برق غیر فعال برای زمان بوجود آمدن اختلال الکتریکی و استفاده از آن
۲	کدهای مخرب و بدافزارها (Malwares)	• کنترل‌های کشف، جلوگیری، و ترمیم به منظور محافظت در برابر کدهای مخرب، به همراه روال‌های مناسب آگاهی کاربران باید پیاده‌سازی شوند. (A.10.4.1) • جایی که استفاده از کد سیار مجاز است، پیکربندی آنها باید به گونه‌ای باشد که اطمینان از تطابق کدهای سیار مجاز با خط مشی های امنیتی تعریف شده، حاصل شود و باید از اجرای کد سیار غیر مجاز جلوگیری شود. (A.10.4.2) • استفاده از نرم‌افزارهای بومی جهت کشف بدافزارها • ایجاد محدودیت‌هایی در جهت ممانعت از دریافت کدهای اجرایی از سوی افراد • مسدود کردن درگاه‌های غیرضروری سیستم به منظور جلوگیری از امکان سوء استفاده به عنوان درهای پشتی
۳	دسترسی غیرمجاز از راه دور	• باید یک خط مشی رسمی اِعمال شده و روشهای مناسب امنیتی جهت محافظت در برابر ریسکهای استفاده از کامپیوترهای سیار و امکانات ارتباطات باید به کار گرفته شوند. (A.11.7.1)

		• باید یک خط مشی، برنامه های عملیاتی و روش های اجرایی توسعه یافته برای فعالیتهای کاری از راه دور اجرا شوند.(A.11.7.2)
۴	وقفه در کار	• فرآیند تنظیم شده باید توسعه یافته و باید جهت استمرار کسب و کار در کل سازمان نگهداری شود که اشاره به الزامات امنیتی اطلاعات مورد نیاز برای استمرار کسب و کار سازمان را دارد. (A.14.1.1) • رخدادهایی که ممکن است باعث وقفه در کار مرکز داده شوند باید به همراه احتمال و خسارت ناشی از وقفه و دیگر پیامدهای امنیتی مشخص شوند. • باید برای نگهداری یا بازیابی عملیات و اطمینان از دسترس‌پذیری در سطح مورد نظر و در زمان مورد نظر برنامه‌ریزی شود. • باید یک چارچوب کلی برای طرح‌های استمرار کسب و کار تدوین شود تا طرح‌ها سازگار بوده و نیازمندیهای امنیتی را به درستی مشخص کنند. همچنین اولویت‌های آزمون و ارزیابی را مشخص نماید. • طرحهای تداوم کسب و کار باید آزمایش شده و به طور منظم ارتقاء یابند تا از به روز بودن و اثر بخشی آنها اطمینان حاصل شود. (A.14.1.5) • هر طرحی که احتمال ایجاد وقفه در کسب و کار را تقویت می‌کند می‌بایستی برکنار و راه‌کار جایگزینی ارائه گردد. • عوامل ایجاد وقفه شناسایی گردند و ریسک حضور این عوامل در طراحی مرکز داده در نظر گرفته شود.
۵	جاسوسی	• هر مورد از تجهیزات که شامل ذخیره رسانه است، قبل از کنار گذاری باید به منظور حصول اطمینان از عدم وجود اطلاعات خاص بررسی شود. اینگونه اطلاعات و نرم افزارهای ثبت شده کنار گذاشته شده باید قبل از کنار گذاری در صورت نیاز بر روی رسانه ای دیگر ثبت گردد. • بکارگیری سیستم تشخیص هویت و شناسایی افراد به صورت جامع • جلوگیری از عکاسی ، فیلمبرداری و ضبط صدا • ثبت تمام ورود و خروج ها • آموزش ضد جاسوسی به کارکنان • تهیه نقشه تأسیسات و قابلیت دسترسی آنها برای افراد مجاز • تهیه لیست تجهیزات و قابلیت دسترسی آنها برای افراد مجاز • جداسازی مکانهای فعالیت افراد • محرمانگی مسیرهای فیزیکی انتقال اطلاعات و انرژی
۶	حملات تروریستی سایبری(هکرها)	• تهیه داده‌های پشتیبان در فواصل زمانی مناسب به منظور جلوگیری از احتمال بروز خرابی در تمامیت و صحت داده‌ها • ردگیری و تهیه سوابق دقیق از عملیات صورت گرفته از سوی هر کاربر به منظور مطالعه و شناسایی رفتار و اقدامات مشکوک صورت گرفته

		• کاهش سطح تماس سرویس‌های مرکز داده به متقاضیان • پرهیز از افشاء ماهیت و رفتار درونی سیستم، نرم افزار/ سخت‌افزار و مولفه‌های نرم‌افزاری به کار رفته در آن به سایرین • اتخاذ سیاست امنیتی مثبت به عنوان یک سیاست امنیتی بازدارنده • استفاده از مولفه‌های امنیتی فعال چون دروازه‌های آتش در محل ورودی ترافیک به شبکه داخلی مرکز داده • به کارگیری سیستم های تشخیص نفوذ مبتنی بر رفتار و امضاء جهت تشخیص به موقع ناهنجاری‌های رفتاری کاربران • آموزش پرسنل به استفاده از کلمات عبور طولانی و پیچیده و تغییر کلمات عبور به طور ادواری • به کارگیری تیمی از متخصیص نفوذ به منظوری شناسایی حفره‌های امنیتی موجود بخصوص در سطح نرم‌افزار و اتخاذ راه‌کارهایی جهت انسداد این حفره‌ها • غیرفعال کردن سرویس‌ها و مولفه‌های عمومی غیر قابل استفاده در سطح مرکز داده • استفاده از مولفه‌های نرم‌افزاری اختصاصی (in-house) به جای استفاده از مولفه‌های عمومی؛ بسیاری ازاین مولفه‌های به دلیل قابل دسترس بودن ضعف‌های امنیتی آنان برای همگان شناخته شده است.
۷	دسترسی غیرمجاز به اطلاعات	• خط مشی کنترل دسترسی باید پایه‌ریزی و مستند سازی شده و بر اساس کسب و کار و الزامات امنیتی برای دسترسی بازنگری شود. (A.11.1.1)

۸	دسترسی غیرمجاز به شبکه	• برای کاربران فقط دسترسی به سرویس هایی باید مهیا شوند که بطور مشخص اجازه استفاده از آنها را دارند.(A.11.4.1) • روشهای مناسب باید برای کنترل دسترسی توسط کاربران بیرونی مورد استفاده قرار بگیرد. • دسترسی فیزیکی و منطقی به درگاهها (پورت‌ها) باید تحت کنترل باشد. • برای شبکه های مشترک به خصوص آنهایی که به خارج از مرزهای سازمانی کشیده شدند ظرفیت کاربران محدود شود. • برای حصول اطمینان از اینکه ارتباطات کامپیوتری و جریان اطلاعات، خط مشی کنترل دسترسی را نقض نکند باید کنترل مسیریابی برای شبکه ها اجرا شود. (A.11.4.7) • حداکثر تعداد اتصال یا نشست‌های همزمان به یک سیستم باید کنترل و محدود شود. این محدودیت توسط مدیر سیستم تعیین می‌شود. (NIST-AC-10) • مرکز داده باید از مکانیزم‌های خودکار برای تسهیل در پایش و کنترل روشهای دسترسی از راه دور استفاده نماید. (NIST-AC-17(1)) • مرکز داده باید از رمزنگاری برای فراهم کردن محرمانگی نشست‌های از راه دور استفاده نماید. (NIST-AC-27(2)) • مرکز داده همه دسترسی‌های از راه دور را از طریق یک نقطه کنترل دسترسی مدیریت شده، کنترل می‌نماید. (NIST-AC-27(3))
۹	دسترسی غیرمجاز به سیستم‌عامل	• دسترسی به سیستم های عامل باید توسط فرآیند اجرایی امن (Logon) کنترل شوند.(A.11.5.1) • همه کاربران باید ID انحصاری برای استفاده شخصی خود داشته باشند و باید یک تکنیک مناسب تأیید، جهت اثبات ادعای ID کاربر انتخاب شود. • سیستم های تنظیم کلمه عبور باید دو سویه بوده و کیفیت کلمه عبور را اطمینان دهد. • استفاده از برنامه های کاربردی که توانایی کنترل کاربردها را داشته باشند به شدت تحت کنترل قرارداده شده و محدود شوند. • برای فراهم نمودن امنیت بیشتر برای کاربردهای دارای ریسک بالا، باید محدودیت هایی در زمان برقراری اتصال اعمال شود.(A.11.5.6)
۱۰	دسترسی غیرمجاز به برنامه‌های کاربردی	• دسترسی به اطلاعات و عملیات سیستمهای کاربردی توسط کاربران و کارکنان پشتیبانی باید طبق خط مشی کنترل دسترسی مشخص محدود گردد.(A.11.6.1) • سیستمهای حساس باید محیط کامپیوتری(محاسباتی) اختصاصی(مجزا) داشته باشند.(A.11.6.2)
۱۱	دسترسی غیر مجاز به اطلاعات یا سیستم‌های حین مبادله با	• خط مشی تبادل رسمی، روش های اجرایی و کنترل ها جهت حفاظت از تبادل اطلاعات با استفاده از همه انواع امکانات ارتباطی باید در محل وجود داشته

	نهادهای خارج از مرکز داده	باشد.(A.10.8.1) • توافقات جهت مبادله اطلاعات و نرم افزار بین سازمان و طرفهای خارج از سازمان باید پایه ریزی و تدوین شوند. • رسانه های حاوی اطلاعات باید در مقابل دسترسی غیرمجاز، سوء استفاده یا انحراف در زمان انتقال به خارج از مرزهای فیزیکی سازمان، حفاظت شود. • خط مشی ها و روش های اجرایی جهت حفاظت از اطلاعات همراه با ارتباطات داخلی سیستمهای اطلاعاتی کسب و کار باید تدوین شده و دائما ارتقاء یابند.(A.10.8.5)

		• الزامات ممیزی و فعالیتهای که شامل بررسی سیستم‌های عملیاتی است، برای کمینه کردن مخاطرات اختلال در فرایند کسب و کار، باید با دقت طرح‌ریزی و تصویب شوند.(A.15.3.1) • رکوردهای ممیزی مربوط به فعالیت‌های کاربران، وقایع استثنایی، و رویدادهای امنیتی باید تولید و نگهداری شوند. این رکوردها برای کمک به تفحصهای آتی و نظارت بر کنترل دسترسی کاربرد دارند. (A.10.10.1) • فرایند اجرایی برای استفاده از مراقبت امکانات پردازش اطلاعات باید پایه ریزی شده و نتایج نظارت فعالیتها باید به طور منظم بازنگری شوند. • امکانات ثبت کردن و ثبت اطلاعات باید در برابر دسترسی بدون مجوز و پنهانی حفاظت شود. • فعالیتهای مدیر و اپراتور سیستم باید ثبت شوند. • خطاها باید ثبت و تحلیل شده و اقدامات مناسب صورت بگیرد. • ساعت سیستمهای پردازش اطلاعات در سازمان یا حوزه امنیتی باید با زمان دقیق مرجع هماهنگ باشند.(A.10.10.6) • در صورت بروز خطا در ثبت رکوردهای ممیزی یا پر شدن ظرفیت محل ذخیره، باید هشدار مناسب به مدیر فنی مربوط داده شده و اقدام مقتضی (توقف ثبت، خاموش کردن سیستم، یا بازنویسی روی رکوردهای قدیمی) انجام شود. (NIST AU-5) • سیستم‌های اطلاعاتی باید مهر زمانی (timestamp) هر رویداد را مشخص نمایند. (NIST AU-8) • سیستم‌های اطلاعاتی باید از اطلاعات ممیزی و ابزارهای ممیزی در مقابل دسترسی غیرمجاز، تغییر یا حذف محافظت کنند. (NIST AU-9) (A.15.3.2) • هر سیستم اطلاعاتی باید امکان ثبت وقایع بیشتر و جزئی‌تر در رکوردهای ممیزی به همراه نوع، محل، و عامل آن فراهم کنند. ((NIST AU-3(1) • در صورتی که حجم رکوردهای ممیزی به ۷۵٪ ظرفیت محل ذخیره رسید، باید سیستم اطلاعاتی هشداری به مدیر سیستم بدهد. ((NIST AU-5(1) • سیستم‌های اطلاعاتی باید قابلیت تحلیل و خلاصه‌سازی رکوردهای ممیزی و تولید گزارش‌های مفید و قابل پیکربندی بر اساس انتخاب رویدادهای خاص را داشته باشند. ((NIST AU-7, AU-7(1) • هر سیستم اطلاعاتی باید قابلیت مدیریت مرکزی محتوای رکوردهای ممیزی تولید شده توسط مولفه‌های مختلف سیستم را داشته باشد. ((NIST AU-3(2) • مرکز داده باید از مکانیزم‌های خودکار برای هشدار فوری به پرسنل امنیتی درباره فعالیت‌های غیرمعمول، استفاده نماید ((NIST AU-6(2)
۱۲	پردازش‌های اطلاعاتی غیر مجاز	

		• سیستم‌های اطلاعاتی باید اطلاعات ممیزی خود را روی رسانه‌های سخت‌افزاری با قابلیت یکبار-نوشتن (write-once_) ثبت نمایند (مانند نوشتن روی CD یا چاپ روی کاغذ) (NIST AU-9(1))

۱۳	تغییر غیرمجاز، از دست دادن یا سوءاستفاده از اطلاعات در برنامه‌های کاربردی	• داده های ورودی برای سیستم کاربردی باید برای حصول اطمینان از صحت و مناسب بودن آنها، اعتبار سنجی شوند. (A.12.2.1) • باید در سیستم‌های کاربردی از وارسی‌های اعتبارسنجی به منظور کشف هر گونه خرابی داده استفاده شود. • الزامات برای اطمینان از درستی و حفاظت از صحت پیام در کاربردها باید مشخص شده و کنترل های مناسب باید مشخص و اجرا شوند. • داده های خروجی یک سیستم کاربردی باید به منظور اطمینان از درستی و مناسب بودن پردازش اطلاعات ذخیره شده با شرایط مربوطه مورد تعیین اعتبار قرار گیرد.(A.12.2.4)
۱۴	حمله فیزیکی، هسته‌ای و اتمی	• استفاده از تکنیکهای استتار بمنظور عدم تشخیص مکان مرکز داده توسط دشمن • استفاده از تکنیکهای اختفا بمنظور عدم تشخیص مکان مرکز داده توسط دشمن • استفاده از تکنیک‌های فریب دشمن بمنظور عدم تشخیص مکان واقعی مرکز داده • تهیه اطلاعات پشتیبان و ارسال آنان به نقطه‌ای خارج از فضای فیزیکی مرکز داده بمنظور حفظ داده ها و اطلاعات • ایجاد یک مرکز داده پشتیبان Offline در محل فیزیکی دیگر بمنظور سرویس دهی در صورت عدم امکان سرویس دهی توسط مرکز اصلی • تربیت تیم های تخصصی بمنظور استفاده جهت ترمیم آسیب ها در شرایط اضطرار • مکان یابی محل فیزیکی مناسب بمنظور ایجاد مرکز داده و استفاده از منابع طبیعی نظیر کوه برای این منظور • ایجاد یک مرکز داده پشتیبان فعال (Active) در محل فیزیکی دیگر بمنظور سرویس دهی در صورت عدم امکان سرویس دهی توسط مرکز اصلی • ایجاد سازه مرکز داده بصورت زیر زمینی و در عمق زمین • ایجاد یک مرکز داده پشتیبان فعال (Active)و یک مرکز داده Offline در محل های فیزیکی دیگر بمنظور سرویس دهی در صورت عدم امکان سرویس دهی توسط مرکز اصلی • پیش بینی تجهیزات لازم بمنظور معدوم ساختن اطلاعات حیاتی در صورت دسترسی دشمن به تأسیسات داخلی مراکز داده • استفاده از نیروهای نظامی و انتظامی به منظور حفاظت فیزیکی از مرکز داده

۱۵	بمب گذاری یا انفجار	• کنترل تردد تجهیزات و بسته ها • طراحی و بکارگیری برنامه حفاظت فیزیکی در برابر آسیبهای ناشی از انفجار (A.9.1.4) • آموزش کارکنان شاغل در مرکز جهت رفع اشکالات و ایرادات بوجود آمده پس از انفجار • ارتباط مستقیم با متخصصان مربوط به خنثی سازی موارد منفجره • وجود تجهیزات و افراد خنثی کننده بمب • طراحی و ایجاد ساختمان مرکز داده بصورت ضد انفجار (حداقل برای بخش بسیار حیاتی مرکز داده)
۱۶	حوادث شیمیایی	• شیلد نمودن و عایق بندی جداره‌های و منافذ ورودی تأسیسات مراکز داده به منظور جلوگیری از نفوذ گازهای شیمیایی به داخل مراکز • استقرار تجهیزات ایمنی از قبیل ماسک و سایر تجهیزات موجود جهت جلوگیری از آسیب پرسنل • نگهداری پادزهرهای مختلف مربوط به انواع گازهای شیمیایی در جعبه کمک‌های اولیه به منظور انجام اقدامات اولیه به مصدومین
۱۷	جنگ الکترومغناطیسی	• مکان یابی نصب تجهیزات به منظور دوری از تجهیزات منشا تداخل مثل خطوط برق فشار قوی و خطوط با جریان بالا • آموزش کارکنان شاغل در مرکز جهت رفع اشکالات مربوط به اختلال های الکترومغناطیسی • رعایت استانداردهای مربوط به کابل کشی و فواصل مربوط به نصب کابل های انتقال داده ، برق و تلفن • استفاده از سیستم برق اضطراری برای مواقع خاص • بکارگیری حفاظهای امواج الکترومغناطیس بر روی بسترهای انتقال • پیش بینی شبکه طیف گسترده جهت جلوگیری از تداخل الکترومغناطیسی
۱۸	ارگانیزم ها (ویروس، باکتری و...)	• کنترل مواد خوراکی • کنترل محیط مرکز داده در خصوص گسترش موارد ارگانیزمی و اقدامات پیشگیرانه • آموزش کارکنان شاغل در مرکز جهت مقابله با موارد ارگانیزمی • ایجاد مرکز بهداشت و درمان به منظور رفع مشکلات با گستردگی محدود در مورد افراد شاغل • نمونه گیری و آزمایش مرتب موارد خوراکی و محیط • آزمایش طبی پرسنل به صورت شش ماهه

۱۹	دسترسی غیر مجاز به سیستم ها، تجهیزات و منطقه فیزیکی	• نقاط دسترسی نظیر نواحی بارگیری یا تحویل و دیگر نقاطی که احتمال ورود اشخاص فاقد صلاحیت وجود دارد کنترل شده و در صورت امکان از سایر بخش‌ها و تأسیسات منفک گردد. • تجهیزات باید به منظور کاهش ریسک های حاصل از تهدیدات و آسیبهای محیط و فرصتهای دسترسی غیرمجاز، حفاظت شوند.(A.9.2.1) • تجهیزات باید جهت حصول اطمینان از تداوم دسترسی و صحت بطور مناسب نگهداری شوند.(A.9.2.4) • تجهیزات، اطلاعات یا نرم افزار نباید بدون مجوز قبلی از محل خارج شوند. (A.9.2.7) • از سامانه های امنیتی (موانعی نظیر دیوارها، گیت های ورودی که با کارت کنترل می شود یا میزهای پذیرش آماده) بمنظور محافظت ناحیه هایی که شامل اطلاعات و سامانه های پردازش اطلاعات باشد، استفاده شود. (A.9.1.1) • نواحی امن بوسیله کنترل های ورودی مناسب جهت اطمینان از اینکه فقط پرسنل مجوز دار اجازه دسترسی داشته باشند محافظت شود. (A.9.1.2) • امنیت فیزیکی لازم برای دفاتر، اتاق ها و تاسیسات، طراحی و بکار گرفته شود.(A.9.1.3) • آموزش های لازم به کابران ارائه گردد. • بکارگیری سیستم حفاظت فیزیکی هوشمند پیرامونی (دوربین های مدار بسته) و هشدار دهنده
۲۰	دسترسی غیر مجاز به رسانه‌های ذخیره‌سازی اطلاعات	• باید دستورالعمل اجرایی برای مدیریت رسانه متحرک تدوین گردد. (A.10.7.1) • در صورت عدم نیاز به یک رسانه، باید به صورت امن و ایمن و طی یک فرآیند رسمی امحاء شود. (A.10.7.2) • مستند سازی سیستم باید در برابر دسترسی غیر مجاز حفاظت شود.(A.10.7.4) • رسانه های ذخیره سازی اطلاعات در محل امن نگهداری شوند. • اطلاعات رسانه قبل از تعویض ثبت گردد. (A.9.2.6) • وجود روش های اجرایی در محل برای مدیریت رسانه متحرک. (A.10.7.1) • در صورت عدم نیاز به یک رسانه، باید به صورت امن و ایمن و طی یک فرآیند رسمی امحاء شود. (A.10.7.2) • شبکه ها باید به منظور حفاظت در برابر تهدیدها و حفظ امنیت سیستمها و برنامه های کاربردی شبکه و داده های در حال انتقال، به طور مناسب مدیریت شوند.(A.10.6.1)

۲۱	دسترسی فیزیکی غیرمجاز به بستر انتقال داده‌ها	• لزوم حفاظت از بسترهای انتقال داده با تدوین سیاست نامه ای در خصوص نحوه دسترسی به آنها، مسئولیتهای افراد در این ارتباط و کد گذاری بسترها ی انتقال (NIST-MP-1)، (NIST-MP-2) و (NIST-MP-3) • نحوه دسترسی، افراد مجاز و نحوه دریافت اطلاعات ورودی به بسترهای انتقال از هر نوع (اطلاعات الکترونیکی ، کاغذی و ...) بایستی مورد کنترل قرار گیرد. (NIST-MP-5) • حفاظت فیزیکی مناسب از کابلها و بکارگیری داکت • قرار دادن کانال انتقال داده‌ها در محیط غیرقابل دسترسی • کنترل بسترهای انتقال داده در زمان کنارگذاری و یا استفاده مجدد آنها.(NIST-MP-7) • استفاده از مکانیزم‌های بازدارنده روی کانال‌های انتقال داده به منظور کاهش احتمال دسترسی فیزیکی غیرمجاز • استفاده از چند کانال‌های ارتباطی به جای یک کانال ارتباطی و انتقال داده‌ها به صورت تصادفی از این کانال‌ها
۲۲	عدم سازگاری با فن‌آوری‌های مدرن جنگ الکترونیک	• جایگزینی فن‌آوری موجود با فن آوری قابل انطباق • استفاده از فن‌آوری‌های مبدل به منظور انطباق فن‌آوری موجود با فن‌آوری مدرن • تلاش برای بروزسازی فن‌آوری جدید با افزودن قابلیت‌های موجود در فن‌آوری‌های مدرن
۲۳	تهدید ناشی از عدم سازگاری با سیستم‌های مدرن اطلاعات عملیات	• استفاده از مولفه‌های مبدل به منظور ایجاد ارتباط و هماهنگی بین سیستم‌های کنونی اطلاعات عملیات و سیستم‌های نوین اطلاعات عملیات
۲۴	تهدید ناشی از عدم سازگاری با فن آوری‌های مدرن جنگ متحرک	• اتخاذ ملاحظاتی برای امکان جابجایی تجهیزات ذخیره سازی داده ها و اطلاعات در زمان بحران بمنظور استفاده در مرکز داده دیگر

۲۵	آسیب یا سرقت (الکترونیکی)	• آموزش کارکنان شاغل در مرکز جهت جلوگیری از سرقت الکترونیکی شناسه‌های هویت آنها • ملزم کردن کارکنان به تغییر کلمات عبور به صورت ادواری • استفاده از کلمات عبور پیچیده، طولانی غیرقابل حدس زدن • دسترسی به اطلاعات طبقه‌بندی شده باید لزوماً با عبور از مکانیسم‌های احراز هویت چندگانه امکان‌پذیر گردد. • کاهش کانال‌های الکترونیکی جهت دسترسی کاربران به منابع داده‌ای و سرویس‌های ارائه شده از سوی مرکز داده • قبل از دسترسی کاربر به اطلاعات و سرویس حیاتی حتماً شناسه هویت کاربر بار دیگر از وی درخواست گردد. • دسترسی به اطلاعات حیاتی مبتنی بر احراز هویت کاربران بر مبنای مشخصه‌های بیومتریک چون مشخصه عنبیه افراد، اثر انگشت، DNA و ... باشد. برای این منظور لازم است که دستگاه‌هایی با امکان تشخیص و دریافت این اطلاعات بر روی سیستم های کامپیوتری مستقر باشد.
۲۶	آسیب یا سرقت (فیزیکی)	• از تجهیزات باید به منظور کاهش ریسک های حاصل از تهدیدات و آسیبهای محیط و فرصتهای دسترسی غیرمجاز، متناسب با ماهیت هر یک حفاظت شود. • آموزش کارکنان شاغل در مرکز جهت جلوگیری از آسیب یا سرقت • از نقشه تأسیسات و موارد زیر بنایی در مکان مناسب (گاوصندوق یا محل مطمئن) حفاظت گردد. • ثبت ورود و خروج افراد • حفاظت از لیست تجهیزات • حفاظت از تجهیزات در زمان انتقال به تعمیرگاه و یا به هنگام تعمیر و رعایت تمهیدات مربوطه • جداسازی مکانهای فعالیت افراد دارای دسترسی های مختلف • رعایت اصول و سطوح طبقه بندی • رعایت محرمانگی مسیرهای فیزیکی انتقال اطلاعات و انرژی
۲۷	اختلال در ارتباطات شبکه	• استفاده از کانال‌های ارتباطی فاقد امکان اختلال • شیلد کردن کانال‌ها و تجهیزات ارتباطی و مکانهای قرار گرفتن این تجهیزات • استفاده از ارتباطات پشتیبان ناهمگون
۲۸	اختلال در سیستم برق	• بکارگیری سیستم توان پشتیبان • استخدام نیروهای متخصص برق به منظور انجام سرویس بلادرنگ در زمان بروز اختلال در سیستم برق • نگهداری سوخت کافی برای ژنراتورهای مولد برق برای شرایط خاص که امکان دسترسی به سوخت تا مدت‌ها وجود ندارد

۲۹	قرار دادن کشور در موقعیت جنگ تمام عیار اطلاعاتی	• الزام به قرار گرفتن در شرایط آماده باش کامل به منظور نظارت بر حسن اجرای تمامی کنترل‌های پیشنهادی (پدافند غیرعامل و امنیت)
۳۰	تهدید ناشی از تحریم فن آوری های پیشرفته خارجی	• تلاش جهت تسلط بر دانش و فناوری ها بمنظور بومی‌سازی فن‌آوری به منظور کاهش دغدغه‌های ناشی از تحریم فن‌آوری • تعامل با بخش های تحقیقاتی و پژوهشی کشور بمنظور بکرگیری حداکثری توان داخلی جهت تولید فناوری های لازم در داخل کشور داخل کشور
۳۱	وابستگی به خارج از کشور در بخش تعمیر و نگهداری	• انتقال دانش تعمیر و نگهداری به متخصصین بومی • استفاده از تکنولوژی‌های بومی موجود • جلوگیری از امکان دسترسی به داده‌های طبقه‌بندی شده و سوابق ذخیره شده بر روی سخت‌افزار و رسانه‌های ذخیره سازی مربوطه با تهیه نسخه پشتیبان و امحاء داده‌های موجود بر روی سیستم‌ها قبل از ارسال به مراکز تعمیر • قطع وابستگی به تعمیر و نگهداری با بومی سازی تکنولوژی مربوطه و انتقال دانش تعمیر و نگهداری به داخل کشور
۳۲	وابستگی به تولیدات سخت افزاری و نرم افزاری خارجی	• انتقال دانش تولید سخت افزارها و نرم افزارها به متخصصین بومی • استفاده حداکثری از محصولات بومی موجود • رعایت ملاحظات امنیتی در استفاده از محصولاتی که نمونه داخلی آنها وجود ندارد
۳۳	تغییر سریع فن آوری (در حوزه جنگ سایبر)	• تلاش جهت تسلط بر دانش و فناوری ها بمنظور بومی‌سازی فن‌آوری به منظور کاهش دغدغه‌های ناشی از تغییرات در فن‌آوری • آموزش نیروی متخصص و کارآمد جهت بهره گیری و انتقال فن‌آوری به داخل کشور • رعایت ملاحظات امنیتی در صورت لزوم استفاده از فناوریهای جدید و مشاوره با بخشهای متخصص آگاه و امین در کشور • تعامل با سازمانهای داخلی مرتبط با دانش و فناوریها بمنظور تسریع در روند بومی سازی فن آوری
۳۴	جهانی شدن	• تعامل با سازمانها و نهادهای مربوطه در داخل کشور بمنظور توجه به چالش‌های پیش روی جهانی شدن جهت ارائه راه‌کارهایی به منظور تطبیق با شرایط جدید • اتخاذ سیاست‌هایی در راستای تغییرات و تمهیدات ایجاد شده بمنظور اعمال در سازمان
۳۵	زیرساخت‌های عمده جهانی نظیر اینترنت	• استفاده از زیرساخت های بومی و قابل اتکاء و اعتماد در صورت وجود • استفاده کنترل شده از زیرساخت‌های جهانی با رعایت مسائل امنیتی و حفاظتی • استفاده از این زیرساخت‌های تنها برای اهداف خاص • استفاده از این زیرساخت‌های بصورت جداگانه (ایزوله) از زیرساختهای اصلی مرکز داده

۳۶	حملات مختل کننده خدمات	• بکارگیری سیستم‌هایی به منظور جلوگیری از نفوذ و شناسایی حملات مختل کننده خدمات در صورت نفوذ، نظیر IDSها و فایروالهای بومی • شناسایی و ثبت الگوهای رفتاری حمله‌کنندگان داخلی به منظور جلوگیری از الگوهای رفتاری مشابه توسط سایر کاربران • پیش بینی و بکارگیری مراکز احتیاط وتشکیل تیمهای CERT در شرایط وقوع وقفه سرویس • تعیین حدمجاز بهره‌مندی کاربران از سرویس‌های ارائه شده • قرار دادن کاربران خاطی و غیرقابل اعتماد در لیست سیاه و ممانعت از سرویس‌دهی به آنان
۳۷	جنگ روانی دشمن	• برگزاری دوره های آگاهسازی برای کارکنان و کاربران در این خصوص • انتشار مستنداتی از اهداف خرابکارانه دشمن در تضعیف روحیه افراد که حاکی از بی‌پایه بودن گفته‌های دشمن دارد
۳۸	تغییر هویت اطلاعات درحال گذر	• استفاده از الگوریتم‌های رمزنگاری بومی، امضاهای دیجیتال در رمزنگاری اطلاعات متناسب با ماهیت و نوع سرویسها به منظور جلوگیری از افشا و امکان دستکاری اطلاعات در حال گذر • عدم استفاده از الگوریتم های رمزنگاری غیرمطمئن بمنظور رمزنگاری اطلاعات در حال گذر • استفاده از مکانیزمهای پنهان نگاری اطلاعات در شرایط لازم بمنظور انتقال اطلاعات مهم • عدم استفاده از کانال‌های ارتباطی بی‌سیم بدون در نظر گرفتن مکانیزمهای امنیتی مطمئن
۳۹	دسترسی غیرمجاز به اطلاعات	• استفاده از مکانیزمهای رمزنگاری اطلاعات و الگوریتم‌های رمزنگاری بومی بمنظور نگهداری اطلاعات بر روی رسانه های ذخیره سازی اطلاعات • عدم استفاده از الگوریتم های رمزنگاری غیرمطمئن بمنظور رمزنگاری اطلاعات • استفاده از مکانیزم‌های احراز هویت برای دسترسی به سرویسها و اطلاعات به منظور جلوگیری از دسترسی غیر مجاز به اطلاعات • پیش بینی تمهیدات امنیتی متناسب با سطح اهمیت و میزان تجمیع اطلاعات • استفاده از کانالهای ارتباطی خاص و غیر مشترک جهت تبادل اطلاعات با پیش بینی تمهیدات امنیتی • استفاده از مکانیزم‌های احراز هویت حداقل ۲ عاملی برای دسترسی به سرویسها و اطلاعات به منظور جلوگیری از دسترسی غیر مجاز به اطلاعات

۴۰	ناآرامی‌های اجتماعی	• محافظت بمنظور عدم افشای محل مرکز داده • حفاظت فیزیکی در برابر آسیبهای ناشی از آشوب های شهری بمنظور جلـوگیری از ورود افراد متفرقه • محافظت بمنظور ذکر نشدن محل مرکز داده در نقشه های جغرافیایی • احداث مرکز داده در مکانهای فیزیکی غیر قابل دسترس مردم عادی
۴۱	ورود و خروج غیر مجاز افراد	• محیط های امنیتی (موانعی نظیر دیوارها، گیت های ورودی که با کارت کنترل می شود یا میزهای پذیرش آماده) باید بمنظور محافظت ناحیه هایی را که شامل اطلاعات و سامانه های پردازش اطلاعات باشد، استفاده شود. (A.9.1.1) • از سامانه های امنیتی (موانعی نظیر دیوارها، گیت های ورودی که با کارت کنترل می شود، دستگاههای X-Ray یا میزهای پذیرش آماده) بمنظور کنترل ورود و خروج افراد و تجهیزات همراه آنها استفاده شود. (A.9.1.1) • بکارگیری دوربین های کنترل تردد و سیستم حفاظت پیرامونی • اجبار در استفاده ازکارت شناسایی توسط افراد و کنترل آن توسط مبادی ذیربط • ثبت زمان ورود و خروج افراد • آموزش کارکنان • جداسازی مکانهای فعالیت افراد دارای طبقه بندی مختلف و رعایـت اصول حیطه بندی • بازدید مرتب کارت شناسایی • استفاده از یونیفورم برای کارکنان • تعبیه یک محل ورود و خروج • بازدید کنندگان به همراه افراد مجوز دار تردد نمایند.

۴۲	عدم رویکرد مداوم برای مدیریت حوادث امنیتی	• باید مسئولیتهای مدیریت و فرآیندهای اجرایی جهت حصول اطمینان از پاسخ، سریع، موثر و مرتب به حوادث امنیتی اطلاعات پایه ریزی شود. (A.13.2.1) • باید مکانیزمهایی برای سنجش و پایش نوع، حجم، و هزینه حوادث امنیتی وجود داشته باشند. (A.13.2.2) • هر مرکز داده بایستی دارای مرکز عملیات امنیتی (SOC) بمنظور مانیتور و کنترل حوادث امنیتی باشد. • بعد از حادثه امنیتی اطلاعات، پی گیری در برابر فرد یا سازمانی صورت می گیرد که شامل اقدام قانونی (چه مدنی ، جزایی) است، شواهد باید جمع آوری و نگهداری شده و برای مطابقت با قوانین جهت مطرح شدن شواهد در یک دادرسی مربوطه ارائه شوند. (A.13.2.3) • سازمان بایستی میزان سرعت واکنش و کارآیی مکانیزمها در شرایط مورد نیاز را، آزمایش نماید. (NIST-IR-3) • سازمان بایستی با طراحی مکانیزمهای اتوماتیک، میزان سرعت واکنش و کارآیی آنرا در شرایط مورد نیاز، بهتر و موثرتر آزمایش نماید. ((1) NIST-IR-3)
۴۳	عدم اصلاح و بازیابی پس از حوادث امنیتی	• رویدادهای امنیتی اطلاعات باید توسط مدیریت کانالهای مناسب تا حد امکان به سرعت گزارش شوند.(A.13.1.1) • مرکز داده بایستی دارای تیم CERT بمنظور ترمیم حوادث احتمالی در صورت وقوع، باشد. • تمام کارکنان پیمانکاران و مصرف کنندگان ثالث مصرف کننده سیستمها و خدمات اطلاعات باید ملزم شوند تا هرگونه ضعف امنیتی مشاهده شده و مشکوک در سیستمها و خدمات را به آن توجه کرده و گزارش دهند.(A.13.1.2)
۴۴	ناامنی یا نادرستی در عملیات پردازش اطلاعات	• روش های اجرایی عملیاتی باید مستند سازی و نگهداری شده، و برای همه کاربران که به آن نیاز دارند در دسترس باشد.(A.10.1.1) • تغییرات در امکانات پردازش اطلاعات و سیستمها باید کنترل شده باشند. • وظایف و حوزه های مسئولیت باید در راستای کاهش فرصت برای افراد غیرمجاز یا تغییرات ناخواسته یا سوء استفاده از دارایی های سازمان تفکیک شوند. • پیشرفت، آزمایش و امکانات عملیاتی باید تفکیک شوند تا دسترسی های غیرمجاز یا تغییرات سیستم عملیاتی را کاهش دهد.(A.10.1.4)
۴۵	عدم امنیت در تعامل با طرفهای ثالث	• استفاده از منابع باید مراقبت و تنظیم گردد. پیش بینی های لازم طبق الزامات ظرفیت آینده جهت حصول اطمینان از عملکرد سیستم ضروری است.(A.10.3.1) • باید معیار پذیرش سیستم های اطلاعاتی جدید، ارتقاء و نسخه های جدید پایه ریزی شده و آزمونهای مناسب سیستم ها در طی پیشرفت و قبل پذیرش انجام

		شوند.(A.10.3.2)
۴۶	خطاهای سیستم	• در استفاده از منابع باید مراقبت گردد. پیش بینی های لازم طبق الزامات ظرفیت آینده جهت حصول اطمینان از عملکرد سیستم ضروری است.(A.10.3.1) • باید معیار پذیرش سیستم های اطلاعاتی جدید، ارتقاء و نسخه های جدید باید پایه ریزی شده و آزمونهای مناسب سیستم ها در طی پیشرفت و قبل از پذیرش انجام شوند.(A.10.3.2)
۴۷	برون‌سپاری خدمات و پردازش اطلاعات	• الزامات امنیتی یک مرکز داده که مدیریت و کنترل تمامی یا بخشی از سیستم‌های امنیتی، شبکه‌ها و محیط‌های کاری آن به سازمانی دیگر واگذار می‌شود، باید در یک قرارداد که بین مرکز داده و طرف دیگر توافق شده است، دقیقا مشخص شود. • افراد و مراکز مجاز در حوزه های مرتبط با مراکز داده استعلام گردد. • برون‌سپاری خدمات مدیریتی، نگهداری و هرگونه خدمات دیگر در این مراکز داده به افراد و مراکز غیر مجاز ممنوع است.
۴۸	عدم بکارگیری نرم‌افزارهای کدباز	• استفاده از نرم‌افزارهای کدباز بجای استفاده از نرم‌افزارهای کدبسته در صورت وجود و پس از بررسی های امنیتی لازم بر روی آن • اتخاذ سیاست تولید کد بجای بکارگیری نرم‌افزارهای بین‌المللی موجود حتی از نوع کد باز و تعامل با مراکز و سازمانهای مجاز در این رابطه
۴۹	نقض صحت[1] و دسترس‌پذیری اطلاعات و سیستم‌های پردازش اطلاعات	• تهیه نسخه پشتیبان از اطلاعات و نرم افزار به طور مرتب و مطابق با خط مشی پشتیبان گیری • استفاده از مکانیزمهای جلوگیری از نقض صحت اطلاعات متناسب با نوع سرویسها و پردازشها • استفاده از مکانیزمهای جلوگیری از نقض دسترس پذیری اطلاعات متناسب با نوع سرویسها و پردازشها
۵۰	عدم حفاظت اطلاعات در شبکه‌ها	• شبکه ها باید به منظور حفاظت در برابر تهدیدها و حفظ امنیت سیستمها و برنامه های کاربردی شبکه و داده های در حال انتقال، به طور مناسب مدیریت شوند. • ویژگی امنیت، سطوح خدمات و الزامات مدیریت همه خدمات شبکه باید مشخص شده و لحاظ گردند. • امنیت شبکه در چند لایه مطابق مدلهای دفاع از عمق طراحی و پیاده سازی گردد.

[1] Integrity

		• باید یک روش اجرایی رسمی ثبت و حذف کاربر در محل برای اعطا و لغو حق دسترسی به همه سیستم ها و سرویس های اطلاعاتی وجود داشته باشد.(A.11.2.1) • تخصیص و استفاده از مجوزها محدود و کنترل شود. • تخصیص کلمات عبور از طریق یک فرآیند مدیریتی رسمی کنترل شود. • مدیریت، حقوق دسترسی کاربران را در فواصل منظم، در راستای استفاده فرآیندهای اصلی، بازنگری کند. (A.11.2.4) • کاربران باید ملزم به رعایت نکات ایمنی در انتخاب و استفاده از کلمات عبور باشند.(A.11.3.1) • کاربران باید مطمئن باشند که تجهیزات بدون مراقبت از حفاظت مناسب برخوردارند. • سیاست میز مرتب برای کاغذها و رسانه ذخیره متحرک و سیاست صحنه نمایش واضح برای امکانات پردازش اطلاعات باید پذیرفته شود.(A.10.3.3) • هر سیستم اطلاعاتی باید محدودیت حداکثر ۳ ورود ناموفق را در طی ۳۰ دقیقه اعمال کند. پس از رسیدن تعداد ورودهای ناموفق به حد نصاب، سیستم باید قفل شده و به طور خودکار پس از یک ساعت به حالت عادی برگردد. (NIST-AC-7)
۵۱	دسترسی غیر مجاز کاربر	• مرکز داده باید مطابق خط مشی‌های استفاده و اِعمال کنترل‌های دسترسی، فعالیت‌های کاربران را مرور کرده و بر آنها نظارت داشته باشد. (NIST-AC-13) • سیستمها باید حسابهای کاربری موقتی و اضطراری را بلافاصله پس از اتمام کار غیرفعال نمایند.((NIST-AC-2(2) • هر سیستم اطلاعاتی باید پس از ۵ دقیقه عدم فعالیت کاربر، نشست وی را قفل نماید و دسترسی مجدد کاربر را منوط به طی مراحل احراز هویت و مجاز شناسی نماید. (NIST-AC-11) • هر سیستم اطلاعاتی باید پس از ۱۵ دقیقه عدم فعالیت کاربر، به طور کامل به نشست خاتمه دهد (log off نماید). (NIST-AC-12) • مرکز داده باید از مکانیزمهای خودکار مدیریت حسابهای کاربری سیستم‌ها استفاده نماید. ((NIST-AC-2(1) • همه سیستم‌های اطلاعاتی باید حساب کاربری بلااستفاده را [پس از مدت زمان مشخص شده در سیاست امنیت سازمان مربوط به مرکز داده] غیر فعال نمایند. (NIST-AC-2(3)) • سیستم اطلاعاتی باید پس از رسیدن تعداد ورودهای ناموفق به حد نصاب، به طور خودکار قفل شده و تنها توسط مدیر سیستم به حالت عادی برگردد. (NIST-AC-7(1))

		• مرکز داده باید از مکانیزم‌های خودکار برای اطمینان از این که همه اعمال ایجاد، تغییر، غیرفعال‌سازی، و حذف بازرسی و به کاربران مقتضی اطلاع داده می‌شود، بهره بگیرند. ((NIST-AC-2 (4)

۵۲	عدم در نظر گرفتن امنیت در سیستم‌های اطلاعاتی به عنوان یک بخش اصلی	• هر گونه درخواست برای تهیه، خرید، یا تولید سیستم‌های اطلاعاتی باید صریحا نیازمندیها و الزامات امنیتی را نیز مشخص کند. • در تمامی بخشهای یک سیستم اطلاعاتی از تولید تا بهره برداری، امنیت بعنوان یک جزء انکار ناپذیر در نظر گرفته شود. • تشکیلات امنیتی و ساختار سازمانی لازم برای امنیت پیش بینی گردد.
۵۳	نقض محرمانگی یا صحت اطلاعات در اثر عدم استفاده یا استفاده نادرست از رمزنگاری	• برای حفاظت از اطلاعات باید یک خط مشی استفاده از کنترل های رمز نگاری توسعه پیدا کرده و اجرا شود.(A.12.3.1) • مدیریت کلید باید جهت پشتیبانی از استفاده سازمان از تکنیکهای رمز نگاری تعبیه شود.(A.12.3.2)
۵۴	عدم اطمینان از امنیت فایل سیستم ها	• از سیستم فایلهای مطمئن استفاده گردد و در این راستا از مشاوره مجموعه های متخصص و مورد اعتماد بهره گرفته شود. • باید روش های اجرایی جهت کنترل نصب نرم افزار بر روی سیستمهای عامل تعبیه شوند.(A.12.4.1)
۵۵	نقض امنیت اطلاعات و نرم‌افزارهای کاربردی سیستم‌عامل	• هر گونه تغییر با استفاده از روش های اجرایی رسمی کنترل تغییرات کنترل شود.(A.12.5.1) • تغییرات در بسته های نرم افزار باید کم شده، به تغییرات لازم محدود شود و همه تغییرات باید شدیداً تحت کنترل باشند.(A.12.5.3) • از هر گونه نشست اطلاعات باید جلوگیری شود.(A.12.5.4) • توسعه و تغییر نرم افزار برون سپاری شده باید توسط مرکز داده نظارت شود.(A.12.5.5) • مرکز داده باید پیکربندی پایه و اولیه هر سیستم اطلاعاتی را تهیه و مستند ساخته و فهرستی از مولفه‌های سازگار سیستم تهیه نماید. • مرکز داده باید هر گونه تغییر در سیستم‌های اطلاعاتی را مستندسازی و کنترل نماید. این تغییرات باید ابتدا توسط مقام مسوول تایید شود. • مرکز داده باید تغییر دادن سیستم‌های اطلاعاتی را محدود به افراد مجاز نماید. • باید پیکربندی امنیتی سیستم‌های اطلاعاتی به نحوی باشد که بیشترین محدودیت را اعمال نماید و سازگار با نیازمندیهای عملیاتی و امنیتی سیستم‌ها شود. (NIST CM-6) • مرکز داده باید از روشهای خودکار برای اعمال محدودیت دسترسی در تغییر سیستم‌های اطلاعاتی استفاده نماید. • مرکز داده باید از روشهای خودکار برای مدیریت، اعمال و بررسی پیکربندی سیستم‌های اطلاعاتی بهره بگیرد.
۵۶	عدم مدیریت آسیب‌پذیری‌های	• اطلاعات به موقع در مورد آسیب پذیری‌های فنی سیستمهای اطلاعاتی مورد

	فنی	استفاده باید کسب شده و اثر آنها بر مرکز داده بررسی شده و تدابیر مناسبی برای مقابله با آنها اتخاذ شود.(A.12.6.1)
۵۷	عدم رعایت قوانین	• تمام الزامات مقرراتی، حقوقی و قراردادی و همه رویکرد سازمان برای تأمین این الزامات باید صریحاً مشخص، مستندسازی شده و برای هر سیستم اطلاعاتی سازمان ارتقاء داده شود.(A.15.1.1) • برای حصول اطمینان از انطباق با الزامات قانون گذاری، مقرراتی و قراردادی در استفاده مادی با توجه به ارتباط با حقوق مالکیت فکری یا استفاده اختصاصی محصولات نرم افزاری، روشهای اجرایی تدوین و اجرا شود.(A.15.1.2) • سوابق مهم باید در برابر مفقود شدن، تخریب و تحریف طبق قوانین قانونی، مقرراتی و قراردادی الزامات کسب و کار، محافظت شوند.(A.15.1.3) • از استفاده کاربران از امکانات پردازش اطلاعات بدون مجوز ممانعت به عمل آید.(A.15.1.5)
۵۸	عدم وجود مدیریت یکپارچه امنیت اطلاعات	• یک سند سیاست امنیتی توسط مدیریت مرکز داده تدوین و تصویب گردیده و منتشر گردد و بر حسب اقتضاء مورد تبادل نظر با تمام کارکنان قرار گیرد. • خط‌مشی های ذکر شده در سند سیاست امنیتی باید به طور منظم و نیز در مواردی که تغییرات مؤثری وجود داشته باشد، مورد بازنگری قرار گیرند تا از تداوم مناسب بودن خط‌مشی اطمینان حاصل شود. • فرم ها، اسناد و سیاست واکنش سریع مرکز داده شامل اهدف، محدوده، قوانین، مسؤلیتها و هماهنگی، همچنین مکانیزمهای کنترلی پیاده سازی، تولید و مرتبا مرور و به روز گردند.(NIST-IR-1)
۵۹	عدم سازگاری با خط مشی‌ها	• مدیران باید از اجرای صحیح تمام روش های اجرایی امنیت در حیطه مسئولیتشان برای دستیابی به تطابق با سند سیاست امنیتی و استانداردها، مطمئن شوند.(A.15.2.1) • سیستم های اطلاعاتی باید به طور منظم از نظر تطابق فنی با استانداردهای اجرایی امنیت مورد بررسی قرار گیرند.(A.15.2.2)
۶۰	فقدان نظام مدیریت امنیت اطلاعات	• مدیریت باید فعالانه از امنیت در سازمان با ساختار شفاف، تعهد آشکار، وظیفه صریح و قبول مسئولیتهای امنیت اطلاعات پشتیبانی کند. (A.6.1.1) • تشکیلات لازم و نیروی انسانی متخصص در زمینه امنی اطلاعات جذب یا تربیت گردند. • مسئولیت‌های حفاظت از هریک از دارایی‌های منفرد و انجام فرآیندهای امنیتی مشخص باید به طور شفاف تعریف شوند.(A.6.1.3) • برای استفاده از امکانات پردازش اطلاعات جدید، باید یک فرآیند صدور مجوز از طرف مدیریت پایه ریزی شود.(A.6.1.4) • باید همکاری مناسبی تحت مجوزهای قانونی، بین سازمانهای تنظیم کننده

		مقررات، تأمین‌کنندگان سرویسهای اطلاعاتی و اپراتورهای مخابراتی ایجاد و حفظ گردد.(A.4.1.7) • رویکرد سازمان برای مدیریت امنیت اطلاعات و اجرای آن (مثال: اهداف کنترل، کنترل ها، سیاستها، فرآیندها، روش های اجرایی امنیت اطلاعات) بصورت مستقل یا طرح ریزی دوره ای یا هنگامی که تغییرات مهم در اجرای امنیت رخ می دهد، بازنگری شود.(A.6.1.8)
۶۱	استخدام یا به کارگماری افراد نامناسب	• نقشهای امنیتی و مسوولیتهای کارکنان، پیمانکاران و کاربران ثالث باید طبق سند سیاست امنیت اطلاعات مرکز داده مشخص و مستند سازی گردند. • بررسی سوابق همه افراد آماده استخدام، پیمانکاران و کاربران ثالث، باید طبق قوانین، اصول و قوانین مربوط و متناسب با الزامات کسب و کار طبقه‌بندی اطلاعات در دسترس باشد. • به عنوان بخشی از تعهد قراردادی افراد، کارکنان، پیمانکاران و کاربران ثالث باید طبق قوانین، اصول و مقررات مربوطه و متناسب با الزامات کسب و کار طبقه بندی اطلاعات در دسترسی را مدنظر داشته و به ریسک‌های ناشی از افشاء اطلاعات و دسترسی غیرمجاز دیگران واقف باشند.
۶۲	عدم آگاهی نیروهای انسانی از مسوولیتها و تعهدات	• مدیریت باید از کارکنان و پیمانکاران و کاربران ثالث بخواهد تا امنیت را طبق خط‌مشی‌های تدوین شده و رویه‌های مرکز داده بکار برند. • همه کارکنان سازمان (مرتبط با مرکز داده)، پیمانکاران و کاربران ثالث، باید آگاهی و آموزش مناسب و خط مشی های به روز شده و روشهای اجرایی که به عملکرد شغلی آنها مربوط می شود، را دریافت کنند. • باید فرآیند انضباطی رسمی برای کارکنانی که تعهدات امنیتی را نقض کردند وجود داشته باشد. • سازمان بایستی آموزشهای لازم در خصوص مسولیتهای آنها و قوانین واکنش سریع در مواقع لازم را به همه کارکنان (مرتبط با مرکز داده) داده و مرتبا به روز نماید. (NIST-IR-2) • سازمان بایستی با ارایه اتفاقات و حوادث شبیه سازی شده در قالب آموزش، میزان کارآیی آموزشهای ارایه شده به پرسنل را در شرایط حیاتی ارزیابی نماید.((NIST-IR-2 (1)
۶۳	تهدیدهای مربوط به تغییر شغل یا انفصال از خدمت کارکنان و پیمانکاران	• مسئولیتها برای آن افرادی که دوره استخدامشان پایان یافته یا تغییر پیدا کرده باید بصورت روشن و واضح بوده و تعیین شود.(A.8.3.1) • همه کارکنان، پیمانکاران و کاربران ثالث باید همه دارایی های سازمان را (آنچه در تصرف دارند) به محض خاتمه استخدام ، قرارداد و توافق بازگردانند.(A.8.3.2) • مجوزهای دسترسی به اطلاعات و امکانات پردازش اطلاعات برای کل کارکنان ،

		پیمانکاران و کاربران ثالث باید به محض اتمام استخدامشان، قرارداد و توافقشان حذف شده یا به محض تغییر، تنظیم شود.(A.8.3.3)
۶۴	دسترسی‌های غیرمجاز طرفهای خارج مرکز داده	• ریسکهای مرتبط با دسترسی به امکانات پردازش اطلاعات سازمان توسط طرف خارج مرکز داده (منظور طرفهای داخل کشور می باشد نه خارج کشور) باید برآورد شده و کنترل‌های امنیتی مناسب پیاده‌سازی گردد.(A.6.2.1) • در قراردادهای با طرفهای خارج مرکز داده شامل دسترسی، پردازش، ارتباط، مدیریت اطلاعات یا تجهیزات، خرید تجهیزات، نصب و غیره باید تمام ملزومات امنیتی مربوط مشخص شوند.(A.6.2.3)
۶۵	عدم تجهیز به سیستم مدیریت بحران و شرایط اضطرار	• نصب سیستم‌های مدیریت بحران • اتخاذ سیاست‌ها و مکانیزم‌های اجرایی جهت جلوگیری از وقوع شرایط اضطرار • آموزش پرسنل برای رویارویی با شرایط اضطرار • تهیه دستورالعمل‌های لازم و ابلاغ آن به زیر مجموعه ها
۶۶	فقدان یک سیستم هشداردهنده سریع و به موقع	• بکارگیری سیستم‌های هشداردهنده سریع در حوزه های مختلف • بکارگیری سیستم‌های هوشمند اعلام خطر در خصوص حملات سایبری (نظیر DIDS) • بکارگیری سیستم‌های اعلام حریق هوشمند • آموزش پرسنل برای استفاده از این سیستم‌ها
۶۷	عدم بکارگیری سازه‌های امن و پایدار	• استفاده از سازه‌های امن و پایدار در طراحی مرکز داده • قرار دادن تجهیزات حساس و آسیب‌پذیر در فضای مطمئن • استفاده از موانع طبیعی علاوه بر سازه‌های مصنوعی (پوشش سازه های مصنوعی در درون موانع طبیعی نظیر عمق زمین یا زیر کوه)
۶۸	تولید اطلاعات غلط و نامطمئن	• شناسایی علل ناشی از تولید اطلاعات غلط اعم از نرم افزاری، سخت افزاری و نیروی انسانی و رفع این موارد
۶۹	عدم بهره مندی از مراکز احتیاط (Backup) امن، ایمن و پایدار	• ایجاد یک مرکز داده پشتیبان فعال (Active)و یک مرکز داده Offline در محل های فیزیکی دیگر بمنظور سرویس دهی در صورت عدم امکان سرویس دهی توسط مرکز اصلی
۷۰	عدم بکارگیری خطوط ارتباطی مطمئن و پایدار	• بکارگیری چندین خطوط ارتباط مطمئن و پشتیبان در کنار همدیگر به منظور پشتیبان ارتباطی یکدیگر • استفاده از تکنولوژی‌های ارتباطی ناهمگون

۷۱	اتصالات ناامن به شبکه‌های اینترنت و اینترانت و فیبر نوری	• طراحی صحیح اتصالات در زمان طراحی مراکز داده بمنظور عدم وجود اتصال ناامن • نظارت و کنترل دوره ای در این خصوص و شناسایی تمامی اتصالات احتمالی ناامن و حذف آنها • ایزوله بودن سرویسهای بین المللی مورد نیاز در مراکز داده از سرویسهای داخلی • ایزوله بودن کامل در بالاترین حد ممکن در خصوص سرویسهای بین المللی مورد نیاز در مراکز داده از سرویسهای داخلی
۷۲	عدم پیش‌بینی برق پشتیبان	• پیش بینی برق UPS برای مرکز داده بمنظور استفاده در صورت قطع برق عادی متناسب با گستردگی، سطح و اهمیت مرکز داده • استفاده از مولدهای تولید برق پشتیبان، بمنظور پشتیبانی از برق UPS متناسب با سطح و اهمیت مرکز داده • نگهداری سوخت کافی برای مولدهای برق بمنظور استفاده در شرایط لازم
۷۳	عدم وجود نیروی انسانی متخصص لازم	• تربیت یا جذب نیروی انسانی متخصص لازم در حوزه های تخصصی مورد نیاز • ارائه آموزشهای عرضی تخصص‌های لازم به کارکنان • اولویت به استفاده از فن‌آوری‌هایی که نیروی متخصص آن در اختیار است. • تشویق کارکنان به فراگیری تخصص‌های متنوع و جدید • برگزاری آزمون‌های دوره‌ای جهت ارزیابی وضعیت آموزشی و کنترل کیفی مهارت‌های فنی آنان • برگزاری مانورهای آموزشی و مدیریت بحران به طور ادواری جهت ارزیابی سرعت عمل و انتقال در کارکنان جهت رویارویی با شرایط واقعی بحران
۷۴	عدم وجود آموزش امنیتی کافی	• برگزاری کلاسهای آگاهسازی و توجیه کارکنان در خصوص خسارات گزاف ناشی از عدم رعایت مسائل امنیتی • برگزاری دوره های آموزشی تخصصی عرضی امنیت برای متخصصین شبکه و امنیت • ارائه آموزشهای عمومی امنیت در سطوح مختلف به مدیران و کارکنان • ابلاغ سیاست‌های امنیتی و موظف نمودن کارکنان به تبعیت از سیاست‌ها با استفاده از مکانیزمهای مدیریتی
۷۵	اشتباهات و غفلت‌ها مانند عدم بکارگیری صحیح تجهیزات، عدم نصب صحیح نرم‌افزارها و برنامه‌های کاربردی، سهل انگاری	• آموزش کارکنان در خصوص نحوه صحیح نصب تجهیزات، نرم‌افزارها، برنامه‌های کاربردی و همچنین کاربری صحیح سیستم ها و تجهیزات • تدوین برنامه‌های ادواری جهت کنترل و شناسایی اشتباهات احتمالی کارکنان • نصب سیستم‌های هشداردهنده که در صورت فراموشی و یا غفلت کاربران هشدار دهد.
۷۶	عدم وجود کنترل روی قوانین	• تدوین سیاست کاری به منظور اجرای کنترل‌های لازم بمنظور اجرای قوانین تدوینی

		• بازبینی دوره ای قوانین و شناسایی قوانین ضعیف و متناقض و انجام تصحیحات لازم • تشویق و تنبیه کارکنان فعال و خاطی
۷۷	اتکا قابل ملاحظه به سیستم‌های ارتباطی بی‌سیم و ماهواره غیر امن	• رمزنگاری داده‌های ارسالی جهت کاهش مخاطرات ناشی از دسترسی غیرمجاز به داده‌ها در شرایط اضطرار به استفاده از این ارتباطات • عدم استفاده از سیستم‌های ارتباطی بی‌سیم بعلت عدم وجود امنیت کافی در این نوع از ارتباطات • استفاده از ارتباطات ماهواره ای داخلی در صورت راه اندازی در آینده در صورت نیاز
۷۸	عدم سازگاری با سیستم اطلاعات جغرافیایی (GIS)	• استفاده از سامانه های مبدل جهت ایجاد سازگاری با سیستم اطلاعات جغرافیایی در صورت نیاز

۷۹	زلزله	• عملیات مکان یابی صحیح و اصولی ساختمان باید در زمان انتخاب مکان مرکز داده انجام شود. • حفاظت فیزیکی در برابر آسیبهای ناشی از سیل، زلزله بایستی طراحی و بکارگرفته شود. (A.9.1.4) • طراحی و مقاومت ساختمان متناسب با کاربری مرکز داده در نظر گرفته شود. • عملیات مقاوم سازی ساختمان انجام گیرد. • آموزش افراد برای مقابله با حوادث (زلزله) • تدوین دستورالعملهای مرتبط با حوادث (زلزله) • تهیه و بکارگیری تجهیزات کمکهای اولیه • چیدمان مناسب تجهیزات جهت مقابله با لرزش های زلزله • تهیه و در دسترس بودن نقشه کلیه تأسیسات فنی و ابنیه ها • تهیه لیست تجهیزات موجود در مرکز داده • آموزش و بکارگیری گروه تعمیر، امداد و نجات • پیش بینی و بکارگیری سیستم روشنایی و برق اضطراری متحرک • پیش بینی سیستم های ارتباط داده پشتیبان بمنظور استفاده در شرایط اضطراری (NIST-CP-8(4)) • پیش بینی ارتباط مستقیم با مرکز زلزله نگاری (Hot line Connection) • پیش بینی تجهیزات جابجایی اشیاء (جرثقیل و ...) • پیش بینی و نصب تجهیزات هشدار وقوع زلزله در ساختمان • ایجاد سایت پشتیبان Active با ارتباط مستقیم و برخط (NIST-CP-6) و (NIST-CP-7) و و یک سایت پشتیبان Active دور • ایجاد و بکارگیری سیستم هوشمند قطع و وصل منابع (برق، آب، گاز) • پیش بینی رایانه های قابل حمل بی سیم جهت بکارگیری در زمان زلزله • پیش بینی ژنراتور برای تولید برق در شرایط قطع برق قبل و بعد از زلزله • استفاده حداکثری از مصالح و تجهیزات مقاوم در برابر آتش در زمان ساخت مرکز داده. • طراحی حفاظت فیزیکی در برابر آسیبهای ناشی از آتش سوزی • اعمال محدودیتها در مورد ممنوعیت ورود مواد آتش زا و پرخطر • تهیه و بکارگیری سیستم های هشداردهنده و اعلام حریق • تهیه و بکارگیری تجهیزات اطفاء حریق • آموزش دوره ای افراد شاغل در مرکز در مورد پیشگیری و مهار آتش • آموزش و بکارگیری گروه اطفاء حریق • ارتباط Online با مرکز آتش نشانی • پیش بینی ارتباط بی سیم با مرکز آتش نشانی

		• پیش بینی ارتباط مستقیم با مرکز زلزله نگاری (Hot line Connection)

۸۱	طوفان و صاعقه	• پیش بینی سیستم برق گیر و Earth جهت انتقال بار الکتریکی اضافی به زمین • ارائه آموزش پیشگیری و مقابله با حوادث برای افراد شاغل در مرکز داده • آموزش و بکارگیری گروه حوادث غیر مترقبه • پیش بینی تجهیزات جابجایی اشیاء (جرثقیل و ...) • ارتباط Online با مراکز امداد و نجات • پیش بینی ارتباط مستقیم با مراکز امداد و نجات (Hot line Connection)
۸۲	سیل	• تجهیز مرکز به سیستم جمع آوری آبهای سطحی • طراحی حفاظت فیزیکی در برابر آسیبهای ناشی از سیل • آموزش و بکارگیری گروه حوادث غیر مترقبه • ارتباط Online با مراکز امداد و نجات • پیش بینی ارتباط مستقیم با مراکز هواشناسی (Hot line Connection) • وجود امکانات ارتباط بی سیم با مراکز امداد و نجات
۸۳	رطوبت و دما	• تهیه و بکارگیری تجهیزات تهویه مطبوع در ساختمان مرکز داده • استفاده از مصالح مناسب در ساخت مرکز داده • استفاده از دماسنج و رطوبت سنج بخصوص در نقاطی که از تجهیزات حساس به دما استفاده می شود • الزام در خصوص عایق بندی کلیه سیستم های حساس به رطوبت و دمای نامناسب • تهیه و بکارگیری سیستم های تهویه اضطراری منظور استفاده در زمان از کارافتادگی سیستم های اصلی
۸۴	دود	• تهیه و بکارگیری نورافکن و مه شکن در نقاط مختلف مرکز داده و پیرامون آن • بکارگیری تجهیزات کم کننده اثرات دود • پیش بینی ارتباط با مرکز هواشناسی
۸۵	سقوط اجسام	• رعایت استحکام مناسب در طراحی سازه مراکز داده متناسب با نوع آنها
۸۶	تداخل الکترومغناطیسی امواج	• مکان یابی نصب تجهیزات به منظور دوری از تجهیزات تداخل کننده مثل خطوط برق فشار قوی و خطوط با جریان بالا • رعایت استانداردهای مربوط به کابل کشی و فواصل مربوط به نصب کابل های انتقال داده ، برق و تلفن در زمان طراحی مرکز داده • آموزش و بکارگیری گروه متخصص در خصوص اختلال های الکترومغناطیسی • بکارگیری حفاظهای امواج الکترومغناطیس بر روی بسترهای انتقال • پیش بینی شبکه طیف گسترده جهت جلوگیری از تداخل الکترومغناطیسی
۸۷	مشکلات تأسیساتی (آب ،گاز، برق، تلفن)	• طراحی مناسب تأسیسات و رعایت استانداردهای نصب مسیرهای انتقال در زمان طراحی مرکز داده

		• استفاده از سیستم های هوشمند هشدار دهنده و کنترل کننده تاسیسات • حفاظت تجهیزات از افت جریان برق یا هر اختلالی که بر اثر عدم پشتیبانی تأسیسات بوجود می آید • استفاده از سیستم های پشتیبان برای آب، گاز، برق و تلفن بمنظور استفاده در صورت اختلال در مسیر اصلی • آموزش و بکارگیری گروه تاسیسات
۸۸	مواد پرخطر	• کنترل و نظارت بمنظور عدم انتقال مواد پرخطر و حساس • بازرسی افراد و تجهیزات به هنگام ورود و خروج • پیش بینی تجهیزات لازم بمنظور مقابله با حوادث احتمالی پیش آمده از طریق این مواد • آموزش و بکارگیری گروه متخصص جهت انجام عکس العمل مناسب
۸۹	تشعشعات رادیواکتیو	• نصب تجهیزات هشدار دهنده جهت اعلام خطر نشت مواد رادیواکتیو در محیط • قرار دادن لباس‌های مخصوص کار در محیط‌های آلوده به تشعشعات رادیواکتیو جهت استفاده پرسنل در صورت نیاز • استفاده از گیت‌های ورودی حساس به تشعشعات رادیواکتیو در تمامی ورودی‌های مراکز داده • تجهیز دیواره‌های داخلی مراکز داده به مواد شیمیایی مخصوص جذب موارد رادیواکتیو • آموزش و بکارگیری گروه متخصص جهت انجام عکس العمل مناسب
۹۰	گرد وغبار و مه	• بکارگیری فیلترهای جلوگیری کننده از ورود گرد و غبار • استفاده از حسگرهای گرد و غبار بمنظور اعلام هشدار در مواقع لازم • آموزش کارکنان در مورد نحوه رفع مشکل • آموزش و بکارگیری گروهی جهت انجام عکس العمل مناسب

۹-۷ ملاحظات امنیتی سطح پایین مراکز داده

اصولاً ملاحظات سطح پایین مراکز داده، بایستی متناسب با هر مرکز داده خاص، و در زمان طراحی و پیاده سازی آن، با درنظر گرفتن ملاحظات امنیتی سطح بالا و میانی که بیان گردید، طراحی و

پیاده سازی گردد. لیکن بمنظور آشنایی با ماهیت ملاحظات این سطح، در ادامه به عنوان نمونه، یک مورد از ملاحظات فنی سطح پایین و اجرایی مراکز داده بیان شده است. بدیهی است جزئیات مربوط به این هر یک از این موارد برای هر مرکز داده بصورت خاص بوده و در زمان طراحی تعیین می گردد.

۹-۷-۱ روش تامین امنیت شبکه مراکز داده

نظر به لزوم ایجاد امنیت بالا در مراکز داده، و بر اساس مدلهای امنیتی Multi Layer Security و Defence In Depth طرح امنیتی ۵ لایه‌ای متناسب با موارد زیر پیشنهاد می گردد:

۱- امنیت فیزیکی و محیطی

۲- امنیت لایه شبکه

۳- امنیت لایه کاربرد

۴- امنیت لایه میزبان

۵- امنیت داده

بمنظور ایجاد امنیت لازم در هر لایه، از ابزارهای امنیتی خاص آن لایه استفاده می گردد. برای این منظور از ابزارهایی نظیر فایروال، سامانه تشخیص و جلوگیری از نفوذ، سامانه پایش شبکه، سامانه‌های کنترل دسترسی، سامانه‌های ضد بد افزار، سامانه‌های تشخیص و رفع آسیب پذیریها، سامانه‌های رمز کننده لایه‌های شبکه و بسیاری ابزارهای امنیتی دیگر متناسب با نوع و ماهیت شبکه یک مرکز داده بهره جسته می‌شود. اما از آنجا که فرآیند امن سازی و به تبع آن امن سازی لایه‌های شبکه، فقط به استفاده از یک سری ابزارهای امنیتی امکان پذیر نمی‌باشد، بلکه فعالیتهایی نظیر "پیکربندی امن کلیه تجهیزات و ابزارهای بکار گرفته شده در ایجاد و توسعه شبکه" و "رویه‌ها و روالهای امنیتی مرتبط با امنیت" نیز بایستی طراحی و اجرا گردند، لازم است در کنار استفاده از تجهیزات امنیتی در هر لایه شبکه، به دو مقوله اشاره شده نیز

توجه گردد.

۸-۹ مراجع

[1] ISO/IEC 27001: Information Technology – Security Techniques –Infromation Security Management Systems – Requirements, 2005.

[2] ISO/IEC 17799: Information Technology – Security Techniques - Code of Practicfe for Infromation Security Management (2nd edition), Feburary 2005.

[3] Federal Information Processing Standards Publication, FIPS PUB 199: Standards for Security Categorization of Federal Information and Information Systems, February 2004.

[4] Federal Information Processing Standards Publication, FIPS PUB 200: Minimum Security Requirements for Federal Information and Information Systems, March 2006.

[5] National Institute of Standards and Technology, NIST SP 800-60: Guide for Mapping Types of Information and Information Systems to Security Categories, Draft Revision November 2007.

[6] National Institute of Standards and Technology, NIST SP 800-53: Recommended Security Controls for Federal Information Systems, Revision 1, December 2006.

جمع‌بندی

در این گزارش بررسی جامعی از تهدیداتی که مراکز داده کشور را مورد هدف قرار می دهند صورت گرفت. بسته به دسته بندیی که از مراکز داده انجام شد این تهدیدات دسته بندی و برای هریک بسته به نوع مراکز داده راهکار و کنترل های لازم ارائه گردید.

با عنایت به نوع نگاه به ملاحظات امنیتی در طراحی مراکز داده (سطح بالا، میانی و پایین) می توان گفت که به مقابله با بسیاری از تهدیدات را می توان با بکارگیری روش هایی در سطوح بالا و میانی پرداخت.

با این حال با توجه به این که در سطح پایین، ملاحظات امنیتی وابسته به نوع محصولات، ابزارها و تکنولوژی به کار رفته برای طراحی و تجهیز مراکز داده بوده و بنابراین نمی توان در این مقوله و بدون توجه به موارد اخیر در مورد راهکارهای طراحی مراکز داده جهت مقابله با تهدیدات موجود به ارائه راهکارهای لازم پرداخت.

این سند شامل ملاحظات سازمان پدافند غیرعامل در طراحی و ساخت مراکز داده در کشور می‌باشد. سازمان پدافند غیر عامل کشور ۳ هدف امنیت، ایمنی و پایداری را در تمام حوزه ها از جمله حوزه فضای سایبر و فاوا (فن‌آوری اطلاعات و ارتباطات) دنبال می نماید. در این سند، این اهدف در مقوله طراحی و پیاده سازی مراکز داده کشور دنبال گردیده است. در ادامه چارچوب و محتویات سند توضیح داده می شود.

در این سند ابتدا شناخت وضعیت فعلی مراکز داده شامل تعاریف، تاریخچه و وضعیت مرکز داده در ایران و جهان آورده شده است. سپس به معماری ها و استانداردهای مراکز داده پرداخته شده و در ادامه

تهدیدات امنیتی متصور برای مراکز داده کشور با رویکرد پدافند غیرعامل بررسی گردیده است. این تهدیدات در ۳ دسته ۱-تهدیدات ناشی از جنگ (سایبر و فیزیکی) و مخاصمات بین المللی ۲- تهدیدات امنیتی ۳- تهدیدات محیطی و طبیعی، مورد توجه قرار گرفته است. نهایتا در ادامه، ضمن ارائه راهکارهای فنی برای تهدیدات بیان شده، الگوی مراکز داده کشور با رویکرد پدافند غیر عامل تدوین گردیده و آورده شده است. در این الگو، ملاحظات پدافند غیر عامل به ۳ سطح بالا، میانی و پایین تقسیم بندی شده است. در ملاحظات سطح بالا، پارامترهای سطح بندی مراکز داده کشور و تعیین یکی از سطوح مهم، حساس یا حیاتی بیان گردیده است. در ملاحظات سطح میانی، کنترلهای پدافند غیر عامل و امنیتی متناسب با تهدیدات احصاء شده و به تفکیک برای هر یک از سطوح مراکز داده مهم، حساس و حیاتی بیان گردیده است. در ادامه به مصادیق ملاحظات سطح پایین مراکز داده نیز اشاره گردیده است، لیکن از آنجا که این ملاحظات وابسته به محصولات و تکنولوژی ها بوده و دائما در حال تغییر است، در زمان طراحی و پیاده سازی هر مرکز داده، بایستی با توجه به ملاحظات سطح بالا و میانی که در این سند بیان شده، با نظارت سازمان پدافند غیر عامل تعیین و اجرا گردند.

تمامی سازمانهای دولتی، غیردولتی که به نوعی درصدد بکارگیری و استفاده از مراکز داده به منظور بهره مندی کاربران و احتمالاً خود سازمان از خدمات ارائه شده می باشند می بایستی ضمن توجه به این گزارش راهکارها و کنترل های لازم را در طراحی مراکز داده را مورد توجه قرار دهند.

پیوست ۱: تعاریف مختلف مرکز داده

در اینجا تعریف‌های مختلف مرکز داده از منابع نسبتاً معتبر توسط کمیتهٔ علمی همایش «نقش مرکز داده در توسعهٔ فن‌آوری ارتباطات و اطلاعات کشور» جمع‌آوری شده است. لازم به ذکر است که تعریف نهایی پیشنهادی همان تعریف ارائه شده زیر می‌باشد:

مرکز داده مکانی است؛

(الف) با امنیت فیزیکی و الکترونیکی بالا، برخوردار از پهنای باند ارتباطی وسیع، متصل به شبکه‌های رایانه‌ای ملی یا جهانی، با خدمات تمام وقت و در دسترس،

(ب) که شامل انواع تجهیزات سخت‌افزاری(رایانه‌ها، سوئیچ‌ها، مودم‌ها، ...) و نرم‌افزاری(پایگاه‌های داده، سرورها، سیستم‌عامل، ...) پیشرفته بوده و از پشتیبانی و نگهداری حرفه‌ای و تمام وقت برخوردار است و

(ج) به پشتیبانی و ارائهٔ انواع خدمات مرتبط با اطلاعات و داده از قبیل خدمات ذخیره، نگهداری و بازیابی داده، خدمات ERP ، میزبانی خدمات اینترنتی، میزبانی ارائهٔ خدمات کاربردی(ASP)، میزبانی برون سپاری خدمات(out-sourcing)، خدمات شبکهٔ اختصاصی مجازی(VPN) و غیره برای شرکت‌های خصوصی یا دولتی، می‌پردازد.

برای رسیدن به یک تعریف جامع و مانع، در ابتدا در جلسات متعددی مفاهیم و ابعاد مرکز داده مورد بحث و بررسی قرار گرفت. سپس ۱۲ تعریف مختلف برای مرکز داده به شرح زیر ارائه گردید. در پایان روی این تعاریف جمع‌بندی شد و تعریف فوق استخراج گردید. آنچه که در تعاریف زیر به چشم می

خورد این است که مرکز داده دارای ویژگی‌هایی است، اجزایی دارد و برای کاربردهایی استفاده می شود. تعریف فوق نیز بر این مبنا تهیه شده است.

رویکرد مرکز داده سه دورهٔ تاریخی را پشت سر گذاشته است، مرحلهٔ مراکز دادهٔ متمرکز که با پیدایش رایانه های بزرگ اولیه آغاز شد، مرحلهٔ مراکز دادهٔ توزیع شده که در دهه ۸۰ میلادی و با پیدایش رایانه های شخصی شروع شد و مرحلهٔ تمرکز مجدد که از اواخر دههٔ ۹۰ و با توسعهٔ شبکه های رایانه ای و اینترنت آغاز گردید. برخی از تعاریف زیر مربوط به دوران اول یا دوم هستند. تعریف جمعبندی فوق، مرکز داده را در شرایط جاری و در دورهٔ سوم توصیف می کند.

تعاریف مختلف مرکز داده

۱- به مراکزی مانند مرکز پردازش کارت اعتباری بانک که مکانی برای پردازش داده های الکترونیکی است مرکز داده اطلاق می شود.

An electronic data processing facility such as a bank's credit card processing center.

http://www.hi-availability.com/pr_ultra_green_glossary.html

۲- مرکز داده انبارهٔ متمرکزی برای ذخیره، مدیریت، و توزیع داده و اطلاعاتی است که این داده ها به حیطهٔ مشخصی از دانش یا کاربرد تعلق دارند. مرکز داده ممکن است دارای یک مرکز عملیات شبکه (NOC) باشد که دسترسی محدود و کنترل شده ای دارد و شامل سیستم های خودکار مراقبت از فعالیتهای سرور، ترافیک وب و عملکرد شبکه بوده و کوچکترین اختلال را به مهندسین گزارش می کند و آنها مشکلات احتمالی را قبل از و قوع مهار می کنند.

Data Centre is a centralized warehouse for the storage, management, and dissemination of data and information organized around a particular area or body of knowledge. The data centre may contain a network operations centre (NOC), which is a restricted access area containing automated systems that constantly monitor server activity, Web traffic, and network performance and report even very slight irregularities to engineers so that they can spot potential problems before they really happen .

http://www.tcs-asp.com/library/glossary.html

۳- مجموعه ای از تجهیزات متمرکز شده (content servers, transaction servers, or web caches)

Collection of centrally located devices (content servers, transaction servers, or web caches)

http://www.cisco.com/en/US/products/sw/conntsw/ps4038/products_configuration_guide_chapter09186a00800ca812.html

۴- محلی برای نگهداری یک یا چند محیط تولید و فرآوری (از قبیل کامپیوترهای سرور، تجهیزات اتصال شبکه، پایگاه های داده، کاربردها) که توسط یک سازمان برای انجام پردازشهای داده های کاربران آن سازمان به کار می رود.

A facility housing the one or more production environments (e.g., server computers, network connectivity devices, databases, applications) that is used by an organization to perform data processing for user organizations .

http://www.donald-firesmith.com/Glossary/GlossaryD.html

۵- مرکز داده مجتمعی برای نگهداری سیستمهای کامپیوتری حیاتی(مأموریت گرا) و اجزای مرتبط آن است. این مراکز معمولا دارای کنترلهای محیطی(تنظیم هوا، جلوگیری از آتش سوزی و غیره)، تدارکات برق پشتیبان، و امنیت بالا می باشند. خدمات اینترنتی و میزبانی وب معمولا محل حضور و ارائهٔ خدمات وب خود را در مراکز داده قرار می دهند.

A facility used to house mission critical computer systems and associated components. They generally include environmental controls (air conditioning, fire suppression, etc.), redundant/backup power supplies, and high security. Internet Service and Web Hosting Providers generally locate their Points of Presence and Web server facilities in data centers .

http://marketing.byu.edu/htmlpages/courses/490r/chapters/glossary.htm

۶- مجموعه‌ای از ابزارهای فوق امن و مقاوم در برابر خرابی که تجهیزات مشتری در آن قرار می‌گیرد و به شبکه‌های ارتباطی متصل است. این ابزارها شامل سرورهای وب، سوییچ‌ها، مسیریاب‌ها، و مودم‌ها است. مکز داده از سایتهای وب شرکتها پشتیبانی می‌کند و محلی برای ISP ها، ASP ها، شرکتهای میزبانی وب و ارئه کنندگان خدمات DSL است.

Highly secure, fault-resistant facilities housing customer equipment that connects to telecommunications networks. The facilities accommodate Web servers, switches, routers and modem racks. Data centers support corporate Web sites and provide locations for CLECs, ISPs, ASPs, Web hosting companies and DSL providers .

http://www.c-b.com/industryinfo/glossaries/telecom.asp

۷- محل فیزیکی سیستمهای رایانه‌ای بزرگ و پایگاه‌های داده

The physical location for mainframe systems and enterprise databases .

http://www.consultingtimes.com/glossary.html

۸- مرکز داده یک انباره مرکزی است که (چه به صورت فیزیکی وچه به صورت مجازی) برای ذخیره سازی، مدیریت، توزیع داده ها و اطلاعات طبقه بندی شده حول انواع دانش یا وابسته به یک تجارت خاص به کار می رود. برای مثال NCDC یک مرکز دادهٔ عمومی است که بزرگترین آرشیو جهانی اطلاعات آب و هوای دنیا به شمار می رود. یک مرکز دادهٔخصوصی ممکن است درون یک سازمان قرار گرفته باشد یا به صورت یک عضو مجزا در خارج از آن قرار بگیرد.

A data center (sometimes spelled datacenter) is a centralized repository, either physical or virtual , for the storage, management, and dissemination of data and information organized around a particular body of knowledge or pertaining to a particular business. The National Climatic Data Center (NCDC), for example, is a public data center that maintains the world's largest archive of weather information. A private data center may exist within an organization's facilities or may be maintained as a specialized facility. According to Carrie Higbie, of Global Network Applications, every organization has a data center, although it might be referred to as a server room or even a computer closet. In that sense, data center may be synonymous with network operations center (NOC), a restricted access area containing automated systems that constantly monitor server activity, Web traffic, and network performance .

http://searchdatabase.techtarget.com/sDefinition/0,,sid13_gci332661,00.html

۹- این تعریف مربوط به دورهٔ دوم است و در قسمت خط کشیده شده وجود مراکز دادهٔ متمرکز را در حال کم شدن می داند.

The department in an enterprise that houses and maintains back-end information technology (IT) systems and data stores - its mainframes, servers and databases. In the days of large, centralized IT operations, this department and all the systems resided in one physical place, hence the name "data center." With today's more distributed computing methods, single data center sites are still common, but are becoming less so . The term continues to be used to refer to the department that has responsibility for these systems, no matter how dispersed they are .

http://www.gartner.com

۱۰- مرکز خدمات اینترنت که معمولا توسط شخص ثالث ارائه می‌شود، شامل تجهیزات مرتبط با اینترنت برای استفادهٔ سازمان‌ها وتشکیلات اقتصادی، ISP ها، ASP ها، شرکتهای تجارت الکترونیک و سایر شرکت‌ها است. مرکز خدمات اینترنت معمولا مکان برون سپاری، سرورها، میزبانی خدمات، شبکهٔ اختصاصی مجازی و سایر شبکه‌ها بوده و انواع خدمات انتقال اطلاعات را ارائه می کند.

IDC (Internet data center)

A data center (typically operated by a third party) containing Internet-related facilities for the use of enterprises, Internet service providers, application service providers (ASPs), e-commerce companies and other firms. IDSs typically provide server outsourcing, hosting and colocation services, Internet connectivity, virtual private networks (VPNs), and other network and transport services.

http://www.gartner.com/6_help/glossary/GlossaryI.jsp

۱۱- مرکز داده بخشی از سازمان یا شرکت است که شامل سیستم‌های رایانه‌ای و تجهیزات مرتبط می‌باشد. ورود داده‌ها و برنامه‌نویسی سازمان هم ممکن است در این محل انجام شود. همچنین یک مرکز کنترل بر کارها نظارت می‌کند.

http://www.datacenterjournal.com

-Data Center :

The department that houses the computer systems and related equipment, including the data library. Data Entry and systems programming may also come under its jurisdiction. A control center is usually provided that accepts work from and releases output to user department.

۱۲- یا ساختمان امن و محافظت شده که شامل انواع رایانه‌ها، سرورها، مسیریاب‌ها، شبکه، سوییچ‌ها و تجهیزات و تخصصهای لازم برای پشتیبانی از انبوه اطلاعات معتبر که قابل دسترسی توسط کاربران گوناگون در اقصا نقاط جهان باشد.

A very well protected and safe building that houses various types of Computers, Servers, Routers, Network, Switches, Equipments and professionals to support a large source of reliable data that is accessible by many large or small users around the clock .

پیوست ۲: فهرست مراکز داده مهم آمریکا و سایر کشورها

در اینجا فهرستی از مراکز داده مهم در آمریکا و دیگر کشورها آورده می‌شود. همان طور که ملاحظه می‌شود بیشترین مراکز داده در کشور آمریکا قرار دارد.

این فهرست از آدرس زیر اقتباس شده است:

http://en.wikipedia.org/wiki/List_of_Data_centers

فهرست مراکز داده ای آمریکا

	Name	City	Website
1	Managed Network Solutions	Bryan, Texas	http://www.managednetworks.com/
2	Alchemy Communications Inc.	Los Angeles, California	http://www.alchemy.net/
3	C I Host	Los Angeles	http://www.cihost.com/
4	C I Host	Chicago	http://www.cihost.com/
5	1-800-HOSTING	Dallas	http://www.800hosting.com/
6	The Planet	Dallas	http://www.theplanet.com/

7	C I Host	Dallas	http://www.cihost.com/
8	C I Host	Newark	http://www.cihost.com/
9	ColoServe	San Francisco	http://www.coloserve.com/
10	Infinex Telecom	San Francisco	http://www.infinex.com/
11	Navisite	Andover, MA	http://www.navisite.com /office_locations.aspx?id =35&office=470
12	Navisite	Atlanta	http://www.navisite.com/ office_locations.aspx?id= 35&office=471
13	Navisite	Chicago	http://www.navisite.com/ office_locations.aspx?id= 35&office=473
14	Navisite	Houston	http://www.navisite.com/ office_locations.aspx?id= 35&office=474

15	Navisite	New York, NY	http://www.navisite.com/office_locations.aspx?id=35&office=478
16	Navisite	San Jose	http://www.navisite.com/office_locations.aspx?id=35&office=479
17	Navisite	Syracuse, NY	http://www.navisite.com/office_locations.aspx?id=35&office=480
18	Navisite	Vienna, VA	http://www.navisite.com/office_locations.aspx?id=35&office=481
19	NYI	New York	http://www.nyi.net/
20	Verio	New York	http://www.verio.com/
21	1&1 Internet	Kansas City	http://1and1.com/
22	SoftLayer	Dallas	http://www.softlayer.com/

فهرست مراکز داده سایر کشورها

	Name	City	Website
United Kingdom			
1	IXEurope City	London	http://www.ixeurope.com/
2	IXEurope West London	London	http://www.ixeurope.com/
3	IXEurope Park Royal	London	http://www.ixeurope.com/
4	IXEurope Slough	London	http://www.ixeurope.com/
5	Navisite Surrey	London	http://www.navisite.com/ office_locations.aspx?id= 35&office=476
6	TeleCityRedbus Harbour Exchange	London	http://www.telecityredbus.com/
7	TeleCityRedbus Meridian Gate	London	http://www.telecityredbus.com/

8	TeleCityRedbus Sovereign House	London	http://www.telecityredbus.com/
9	VSNL Stratford	London	http://www.connexions4london.co.uk/ colocation/tyco_colocation.html
Germany			
10	Colt Telecom	Hamburg	http://www.colt.net/
11	TeleCityRedbus	Frankfurt	http://www.redbus.de/
12	IXEurope	Frankfurt	http://www.ixeurope.com/
13	IXEurope	Dusseldorf	http://www.ixeurope.com/
14	IXEurope	Munich	http://www.ixeurope.com/
Canada			
15	Provision Data Systems	Kelowna	http://www.provisiondata.com/
16	dotServing	Montreal	http://www.dotserving.com/
17	PEER 1	Vancouver	http://www.peer1.com/

18	PEER 1	Toronto	http://www.peer1.com/
19	PEER 1	Montreal	http://www.peer1.com/
Brazil			
20	Alog	Rio de Janeiro	http://www.alog.com.br/
India			
21	Navisite	Guragon	http://www.navisite.com/ office_locations.aspx?id= 35&office=477
Ukraine			
22	Colocall	Kiev	http://www.colocall.net/
23	Volia	Kiev	http://www.dc.volia.com/

پیوست ۳: اصطلاحات و مفاهیم مهم مرکز داده

در این پیوست مفاهیم و اصطلاحات مهم در مراکز داده ارائه شده است. در اینجا تنها تمرکز روی اصطلاحات اصلی مراکز داده بوده است. اصطلاحات دیگر فنی که مرتبط با شاخه‌های دیگر مانند سخت‌افزار هستند، آورده نشده‌اند.

معادل فارسی	اصطلاح انگلیسی	شرح
مرکز داده	Data Center	- مرکز داده مکانی است: الف) با امنیت فیزیکی و الکترونیکی بالا، برخوردار از پهنای باند ارتباطی وسیع، متصل به شبکه‌های رایانه‌ای ملی یا جهانی، با خدمات تمام وقت و در دسترس ب) که شامل انواع تجهیزات سخت‌افزاری (رایانه‌ها، سوییچ‌ها، مودم‌ها، ...) و نرم‌افزاری (پایگاه‌های داده، سرورها، سیستم‌عامل، ...) پیشرفته بوده و از پشتیبانی و نگهداری حرفه‌ای و تمام‌وقت برخوردار است و ج) به پشتیبانی و ارائهٔ انواع خدمات مرتبط با اطلاعات و داده از قبیل خدمات نگهداری و بازیابی داده، خدمات ERP، میزبانی خدمات اینترنتی، میزبانی ارائهٔ خدمات کاربردی (ASP)، میزبانی برون‌سپاری خدمات و غیره برای

معادل فارسی	اصطلاح انگلیسی	شرح
		شرکت‌های خصوصی یا دولتی، می‌پردازد. - مرکز داده بخشی از سازمان یا شرکت است که شامل سیستم‌های رایانه‌ای و تجهیزات مرتبط می‌باشد. ورود داده‌ها و برنامه‌نویسی سازمان هم ممکن است در این محل انجام شود. همچنین یک مرکز کنترل بر کارها و ورودی و خروجی مرکز نظارت می‌کند.
کنترل دسترسی اختیاری	DAC	Discretionary Access Control
داده کاوی	Data mining	
منع سرویس	Denial of Service (DoS)	نوعی از حمله که در آن هدف قطع سرویس یا کاهش سطح سرویس و دسترسی است.
فایل سیستم توزیع شده	DFS	Distributed File System
مرکز پردازش داده	DPC	Data Processing Center
خط مشی	EDRP	Encrypted Data Recovery Policy

معادل فارسی	اصطلاح انگلیسی	شرح
رمزنگاری داده		
رمزنگاری داده	Data Encryption	
فایل سیستم رمز شده	EFS	Encrypting File System
استاندارد پردازش اطلاعات فدرال	FIPS	Federal Information Processing Standard
اتاق تجهزات شبکه	NER	Network Equipment Room
آرایهٔ تکراری از دیسک‌های کم‌هزینه	RAID	Redundant Array of Inexpensive Disks
سطوح RAID	RAID level	RAID 0 Striping. No redundancy. Fastest. - Provides maximum storage. No fault tolerance. RAID 1 Disk mirroring. Good performance. - Fault tolerant. Only option if using 2 drives.

معادل فارسی	اصطلاح انگلیسی	شرح
		- RAID 2 Error correction data written to separate disk. - RAID 3 Striping (small stripe size) with one parity disk. - RAID 4 Striping (large stripe size) with one parity disk. - RAID 5 Striping with parity. Parity information is distributed across all drives. Good performance. Fault tolerant. Slowest to rebuild (if one disk is replaced). Better storage than RAID 1. Requires at least 3 disks. Tolerant of a single disk failure. - RAID 6 RAID 5 with an extra parity disk. Tolerant of two disks failing. - RAID 0+1 Mirrored array (RAID 1) whose segments are RAID 0 arrays, i.e. mirroring of striped sets. - RAID 10 Striped array (RAID 0) of mirrored sets (RAID 1). - RAID 53 Combination of RAID 0 and RAID 3. Each stripped set (of RAID 0) are RAID 3 sets.
پنج نُه	5-Nines	دسترس‌پذیری در ۹۹.۹۹۹ درصد مواقع

معادل فارسی	اصطلاح انگلیسی	شرح
فعال/غیرفعال	Active/passive	سیستمی که در آن یک مؤلفه افزونه یا سرور، فعال است در حالی که دیگری در دسترس است ولی در حالت Standby است.
	Active/standby	سیستمی که در آن یک مؤلفه افزونه یا سرور، فعال است در حالی که دیگری آماده جایگزین شدن در طی یک تأخیر است. تأخیر جایگزینی این روش کمتر از حالت فعال/غیرفعال است.
	Application failover	فرآیندی که طی آن برنامه کاربردی به علت خرابی سرور اصلی، روی سرور پشتیبان آغاز به کار می‌کند. نه تنها برنامه، بلکه همه دیسکها و آدرس‌های IP اتصال کاربران به سرور جدید مهاجرت می‌کنند.
دسترس‌پذیری	Availability	مدت زمانی که سیستم در دسترس است. معمولا به صورت درصدی از یک سال محاسبه می‌شود. به عنوان مثال ۹۹.۹۵ درصد دسترس‌پذیری معادل ۴.۳۸ ساعت توقف در یک سال است. در مبحث امنیت اطلاعات، دسترس‌پذیری به معنای در دسترس بودن منابع برای کاربران مجاز است.
جایگزینی آبشاری	Cascading failover	قابلیت یک برنامه کاربردی در انتقال به محل دوم در هنگام خرابی، و در صورت خرابی مجدد انتقال به محل بازیافت در یک سایت دیگر.

معادل فارسی	اصطلاح انگلیسی	شرح
رده سرویس	Class of service	مکانیزمی برای کنترل ترافیک در شبکه با مشخص کردن اولویت پیام یا بسته
متقاضی سرویس (مشتری)	Client	بخش کارخواه (درخواست کننده خدمت) در معماری کارخواه/کارساز. یک کارخواه معمولاً برنامه‌ای است که روی یک PC اجرا می‌شود و برای انجام کارهای خود به یک کارساز (سرور) متکی است.
کلاستر	Cluster	گروهی از سیستمها که با یکدیگر به عنوان یک سیستم واحد به منظور ارائه سرویس سریع و بی‌وقفه کار می‌کنند. یک کلاستر به اندازه کافی نرم‌افزار و سخت‌افزار افزونه دارد که یک خرابی نتواند در سرویس‌دهی آن تأثیر گذارد.
کلاستر قاره‌ای	Continental cluster	گروهی از کلاسترها که از یک شبکه ارتباطی برای افزونگی داده و ارتباط، به منظور تحمل خرابی کلاسترهای مختلف (معمولا از مراکز داده‌ای مختلف) استفاده می‌کنند. کلاسترهای قاره‌ای اغلب در شهرها یا کشورهای مختلف پراکنده‌اند و ممکن است هزاران کیلومتر با یکدیگر فاصله داشته باشند.
کنترلر	Controller	ابزاری برای کنترل انتقال داده از کامپیوتر به ابزارهای جانبی و بالعکس.

معادل فارسی	اصطلاح انگلیسی	شرح
افزونگی داده	Data replication	روشی برای تحمل خرابی که در آن داده از یک سایت به سایت دیگر کپی می‌شود.
ناحیه غیرنظامی	Demilitarized zone (DMZ)	ناحیه‌ای از شبکه بین شبکهٔ داخلی و شبکه بیرونی، که حفاظت کمتری نسبت به شبکه داخلی از آن می‌شود و معمولا سرورهای با دسترسی از بیرون در آن ناحیه قرار داده می‌شوند.
تقسیم بار پویا	Dynamic load sharing	توانایی توزیع خودکار ترافیک بین چند مسیر.
فایروال، حفاظ	Firewall	ابزار (تلفیقی از نرم‌افزار و سخت‌افزار) یا نرم‌افزار برای کنترل و پالایش ترافیک در حال گذر بین شبکه داخلی و خارجی.
شبکه ضربانی	Heartbeat network	شبکه‌ای که ارتباط مطمئن بین دو کلاستر فراهم می‌کند. این ارتباط برای تبادل پیامهای ضربانی و سیگنالها به کار می‌رود.
سیستم تهویه و گرمایش	Heating, ventilation, and air-conditioning (HVAC)	این عبارت معمولاً برای سیستم تهویه هوای مرکز داده به کار می‌رود.
	Hot swap	تعویض یک مؤلفه سخت‌افزاری بدون خاموش کردن سیستم.
پشتیبان‌گیری بدون شبکه	LAN-free backup	روشی در تهیه نسخه پشتیبان که در آن یک سیستم SAN عملیات واقعی I/O پشتیبان‌گیری را انجام می‌دهد و دیگر نیازی

معادل فارسی	اصطلاح انگلیسی	شرح
		به انتقال داده پشتیبان از ابزارهای شبکه نیست.
تقسیم بار	Load sharing	تقسیم بار I/O یا کار بین چند مؤلفه زیر سیستم.
کلاستر محلی	Local cluster	کلاستری که تنها در یک مرکز داده واقع شده است. این نوع کلاستر قابلیت تحمل حادثه را ندارد.
جایگزینی دستی	Manual failover	نوعی از Failover که نیاز به مداخله انسان برای آغاز یک برنامه یا سرویس در یک گره دیگر دارد.
میانگین زمان بین خرابی‌ها	Mean time between failures (MTBF)	میانگین زمان بین دو خرابی متوالی که روی تعداد زیادی از خرابی‌ها محاسبه شده باشد.
میانگین زمان تا خرابی	Mean time to failure (MTTF)	میانگین زمان از ابتدای شروع به کار سیستم تا اولین خرابی که با استفاده از تعداد زیادی سیستم مشابه محاسبه شده باشد.
میانگین زمان تعمیر	Mean time to repair (MTTR)	میانگین زمان تعمیر یک مولفه یا یک سیستم که با استفاده از زمان تعداد زیادی از تعمیرات محاسبه شده باشد.
کلاستر شهری	Metropolitan cluster	کلاستری که در گستره یک شهر پراکنده است.
	Network attached storage (NAS)	دستگاه‌های ذخیره‌سازی مبتنی بر فایل که به شبکه IP متصل بوده و سرویسهای اشتراک داده تحت بسترهای مختلف ارائه می‌کند. از پروتکلهای مختلفی مانند CIFS، NFS و HTTP استفاده

معادل فارسی	اصطلاح انگلیسی	شرح
		می کند.
	Plenum	از واژه لاتین *plenum* گرفته شده است و به ناحیه‌ای در مرکز داده گفته می‌شود که برای انتقال هوای خنک‌کننده به رک‌ها مورد استفاده قرار می‌گیرد (مانند فضای بین کف و کف کاذب)
نقطه توزیع	Point of distribution (POD)	یک رک که حاوی سوییچها، سرورهای ترمینال، و درگاههای اتصال کابلها است.
واحدهای توزیع برق	Power distribution units (PDUs)	high- An electrical distribution box fed by a amp three-phase connector with power outlets .and circuit breakers
سرور واقعی	Real server	سرور فیزیکی که پشت سر سرور مجازی سرویس‌دهنده به کاربر قرار دارد.
	Remote failover	Failover روی یک گره دیگر در یک مرکز داده دیگر یا محل دور.
مقیاس‌پذیری، گسترش‌پذیری	Scalability	قابلیت سیستم برای افزایش اندازه، ارتباط و کارایی.
تک نقطه شکست	Single point of failure (SPOF)	مؤلفه‌ای از کلاستر یا گره که در صورت خرابی دسترسی به برنامه‌های کاربردی و سرویس‌ها قطع می‌شود.
	Split-brain	هنگامی اتفاق می‌افتد که اتصال ضربانی (heartbeat link)

معادل فارسی	اصطلاح انگلیسی	شرح
	syndrome	قطع شده و باعث می‌شود که کلاستر به دو گروه سرورها تقسیم شده و هر گروه خود را مستقل و معتبر پنداشته و برنامه‌های مشابهی را بالا می‌آورند. که منجر به تغییر داده‌های مشابه شده که خرابی داده را باعث می‌شود.
آماده به‌کار	Standby	نقش مؤلفه افزونه که مؤلفه دیگر فعال را تحت نظارت داشته و آماده جایگزین شدن آن در صورت خرابی آن است.
شبکه حافظه	Storage area network (SAN)	یک زیرساخت پرسرعت، مقیاس‌پذیر، مختص سرورهای ذخیره‌ساز و برای انتقال سطح بلوکی بین تمام دستگاه‌ها.
جایگزینی شفاف	Transparent failover	برنامه کارخواه که در صورت خرابی سرور به صورت خودکار و بدون درگیری کاربر به سرور دیگری متصل می‌شود.
جایگزینی شفاف IP	Transparent IP failover	انتقال آدرس IP از دستگاه خراب به دستگاه سالم دیگر در همان زیرشبکه برای ادامه سرویس‌دهی به کاربران از همان نام و آدرس
سرور مجازی	Virtual server	یک کارساز مجازی روی توزیع کننده بار که تنها یک آدرس IP، پروتکل، و درگاه به کارخواهان برای یک سرویس خاص ارائه می‌کند. در عمل کارساز مجازی تنها سرویسها را به کارسازهای واقعی مسیردهی می‌کند.