نظام فنی و اجرایی
پدافند غیرعامل

سازمان پدافند غیرعامل کشور
معاونت طرح ریزی و نظارت فنی

الزامات و ملاحظات پدافند غیرعامل مراکز داده

ویرایش اول: مهرماه ۱۳۹۹
شماره : ۱۲۰۱-ث

به نام خدا

نظامات فنی و مهندسی پدافند غیرعامل ایران

الزامات و ملاحظات پدافند غیرعامل مراکز داده (سایبری، الکترومغناطیس، کالبدی)

شماره: ۱۲۰۱-ث

ویرایش اول- مهرماه ۱۳۹۹

الزامات و ملاحظات
پدافند غیرعامل مراکز داده
(سایبری، الکترومغناطیس، کالبدی)

سازمان پدافند غیرعامل(قرارگاه پدافند کالبدی، معاونت طرح ریزی و نظارت فنی، قرارگاه پدافند سایبری، قرارگاه پدافند الکترونیک)

اعضای کمیته تخصصی

شماره: ۱۲۰۱-ث- مهرماه ۱۳۹۹

- دکتر غلامرضا جلالی
- دکتر علی اصغر زارعی
- مهندس مجتبی حائری
- مهندس مسعود مینوئیان
- مهندس محمدباقر ایزدی
- مهندس علیرضا خردمندیان
- مهندس هادی کریمی نیسیانی
- دکتر ذبیح ا... حسن شاهی
- مهندس مریم السادات خاتمی
- مهندس امیرحسین فتحی

عنوان و نام پدیدآور	:	الزامات و ملاحظات پدافند غیرعامل مراکز داده (سایبری، الکترومغناطیس، کالبدی)/ تدوین مجتبی حایری ... [و دیگران]؛ [برای] سازمان پدافند غیر عامل کشور، معاونت طرح‌ریزی و نظارت فنی ... [و دیگران].
مشخصات نشر	:	تهران: نیلوفران، ۱۳۹۹.
مشخصات ظاهری	:	۶۰ ص.: جدول.
شابک	:	978-600-7935-53-8
وضعیت فهرست نویسی	:	فیپا
یادداشت	:	تدوین مجتبی حایری، محمدباقر ایزدی، مسعود مینوییان، هادی کریمی‌نیسیانی.
یادداشت	:	عنوان دیگر: الزامات و ملاحظات پدافند غیرعامل مراکز داده شماره ۱۲۰۱ - ث.
عنوان دیگر	:	الزامات و ملاحظات پدافند غیرعامل مراکز داده شماره ۱۲۰۱ - ث.
موضوع	:	سازمان پدافند غیر عامل کشور -- قوانین و رویه‌ها
موضوع	:	دفاع غیر نظامی
موضوع	:	Civil defense
شناسه افزوده	:	حائری، مجتبی ۱۳۳۴ ، گردآورنده
شناسه افزوده	:	سازمان پدافند غیر عامل کشور. معاونت طرح‌ریزی و نظارت فنی
رده بندی کنگره	:	UA۹۲۶
رده بندی دیویی	:	۳۶۳/۳۵
شماره کتابشناسی ملی	:	۷۳۲۴۱۹۶

سازمان پدافند غیرعامل کشور
معاونت طرح ریزی و نظارت فنی

نام کتاب: الزامات و ملاحظات پدافند غیرعامل مراکز داده- شماره: ۱۲۰۱-ث
تدوین: مهندس مجتبی حائری، مهندس محمدباقر ایزدی، مهندس مسعود مینوئیان، مهندس علیرضا خردمندیان، مهندس هادی کریمی نیسیانی
صفحه آرا: زهرا سالمی نژاد
شمارگان: ۲۰۰ نسخه
انتشارات: نیلوفران
نوبت چاپ: اول، مهرماه ۱۳۹۹
شابک: ۹۷۸-۶۰۰-۷۹۳۵-۵۳-۸

از اندیشمندان و متخصصین محترم تقاضا می‌شود جهت بارورتر شدن و غنای علمی این سند نظرات و پیشنهادات خود را از طریق مراجعه به آدرس اینترنتی www.paydarymelli.ir و تکمیل فرم نظرخواهی نظامات فنی و مهندسی پدافند غیرعامل به نشانی پست الکترونیکی pdrcet51@gmail.com ارسال نمایند و یا به شماره ۰۲۱-۲۵۹۳۵۲۴۶ فکس نمایند.

فهرست

پیشگفتار

امروزه می توان با به کارگیری اقدامات مؤثر، کاربردی فنی و مهندسی و حتی الامکان کم هزینه و چند منظوره در مرحله قبل از بحران، میزان زیادی از شدت و گستردگی خسارات و تلفات ناشی از خطرات (نظامی و غیر نظامی- طبیعی) کاست. از مهم ترین این اقدامات، استفاده از اصول پدافند غیرعامل به عنوان راه حلی جهت کاهش آسیب پذیری در برابر خطرات مختلف با افزایش کارایی هنگام روبرو شدن با مخاطرات است.

الزامات و ملاحظات فنی و مهندسی پدافند غیرعامل مجموعه ای از ضوابط فنی، اجرایی و حقوقی لازم الاجرا در طراحی، نظارت و اجرای تأسیسات، زیربناها و ساختمان های کشور است که باعث افزایش بازدارندگی، کاهش آسیب پذیری، ارتقا پایداری ملی، تداوم فعالیت های ضروری و تسهیل مدیریت بحران در برابر تهدیدات و اقدامات نظامی دشمن و حفظ جان و مال انسان در برابر حوادث می شود.

آنچه الزامات و ملاحظات پدافند غیرعامل مراکز داده(سایبری، الکترومغناطیس و کالبدی) را از سایر ضوابط و مقررات فنی و مهندسی متمایز می سازد، الزامی بودن، اختصاری بودن و سازگار بودن آن با شرایط کشور از حیث نیروی انسانی، امکانات، توان اقتصادی، اقلیمی و محیطی است تا از این طریق نیل به اهداف پدافند غیرعامل ممکن شود.

در حقیقت این الزامات و ملاحظات مجموعه ای از حداقل های مورد نیاز و باید ها و نباید های فنی و مهندسی در حوزه پدافند غیرعامل است که با توجه به شرایط فنی و اجرائی و توان مهندسی کشور و با بهره گیری از آخرین دستاوردهای روز ملّی و بین المللی و برای آحاد جامعه کشور، تهیه و تدوین شده است.

بدین وسیله از تلاش ها و زحمات همه کسانی که به نحوی در تدوین این مجلد همکاری نموده اند، سپاسگزاری می نمایم.

رییس سازمان پدافند غیرعامل کشور

سرتیپ پاسدار غلامرضا جلالی

فصل اول

کلیات

مقدمه

فناوری‌های اطلاعاتی و ارتباطی در همه عرصه‌های اجتماعی تأثیرگذار بوده و زمینه‌ساز جهش جامعه به سوی پدیده دانش‌بنیان شدن می باشد. امروزه شاخص بهره‌گیری از فناوری‌های اطلاعاتی و ارتباطی در جهان به‌عنوان یکی از اساسی ترین شاخص‌های توسعه‌یافتگی مطرح است. بهره‌گیری از این فناوری‌ها، کلیه فرآیندها و فعالیت‌های اقتصادی، فرهنگی، صنعتی، سیاسی و روابط اجتماعی جوامع را تحت تأثیر تغییراتی اساسی و پایه‌ای خود قرار داده و از مهم‌ترین زیرساخت‌ها در جوامع دانایی محور، زیرساخت‌های ارتباطی و اطلاعاتی می‌باشند.

در این راستا جمهوری اسلامی ایران در همه سطوح در حال سیر مراحل الکترونیکی شدن می باشد. به همان نسبت که زیرساخت های جامعه الکترونیکی می‌شود، انگیزه گروه‌های ساختاریافته و غیر ساختاریافته برای اختلال، تخریب، دسترسی و دستیابی غیر مجاز به اطلاعات در همه سطوح افزایش می‌یابد. امروزه یکی از مقوله‌های مورد نظر برای موفقیت در صحنه نبرد، انجام اقدامات علیه زیرساخت‌های اطلاعاتی و ارتباطی طرف مقابل است به گونه ای که اکثر ارتش‌ها برای این کار، اقدام به ایجاد یگان‌های سایبری نموده‌اند. توسعه کمی و کیفی منابع تولید اطلاعات، محققین را به توسعه فناوری‌های نگهداری و مدیریت اطلاعات

وا داشته به صورتی که هر روزه شاهد توسعه کمی و کیفی تکنیک‌ها و تاکتیک‌های ذخیره‌سازی، نگهداری و مدیریت داده‌ها و اطلاعات می‌باشیم.

مراکز داده یکی از مهم‌ترین بخش‌های زیرساخت اطلاعاتی محسوب می‌شود که علاوه بر نگهداری از اطلاعات، پشتیبانی از سرویس‌ها را نیز بر عهده دارند؛ بنابراین ضروری است در کنار کارآمدی مراکز داده به مقوله مقابله مؤثر با تهدیدات فیزیکی، سایبری، امنیتی، ترکیبی و حصول اطمینان از عملکرد صحیح آنها و آسیب ناپذیر بودن در هر شرایطی اعم از بحران و جنگ و نفوذ سایبری و ... توجه لازم بشود.

مراکز داده علاوه بر ابنیه و تجهیزات مراقبت و کنترل، دارای زیرساخت ارتباطی و ذخیره‌سازی داده‌ها می‌باشند؛ لذا به جهت کاهش آسیب پذیری و امکان ارائه خدمات و برای مصون بودن از اختلال و سرقت اطلاعات، رعایت الزامات و ملاحظات در سه بخش سایبری، الکترومغناطیس و کالبدی و شرح آنچه در ادامه خواهد آمد، ضروری است. مراکز داده متناسب با ضریب اهمیت داده‌های آنها و همچنین سرویس‌هایی که از آنها اطلاعات دریافت و پس از پردازش به مبادی ذیربط، اطلاعات پردازش شده را ارائه می‌دهند، از لحاظ سطح بندی حفاظتی به سه دسته؛ مهم، حساس و حیاتی تقسیم می‌گردند.

در فصل اول این سند به کلیات و تعاریف پرداخته شده و در فصل دوم به الزامات پدافند سایبری مراکز داده مشتمل بر؛ الزامات سازمانی و مدیریتی، طراحی و معماری شبکه و امنیت شبکه، قرارداد با کارگزاران بیرونی، گواهی نامه ها، مستندات، برچسب گذاری و راهنمای شناسایی، نرم افزار، ضد بدافزار، سیستم عامل، ارتباطات، تجهیزات سخت افزاری، کارایی، مقیاس پذیری، فناوری های نوین مورد استفاده، پشتیبان گیری، بازیابی و امحاء اطلاعات، ورود و خروج رایانه همراه و اقلام ذخیره ساز، کابل، نیروی انسانی و آموزش، برونسپاری، تعمیر و پشتیبانی پرداخته می شود. فصل سوم اختصاص به موضوع حفاظت الکترومغناطیس مراکز داده شامل چهار بخش؛ قرارداد کارگزاران، شیلدینگ، فیلترینگ و ارتینگ دارد و فصل چهارم الزامات و ملاحظات پدافند کالبدی که در برگیرنده الزامات و ملاحظات مربوط به بخش های؛ مکان یابی، طراحی محوطه، معماری، سازه، تاسیسات برقی و مکانیکی و حفاظت فیزیکی می شود.

۱-۱ هدف

هدف اصلی این سند ارائه الزامات و ملاحظات پدافند غیرعامل مراکز داده در حوزه‌های سایبری، الکترونیک (الکترومغناطیس) و کالبدی می‌باشد.

۱-۲ اهداف فرعی

- پیاده‌سازی نظام یکپارچه جهت تعیین سطح اهمیت و کاهش آسیب پذیری، افزایش تاب آوری و پایداری در مراکز داده و مصونیت در قبال حملات سایبری و سرقت اطلاعات و ... متناسب با سطح اهمیت مرکز داده است.
- نهادینه کردن الزامات و ملاحظات پدافند غیرعامل در طراحی و ساخت مراکز داده جدید
- کاهش آسیب پذیری مراکز داده موجود
- ترویج پراکنده‌سازی و ایجاد مراکز پشتیبان برای مراکز داده حیاتی، حساس و مهم به منظور تقلیل سطح اهمیت آنها، کاهش جذابیت برای دشمن و تبعات اختلال در آنها

۱-۳ دامنه کاربرد

- مراکز داده حیاتی، حساس و مهم اعم از موجود (در حال بهره‌برداری) و جدید (در دست مطالعه، طراحی و اجرا) می‌باشد.

۱-۴ گروه بندی مراکز داده

مراکز داده به لحاظ موقعیت قرارگیری در یک فضا، می‌توانند حالات مختلفی داشته باشند که در دسته‌های زیر گروه بندی می‌شوند:

گروه ۱- اتاق و یا اتاق‌های مرکز داده: مرکز داده‌ای که در یک و یا چند اتاق از یک طبقه ساختمان و یا یک ساختمان، به صورت مجزا استقرار دارد و مراکز اسناد، رایانه‌ها و داده‌های اطلاعاتی به صورت متمرکز در آن اتاق یا اتاق‌ها قرار دارند.

گروه ۲- مرکز داده مستقر در طبقه یک ساختمان: مرکز داده‌ای که در یک یا چند طبقه (طبقات همکف، بالایی و یا زیرزمین) از یک ساختمان استقرار دارد و تمامی مراکز اسناد، رایانه‌ها و داده‌های اطلاعاتی به صورت متمرکز درهمان یک طبقه یا چند طبقه همان ساختمان قرار دارند.

گروه ۳- ساختمان مرکز داده: اختصاص یک ساختمان مستقل به مرکز داده، این ساختمان ممکن است شامل یک یاچند طبقه و یا چند اتاق باشد و تمامی مراکز اسناد، رایانه ها و داده های اطلاعاتی به صورت متمرکز در این ساختمان قرار دارند.

گروه ۴- مجموعه (سایت)مراکز داده: مرکز داده ای که شامل چند ساختمان در یک سایت و یا بخش مستقلی از یک سایت قرار دارد و تمامی مراکز اسناد، رایانه ها و داده های اطلاعاتی در ساختمان های این سایت استقرار دارند.

۵-۱ تعاریف و اصطلاحات

۱-۵-۱ مرکز داده حیاتی: مرکز داده‌ای است که داده‌های موجود در آن در سطح ملی بوده و در صورت تحمیل خسارت، تبعات جبران ناپذیری در سطح ملی ایجاد می شود.

۲-۵-۱ مرکز داده حساس: مرکز داده‌ای است که داده‌های موجود در آن در سطح منطقه ای (چند استانی) بوده و در صورت خسارت دیدن تبعات جبران ناپذیری در سطح منطقه ای ایجاد می شود.

۳-۵-۱ مرکز داده مهم: مرکز داده‌ای است که داده‌های موجود در آن در سطح استانی بوده و یا استفاده کنندگان آن در سطح یک استان پراکنده می‌باشند و در صورت خسارت دیدن تبعات جبران ناپذیری در سطح یک استان ایجاد می شود.

۴-۵-۱ پدافند سایبری: مجموعه‌ای از اقدامات دفاعی عامل و فعّال، برای شکست‌دادن تهدیدهای سایبری است که به نقض یا تهدید به نقض معیارهای امنیتی فضای سایبری کشور نموده‌اند. این مجموعه، شامل اقداماتی برای تشخیص، توصیف، دفاع در مقابل تهدید، کاهش تهدید و نهایتاً بازگرداندن فضای سایبر به پیکربندی امن است. آن بخش از اقدامات پدافند سایبری که در مواجهه با «تهدید به نقض معیارهای امنیتی» انجام می‌شوند، جنبه‌ی محافظتی (پدافندی غیرفعال) و پیشگیرانه دارند که قبل از وقوع جنگ سایبری توسط دشمن انجام می گیرند و بخش دیگر اقدام‌های پدافند سایبری که در مواجهه با «اقدام به نقض معیارهای امنیتی» انجام می‌شوند و جنبه‌ی پدافندی فعال در مواجهه با جنگ سایبری دارند. بخشی از اقدام‌های پدافندی در داخل فضای سایبر خودی و بخش دیگری از آن‌ها در داخل فضای سایبر دشمن انجام خواهند شد.

۵-۵-۱ مصونیت سایبری (Cyber Inviolability): عالی‌ترین سطح از امنیت سایبری است که حاصل طی‌شدن چرخه‌ی تعالی برای امنیت سایبری می باشد. مصونیّت سایبری، نتیجه‌ی محافظت از فضای سایبر یا قابلیت‌های سایبری محسوب می‌شود. ضمنا دست‌یابی به بازدارندگی پدافندی، صرفاً با تحقق دو ویژگی مصونیت و تاب‌آوری، امکان‌پذیر است.

۱-۵-۶ تاب‌آوری (انعطاف پذیری) سایبری (Cyber Resilience): تاب‌آوری، توانایی تداوم یا بازگشت به عملیات عادی در صورت وقوع برخی از اختلال‌ها، اعم از طبیعی یا انسانی، و عمدی یا غیرعمدی است. هدف پدافند سایبری، این است که در مواجهه با هرگونه شکست (اعم از جاسوسی یا حمله)، تاب‌آوری لازم برای اجرای ماموریت را داشته باشد. بر این اساس، فرماندهان باید طرح‌های ماموریت جایگزین، فرآیندهای اضطراری، و تقویت و گزینه‌های جایگزین را توسعه دهند و به‌طور مشابه، برای تاب‌آوری سامانه‌های سایبری، برنامه‌های سامانه جایگزین، فرآیندهای اضطراری پشتیبان‌گیری و گزینه‌های پیکربندی جایگزین/ را راه‌اندازی مجدد نمایند.

۱-۵-۷ تهدید سایبری (Cyber threat): عاملی خوف‌ناک است که می‌تواند از طریق برقراری ارتباط یا احساس، از یک آسیب‌پذیری سایبری، بهره‌برداری کند. انواع تهدید سایبری که نظام پدافند سایبری با آن مواجه اند عبارتند از: تهدید ناشی از دولت یک کشور، سازمان‌های غیردولتی (اعم از رسمی و غیررسمی، مشروع و غیرمشروع)، گروه‌های کوچک و افراد حقیقی.

۱-۵-۸ حمله (تهاجم) سایبری (Cyber Attack): استفاده‌ی تهاجمی از سلاح سایبری است که با هدف آسیب‌رساندن به یک هدف مشخص انجام شده باشد. به مفهوم روشن تر حمله سایبری، ترکیبی از اقدامات بهره‌برداری از آسیب‌پذیری و سایر قابلیت‌های توانمندساز است که با هدف ممانعت یا دستکاری اطلاعات و یا زیرساخت انجام شود.

۱-۵-۹ آسیب‌پذیری سایبری (Cyber Vulnerability): به ویژگی (نقص یا ضعف) یک موجودیت سایبری اطلاق می‌شود که در طراحی، پیاده‌سازی، یا عملیات و مدیریت آن موجودیت ایجاد و مستعد بهره‌برداری است و می‌تواند مورد سوءاستفاده قرار گرفته و منجر به نقض اهداف یا خط‌مشی پدافند سایبری شود.

۱-۵-۱۰ پدافند الکترومغناطیس:یا حفاظت جامع الکترومغناطیس، مجموعه اقداماتی است که در برابر هرگونه تهدیدات توان بالای الکترومغناطیسی علیه تجهیزات الکترونیکی انجام می شود. حفاظت جامع الکترومغناطیس شامل شیلدینگ، فیلترینگ و ارتینگ می باشد.

۱-۵-۱۱ پدافند کالبدی: به مجموعه اقدامات فنی و مهندسی که به منظور ارتقاء پایداری، کاهش آسیب پذیری و تداوم خدمات ضروری دارایی های فیزیکی مراکز ثقل کشور انجام می شود، اطلاق می گردد.

۱-۶ ضوابط

به منظور کاربردی نمودن الزامات و ملاحظات تدوین شده، توجه به موارد زیر ضروری است:
الزام: باید و نبایدهائی که رعایت آنها برای به ثمر رسیدن نتایج مطلوب امری ضروری است.

ملاحظه: توصیه ای که رعایت آن باعث اثربخش تر شدن در رسیدن به هدف می باشد.

-اولین اقدام برای کاربرد الزامات و ملاحظات مراکز داده، تعیین سطح اهمیت مرکز مورد نظر است که به پیشنهاد دستگاه اجرایی ذیربط و تایید سازمان پدافند غیرعامل انجام می شود.

-رعایت الزامات ضروری و مورد تاکید است و در ارزیابی و نظارت مورد مطالبه قرار می گیرد. ملاحظات بصورت توصیه بوده و می توانند در صورت امکان مورد استفاده قرار گیرند. در جدول شماره۱-۱ علائم استفاده شده به منظور شناسایی الزام و ملاحظه آورده شده است.

جدول شماره ۱-۱ علائم مربوط به الزامات و ملاحظات

نوع الزام/ملاحظه	علائم
الزام	❊
ملاحظه	○
عدم انطباق با سطح اهمیت مرکز	—

فصل دوم

الزامات و ملاحظات پدافند سایبری

مقدمه

زندگی بشر از عصر تولید انبوه به عصر ارتباطات نامحدود و مدیریت اطلاعات و دانش ارتقاء یافته است به گونه‌ای که چارچوب ساختاری تشکیل دهنده این عصر را عناصری چون تولید، پردازش، انتقال و مدیریت اطلاعات و ارتباطات تشکیل می دهند و لذا درآغاز قرن جدید نیازمندی های زندگی بشر، (بانک ها، موسسات تجاری، سیستم های مخابراتی و...) به الکترونیک و مدارات الکترونیکی وابستگی خاصی پیدا کرده اند. در پی این وابستگی، تهاجم به مدارات الکترونیکی نیز در برنامه های نظامی و استراتژیک کشورهای مهاجم قرار گرفته است. با گسترش و افزایش حجم اطلاعات و حرکت به سمت فناوری اطلاعات و سیستم های الکترونیکی به جرات می توان گفت که یکی از مهم‌ترین مؤلفه های زیرساخت های ارتباطی کشور مراکز داده است که این مراکز به عنوان قلب تپنده اطلاعات و ارتباطات محسوب می گردند. مراکز داده به دلیل وجود تجهیزات الکترونیکی و رایانه‌ای ارزشمند و فرآیندهای اطلاعاتی پیچیده و حجیم انجام امور اجرایی، اقتصادی، اجتماعی و خدمات عمومی در سطوح ملی، منطقه‌ای و محلی دارای درجه اهمیت فراوانی خواهند بود که متناسب با سطح تأثیر گذاری بایستی، امنیت و پشتیبانی از آنها مورد توجه قرار گیرد. از اینرو رعایت الزامات و ملاحظات حوزه سایبری حائز اهمیت بوده که در این فصل الزامات و ملاحظاتی که از منظر پدافند سایبری باید رعایت شوند، ارائه شده است.

	۲-۱ الزامات سازمانی و مدیریتی	سطح بندی مراکز داده		
		حیاتی	حساس	مهم
۱	مجری، مشاور، پیمانکاران و کارکنان مرکز داده در مراحل مختلف اعم از طراحی، نصب و پیاده سازی، راه اندازی، توسعه، ارائه خدمات و ... در مرکز داده همواره سیاست ها، نظرات، الزامات و ملاحظات ابلاغی سازمان پدافند غیرعامل را رعایت نموده و نسبت به اجرای آنها مداومت داشته و تبعیت کامل نمایند.	*	*	*
۲	سازوکارهای مدیریت تداوم کسب و کارها و خدمات ضروری در شرایط اضطراری در شبکه (BCP[1]) ابلاغ و نظارت مستمر بر روند عملیاتی شدن آن اجرا گردد.	*	*	*
۳	سازوکارهای تاب آوری[2] و انعطاف پذیری شبکه در زمان بحران تدوین گردد و نظارت مستمر بر روند عملیاتی شدن آن اعمال گردد.	*	*	*
۴	سازوکارهای بازیابی از فاجعه در شرایط اضطراری در شبکه(DRP[3]) ابلاغ و نظارت مستمر بر روند عملیاتی شدن آن انجام پذیرد.	*	*	*
۵	فرایندهای کاری دقیق و قابل اجرا، برای قبل، در آستانه، حین و بعد از رخدادهای سایبری بصورت کارا تعریف و اجرایی شود. ضمنا در هر شرایط، باید فرمانده عملیات مشخص باشد.	*	*	*
۶	بر صیانت از دارایی ها و سرویس های اولویت دار (بر اساس اصل جذابیت هدف برای دشمن) تمرکز گردد.	*	*	*
۷	مرکز داده جهت اجرای مطلوب سند، نسبت به برگزاری کارگاه های آموزشی برای کارکنان خود اقدام نمایند.	*	*	*

1-Business Continuity Plan 2-Resiliency 3-Disaster Recovery Plan

	۱-۲ الزامات سازمانی و مدیریتی	سطح بندی مراکز داده		
		حیاتی	حساس	مهم
۸	مرکز داده جهت ارزیابی و ارتقای آمادگی ها، نسبت به برگزاری رزمایش‌ها و تمرین های سایبری با همکاری و هماهنگی کامل با سازمان پدافندغیرعامل اقدام نماید.	*	*	*
۹	در مرکز داده کمیته مدیریت امنیت و پدافند سایبری تشکیل شود.	*	*	*
۱۰	در مرکز داده تیم عملیات سایبری تشکیل گردد.	*	*	*
۱۱	کارکنان در بدو بکارگیری می‌بایست در کارگاه آموزشی با عنوان «الزامات و ملاحظات پدافند غیر عامل در مرکز داده» که توسط کمیته پدافند غیر عامل مرکز داده برگزار می‌شود، شرکت و نمره قبولی کسب نمایند.	*	*	*

	۲-۲ الزامات و ملاحظات طراحی و معماری شبکه و امنیت شبکه	سطح بندی مراکز داده		
		حیاتی	حساس	مهم
۱	در شبکه و بستر ارتباطی مرکز داده باید از متدولوژی دفاع در عمق و دفاع لایه به لایه بهره گیری شود. در این متدولوژی، در عمق فضای سایبر، در هشت لایه، شامل لایه‌های «شبکه»، «ارتباطات (خطوط ارتباطی)»، «سامانه اطلاعاتی»، «سیستم‌عامل»، «کاربرد»، «تجهیزات انتهایی»، «محتوا (داده)» و «دسترسی فیزیکی» به مورد اجرا گذاشته می‌شود. در این متدولوژی، نیروی انسانی، فرایندهای کاری و سیاست های سازمان نیز دخیل می باشند.	*	*	*
۲	در تمام سطح شبکه، باید از معماری شبکه و معماری امنیتی منطبق بر متدولوژی دفاع در عمق و دفاع لایه به لایه استفاده شود.	*	*	*
۳	کلیه لاگ ها، رخدادها و اطلاعات وضعیتی در شبکه ها، نرم افزارها، بستر ارتباطی و... باید رویدادنگاری و به صورت بلادرنگ به سامانه جمع‌آوری و همبسته سازی رخدادها(SIEM) در مرکز مانیتورینگ متمرکز (SOC) ارسال شوند.	*	*	*

۲-۲ الزامات و ملاحظات طراحی و معماری شبکه و امنیت شبکه		سطح بندی مراکز داده		
		حیاتی	حساس	مهم
۴	استفاده از SIEM بومی و مورد تایید سازمان پدافندغیرعامل کشور الزامی است.	*	*	*
۵	سازوکار لازم برای ایجاد و عملیاتی نمودن آگاهی وضعیتی[1]، در شبکه اجرا شود.	*	*	*
۶	تمامی لاگها، رخدادها، هشدارها و ... در سطوح مختلف اعم از کاربری، هسته، تجهیزات، ارتباطات و ... با رعایت اصول پدافندی مانند Signing، Time Stamp، Indexing و ... در پایگاه داده مناسب ذخیره گردد. بدیهی است یکی از کارکردهای این پایگاه داده، مکانیزم کشف منشا حملات [2] است.	* ۱۲ ماه	* ۶ ماه	* ۶ماه
۷	امکان جمع آوری اطلاعات فارنزیک در مرکز داده به نحوی که از این اطلاعات بتوان در تشخیص تخلفات احتمالی بهره جست، وجود داشته باشد.	*	*	*
۸	جهت رصد و پایش ملی، مرکز داده امکان اتصال سنسورهای مورد نیاز به مرکز رصد و پایش سازمان پدافند غیرعامل را فراهم نماید.	*	*	*
۹	مرکز داده باید برای شناسایی، هشدار و مراقبت از شبکه در مقابل تهدیدات نوین مانند Zero Dayها، APT[3]ها، AET[4]ها و Botnetها سازوکار علمی، فنی و مدیریتی را تدوین و اجرا نماید.	*	*	*
۱۰	مرکز داده بنابر الزامات و ملاحظات سازمان پدافند غیر عامل، نسبت به تشکیل و راه اندازی تیم مقابله با حملات سایبری (CSIRT)[5]، اقدام نماید. این تیم با مرکز ماهر وزارت ارتباطات و قرارگاه پدافند سایبری کشور در تعامل مستمر باشد.	*	*	*
۱۱	اجرا و پیاده سازی سازوکار جامع و یکپارچه رصد، پایش، تشخیص، هشدار و امداد رایانه‌ای بصورت ۲۴*۷ الزامی است.	*	*	○
۱۲	نیروی انسانی مستقر در مرکز عملیات امنیت باید در ۳ دسته (پایشگر، تجزیه و تحلیل گر و متخصص امنیت سایبری) سازماندهی شوند.	*	*	○

1-Situational Awareness
2-Forensic
3-Advanced Persistent Threat
4-Advanced Evasion Technique
5-Computer Security Incident Response Team

	۲-۲ الزامات و ملاحظات طراحی و معماری شبکه و امنیت شبکه	سطح بندی مراکز داده		
		حیاتی	حساس	مهم
۱۳	فرآیندهای کاری بین تیم‌های SOC، NOC و CSIRT تدوین و اجرایی گردد.	*	*	*
۱۴	بازرسی‌های اضطراری از قبل پیش بینی نشده و درصورت نیاز بازنگری معماری امنیتی و پدافندی تمام شبکه و در تمام سطوح اعم از سطح کاربری، سطح هسته شبکه، سطح ارتباطات بر اساس معماری امن و لایه به لایه صورت پذیرد.	*	*	*
۱۵	در تمام سطوح طراحی، نصب و پیاده سازی، راه اندازی، توسعه، ارائه خدمات و ... از نرم افزارها، توانمندی ها و فناوری های بومی و امن داخلی بهره جویی شود	*	*	○
۱۶	مرکز داده نسبت به شناسایی گلوگاه‌ها (SPOF[1])، در تمام سطوح فنی، مدیریتی، فرآیندی و پشتیبانی اقدام نماید و برای رفع آنها، تدابیر لازم را اتخاذ نماید.	*	*	○
۱۷	وضعیت باز و بسته شدن درب ها و رک های دربردارنده سرورهای حیاتی باید لاگ شود و این لاگ برای مرتبط سازی[2] به SIEM منتقل شود.	*	○	○
۱۸	تمام وضعیت عملکردی شبکه(NOC) باید از طریق ایمن (پروتکل Syslog یا SNMP V3) به مرکز عملیات امنیت ارسال و مورد پایش قرار گیرد.	*	*	○
۱۹	بازبینی پیکربندی امن تمام اجزای شبکه بالاخص اجزای حیاتی مانند سوییچ‌ها و روترهای اصلی، تجهیزات امنیتی و... و امن سازی آنها در بازه‌های زمانی یک ماهه و بصورت مستمر مطابق با دستورالعمل های موجود صورت پذیرد و از پیکربندی امن تمام تجهیزات، اطمینان حاصل شود.	*	*	*
۲۰	تجهیزات اساسی دخیل در شبکه باید از مکانیزم احراز هویت مناسب (چندعامله[3]) بهره گیرد.	*	*	*
۲۱	در تمام شبکه باید دقیقا مشخص باشد هر نفر با چه سطح دسترسی به کدام تجهیز در گستره شبکه دسترسی دارد. نگهداری تمام لاگ ها مطابق با اصول نگهداری لاگ ها الزامی است. (این لاگ ها برای مرتبط سازی به مرکز عملیات امنیت سایبری ارسال شود).	*	*	*

1-Single Point of Failure 2-Corrolation 3-Multi Factors

	۲-۲ الزامات و ملاحظات طراحی و معماری شبکه و امنیت شبکه	سطح بندی مراکز داده		
		حیاتی	حساس	مهم
۲۲	سازوکار مناسب و امن جهت تولید، مدیریت و امحای کلیدهای رمزنگاری باید اجرا شود.	*	*	*
۲۳	بهره گیری از تمام زیرساخت‌ها و پهنای باند در اختیار کشور، با اولویت شبکه ملی اطلاعات، برای تداوم خدمت رسانی صورت پذیرد.	*	*	*
۲۴	افزایش تعداد نوبت‌های پشتیبان گیری بلادرنگ از سامانه‌ها و پایگاه داده‌های حیاتی و ذخیره سازی داده‌ها و اطلاعات آنها بصورت Online و Offline به منظور استفاده در سریع ترین زمان ممکن و تست عملیاتی بودن آنها صورت پذیرد.	*	*	○
۲۵	اجرای سازوکارهای مربوط به ثبت لاگ‌های شبکه به منظور تعیین دقیق منشا رخدادهای سایبری با استفاده از تجهیزات و روش‌های مناسب انجام شود.	*	*	○
۲۶	برگزاری تمرینات مدیریت صحنه رخداد سایبری[1] مطابق با متدولوژی شش گامی برای حملات سایبری محتمل و شاخص (مراحل آماده سازی[2] ، شناسایی[3] ، محدودسازی[4] ، پاک سازی[5]، بازیابی[6] و مستند سازی آموخته ها[7])	*	*	*
۲۷	آماده سازی تجهیزات یدک به منظور جایگزینی سریع در شرایط اضطراری (تجهیزاتی که همانند تجهیز اصلی پیکربندی و برنامه ریزی شده اند تا سریعا جایگزین تجهیزات اصلی آسیب دیده شود) صورت پذیرد.	*	○	○
۲۸	برای کاهش حملات منع سرویس توزیع شده(DDOS) در لایه‌های مختلف (دو، سه، چهار و هفت) باید تمهیداتی اندیشیده شود تا با استفاده از سازوکار ابری بومی و امن داخلی، از اختلال در ارائه خدمات جلوگیری نمود.	*	*	*
۲۹	ترافیک غیرعادی ورودی و خروجی شبکه در DMZهای مختلف و بر روی پروتکل های گوناگون رصد گردد	*	*	*

1-Incident Handling
2-Preparation
3-Identification
4-Containment
5-Eradication
6-Recovery
7-Lesson-Learned

	۲-۲ الزامات و ملاحظات طراحی و معماری شبکه و امنیت شبکه	سطح بندی مراکز داده		
		حیاتی	حساس	مهم
۳۰	به منظور افزایش اعتماد به شبکه، سازوکار افزونگی، پشتیبان گیری، در دسترس پذیری[1] و توسعه پذیری[2] را متناسب با ملاحظات امنیتی و پدافندی در سطوح مختلف کارکردی رعایت گردد.	*	*	*
۳۱	مرکز داده باید براساس اهمیت و سطح بندی خدمات و میزان ترافیک محتمل نسبت به تهیه طرح پایدارسازی با استفاده از روش هایی از قبیل توزیع بار[3]، تحمل پذیری خطاء[4] در کلیه تجهیزات را تهیه، ارزیابی و اجراء نماید و با توجه به تغییر بهره برداری از سرویس ها در زمان، آن را بروز نماید.	*	*	○
۳۲	کلیه ارتباطات شبکه بوسیله الگوریتم های رمزنگاری مورد تائید مراجع ذیربط باید رمزنگاری شوند.	*	*	○
۳۳	تمام کلیدهای مورد استفاده، باید بصورت مطمئن در ماژول امنیتی سخت‌افزاری(HSM[5]) بومی و امن نگهداری شود.	*	*	*
۳۴	اقدامات لازم جهت بهره گیری از ساختار بومی و امن PKI[6] برای مرکز داده، انجام گیرد.	*	○	○
۳۵	تمهیداتی برای استفاده از راهکار جزیره ای سازی شبکه[7] برای مقابله و کاهش اثرات حملات سایبری، اندیشیده و تمرین شود.	*	*	○
۳۶	برای ارتباطات بین مراکز داده و هم چنین ارسال اطلاعات از الگوریتم های رمزنگاری مناسب مورد تایید مراجع ذیربط بهره برده شود.	*	*	*
۳۷	ارائه دسترسی راه دور به افراد در خارج از مرکز باید دارای ضوابط خاصی باشد. استفاده از پروتکل های ناایمن RDP، SSH، VNC، Telnet و یا نرم افزارهای Team Viewer، AnyDesk و ... ممنوع است و برای اتصال مدیر شبکه با تجهیزات باید از بستر رمزنگاری شده با الگوریتم و طول کلید مناسب استفاده گردد.	*	*	*
۳۸	برای نظارت و کنترل بر دسترسی های راه دور کاربران مجاز و یا نفرات داخل مرکز (به ویژه مدیران شبکه که دسترسی بالایی دارند) به تجهیزات مستقر در مراکز داده و منابع حساس شبکه سازمان اعم از سرورها، تجهیزات شبکه ای و امنیتی و ... باید از تجهیزات مدیریت دسترسی های ویژه(PAM[8]) استفاده گردد.	*	*	*

1-High Availability
2-scalability
3-Load Balancing
4-Fualt Tolerant
5-Hardware Security Module
6-Public Key Infrastructure
7-Network Islanding
8-Privileged Access Management

	۲-۲ الزامات و ملاحظات طراحی و معماری شبکه و امنیت شبکه	سطح بندی مراکز داده حیاتی	حساس	مهم
۳۹	مراکز داده، باید از DNS Serverهای داخل کشور پرس و جو نمایند و DNSهای داخلی را به عنوان DNS Server اصلی انتخاب نمایند. به عبارت دیگر باید Iran Access باشند.	*	*	*
۴۰	مراکز داده برای خدمات خود که به زیرساخت های حیاتی کشور ارائه می‌نمایند، باید سازوکار DNSSEC را برای آن مراکز، پیکربندی نمایند.	*	○	○
۴۱	به منظور جلوگیری از نفوذ به مرکز داده لازم است در طراحی و پیاده سازی سرویس ها، شبکه و امنیت شبکه مرکز، تمام موارد غیرضروری و بلا استفاده در تمام تجهیزات سخت افزاری و نرم افزاری غیرفعال گردد.	*	*	*
۴۲	استفاده از تجهیزات امریکایی در مراکز داده مورد استفاده در زیرساخت های حیاتی کشور، در تمام سطوح شبکه ممنوع است.	*	○	○
۴۳	استفاده از افزونگی مناسب (نرم افزار، سخت افزار، ارتباطات و اطلاعات) در تمام اجزای شبکه لازم است.	*	*	*
۴۴	شبکه و اجزای آن مانند سامانه ها، ارتباطات و ... در تمام مدت از سازوکار دسترس پذیری بالا [1] برخوردار باشد و سازوکار تحمل خطا[2] اندیشیده و اجرایی گردد.	*	*	*
۴۵	برای جلوگیری از انتشار حملات از طریق بهره گیری از آسیب پذیری های یک برند خاص، استفاده از راهکار Multi-Branding در شبکه بالاخص در تجهیزات اساسی شبکه و تجهیزات امنیت شبکه، الزامی است.	*	*	○

	۲-۳ الزامات قرارداد با کارگزاران و سرویس دهندگان خارج از سازمان	سطح بندی مراکز داده حیاتی	حساس	مهم
۱	مرکز داده به منظور حفظ پایداری و امنیت ضروریست نسبت به درج حداقل موارد زیر در قراردادهای دریافت خدمات خود به عنوان تعهدات سرویس گیرنده اقدام نماید: • مکانیزم اعلام حادثه امنیتی به مرکز داده • نحوه دسترسی فیزیکی در صورت اجاره مکان و فضا • نحوه تأمین الزامات تسهیلات در صورت اجاره سرور و تجهیزات • تعهدات لازم در خصوص عدم انجام رفتار غیر متعارف در گرفتن سرویس	*	*	*

1-High Availability 2-Fault Tolerance

	۲-۴ الزامات گواهی نامه ها	سطح بندی مراکز داده		
		حیاتی	حساس	مهم
۱	مرکز داده بمنظور حفظ و مراقبت از دارایی‌های اطلاعاتی خود نسبت به پیاده سازی استاندارد مدیریت امنیت اطلاعات (ISMS) اقدام و گواهی نامه ان را از مراجع ذیصلاح داخلی اخذ و تمدید آن را در برنامه سالیانه خود قرار دهد.	*	*	*

	۲-۵ الزامات مستندات	سطح بندی مراکز داده		
		حیاتی	حساس	مهم
۱	مرکز داده باید کلیه مستندات مرتبط با پدافند غیر عامل خود را مطابق با استانداردهای معتبر از قبیل ISO ۲۷۰۰۰ و ITIL تدوین و نگهداری نماید.	*	*	*
۲	مرکز داده در شناسنامه تجهیزات خود باید حداقل موارد پدافندی و امنیتی زیر را درج نماید. - ذکر مشروح و دقیق مشخصات سیستم عامل ها و نرم‌افزارهای (از جمله نرم‌افزارهای طرف ثالث) مورد استفاده در مرکز داده در سند مستندات سیستم - تامین مشخصات زنجیره شامل فروشنده، خریدار و تأیید کننده و نگهدارنده - گواهی نامه‌های امنیتی - تنظیمات امنیتی و نحوه اعمال - سطح طبقه بندی - محل و نحوه نگهداری - تعامل و تبادل اطلاعات با سایر تجهیزات - پرسنل مجاز دسترسی فیزیکی و منطقی - مکانیزم بروزرسانی امن	*	*	*

	۲-۶ الزامات برچسب گذاری و راهنمای شناسائی	سطح بندی مراکز داده		
		حیاتی	حساس	مهم
۱	مرکز داده موظف به انجام برچسب گذاری بر روی تجهیزات با روش استاندارد است و توصیه می‌شود از استاندارد ANSI/TIA/EIA-۶۰۶-A استفاده گردد.	*	*	*

	۲-۶ الزامات برچسب گذاری و راهنمای شناسائی	سطح بندی مراکز داده		
		حیاتی	حساس	مهم
۲	استفاده از رنگ پچ کوردها برای تفکیک نوع ارتباطات از قبیل داخلی اینترنت و ... مورد اقدام قرار گیرد.	*	*	○

	۲-۷ الزامات و ملاحظات نرم افزار	سطح بندی مراکز داده		
		حیاتی	حساس	مهم
۱	هر مؤلفه نرم‌افزاری، باید مطابق با مستندات سیستم، قادر به ارائه تمام خدمات مورد انتظار به کاربران خود باشد.	*	○	○
۲	طراحی و پیاده سازی هر نرم‌افزار، باید بر مبنای اصول مهندسی نرم‌افزار انجام شده باشد.	*	○	○
۳	هر مؤلفه نرم‌افزاری، باید سازوکارهایی برای اجتناب، کشف و مدیریت انواع خطاهایی که می‌توانند منجر به افشا یا تغییر غیرمجاز داده‌های حساس شوند، را در خود داشته باشد.	*	*	○
۴	نرم افزار مورد استفاده باید بومی و امن باشد. برابر قوانین کشور، در صورت وجود محصول بومی امن، خرید و بکارگیری محصول خارجی ممنوع است.	*	*	○
۵	مرکز داده، باید مشخصات کامل تمام سیستم عامل‌ها و نرم‌افزارهایی (از جمله نرم‌افزارهای طرف ثالث) را که قرار است در مرکز داده استفاده شود، به طور مشروح و دقیق، در سند مستندات سیستم ذکر کند.[1]	*	*	*
۶	مرکز داده باید روالی را برای تهیه لیستی کامل از همه سیستم عامل ها و نرم‌افزارهای نصب‌شده روی سامانه ها، پایگاه‌های داده و...، به طور مشروح و دقیق ذکر کند. طبق این روال، باید بتوان نام نسخه، شماره نسخه و تاریخ نصب هر نرم‌افزار نصب شده در مرکز داده را مشخص کرد.	*	*	*
۷	استحکام، اصالت و یکپارچگی ساختار نرم افزار، سیستم عامل و پایگاه داده‌های مورد استفاده در هر لایه احراز گردد.	*	*	*
۸	ارزیابی دوره ای و مستمر نرم افزارها، میان افزارها، سخت افزارها و ارتباطات مورد استفاده مطابق با شاخص های استاندارد بین المللی و اختصاصی ابلاغی صورت پذیرد.	*	*	*

۱ - نرم‌افزار طرف ثالث، اصطلاحاً به نرم‌افزاری گفته می‌شود که نه یک برنامه کاربردی است و نه یک نرم‌افزار تجاری. این گونه نرم‌افزارها، توسط یک طرف ثالث برای اهداف خاصی و در مقیاس محدود تولید می شوند.

	۷-۲ الزامات و ملاحظات نرم افزار	سطح بندی مراکز داده		
		حیاتی	حساس	مهم
۹	ارتباطات سیستم عامل، و دیگر نرم افزارها باید بر اساس لیست سفید محدود شود.	*	*	*
۱۰	برای سرویس های حیاتی راهکار به روز رسانی غیربرخط (بدون ارتباط با اینترنت) سیستم عامل بدون ایجاد اختلال و وقفه در عملکرد سامانه صورت پذیرد.	*	*	*
۱۱	برای سرویس های غیرحیاتی، راهکار به روز رسانی مطابق با اصول امنیت سایبری انجام شود.	-	*	*
۱۲	تعداد کاربران مجاز سیستم عامل و پایگاه داده به حداقل ممکن کاهش یابد.	*	*	*
۱۳	کلیه رخدادها رویدادنگاری شده و توسط ارتباط رمزنگاری شده با الگوریتم امن، به سمت سامانه مدیریت رخدادهای امنیتی بومی (SIEM)، فرستاده شوند.	*	*	*
۱۴	برای سرویس ها و سرورهای حیاتی تمام نرم‌افزارها، سفت افزارها و برنامه های نصب شده روی مدارهای مجتمع باید در پردازش داده‌ها و تولید خروجی، هیچ گونه خطایی نداشته باشند.	*	○	○
۱۵	نرم افزارهای اساسی مورد استفاده در مرکز داده، باید جلوی هرگونه دستکاری و تغییر نرم افزار یا سفت افزار موجود را، جز از طریق روالی که برای ارتقا نرم افزار یا جایگزینی سفت افزار پیش بینی شده است، بگیرد.	*	○	○
۱۶	مرکز داده، باید نرم‌افزارهایی مستقل را برای کنترل و نظارت بر درستی عملیات پردازش داده‌ها، کشف خطاهایی که در عملیات پردازش داده رخ می دهند و چگونگی مدیریت و تصحیح خطاها، تولید نماید.	*	○	○
۱۷	سیستم عامل های مورد استفاده، باید به گونه ای سفارش شده باشد که قبل از نصب نرم‌افزار روی سیستم، گواهی دار بودن آن را مورد تحقیق قرار دهد.	*	○	○
۱۸	باید تمهیداتی اندیشیده شود تا مکانیزم های امنیتی و پدافندی مناسب و مورد تایید برای مدیریت و حفاظت از پروفایل کاربران در مقابل مکانیزم های داده کاوی و حفظ حریم خصوصی پیاده سازی و اجرا گردد.	*	*	*
۱۹	در تمام سطوح طراحی، نصب و پیاده سازی، راه اندازی، توسعه، ارائه خدمات و ... از نرم افزارها، توانمندی ها و فناوری های بومی و امن داخلی بهره گرفته شود.	*	*	*

	۲-۷ الزامات و ملاحظات نرم افزار	سطح بندی مراکز داده		
		حیاتی	حساس	مهم
۲۰	وجوه مختلف حفظ محرمانگی مانند محرمانگی اطلاعات، محرمانگی کاربران، محرمانگی پروفایلینگ و ... پیاده سازی گردد و از اجرای صحیح آنها اطمینان حاصل شود.	*	*	*
۲۱	هیچ یک از تجهیزات قابل برنامه ریزی مورد استفاده از جمله کارت هوشمند، نباید اجازه جایگزینی یا تغییر برنامه نصب شده روی خود را دهند، مگر در شرایطی که این کار برای آماده‌سازی وسیله یا نرم‌افزار برای استفاده، لازم باشد.[۱]	*	○	○
۲۲	کاربران عمومی مرکز داده، نباید به کد منبع هیچ یک از نرم‌افزارهای نصب‌شده روی سیستم ها، دسترسی داشته باشند.	*	*	*
۲۳	جهت جلوگیری از دسترسی و دستیابی غیرمجاز به نرم افزار و یا برنامه‌های کاربردی مرکز داده باید کاربران این برنامه‌ها با روش های امن نظیر زیرساخت کلید عمومی بومی، تصدیق هویت گردد و این تصدیق هویت باید به‌صورت دو طرفه باشد.	*	*	*
۲۴	هر برنامه کاربردی مورد استفاده، باید برای مواجهه با تمام خطاهای نرم‌افزاری که به طور بالقوه، نسبت به آنها آسیب پذیر است و ممکن است در زمان اجرای آن به وقوع بپیوندند، آماده پاسخگویی باشد. [۲]	*	○	○
۲۵	نرم افزارها و برنامه‌های کاربردی مورد استفاده، باید برای مواجهه با تهدیدات بدافزارها[۳] آماده باشد. مرکز داده، باید روال‌هایی را برای محافظت دائم از نرم افزارها، در مقابل چنین تهدیداتی اندیشیده، و به طور مشروح و دقیق ذکر کرده باشد.[۴]	*	*	*
۲۶	به منظور جلوگیری از نفوذ در نشست‌های برنامه کاربردی، مرکز داده موظف است در کلیه نرم افزارها و برنامه‌های کاربردی خود تعیین حد آستانه زمانی نشست را اعمال نماید.	*	*	*

۱-جایگزینی یا تغییر برنامه نصب شده روی یک وسیله، ممکن است توسط دیگر برنامه‌های نصب شده روی سیستم، یا به طور فیزیکی، توسط افرادی که حافظه شامل آن کد را جایگزین می کنند، انجام شود.

۲- مثال هایی از چنین خطاهایی عبارتند از: خطای سرریز پشته، خطای سرریز مقادیر عددی، خطای منطقی مانند تقسیم بر صفر، خطای خروج از کران بالای آرایه و غیره.

3-malicious software

۴-بدافزار، به هر برنامه ای گفته می‌شود که هدف آن، نقض امنیت سیستم باشد. ویروسها، کرمها، اسبهای تروا و بمبهای منطقی، مثال هایی از انواع بدافزارها هستند.

	۷-۲ الزامات و ملاحظات نرم افزار	سطح بندی مراکز داده		
		حیاتی	حساس	مهم
۲۷	تمام نرم‌افزارهای مورد استفاده، باید تمام داده‌های ورودی به سیستم را قبل از پردازش آنها، مورد بررسی قرار دهند. هیچ نرم‌افزاری نباید قبل از اطمینان به اعتبار داده‌های ورودی، مجاز به پردازش آنها باشد. [1]	*	*	*
۲۸	نرم افزارها و برنامه های کاربردی، تنها باید به مدیر سیستم که قبلاً احراز هویت شده باشد اجازه تغییرات روی سیستم را بدهد.	*	*	*
۲۹	نرم افزارها و برنامه های کاربردی، تنها باید به شیوه‌های از قبل تعیین شده و مشخص، اجازه نصب، بروز رسانی یا برداشتن نرم‌افزار از روی سیستم را بدهد.	*	*	○
۳۰	مرکز داده باید تمهیدات مناسب و امنی را برای مدیریت وصله [2] اندیشیده و اجرا نماید.	*	*	*
۳۱	باید تمهیداتی جهت نصب سریع و به موقع وصله‌های امنیتی دریافت شده از سوی مراجع ذی صلاح در مرکز داده اندیشیده شود.	*	*	○
۳۲	به منظور حصول اطمینان از رفع کامل آلودگی و قبل از بکارگیری مجدد نرم افزار، برنامه کاربردی و ... در شبکه رعایت اصل سایه سازی [3] با ایزوله سازی و تست سامانه‌های آسیب دیده در این شبکه، در دستور کار قرار گیرد.	*	*	*
۳۳	مرکز داده باید مشخصات کامل نسخه فعلی تمام نرم‌افزارهای نصب شده را در جایی دیگر و با رعایت اصول پشتیبان گیری ذخیره کرده باشد.	*	*	○
۳۴	سند طرح تداوم فعالیت‌های ضروری(BCP) در حوزه نرم افزاری تدوین و سازوکار اجرای آن برای مراحل قبل، در آستانه، حین و پس از رخداد سایبری تمرین شود.	*	*	*
۳۵	سند طرح بازیابی از فاجعه(DRP) در حوزه نرم افزاری تدوین و سازوکار اجرای آن برای مراحل حین و پس از رخداد سایبری تمرین شود.	*	*	*

[1]-داده‌های ورودی یا ممکن است به طور دستی توسط کاربر، وارد سیستم شوند؛ یا آنکه از منابع خارجی (مانند حافظه فلش یا کانال شبکه) توسط سیستم دریافت شوند.

2-Patch Management
3-Shadowing

	۲-۸ الزامات ضد بدافزار	سطح بندی مراکز داده		
		حیاتی	حساس	مهم
۱	مرکز داده موظف است با توجه به عملکرد و تهدیدات مرکز داده نسبت به تعیین نوع ضدبدافزارها و همچنین چرخه ماندگاری و نحوه بروز رسانی امن آنها اقدام نماید. بکارگیری ضد بد افزار بومی و امن الزامی می‌باشد.	*	*	*

	۲-۹ الزامات و ملاحظات سیستم عامل	سطح بندی مراکز داده		
		حیاتی	حساس	مهم
۱	برای اطمینان از امنیت سیستم عامل و به حداقل رساندن آسیب‌های آن مرکز داده می‌باید در همه سطوح از سیستم عامل‌های متن باز امن شده نظیرلینوکس و BSD استفاده نماید. (در شرایطی که استفاده ازسیستم عامل متن باز ممکن نباشد مرکز داده می‌تواند از سیستم عامل متن بسته استفاده نماید. در صورت استفاده از سیستم عامل های متن بسته می‌باید امن سازی و محکم سازی روی این سیستم عامل ها با آخرین توصیه نامه‌ها صورت پذیرد). سازمان پدافند غیرعامل- قرارگاه پدافند سایبری کشور درخصوص امن سازی سیستم عامل‌های لینوکس CentOS، Ubuntu و ویندوز، کتاب‌های امن سازی اضطراری سیستم عامل‌های لینوکس (CentOS، Ubuntu) و سیستم عامل ویندوز سرور را در تیرماه ۱۳۹۷ تدوین و منتشر نموده است که می توان به این منابع، مراجعه نمود.	*	*	○

	۲-۱۰ الزامات و ملاحظات ارتباطات	سطح بندی مراکز داده		
		حیاتی	حساس	مهم
۱	مؤلفه های ارتباطاتی مرکز داده، باید مانع از افشاء داده‌های حساس، دستکاری و تغییر غیرمجاز داده‌های ارسال شده روی کانال های شبکه مخابراتی شوند.	*	*	○
۲	شبکه ارتباطی مرکز داده، برای رمزگذاری داده‌های ارسالی باید از الگوریتم های معتبر و استاندارد (مانند الگوریتم رمزنگاری متقارن AES با کلید ۲۵۶ بیتی) و یا از الگوریتم های بومی و امن مورد تایید نهادهای متولی استفاده کند.	*	*	*

	۲-۱۰ الزامات و ملاحظات ارتباطات	سطح بندی مراکز داده		
		حیاتی	حساس	مهم
۳	برای اطمینان از عدم دستکاری و تغییر داده‌ها، تمام داده‌های ارسال شده باید در طرف گیرنده، احراز هویت شوند.	*	*	*
۴	سامانه ارتباطی، نباید مجاز به پذیرش داده‌های رمز نشده یا داده‌های امضا نشده باشد.	*	*	*
۵	سامانه ارتباطی مرکز داده، باید برای جلوگیری و کشف فرایندهای نفوذ از طریق ارتباطات شبکه ای، به ابزارهای دفاعی مناسب مجهز شده باشند.	*	○	○
۶	سامانه ارتباطی، در صورت وقوع وقفه ارتباطی، باید اطلاعات ممیزی[1] فعالیت های خود را در مدت زمان وقفه ارتباطی، ثبت و ذخیره کند.[2]	*	*	*
۷	مرکز داده، باید برای مقابله با انواع تهدیدات شبکه ای و ارتباطی چندین نوع نرم‌افزار محافظ تدارک ببینند.	*	○	○
۸	سند طرح تداوم فعالیت‌های ضروری(BCP) در حوزه ارتباطات تدوین و سازوکار اجرای آن برای مراحل قبل، در آستانه، حین و پس از رخداد سایبری تمرین شود.	*	*	*
۹	سند طرح بازیابی از فاجعه(DRP) در حوزه ارتباطات تدوین و سازوکار اجرای آن برای مراحل حین و پس از رخداد سایبری تمرین شود.	*	*	*
۱۰	مرکز داده باید نحوه اتصال خود را با تأمین کنندگان پهنای باند در قالب چارچوبی مشخص و یا قرارداد تعیین نماید به گونه‌ای که کلیه الزامات مرتبط از قبیل کیفیت سرویس، نحوه دریافت خدمات، چگونگی نگهداری مسیر و تجهیزات پایش در آن لحاظ نماید.	*	○	○

	۲-۱۱ الزامات و ملاحظات تجهیزات سخت افزاری	سطح بندی مراکز داده		
		حیاتی	حساس	مهم
۱	در صورت عدم کفایت تجهیزات سخت افزاری بومی و ضرورت استفاده از تجهیزات سخت افزاری غیربومی، این تجهیزات باید به تائید سازمان پدافند غیرعامل برسند.	*	*	*

۱- اطلاعات ممیزی، به مستنداتی گفته می‌شود که میتوان بر اساس آن، دقت نتایج انتخابات را تحقیق کرد. برای تهیه چنین مستنداتی، لازم است تمام فعالیتهای سیستم، ثبت و در جایی مطمئن نگهداری شوند.

2-audit trail

	۲-۱۱ الزامات و ملاحظات تجهیزات سخت افزاری	سطح بندی مراکز داده		
		حیاتی	حساس	مهم
۲	به منظور جلوگیری از دستیابی به اطلاعات سرورها حتی در سرقت فیزیکی ضروریست کلیه سرورهای حساس مرکز داده دارای کیس امن باشند.	*	○	○
۳	سند طرح تداوم فعالیت‌های ضروری(BCP) در حوزه سخت افزار تدوین و سازوکار اجرای آن برای مراحل قبل، در آستانه، حین و پس از رخداد سایبری تمرین شود.	*	*	*
۴	سند طرح بازیابی از فاجعه(DRP) در حوزه سخت افزار تدوین و سازوکار اجرای آن برای مراحل حین و پس از رخداد سایبری تمرین شود.	*	*	*

	۲-۱۲ الزامات و ملاحظات کارایی	سطح بندی مراکز داده		
		حیاتی	حساس	مهم
۱	زمان پاسخ یکی از مهمترین معیارها برای کارایی زیرساخت مراکز داده، است. برای موثر بودن پایش و به دست آوردن ارزیابی دقیق از کارایی زیرساخت باید حداقل، حداکثر و میانگین زمان پاسخ اندازه گیری شود و میزان بهینه زمان، مدنظر قرار گیرد.	*	*	○
۲	همه سیستم های فیزیکی موجود در زیرساخت مراکز داده شامل سرورها، سوئیچ ها، سیستم های ذخیره سازی و ... باید مدیریت و پایش شوند. بدین منظور نیاز به ایجاد یک پلتفرم شامل مجموعه ای از ابزارها برای مانیتورینگ و کنترل سیستم های فیزیکی است.	*	*	*
۳	مرکز داده باید سازوکار تجزیه و تحلیل ترافیک به صورت بلادرنگ جهت مدیریت جریان داده‌ها را اجرایی نماید و سیاست‌های مورد نیاز برای داشتن حداکثر کارایی را مشخص کند. معماری شبکه باید حداقل، متوسط، و اوج الگوی ترافیک شبکه را پیش بینی کند.	*	*	○
۴	ظرفیت ذخیره سازی و ظرفیت بافر دو عامل تاثیرگذار بر کارایی مرکز داده هستند. لذا در مراحل طراحی، پیاده سازی و بهره برداری باید این موضوعات مورد توجه جدی قرار گیرد و تمهیداتی جهت مقیاس پذیری آنها اندیشیده شود.	*	*	*

	۱۲-۲ الزامات و ملاحظات کارایی	سطح بندی مراکز داده		
		حیاتی	حساس	مهم
۵	مرکز داده باید به صورت پویا سیستم‌ها و منابع را بر اساس بار کاری اولویت بندی کند. علاوه بر این باید سیاست‌هایی در مورد بار کاری و مدیریت منابع وجود داشته باشد تا این اطمینان حاصل شود که حداکثر بهره‌وری و کارایی تضمین می شود.	*	○	○
۶	به منظور دسترسی‌پذیری بالا [1] در مرکز داده، سیستم ها، شبکه و برنامه‌ها باید طوری طراحی شوند که قدرت تحمل‌پذیری خطا[2] را داشته باشند.	*	*	*
۷	به منظور دسترسی‌پذیری بالا در مرکز داده، در هنگام ساخت سرویس‌ها باید همه اجزای اصلی یک سرویس به عنوان واحدهای جدا و قابل تکرار (ماژولار) طراحی گردد.	*	○	○
۸	در مراکز داده‌ای که خدمات Collocation، ارائه می نمایند برای سرویس ها و یا زیرساخت های حیاتی که از مرکز داده فوق خدمات می گیرند، باید تاخیری در حد میلی ثانیه را در سراسر شبکه ارائه دهند.	*	*	*
۹	در مراکز داده‌ای که خدمات Collocation، ارائه می نمایند باید سازوکاری اعمال شود تا هر درخواست اولویت بندی گردد و بر اساس آن، برای سرویس ها و یا زیرساخت های حیاتی که از مرکز داده فوق خدمات می گیرند دارای اولویت تقدم اجرا درنظر گرفته شود.	*	*	*
۱۰	در مراکز داده‌ای که خدمات Collocation، ارائه می نمایند باید سازوکاری اعمال شود تا تخصیص کارآمد و موثر منابع متناسب با بار کاری برای سرویس ها و یا زیرساخت های حیاتی که از مرکز داده فوق خدمات می گیرند، عملیاتی شود.	*	*	*
۱۱	در مراکز داده‌ای که خدمات Collocation، ارائه می نمایند باید ارائه دهندگان سرویس برای سرویس ها و یا زیرساخت های حیاتی که از مرکز داده فوق خدمات می گیرند با پایش و ارزیابی مداوم دسترسی پذیری زیرساخت و سرویس های ارائه شده از منظر امنیتی و عملکردی، کیفیت سرویس(QoS[3]) را تضمین نمایند.	*	*	*
۱۲	در مراکز داده‌ای که خدمات Collocation، ارائه می نمایند باید ارائه دهندگان سرویس برای سرویس ها و یا زیرساخت های حیاتی که از مرکز داده فوق خدمات می گیرند، باید امکان بازیابی یک سیستم از سخت افزار محض بدون نیاز به نصب سیستم عامل و یا نرم افزار فراهم شود. [4]	*	*	*

1-High Availability
2-Fault Tolerance
3-Quality of Service
۴- توانایی بازیابی به صورت bare-metal

	۲-۱۳ الزامات و ملاحظات مقیاس پذیری	سطح بندی مراکز داده		
		حیاتی	حساس	مهم
۱	مقیاس پذیری باید برای مشتریان کاملا شفاف و بدون درگیر کردن آن‌ها در جزئیات باشد.	*	*	○
۲	مقیاس‌پذیری باید در سطوح مختلف شامل مقیاس پذیری سرورها، مقیاس پذیری شبکه و مقیاس پذیری سکو پیاده سازی شود.	*	○	○
۳	مرکز داده باید توانایی مقیاس پذیری هم به صورت افقی [۱] و هم به صورت عمودی [۲] را داشته باشد[۳]	*	*	*
۴	مرکز داده باید یک استراتژی ارائه دهد که تضمین کند زیرساخت توانایی پشتیبانی از تقاضاهای منابع که بر آن اعمال می‌شود، را دارد.[۴]	*	*	○
۵	مرکز داده باید قابلیت تجزیه و تحلیل و مدیریت تقاضاها را داشته باشد تا بتواند حجم تقاضاها، نقاط اوج تقاضا، و تقاضاهای غیر قابل انتظار را پیش بینی نماید و در ضمن عکس العمل مناسب برای برطرف کردن آن‌ها را ارائه دهد.	*	○	○
۶	به منظور مقیاس پذیری مناسب مرکز داده، توجه به محدودیت های ظرفیتی بالقوه موجود در توزیع کننده بار ضرورت دارد، از جمله این محدودیت ها پهنای باند توزیع کنندهٔ بار، ظرفیت CPU و RAM در توزیع کنندهٔ بار[۵]، توانایی توزیع کنندهٔ بار در پخش صحیح بار بین سرورهای کاربردی و پهنای باند بین توزیع کننده بار و سرورهای کاربردی است.	*	*	*
۷	مرکز داده باید قابلیت شناسایی محدودیت های منابع و مدیریت[۶] آنها را داشته باشد و برای کنترل محدودیت ها، برنامه و پایگاه داده معماری مناسبی داشته باشد.	*	*	*

1-Horizontal 2-Vertical

۳-مقیاس‌پذیری افقی به معنای اضافه کردن سرورجدید و افزایش ظرفیت است که برای کاربردهای stateless مناسب است. در حالی که مقیاس‌پذیری عمودی به معنای جابه‌جا کردن سرور موجود با یک نمونه دیگر یا تغییر مشخصات سخت‌افزاری آن است و برای برنامه‌های stateful کاربرد دارد.

۴-مهمترین قابلیت‌های این استراتژی که برنامه‌ریزی برای ظرفیت را تضمین کند، شامل این موارد است: آگاهی از الگوی مصرفی منابع و چگونگی تغییر آن در طول روز، یا در طول یک هفته، در روزهای تعطیل و نیز در فصول مختلف، آگاهی از نحوه پاسخ‌دهی برنامه‌ها به بار کاری خود به طوری که بتوان تعیین کرد چه زمانی، چه نوع از ظرفیت اضافی را نیاز خواهیم داشت، آگاهی از ارزش سیستم‌های موجود تا بتوان مشخص کرد که چه موقع افزودن ظرفیت ارزش ایجاد می‌کند و چه موقع فاقد ارزش است.

5-Load Balancer

۶-نمونه‌هایی از محدودیت‌های منابع قابل شناسایی شامل پهنای باند بین سرور برنامه کاربردی و تجهیزات ذخیره‌سازی شبکه، عملیات ورودی/خروجی برای خواندن و نوشتن بر روی دیسک، پهنای باند بین سرور برنامه و سرور پایگاه داده، عملیات ورودی/خروجی دیسک برای خواندن و نوشتن بر روی پایگاه داده و میزان فضای دیسک برای پشتیبانی از ذخیره‌سازی می‌باشد.

	۱۳-۲ الزامات و ملاحظات مقیاس پذیری	سطح بندی مراکز داده		
		حیاتی	حساس	مهم
۸	اگر یک ماشین مجازی از کار بیفتد، زیرساخت مرکز داده باید بتواند بدون وقفه به کار خود ادامه دهد.	*	*	*
۹	جفت‌شدگی[1] بین اجزای برنامه باید بسیار کم باشد، به طوری که خرابی هر یک از اجزا، روی دسترس‌پذیری کلی برنامه تاثیری نداشته باشد.	*	*	*
۱۰	برنامه‌ها باید تا حدممکن با قرار دادن اطلاعات وضعیت در خارج از برنامه، بدون وضعیت بشوند و تا جایی که امکان دارد، پردازش از داده جدا شود.[2]	*	*	*
۱۱	درصورت استفاده از فناوری مجازی سازی، از سازوکار خوشه بندی ماشین های مجازی استفاده گردد.[3]	*	○	○
۱۲	برای بازیابی مرکز داده، خدمات و یا برنامه‌ها به حالت قبل، باید طرح بازیابی در زمان بروز حوادث غیرمترقبه و جایگزینی با مراکز ثانویه ایجاد و اجرایی گردد.	*	*	*
۱۳	برای حفاظت از تجهیزات و داده‌های مرکز داده در مقابل حوادث طبیعی و غیر طبیعی (انسان ساز)، باید سازوکار شناسایی، تجزیه و تحلیل و مدیریت مخاطرات بصورت مستمر انجام پذیرد.	*	*	*
۱۴	مرکز داده باید فرآیندهایی برای پیاده سازی هرگونه تغییرات در زیرساخت فراهم کرده باشد. فرآیندهای مدیریت تغییر[4] باید به عنوان معیار تلقی شده و سبب کاهش خطای انسانی در شرایط بحرانی شود.	*	○	○
۱۵	مرکز داده باید به منظور حفظ پایداری خدمات، قبل ازهرگونه تغییر در زیرساخت و فرآیندهای عملیاتی باید مخاطرات امنیتی و پدافندی آن بررسی و سازوکاری جهت به حداقل رساندن آن تدوین و تعیین نماید.	*	*	○
۱۶	مرکز داده باید از اصول اولیه مدیریت ظرفیت[5] شامل اندازه‌گیری دقیق تمام بارهای الکتریکی و مکانیکی، ارائه مدلی برای تامین ظرفیت و سنجش بلادرنگ تا حد ممکن استفاده نماید.	*	*	*

1-Coupled

۲- از جمله روش های این کار شامل قرار دادن وضعیت در سمت کاربر، قرار دادن اطلاعات وضعیت در پایگاه داده و یا تهیه چندین کپی از داده است.

۳- در این روش در صورت بروز مشکل یا خطاهای سخت‌افزاری در یک سرور فیزیکی و عدم امکان پاسخ‌دهی آن به درخواست‌ها، به صورت خودکار ماشین‌های مجازی آن، به سرور فیزیکی دیگری در همان خوشه انتقال می‌یابد. در نتیجه دسترسی‌پذیری و پایداری منابع تضمین می‌شود.

4-Change Management

5-Capacity Management

	۲-۱۳ الزامات و ملاحظات مقیاس پذیری	سطح بندی مراکز داده		
		حیاتی	حساس	مهم
۱۷	مرکز داده به منظور پایداری زیرساخت و خدمات باید یک استراتژی برای چرخه عمر[1] آن ارائه دهند. استراتژی چرخه عمر باید مبتنی بر یک برنامهٔ نگهداری پیشگیرانه [2] و پیشگویانه [3] باشد. این استراتژی به همراه استراتژی‌های دیگر که بر روی افزایش چرخهٔ عمر و طولانی‌تر شدن زمان متوسط بین خرابی[4](MTBF) سیستم ها، تجهیزات، قطعات و مرکز داده تمرکز دارند ارائه گردد. این استراتژی باید راهکارهایی را برای چرخش تجهیزات، جایگزینی تجهیزات و جایگزینی قبل از شکست ارائه دهد.	❋	❋	❋

	۲-۱۴ الزامات فناوری های نوین مورد استفاده	سطح بندی مراکز داده		
		حیاتی	حساس	مهم
۱	ویژگی‌های منحصر به فرد رایانش ابری منافع بسیاری دارد، اما وجود همه این ویژگی ها، تهدیدات امنیتی خاصی نیز به دنبال خواهد داشت، لذا باید الزامات و ملاحظات امنیتی و پدافند سایبری مربوطه به دقت رعایت گردد. از این رو سندی تحت عنوان "الزامات و ملاحظات پدافند سایبری در فناوری رایانش ابری" در سازمان پدافندغیرعامل تهیه و تدوین شده است که برای اطلاع بیشتر به آن مراجعه شود.	❋	❋	❋

	۲-۱۵ الزامات و ملاحظات پشتیبان گیری، بازیابی و امحاء اطلاعات	سطح بندی مراکز داده		
		حیاتی	حساس	مهم
۱	مرکز داده باید سیاست های امنیتی-پدافندی مناسبی را برای پشتیبان گیری ارائه نماید.	❋	❋	❋
۲	در تمامی مراحل پشتیبان گیری شامل انتقال، ذخیره سازی و دسترسی باید به صورت خودکار باشد تا امنیت و پایداری داده ها تضمین شود.	❋	❋	❋
۳	داده های کاربران باید قبل از انتقال بر روی سیستم خودشان رمزنگاری شوند سپس داده‌های رمز شده با استفاده ازپروتکل امن رمزنگاری به سرورهای اصلی انتقال داده شوند.	❋	❋	○

1-Life Cycle
2-Proactive
3-Predictive
4-Mean Time Between Failures

	۲-۱۵ الزامات و ملاحظات پشتیبان گیری، بازیابی و امحاء اطلاعات	سطح بندی مراکز داده		
		حیاتی	حساس	مهم
۴	حداقل یک مرکز داده با داده های تکراری در موقعیت جغرافیایی مناسب که کمتر تحت تاثیر بلایای طبیعی و غیرطبیعی قرار گیرد، وجود داشته باشد.	*	*	○
۵	پشتیبان گیری بر حسب تغییرات یا به صورت ساعتی، روزانه، هفتگی، ماهانه و یا بر حسب نیاز کاربران زمان بندی شود.	*	○	○
۶	مرکز داده باید با پیش بینی و برنامه ریزی در مورد حوادث و نحوه بازیابی از آنها، زمان قابل قبولی را برای بازیابی داده ها تضمین نماید. این زمان بازیابی، زمان انتقال بر روی شبکه را نیز شامل می شود.	*	○	○
۷	بازیابی باید به صورت لایه بندی شده و یا به عبارتی اولویت دار با اولویت داده های حیاتی صورت پذیرد.	*	*	*
۸	برای سرویس های حیاتی، باید سازوکار امکان بازیابی یک سیستم از سخت افزار محض بدون نیاز به نصب سیستم عامل و یا نرم افزار فراهم شود. [۱]	*	*	*
۹	مرکز داده باید ثبات و قابلیت اطمینان زیرساخت خود را برای نگهداری کپی های پشتیبان سرویس گیرندگان تضمین نماید.	*	○	○
۱۰	مرکز داده باید بعد از هر پشتیبان گیری از صحت آن اطمینان حاصل و تأیید گردد. ضمنا اطلاعات به درستی ذخیره و قابل بازیابی باشند.	*	*	○
۱۱	انجام آزمون‌های بازیابی قابل ممیزی باید به صورت منظم برای تضمین RTO[۲] و RPO[۳] انجام شود.	*	*	*
۱۲	مرکز داده باید نظام و تدابیر مشخصی برای امحاء اطلاعات داشته باشد.	*	○	○

	۲-۱۶ الزامات ورود و خروج رایانه همراه و اقلام ذخیره ساز	سطح بندی مراکز داده		
		حیاتی	حساس	مهم
۱	باید به منظور کاهش تهدیدات داخلی در مرکز داده و جلوگیری از نشت و سرقت اطلاعات ورود و خروج اقلام ذخیره ساز اطلاعات از قبیل رایانه همراه، دیسک فشرده، فلش مموری برابر فرآیند مشخص و کنترل شده باشد و حداقل با تکمیل فرم مربوطه و تأیید آن امکان پذیر باشد.	*	*	*

۱- مرکز داده با استفاده از این قابلیت می‌تواند در شرایط بسیار بحرانی، زمانی که سیستم عامل سرور نیز دچار مشکل شده و قادر به بالا آمدن نمی‌باشد، و یا سرور دارای سیستم عامل نمی‌باشد، اقدام به بازگرداندن داده‌های کاربران نمایند و به این ترتیب پایداری سیستم را تضمین نمایند.

2-Recovery Time Objective 3-Recovery Point Objective

	۲-۱۷ الزامات و ملاحظات کابل	سطح بندی مراکز داده		
		حیاتی	حساس	مهم
۱	به منظور اطمینان از پایداری سرویس‌های مرکز داده در کابل کشی موارد زیر رعایت گردد: ـ جلوگیری از ازدحام کابل‌ها (توصیه حداکثر ۲۸۸ زوج سیم یا کواکسیال در ناحیه توزیع منطقه‌ای) ـ استفاده از کابل های استاندارد ـ برچسب گذاری‌های رک، کابینت تجهیزات و کابل ـ استفاده از سیستم رنگ بندی کابل ـ مسیردهی به کابل‌ها ـ پیش بینی توسعه آتی ـ نصب صحیح کابل ها به تجهیزات ـ بازبینی دوره‌ای کلیه کابل ها و اتصالات و یا در هنگام ـ جابه‌جایی و تغییر ـ حذف کابل‌های بلا استفاده ـ بازبینی باندینگ ها و اتصالات به زمین ـ رعایت توصیه‌های تأمین کننده کابل ـ ایجاد فاصله استاندارد بین کابل های برق و دیتا ـ استفاده از محافظ نوسان و نویزگیر در سطوح مختلف	*	*	*
۲	به منظور کاهش دسترسی غیر مجازدر مرکز داده، مسیر کابل ها نباید از فضاهای دسترسی عموم و ساده عبور کند در صورت اجبار داخل لوله یا ترانک بسته و یا مسیر امن عبور داده شوند.	*	*	○

	۲-۱۸ الزامات نیروی انسانی و آموزش	سطح بندی مراکز داده		
		حیاتی	حساس	مهم
۱	صلاحیت امنیتی کلیه کارکنان مرکز داده متناسب با سطح دسترسی و دستیابی آنها به اطلاعات لازم، قبل از بکار گیری از مراجع ذیصلاح استعلام گردد.	*	*	*
۲	مرکز داده باید مشاغل و تخصص‌های حساس را شناسایی و نسبت به همتا پروری و جانشین سازی جهت جلوگیری از وابستگی کامل به شخص یا کارشناس خاص جلوگیری به عمل آورد.	*	*	*
۳	باید کلیه دسترسی‌های اعطایی به کارکنان و پیمانکاران پس از تغییر شغل و یا اتمام همکاری سلب گردد.	*	*	*

	۱۹-۲ الزامات برونسپاری، تعمیر و پشتیبانی	سطح بندی مراکز داده		
		حیاتی	حساس	مهم
۱	در مرکز داده، برون سپاری خدمات امنیت سایبری در قالب MSSP[1] به شرکت‌ها و موسسات دیگر ممنوع است.	*	*	*
۲	کلیه پیمانکاران مرکز داده قبل ازارجاع هر گونه کار متناسب با نوع و ماهیت کار باید دارای تأییدیه امنیتی و صلاحیتی از سوی حراست مرکز باشند.	*	*	*
۳	لازم است در تنظیم قراردادهای مرتبط با دسترسی به دارایی‌های مرکز داده موارد مرتبط مندرج در این سند را در قرارداد لحاظ نموده بصورتی که پیمانکار به نحوه واضح و روشن به تکالیف و تعهدات خود آگاه شود. ضمناً در قرارداد بیان شود علاوه بر موارد تصریح شده رعایت کلیه موارد امنیتی اعلامی از مراجع ذی صلاح الزامی است و عدم اشاره کارفرما به برخی از موارد لازم موجب سلب مسئولیت پیمانکار نمی‌شود.	*	*	*
۴	در صورتی که انجام کار مستلزم ارجاع کار از سوی پیمانکار به مرجع ثالثی باشد لازم است پیمانکار کلیه مسئولیت‌های ناشی از فعالیت‌های مرجع ثالث را بپذیرد در این خصوص تمام ملاحظات امنیتی و پدافندی که برای پیمانکار تبیین شده عیناً برای مرجع ثالث لازم الاجراست.	*	*	*
۵	قبل از ارسال تجهیزات برای تعمیر و پشتیبانی به خارج مرکز داده باید اطمینان کامل از امحاء کلیه اطلاعات و تنظیمات حاصل گردد.	*	*	*

1-Managed Security Service Provider

فصل سوم

الزامات و ملاحظات حفاظت مراکز داده در برابر امواج الکترومغناطیس

مقدمه

تهدیدات شناخته شده حوزه الکترومغناطیس عمدتا پالس الکترومغناطیس ناشی از تهدید جاسازی شده در چمدان، خودرو، کامیون و نیز پالس الکترومغناطیس ناشی از انفجارات اتمی در ارتفاعات بالا (HEMP) است و اگر چه محدود به این ها نیست و پیوسته سناریوهای جدیدی برای ایجاد آسیب الکترومغناطیسی به روش تشعشعی یا هدایتی مطرح می شود اما پالس توان بالا ناشی از تهدیدات الکترومغناطیسی می تواند منجر به آشفتگی سیستم های کامپیوتری، بازنشانی (Reset) آنها و یا حتی تخریب فیزیکی تجهیزات الکترونیکی شود. به همین دلیل، الزامات و ملاحظات این بخش با هدف حفاظت جامع الکترومغناطیس (شامل شیلدینگ، فیلترینگ و ارتینگ) در مراکز حیاتی/ حساس/ مهم ارائه می گردد تا احتمال آسیب پذیری این مراکز کاهش یابد.

ردیف	۳-۱ الزامات قرارداد با کارگزاران بیرونی	سطح بندی مراکز داده		
		حیاتی	حساس	مهم
۱	ضروری است کارفرمایان پروژه حفاظت جامع الکترومغناطیس را در سه قرارداد مجزا به شرح ذیل تنظیم کنند: (الف) پروژه اجرای حفاظت جامع الکترومغناطیس، توسط شرکت مجری شیلد انجام شود. (ب) پروژه ارزیابی توسط فرد حقوقی یا شرکتی مستقل از شرکت مجری انجام شود. (ج) پروژه تعمیر و نگهداری پنج ساله، پس از تائید شیلد توسط شرکت مجری انجام شود.	*	*	*

ردیف	۳-۲ الزامات و ملاحظات شیلدینگ	سطح بندی مراکز داده		
		حیاتی	حساس	مهم
۱	انجام مطالعات تهدید شناسی به منظور تعیین سناریوهای محتمل تهدید و طراحی سناریوی مقابله با آن الزامی است و نتایج این مطالعات مبنای تعیین ضریب شیلدینگ لازم خواهد بود.	*	*	*
۲	در صورتی که مجاورت با منابع تشعشع امواج الکترومغناطیس اجتناب ناپذیر باشد، ضروری است ضریب شیلدینگ به مقدار لازم افزایش یابد تا اختلالات ناشی از منابع پیرامونی به حداقل رسد.	*	*	*
۳	برای مقابله باتهدیدات الکترومغناطیسی ناشی از تسلیحات الکترو مغناطیس پایه، ضروری است سقف، کف و تمام دیوارهای اتاق کامپیوتر (سرور و شبکه)، اتاق‌های مرتبط با مانیتورینگ فنی و مانیتورینگ مراقبتی شیلد شده و ضریب شیلدینگ آن‌ها حداقل های "آیین نامه اجرایی پدافند غیرعامل در حوزه بحران های الکترومغناطیسی" دستگاه یا مرکز مربوطه را برآورده سازد.	*	*	*
۴	برای کلیه درب‌های ورود به اتاق شیلد، اتاق تله، مطابق با مشخصات استاندارد MIL-STD-188-125-1 ایجاد گردد. بهتر است دالان اتاق تله، دارای حداقل یک خم ۹۰ درجه باشد.	*	*	○
۵	استفاده از شیلدهای مدولار و ساندویچی در مناطق با رطوبت بالا ممنوع است.	*	*	*
۶	برای افزایش عمر اتاق شیلد، ضروری است تمامی حرکات و انتقالات معمول نظیر ارتعاشات، افتادگی، انتقال حرارت به داخل محفظه یا از داخل به بیرون، میزان رطوبت و راه‌های نفوذ آب در مرحله طراحی در نظر گرفته شود.	*	○	-

۷	برای کاهش نفوذ امواج الکترومغناطیس، ضروری است مرکز داده فاقد پنجره باشد و تا حد امکان از تعداد منافذ و لوله‌ها و نیز از ابعاد آن‌ها کاسته شود.	*	○	-
۸	پس از نصب شیلد و ملحقات توسط شرکت مجری، ارزیابی اولیه توسط شرکت ارزیاب طبق چک لیست مقدماتی پیوست (الف) انجام شود و در صورت تأیید، آزمون تشعشع طبق استاندارد IEEE299 انجام شود.	*	*	○

ردیف	۳-۳ الزامات و ملاحظات فیلترینگ	سطح بندی مراکز داده		
		حیاتی	حساس	مهم
۱	تمامی منافذ اتاق‌های شیلد شده، دارای فیلترهای حذف سیگنال الکترومغناطیسی با حداقل ضریب تضعیف ۸۰ دسی بل باشند. منافذ ذکر شده شامل تمام لوله‌های ورودی نظیر لوله‌های سیستم تهویه، سرمایشی/گرمایشی و تخلیه گاز می‌باشد. هم‌چنین تمامی خطوط منابع تغذیه، خطوط تلفنی، خطوط کنترلی و خطوط داده، در محل ورود به محفظه شیلد دارای فیلتر با حداقل ضریب تضعیف ۸۰ دسی بل در باند فرکانسی مربوط باشند.	*	-	-
۲	تمامی منافذ اتاق‌های شیلد شده، دارای فیلترهای حذف سیگنال الکترومغناطیسی با حداقل ضریب تضعیف ۶۰ دسی بل باشند. منافذ ذکر شده شامل تمام لوله‌های ورودی نظیر لوله‌های سیستم تهویه، سرمایشی/گرمایشی و تخلیه گاز می‌باشد. هم‌چنین تمامی خطوط منابع تغذیه، خطوط تلفنی، خطوط کنترلی و خطوط داده، در محل ورود به محفظه شیلد دارای فیلتر با حداقل ضریب تضعیف ۶۰ دسی بل در باند فرکانسی مربوطه باشند.	-	*	-
۳	تمامی منافذ اتاق‌های شیلد شده، دارای فیلترهای حذف سیگنال الکترومغناطیسی با حداقل ضریب تضعیف ۴۰ دسی بل باشند. منافذ ذکر شده شامل تمام لوله‌های ورودی نظیر لوله‌های سیستم تهویه، سرمایشی/گرمایشی و تخلیه گاز می‌باشد. هم‌چنین تمامی خطوط منابع تغذیه، خطوط تلفنی، خطوط کنترلی و خطوط داده، در محل ورود به محفظه شیلد دارای فیلتر با حداقل ضریب تضعیف ۴۰ دسی بل در باند فرکانسی مربوطه باشند.	-	-	*
۴	تمام فیلترهای قدرتی و مخابراتی، به ویژه فیلترهای منابع تغذیه، باید مجهز به سیستم‌های حفاظت کننده حالت گذرا (نظیر سرج ارستر) باشند.	*	*	*
۵	کلیه کابل‌ها و لوله‌های ورودی در محل ورود به اتاق شیلد باید داخل لوله موجبری با مشخصات تعیین شده طبق استاندارد MIL-STD-188-125-1 قرار گیرند. هم‌چنین، فاصله بین کابل‌ها و بدنه موجبر با فیلر پر شود.	*	*	○

ردیف	۳-۳ الزامات و ملاحظات فیلترینگ	سطح بندی مراکز داده		
		حیاتی	حساس	مهم
۶	تا حد امکان خطوط داده و صوتی، قبل از رسیدن به سازه شیلد به فیبر نوری تبدیل شوند و از طریق لوله موجبری طبق بند ۳-۳-۵ وارد اتاق شیلد شوند. هم‌چنین، تمامی خطوط کنترلی (نظیر کنترل تهویه و...) قبل از ورود به شیلد، مجهز به فیلتر مناسب (حذف کننده حالت گذرا) باشند.	*	*	○
۷	هنگام آزمون تشعشعی، در صورتی که اتاق هنوز عملیاتی نشده، تنها منافذ مربوط به لوله‌های آب، مجاز به پوشانده شدن با فویل آلومینیوم است و منافذی که محل عبور کابل‌های مختلف است، باید کابل مربوطه عبور داده شود و حد فاصل کابل و لوله با فیلر پر شود.	*	*	*

ردیف	۳-۴ الزامات و ملاحظات ارتینگ	سطح بندی مراکز داده		
		حیاتی	حساس	مهم
۱	به منظور مقاومت مرکز داده در مقابل رعد و برق و اختلالات تغذیه ضروری است مبنای اهمی سیستم زمین مطابق با کمینه اعلامی برای تجهیزات در نظر گرفته شود. حداکثر مقدار مقاومت مجاز زمین با دستگاه ارت سنج، ۲ اهم است. در صورتی که بر اساس مشخصات تجهیزات به کار رفته، تشخیص داده شود که مقدار کم‌تری مورد تأیید است، مقدار مقاومت مجاز زمین، به مقدار جدید تقلیل می‌یابد.	*	*	*
۲	برای تأمین زمین مناسب برای کابینت‌ها، هر کابینت یک تسمه جدا جهت اتصال به زمین اصلی داشته باشد. سپس، تسمه زمین هر کابینت به یک تسمه اصلی متصل به بدنه محفظه شیلد وصل شود و در نهایت با کابل مسی به چاه زمین ختم گردد. به علاوه ضروری است اتصالات تسمه‌ها و پیچ‌های استفاده شده نیز مسی باشند.	*	*	○
۳	اتصال زمین اتاق کامپیوتر (سرور و شبکه) از سایر اتصالات زمین، به ویژه اتصال زمین برق تفکیک شود. و طراحی بر اساس ملاحظات استاندارد MIL-STD-188-124 انجام گردد.	*	*	*
۴	لوله‌های فلزی ورودی به فضای شیلد، قبل و بعد از شیلد به زمین متصل گردند.	*	*	○
۵	کابل‌های داده که در زیر کف کاذب قرار می‌گیرند، در سینی‌های فلزی جای داده شوند که به سیستم زمین متصل است. مسیردهی به کابل‌های زیر کف باید با توجه به دیگر سیستم‌هایی که آن‌جا قرار دارند، برنامه ریزی شود.	*	*	○
۶	به منظور ایجاد شیلد ذاتی در سازه بتون آرمه، پیشنهاد می گردد کلاف های آرماتورهای سقف و دیواره ها به هم وصل شوند تا یک قفس فارادی ایجاد شود.	*	○	○

فصل چهارم

الزامات و ملاحظات پدافند کالبدی

مقدمه

طبق تئوری «واردن» مراکز داده در دومین حلقه از حلقه‌های دفاعی یک کشور قرار می گیرند و از مهمترین زیرساخت‌ها در جامعه دانایی محور، زیرساخت‌های ارتباطی و اطلاعاتی می‌باشند. لذا برای ایجاد و توسعه استراتژی، باید بخش کالبد مراکز داده آسیب ناپذیر یا انعطاف پذیر باشند. با توجه به امکان گسترش حملات تروریستی و خرابکارانه در تمام زیرساخت‌های حیاتی، حساس و مهم کشور و اهمیت مرکز داده و با توجه به بالا رفتن حجم مبادلات داده بین کاربرها نیاز مبرمی به مراکزی که بتوانند مدیریت، نگهداری و امنیت اطلاعات را تضمین کنند وجود دارد . از طرفی ایجاد ساختار تدافعی لایه به لایه و لحاظ اقدامات پیش‌بینانه و پیشگیرانه و در نظر گرفتن اقدامات واکنشی، میزان تلفات را هنگام وقوع بحران به حداقل می رساند. کاهش آسیب‌پذیری یک مرکز داده مستلزم شناخت کامل از آن، نوع کاربری، رصد و پایش تهدیدات (متناسب با نحوه عملکرد، مکان نصب و سطح کاربری یک مرکز داده) می‌باشد و جهت محقق شدن این امر، نیاز به رعایت الزامات حوزه پدافند کالبدی در تمام بخش های تخصصی با شناخت تهدیدات و پیش بینی راهکارهای مناسب برای تداوم فعالیت در زمان بحران، مکان یابی مناسب (مکان یابی سایت اصلی و مکان یابی در سایت انتخاب شده)، طراحی معماری پایدار متناسب با عملکرد (مسیرهای دسترسی، فضاهای باز و نوع پوشش، شبکه های زیر ساختی و ...)، طراحی و محاسبه سازه ای مستحکم، طراحی تاسیسات مکانیکی و الکتریکی و حفاظت فیزیکی مناسب، مطابق با دانش روز و با رعایت ضوابط پدافند غیرعامل می باشد.

۱-۴- الزامات و ملاحظات مکان یابی

مکان یابی فرایندی است که از طریق آن می توان بر اساس شرایط تعیین شده و با توجه به منابع و امکانات موجود، بهترین محل مورد نظر برای یک فعالیت را تعیین کرد. از طرفی اولین گام برای مصون سازی و کاهش آسیب پذیری مرکز داده جدیدالاحداث، انتخاب مکان مناسبی است که با توجه به محدودیت ها و قابلیت های طرح، شرایط لازم برای به حداقل رساندن تهدیدات انسان ساخت و آسیب پذیر را داشته باشد..

در این بخش الزامات و ملاحظات مکان یابی مراکز داده با رویکرد پدافند غیرعامل در قالب جدول شماره ۱-۴ ارائه می شود.

ردیف	۱-۴- الزامات و ملاحظات مکان یابی	سطح بندی مراکز داده			
		حیاتی	حساس	مهم	گروه ۴،۳
۱	الزامات و ملاحظات مندرج در سند " آئین نامه ضوابط پدافند غیرعامل در مکان یابی مراکز حیاتی و حساس" ابلاغی سازمان پدافندغیرعامل کشور رعایت شود.	*	*	○	۴،۳
۲	از قرار نداشتن مجموعه در پهنه‌های مواجه با سوانح طبیعی از قبیل گسل ها و مسیل ها اطمینان حاصل شود.	*	*	*	۴،۳
۳	کاربری های همجوار با سایت باید دارای شرایط ذیل باشد: ● عدم احداث یا ایجاد مراکز داده در مجاورت کاربری‌های ناسازگار و خطرزا از قبیل، شیمیایی، میکروبی، پرتوی، امواج الکترومغناطیسی، انفجاری ● رعایت فاصله مناسب از منابع تشعشع امواج الکترومغناطیس نظیر ایستگاه‌های انتقال برق، خطوط برق فشار قوی، رادارهای فرودگاهی و نظامی، ایستگاه‌های فرستنده رادیویی و تلویزیونی ● عدم احداث مرکز داده در مجاورت اهداف جذاب برای دشمن اعم از مراکز حیاتی، حساس و مهم و مراکز نظامی	*	*	*	همه موارد
۴	مرکز داده حداقل دارای دو مسیر دسترسی امن، کاملا مجزا و مستقل باشد.	*	*	*	۴،۳

ردیف	۴-۱- الزامات و ملاحظات مکان یابی	سطح بندی مراکز داده			
		حیاتی	حساس	مهم	گروه
۵	مراکز داده همجوار با مراکز جمعیتی مانند نمایشگاه ها محل کنفرانس ها، کانون تجمعات و اعتراضات نباشند.	*	*	*	۴.۳
۶	محل احداث مرکز داده باید قابلیت تامین زیرساخت برق رسانی از دو پست اصلی برق بصورت مستقل را داشته باشد.	*	*	○	۴.۳
۷	در انتخاب محل مرکز داده استفاده از شرایط طبیعی زمین اعم از توپوگرافی و پوشش گیاهی برای ایجاد محدودیت دید و تیر دشمن، مورد توجه قرار گیرد.	*	*	*	۴.۳
۸	محل مرکز داده طوری انتخاب گردد که ارائه خدمات توسط نیروی انتظامی، آتش نشانی و اورژانس به مرکز داده در اسرع وقت میسر باشد.	*	*	○	۴.۳
۹	زمین محل احداث، وسعت کافی جهت پراکنده سازی مستحدثات و تجهیزات همچنین توسعه آتی را داشته باشد.	*	*	*	۴.۳
۱۰	برای احداث مرکز داده در مناطق مرزی، فاصله مناسب از مرز با نظرخواهی از دستگاه های امنیتی استان رعایت شود.	*	*	○	۴.۳
۱۱	مکان مرکز داده از حیث وجود سابقه ناامنی و اغتشاشات و همچنین فعالیت گروهک ها و سازمان های معاند ارزیابی شود.	*	*	*	۴.۳

۲-۴- الزامات و ملاحظات طراحی محوطه

ایجاد ایمنی حداکثری، ، امنیت و پایداری مجموعه(سایت) یا ساختمانی که مرکز داده در آن واقع شده است امری ضروری است به نحوی که با ادغام شکل، فرم و عملکرد برای رسیدن به تعادل در میان عناصر طراحی و ایجاد امنیت هماهنگ باشد.

ردیف	۲-۴ الزامات و ملاحظات طراحی محوطه	سطح بندی مراکز داده			
		حیاتی	حساس	مهم	گروه
۱	به منظور مصون سازی و کاهش آسیب پذیری ها، محوطه مراکز داده که ظرفیت حملات تروریستی بواسطه عوارض طبیعی و مصنوعی را دارا می‌باشند، باید مورد مطالعه و طراحی واقع گردد.	*	*	*	۴،۳
۲	مسیرها و معابر مرتبط با مراکز داده قابلیت پاسخگویی در مواقع اضطراری برای تخلیه، تردد خودروهای آتش نشانی و امدادی را داشته باشند.	*	*	*	۴،۳
۳	در فضای پیرامونی مراکز داده و محوطه، از موانع بتنی، راه بند، مبلمان شهری (نیمکت، گلدان و ...) قبل از ورود به سایت و محوطه تا مکان مرکز داده برای مقابله با عملیات تروریستی و خرابکارانه توسط خودروی انتحاری استفاده شود.	*	*	*	۴،۳
۴	به منظور افزایش ضریب امنیتی در طراحی عرض ورودی و خروجی ها و دسترسی ها، افزایش سطح امنیتی سایت مورد نظر قرار گیرد.	*	*	*	۴،۳
۵	درب ورودی محوطه به طور مستقیم در امتداد ورودی ساختمانی که مرکز داده در آن قرار دارد، نباشد.	*	*	*	۴،۳
۶	فضای مشخص و مناسب برای بازرسی خودروها قبل از ورود به محوطه سایت مرکز در نظر گرفته شود.	*	*	*	۴،۳
۷	سر درب و کلیه ملحقات ورودی به نحوی طراحی و ساخته شوند که امکان ریزش اجزای آنها و انسداد مسیر در اثر عملیات تروریستی و خرابکارانه وجود نداشته باشد.	*	*	*	۴،۳
۸	کلیه اجزا و دارایی های سایت از حیث اهمیت دسته بندی شده و متناسب با سطح اهمیت حفاظت شوند.	*	*	*	۴

ردیف	۴-۲ الزامات و ملاحظات طراحی محوطه	سطح بندی مراکز داده			
		حیاتی	حساس	مهم	گروه
۹	به منظور جلوگیری از تمرکز دارائی‌ها پراکندگی مناسب دارایی‌ها در محوطه سایت صورت پذیرد.	*	*	*	۴
۱۰	در طراحی محوطه و معابر با جانمایی مناسب عناصر معماری نظیر؛ پوشش گیاهی و آب نما، دسترسی به ساختمان اصلی مرکز داده کانالیزه و کنترل شود.	*	*	*	۴،۳
۱۱	هرگونه احداث و یا ایجاد پارکینگ در ساختمان مرکز داده ممنوع می باشد. (بویژه در طبقات فوقانی و تحتانی)	*	*	○	۳،۲،۱
۱۲	پارکینگ خودروهای سواری سبک از مرکز داده حداقل ۱۵ متر فاصله داشته باشد.	*	*	*	۴،۳
۱۳	ساختمان مرکز داده در امن ترین قسمت سایت با فاصله ایمن از بخش های دارای خطر بالقوه نظیر؛ ایستگاه گاز، مخازن سوخت، ورودی ها، تردد خودروها، انبارها و محل تعمیر و نگهداری باشد.	*	*	*	۴،۳
۱۴	در مراکز موجود، در صورت رعایت نشدن فواصل ایمن، انجام اقدامات مهندسی اعم از احداث دیوار، موانع و استحکامات و در صورت عدم کفایت راه کارهای مذکور، جابه جایی مرکز داده الزامی است.	*	*	*	۴،۳
۱۵	در صورت وجود اشرافیت بر مراکز داده موجود، با تمهیدات لازم و روش های ممکن نظیر کاشت درخت، این اشرافیت مرتفع گردد.	*	*	○	۴،۳
۱۶	فضاهای باز محوطه با تمهیدات لازم به گونه‌ای طراحی و اجرا شود که قابلیت بهره داری در شرایط بحرانی و اضطراری را داشته باشند.	*	*	○	۴،۳

۴-۳ الزامات و ملاحظات معماری

آرایش فضاهای ساختمانی و نحوه ارتباط آنها می تواند زمینه ساز بهبود عملکرد مرکز و کاهش آسیب پذیری آن گردد. تعیین طرح هندسی بنا، موقعیت بازشوها، نحوه دسترسی ها، ضریب اطمینان بالای فضاها در شرایط عادی و بحران جهت مدیریت آسان، کاهش اثر و افزونگی خرابی مواردی هستند که باید مورد توجه قرار گیرد. در این بخش از سند الزامات و ملاحظات معماری با رویکرد پدافند غیرعامل در قالب بخش ۳-۴ ارائه می شود.

ردیف	۴-۳ الزامات و ملاحظات معماری	سطح بندی مراکز داده			
		حیاتی	حساس	مهم	گروه
۱	رعایت ضوابط معماری طراحی ساختمان ذیل بند ۲۱-۲-۳ مقررات ملی ساختمان مبحث ۲۱ (ویرایش سال ۱۳۹۵) الزامی است.	*	*	*	۳.۲.۱
۲	حجم و نمای ساختمان مرکز داده همگون و حتی الامکان مشابه سایر ساختمان های همجوار باشد و براحتی قابل تشخیص از دیگر ساختمان ها نباشد. (نمای ساختمان مرکز داده معرف عملکرد ساختمان نباشد)	*	*	*	۴.۳
۳	در طراحی معماری ساختمان مرکز داده، فضاهای دارای اهمیت بیشتر با اقداماتی نظیر فاصله گرفتن از پوسته و استقرار در هسته مرکزی ساختمان، ورودی از بخش های دارای خطر آتش سوزی و... و قرارگرفتن در موقعیت و محلی که دارای حداقل تردد است، از سطح حفاظتی امن تر بالاتر از سایر فضاها برخوردار شوند.	*	*	*	۳.۲.۱
۴	تعداد و اندازه پنجره‌ها در نمای ساختمان، محدود و میزان سطوح شیشه‌ای نما حداکثر ۱۵ درصد سطح کل نما باشد.	*	*	*	۳.۲
۵	در صورت جانمایی مرکز داده در طبقات منفی، دسترسی مجزا برای آن در نظر گرفته شود.	*	*	*	۳.۲.۱
۶	ورودی ها و خروجی های ساختمان مرکز داده به طور خاص و مجزا قابل کنترل باشد.	*	*	*	۳.۲
۷	ورودی ساختمان مرکز داده به نحوی جانمائی و طراحی شود که اثرات موج انفجار را به حداقل برساند.	*	*	*	۳.۲
۸	اتاق سرور مرکزی دارای پنجره ای به خارج و خروجی مستقل از ساختمان نداشته باشد.	*	*	*	همه گروه ها
۹	دیوارهای جدا کننده اتاق سرور از بخش های دیگر، دارای مقاومت حداقلی ۲ ساعت در برابر حریق باشند.	*	*	*	همه گروه ها
۱۰	مصالح مصرفی ساختمان با رعایت اصل هزینه فایده، در برابر حریق و جاذب انرژی، مقاوم باشند.	○	○	○	همه گروه ها

۴-۴- الزامات و ملاحظات سازه

با توجه به لزوم پایداری سازه، ساختمان مرکز داده لازم است مقاومت لازم دربرابر بارهای انفجاری را داشته باشد تا سطح عملکرد مورد نظر تامین شود. در این بخش از سند، صرفا الزامات کلیدی ارائه شده است، لذا برای طراحی جزئیات، استفاده از کتب و منابع علمی معتبر داخلی و خارجی توصیه می گردد.

ردیف	۴-۴ الزامات و ملاحظات سازه	سطح بندی مراکز داده			
		حیاتی	حساس	مهم	گروه
۱	برای طراحی سازه مراکز داده انجام مطالعات تهدیدشناسی به منظور تعیین سناریوهای محتمل تهدید و سلاح معیار در طراحی الزامی است.	*	*	*	همه گروه‌ها
۲	استفاده از ساختمان‌های موجود به عنوان مرکز داده، منوط به انجام مطالعات و اثبات پایداری و استحکام بنا برای مراکز داده و در صورت لزوم مقاوم سازی ساختمان در برابر سلاح معیار بر مبنای سطح عملکرد مربوط است.	*	*	*	همه گروه‌ها
۳	در سازه‌های سطحی، تخریب پیش رونده در اثر تخریب موضعی و یا حذف المان‌های اصلی سازه در طراحی سازه کنترل شود.	*	*	*	همه گروه‌ها
۴	مبنای سطح عملکرد ساختمان مرکز داده در برابر انفجار، مطابق بند ۲۱-۱-۷ مبحث ۲۱ مقررات ملی ساختمان (ویرایش سال ۱۳۹۵) است که در سطح بی وقفه برای مبنای طراحی مورد استفاده قرار گیرد.	*	*	-	همه گروه‌ها
۵	سطح عملکرد ساختمان مرکز داده در برابر انفجار، مطابق بند ۲۱-۱-۷ مبحث ۲۱ مقررات ملی ساختمان (ویرایش سال ۱۳۹۵) در سطح ایمنی جانی مبنای طراحی قرار گیرد.	-	-	*	همه گروه‌ها
۶	در صورت برآورده نشدن سطح عملکرد بدون وقفه در برابر سلاح معیار، به منظور تحقق میزان حفاظت زیاد وخسارت سطحی ساختمان و سازه مرکز داده به صورت مدفون یا زیرزمینی احداث شود.	*	O	-	همه گروه‌ها

ردیف	۴-۴ الزامات و ملاحظات سازه	سطح بندی مراکز داده			
		حیاتی	حساس	مهم	گروه
۷	در خصوص سازه زیرزمینی، عمق (ارتفاع روباره) بر اساس میزان نفوذ سلاح معیار و مدل سازی تاثیر انفجار بر سازه با ضریب اطمینان ۱ تا ۱,۵ تعیین گردد.	*	○	-	همه گروه‌ها
۸	با توجه به دو عامل مقاومت در برابر آتش و کاهش اثرات بارهای دینامیکی، استفاده از اسکلت بتنی ارجحیت دارد.	○	○	○	۴و۳،۲،۱
۹	در سازه های دارای اسکلت فلزی از اتصالات پیچ و مهره ای استفاده گردد.	○	○	○	همه گروه‌ها
۱۰	استفاده از وسایل مکانیکی مانند جداسازها و میراگرها که باعث افزایش استهلاک انرژی می شوند، برای سامانه های سازه‌ای مقاوم در مقابل انفجار توصیه می شود.	○	○	○	همه گروه‌ها
۱۱	در ساختمان های موجود، فضاهای مجاور دیوارهای برشی، طبقات منفی و فضای امن ساختمان (در صورت وجود) برای ایجاد مرکز داده از نظر سازه‌ای ارجحیت داشته و توصیه می شوند.	○	○	○	همه گروه‌ها

۵-۴- الزامات و ملاحظات تاسیسات برقی و مکانیکی

یکی از مهم ترین و حساس ترین بخش های کالبدی و ساختمانی به منظور تداوم عملکرد مراکز داده، تاسیسات برقی و مکانیکی مربوط به ساختمان مرکز داده است. در طراحی یک مرکز داده امن با توجه به سطح اهمیت آن، سیستم برق باید به نحوی تامین و توزیع شود که احتمال قطع برق تجهیزات، حتی در شرایط بحران به کمترین حد ممکن برسد و به موازات آن در حوزه ی تأسیسات مکانیکی، کاهش آسیب پذیری و استمرار فعالیت سامانه ها مورد توجه قرار گیرد. این تاسیسات باید در درجه اول آسیب جدی نبینند و در صورت آسیب دیدگی، قابل مرمت باشند و در نهایت نیز بر اثر آسیب دیدگی و تخریب تاسیسات، تلفات جانی حداقل باشد. بنابر این ملاحظات و الزامات مندرج در بخش ۵-۴ در طراحی، اجرا و بهره برداری مناسب تأسیسات برقی و مکانیکی ارائه شده است.

ردیف	۵-۴ الزامات و ملاحظات تاسیسات برقی و مکانیکی	سطح بندی مراکز داده			
		حیاتی	حساس	مهم	گروه
۱	الزامات و ملاحظات تاسیسات برقی و مکانیکی ذیل فصل ۲۱-۷ مبحث ۲۱ مقررات ملی ساختمان (ویرایش سال ۱۳۹۵) برای ساختمان مراکز داده لازم الاجرا است.	*	*	*	همه گروه ها
۲	در مورد انشعابات و خطوط انتقال انرژی، آب، برق، ارتباطات و ... موارد ذیل رعایت شود: - از کمترین علائم شناسایی استفاده شود. - بصورت مدفون زیر خاک و یا محصور در محفظه اجرا شوند. - در جانمایی آنها به عدم تمرکز و اثرات تخریبی متقابل توجه شود.	*	*	*	همه گروه ها
۳	انرژی الکتریکی مورد نیاز مرکز داده باید از دو پست برق مجزا تأمین شود و همچنین سیستم ژنراتور و UPS آن باید N +1 باشد. (برای مرکز حیاتی باید ۳ پست مجزا باشد)	*	*	*	همه گروه ها
۴	مولدهای برق، ژنراتورها و محل استقرار ترانسفورماتورها در مکان سرپوشیده یا در فضای زیرزمینی باشند.	*	*	*	همه گروه ها
۵	مولدهای برق، ژنراتورها و ترانسفورماتورها بصورت غیر متمرکز و در نواحی مختلف قرار گیرند.	*	*	*	همه گروه ها
۶	حداقل توان UPS با در نظر گرفتن باطری‌های داخلی آن برای مدت ۷ الی ۱۵ دقیقه (باتوجه به زمان به کار افتادن مولد برق و ژنراتور) درنظر گرفته شود.	*	*	*	همه گروه ها
۷	میزان توان مولد برق (ژنراتور) می‌بایست ۱۵% بیشتر از توان UPS درنظر گرفته شود و درهنگام کار باید ۷۰% زیربار باشد.	*	*	*	همه گروه ها

ردیف	۵-۴ الزامات و ملاحظات تاسیسات برقی و مکانیکی	سطح بندی مراکز داده			
		حیاتی	حساس	مهم	گروه
۸	میزان سوخت ذخیره شده برای مولدهای برق (ژنراتورها) حداقل ۷۲ ساعت کارکرد، در بار کامل مرکز داده لازم است.	*	*	*	همه گروه ها
۹	محل قرارگیری مخزن ذخیره سوخت باید به اندازه کافی دور از مولد برق (ژنراتور) و حتی المقدور بصورت مدفون جانمائی شده باشد. از مخزن ذخیره سوخت نیز همانند دستگاه مولد برق (ژنراتور) محافظت گردد.	*	*	*	همه گروه ها
۱۰	محل مخازن ذخیره سوخت، دارای فاصله ایمن از ساختمان اصلی مرکز داده و موتورخانه باشد.	*	*	*	همه گروه ها
۱۱	تابلوهای اصلی مرکز باید از درجه حفاظت (IP۵۴) برخوردار باشند (به منظور حفاظت در برابر تهدیدات گرافیتی).	*	*	*	همه گروه ها
۱۲	کانال و مسیر عبور استاندارد کابلی توکار برای اتاق سرور اجرا شود. کانال های مذکور دارای درپوش مناسب بوده و برای جلوگیری از اختلال در دادهٔ بین مسیر کابل های داده (Data) و برق فاصله ایجاد نماید.	*	*	*	همه گروه ها
۱۳	روکش تمامی سیم ها و کابل ها از نوع بدون دود و بدون هالوژن(LSZH) انتخاب شوند.	*	*	*	همه گروه ها
۱۴	در صورت از کار افتادن روشنایی اصلی، علائم و چراغ های اضطراری به گونه ای جانمایی شوند که تسهیل کننده خروج اضطراری باشند.	*	*	*	همه گروه ها

ردیف	۵-۴ الزامات و ملاحظات تاسیسات برقی و مکانیکی	سطح بندی مراکز داده			
		حیاتی	حساس	مهم	گروه
۱۵	چراغ های روشنایی و قاب و اتصالات آن شکننده نبوده و دارای جنس نرم و انعطاف پذیر باشند.	*	*	*	همه گروه ها
۱۷	سیستم تهویه مطبوع مرکز داده بر اساس بالاترین ظرفیت مورد نیاز با پیش بینی توسعه فضاها و تجهیزات در آینده طراحی شود.	*	*	*	همه گروه ها
۱۸	سامانه تخلیه هوای اتاق های باطری و UPS مراکز داده، برای جلوگیری از اختلاط هوای اگزاست آن با هوای اگزاست تهویه عمومی، مستقل باشد.	*	*	*	همه گروه ها
۱۹	کلیه تاسیسات مراکز داده مستقل از ساختمان های مجاور طراحی شود. البته می توان به عنوان سیستم جایگزین در مواقع بحران از آنها نیز استفاده نمود.	*	*	*	همه گروه ها
۲۰	سیستم سرمایش و دفع حرارت رک ها، مانیتورها و سایر تجهیزاتی که نیاز به دفع حرارت دارند باید مستقل از سیستم تهویه مطبوع ساختمان مرکز داده طراحی گردد.	*	*	*	همه گروه ها
۲۱	وجود و نصب هرگونه انشعاب گاز حتی جهت اجاق گاز آبدارخانه در داخل مراکز داده ممنوع است.	*	*	*	همه گروه ها
۲۲	پریزهای اتاق سرور نباید از یک پانل یا از یک فاز مشترک با تجهیزات شبکه و سرورها استفاده کند.	*	*	*	همه گروه ها

ردیف	۵-۴ الزامات و ملاحظات تاسیسات برقی و مکانیکی	سطح بندی مراکز داده			
		حیاتی	حساس	مهم	گروه
۲۳	استفاده از سیستم سرمایش و گرمایش آبی در مراکز داده ممنوع می باشد.	*	*	*	همه گروه ها
۲۴	ایجاد سامانه سرمایش موازی برای مراکز داده الزامی است.	*	*	*	همه گروه ها
۲۵	تاسیسات و تجهیزات مکانیکی و برقی و قطعات مربوط تولید داخلی کشور بوده تا سهولت در راه اندازی و بهره برداری و همچنین تعمیرات و نگهداری آنها میسر گردد.	*	*	*	همه گروه ها
۲۶	در تأمین تجهیزات و قطعات الکتریکی مورد نیاز، به یکسان بودن نماد تجاری (برند) و حتی المقدور ظرفیت تجهیزات توجه شود تا در صورت اضطرار بتوان از هر یک از آنها به جای قطعه یا تجهیز معیوب استفاده نمود.	*	*	*	همه گروه ها
۲۷	طراحی و اجرای سامانه های مدیریت هوشمند تاسیسات ساختمان، با رعایت الزامات امنیتی، توسط شرکت های غیر وابسته به بیگانه انجام شود.	*	*	*	همه گروه ها
۲۸	ورود هوای تازه به هواساز مراکزداده از سطح معابر، گذرگاه‌ها و کلیه اماکن دارای احتمال فروریزش آوار یا دسترسی غیرمجاز ممنوع است. در صورت اضطرار بایستی تمهیدات اجرایی لازم پیش بینی شود.	*	*	*	همه گروه ها
۲۹	در مراکز داده زیرزمینی، تعبیه فن فشار مثبت و اگزاست فن جهت خارج کردن دود الزامی است.	*	*	*	۳
۳۰	سیستم اعلام حریق قابلیت جداسازی نواحی را با استفاده از نصب حسگرهای مناسب، داشته باشد.	*	*	*	همه گروه ها

ردیف	۵-۴ الزامات و ملاحظات تاسیسات برقی و مکانیکی	سطح بندی مراکز داده			
		حیاتی	حساس	مهم	گروه
۳۱	در اتاق سرور مراکز داده که افرادی در آن مستقر نیستند استفاده از گاز منواکسید کربن(CO_2) جهت اطفاء حریق بلامانع است ولیکن در سایر مکان‌های مراکز داده که کارکنان در آن مستقرند از گازهای دیگر (نظیر هالوکربن، FM 200، آیروسل یا آرگونایت) با توجه به سهولت شارژ کپسول در بازار داخلی، به عنوان گاز اطفاء حریق مناسب استفاده شود.	*	*	*	همه گروه‌ها
۳۲	استفاده از آب به عنوان عامل اطفاء حریق مطلقاً ممنوع است.	*	*	*	همه گروه‌ها
۳۳	به منظور هشدار و اخطار بموقع به ساکنین ساختمان مرکز داده درهنگام تهدید، ساختمان دارای سیستم اطلاع رسانی و زنگ خطر باشد.	*	*	*	همه گروه‌ها
۳۴	خط تلفن اضطراری مجزا از سیستم تلفن بطور مستقیم به ایستگاه مرکزی کنترل و نظارت متصل شود.	*	*	*	همه گروه‌ها
۳۵	محل قرار گیری تجهیزات برقی و مکانیکی مرکز داده در برابر دسترسی افراد غیر مجاز محافظت شود.	*	*	*	همه گروه‌ها
۳۶	بازرسی‌های دوره‌ای و امور مربوط به نگهداری و تعمیر (نت) تاسیسات و تجهیزات برقی و مکانیکی در دوره‌های زمانی روزانه، هفتگی، ماهانه و سالانه به صورت مرتب صورت پذیرد.	*	*	*	همه گروه‌ها
۳۷	نصب سامانه سنجش، تشخیص و اعلام دود، حریق، حرارت و رطوبت در اتاق سرور الزامی است.	*	*	*	همه گروه‌ها

ردیف	۵-۴ الزامات و ملاحظات تاسیسات برقی و مکانیکی	سطح بندی مراکز داده			
		حیاتی	حساس	مهم	گروه
۳۸	نقشه های تأسیسات برقی و مکانیکی مرکز داده در محل مناسب و امن نگهداری شده و در صورت تغییر، به روز رسانی گردند تا در شرایط لازم قابل استفاده باشند.	*	*	*	همه گروه ها
۳۹	در اتاق های سرور ایجاد فشار مثبت به جهت جلوگیری از ورود آلاینده ها به داخل فضا الزامی است.	*	*	*	همه گروه ها
۴۰	عبور لوله های آب و فاضلاب داخل و یا محیط پیرامونی از داخل یا پیرامون مرکز داده ممنوع است.	*	*	*	همه گروه ها
۴۱	در صورت امکان تجهیزات هواساز که احتمال خرابی بیشتری دارند (مانند فن، الکتروموتور و امثال آن) برای جایگزینی بدون وقفه به صورت دو یا چندگانه محاسبه، طراحی و نصب شود.	*	*	*	همه گروه ها
۴۲	جعبه های تقسیم و ترمینال ها از نوع مقاوم در برابر حریق، ضربه، ضد جرقه و اثر موج انفجار باشند.	*	*	○	همه گروه ها
۴۳	تمهیدات لازم جهت حفاظت از تاسیسات و تجهیزات مرتبط با اتاق سرور نظیر هواساز و اگزاست فن انجام گردد.	*	*	○	همه گروه ها
۴۴	در هواساز مراکز داده علاوه بر فیلترهای معمول از فیلترهای ویژه (Hepa) جهت جذب ذرات میکروبی و شیمیایی در وضعیت بحران استفاده گردد.	*	*	○	همه گروه ها

۶-۴ -الزامات و ملاحظات حفاظت فیزیکی

مراکز داده از اهداف مورد توجه دشمنان برای ایجاد اختلال و وقفه در عملکرد شان به شمار می آید، بدین منظور رعایت اصول، الزامات و ملاحظات حفاظت فیزیکی برای جلوگیری از تهدیدات امنیتی امری ضروری است.

ردیف	۶-۴ -الزامات و ملاحظات حفاظت فیزیکی	سطح بندی مراکز داده			
		حیاتی	حساس	مهم	گروه
۱	دسترسی سلسله مراتبی به بخش های مختلف رعایت شود و افراد و خودروهای مجاز صرفا امکان تردد در بخش های تعریف شده را داشته باشند.	*	*	*	۴،۳
۲	دوربین ها و سنسورهای حفاظتی تصویر، صدا، حرکت، حرارت (مادون قرمز) محوطه و دیوار پیرامونی را پوشش داده و تصاویر ضبط شده و مرتبا کنترل شوند.	*	*	*	۴،۳
۳	نخستین ورودی ساختمان توسط نگهبان محافظت شده و کارمندان هر بخش از همدیگر مجزا شوند.	*	*	*	۴،۳
۴	سیستم های قفل گذاری و کنترل های دسترسی و تعیین اعتبار بر اساس بیومتریک (اثرانگشت، شبکیه یا عنبیه چشم، صدا، چهره و شکل هندسی دست و غیره) مورد استفاده قرار گیرد.	*	*	*	همه گروه ها
۵	همجواری محوطه در قالب محدوده کنترل شده تحت نظارت بوده و حفاظت از آن پایش تصویری مستمر انجام گیرد.	*	*	O	۴،۳
۶	ورود پیاده و سواره به محوطه، بطور همزمان با سامانه های هوشمند و حفاظت فیزیکی کنترل شود.	*	O	O	۴،۳
۷	عدم نصب تابلو موقعیت و کارکرد و همچنین در نظر گرفتن کاربری پوششی برای مراکز داده حیاتی الزامی است.	*	*	O	۴،۳
۸	دیوارهای پیرامونی دارای حداقل ارتفاع ۲/۵ متر و مقاومت کافی در برابر تهدیدات برآورد شده باشند.	*	*	O	۴،۳

Passive Defense Requirements And Considerations For Data Center

سازمان پدافند غیر عامل کشور
معاونت طرح ریزی و نظارت فنی

قیمت: ۱۵۰۰۰ تومان