جمهوری اسلامی ایران

فرماندهی کل قوا

کمیته دائمی پدافند غیرعامل کشور

شماره: ۱/۲۹۳۱/ک ۱۶۰

تاریخ: ۱۴۰۲/۰۸/۲۲

بسم الله الرحمن الرحیم

« مسئله پدافند غیرعامل مسئله بسیار مهمی است و هر روزی که می‌گذرد بر اهمیت پدافند غیرعامل افزوده می‌شود، یعنی شیوه‌های تهاجم دشمنان به نحوی است که پدافند در مقابل آنها در قالب پدافند غیرعامل کاملا پیچیده و مهم و علمی و همه جانبه است. »

مقام معظم رهبری و فرماندهی کل قوا (مدظله العالی) - ۱۳۹۷/۰۸/۰۶

« کارگروه (کمیته) دائمی پدافند غیرعامل کشور به ریاست رئیس ستاد کل نیروهای مسلح بالاترین مرجع تصمیم گیری در حوزه پدافند غیرعامل کشور است که تصمیمات آن با ابلاغ رئیس کارگروه مزبور، برای همه دستگاه‌های لشکری، کشوری، بخش دولتی و عمومی غیردولتی لازم الاجراست. . . . »

قانون تشکیل سازمان پدافند غیرعامل کشور - ۱۴۰۲/۰۶/۱۲

تصویب‌نامه

"با صلوات بر محمد و آل محمد و احترام"

وزارت کشور – وزارت دفاع و پشتیبانی نیروهای مسلّح – وزارت اطلاعات
معاون هماهنگ‌کننده ستاد کل نیروهای مسلح– سازمان برنامه و بودجه کشور
وزارت ارتباطات و فناوری اطلاعات – وزارت راه و شهرسازی – سازمان پدافند غیرعامل کشور

به استناد تبصره۱ قانون تشکیل سازمان پدافند غیرعامل کشور مصوب مجلس شورای اسلامی و ماده۸ اساسنامه این سازمان- مصوّب مقام‌معظّم رهبری- هفتادوهفتمین جلسه کارگروه (کمیته) دائمی پدافند غیرعامل کشور در تاریخ ۱۴۰۲/۰۶/۲۸ تشکیل گردید و پیشنهاد آن سازمان با موضوع نظام فنی‌وتخصصی حفاظت از زیرساخت‌های کشور را بررسی و به‌شرح‌زیر تصویب‌نمود؛

نظام فنی و تخصصی حفاظت از زیرساخت‌های کشور

مقدمه

پیاده‌سازی و اجرای دقیق طرح راهبردی حفاظت از زیرساخت‌های کشور- مصوبه شماره ۲۳۰۱ کمیته دائمی پدافند غیرعامل کشور- در مراحل طراحی، ساخت و بهره‌برداری از مراکز زیرساختی مستلزم بکارگیری دانش تخصصی و بهره‌گیری از نظام فنی یکپارچه در موضوع حفاظت از زیرساخت در جهت تضمین تداوم کارکرد و ارتقاء تاب‌آوری و آمادگی این مراکز در مواجهه با تهدیدات جدید در کشور می‌باشد. از این رو در اجرای جزء ۲ از بند (ی) ماده۱۰ این طرح و بمنظور ارتقاء دانش فنی و مهندسی پدافند غیرعامل و همچنین پیاده‌سازی زیست بوم یکپارچه حفاظت از زیرساخت در سطح ملی، نظام فنی و تخصصی حفاظت از زیرساخت‌های کشور برای هماهنگی، هم‌افزایی، وحدت‌رویه و مشارکتِ ملی کلیه ذی‌نفعان در حفاظت از زیرساخت‌ها و شریان‌های با اهمیت کشور، جهت اجرا ابلاغ می‌گردد.

ماده ۱– تعاریف و اختصارات

الف– عمومی

۱) **سازمان:** سازمان پدافند غیرعامل کشور

۲) **کمیته دائمی:** کارگروه (کمیته) دائمی پدافند غیرعامل کشور

۳) **نظام:** مجموعه‌ای یکپارچه شامل عوامل، اصول، برنامه‌ها، فرآیندها، اسناد (مقرّرات، ضوابط و دستورالعمل‌ها) مربوط به پدیدآوری، طراحی، ساخت و بهره‌برداری مراکز زیرساختی می‌باشد.

۴) **طراحی:** مجموعه‌ای از فرآیندها که الزامات و یا خواسته‌ها را به ویژگی‌های مشخص شده یا به مشخصات فنّی تبدیل می‌کند.

۵) **ساخت:** طیف گسترده‌ای از فعالیت‌های مهندسی که به منظور ایجاد، تغییر و یا بازسازی یک مرکز زیرساختی انجام می‌شود.

۶) **اجرا:** انجام فعالیت‌های مربوط به تامین کالا، عملیات اجرایی و سازماندهی برای بهره‌برداری از یک مرکز زیرساختی است.

۷) **بهره‌برداری:** ورود فعالیت‌های یک مرکز زیرساختی به مرحله عملیاتی و ارائه خدمات توسط آن بطوریکه به ما اطمینان دهد عملکرد طرح، طبق دستورالعمل تهیه شده به وسیله طراح بوده و اهداف طرح برآورده شده است.

۸) **دستگاه نظارت:** شخصی است حقیقی یا حقوقی، دارای صلاحیت در حوزه پدافند غیرعامل که برای کنترل و حصول اطمینان از صحّت اجرای یک مرکز طبق اسناد، مدارک، نقشه‌های اجرایی و مشخصات فنّی اقدام می‌کند.

۹) **نظارت عالیه:** نظارتی است مستمر همراه با بازدیدهای منظّم برای ارزیابی و کنترل روند پیشرفت کیفی (ارزیابی اثربخشی اقدامات و رعایت نظامات پدافند غیرعامل) و کمّی (فیزیکی، ریالی و زمانی) یک مرکز زیرساختی که توسط سازمان یا نماینده آن با هدف هماهنگی بین کلّیه عوامل دست‌اندرکار در مراحل طراحی، اجرا و بهره‌برداری صورت می‌پذیرد.

۱۰) **مشاور پدافند غیرعامل:** ظرفیتی حقیقی یا حقوقی که توسط سازمان برای تهیه و یا نظارت بر انجام فرآیند مطالعه، طراحی یا اجرای طرح‌های پدافندغیرعامل احراز صلاحیت شده و در چارچوب اختیارات تعیین شده معرفی می‌شود. مشاور پدافند غیرعامل، گواهی‌نامه صلاحیت انجام خدمات مشاوره پدافند غیرعامل خود را در گروه‌های تخصصی ذی‌ربط از سازمان دریافت می‌کند.

۱۱) **پایان کار پدافند غیرعامل:** تأییدیه‌ای مکتوب حاکی از اتمام عملیات اجرایی طرح حفاظت از زیرساخت با رعایت اصول، الزامات و ملاحظات فنّی پدافند غیرعامل که پس از حصول اطمینان از اجرای تمهیدات و احکام پدافند غیرعامل و تأیید دستگاه نظارت، توسط سازمان صادر می‌شود.

ب– تخصصی[1]

۱) **حفاظت از زیرساخت**[2]**:** مجموعه تدابیر و اقدامات پدافند غیرعاملی که توانایی و آمادگی عملیاتی زیرساخت و تداوم کارکرد آن و دستگاه‌های اجرایی مسئول برای پاسخ مؤثر به حوادث و سوانح ناشی از تهدیدات نظامی، امنیتی و تروریستی، سایبری زیرساختی و تهدیدات از درون دشمن‌پایه را افزایش می‌دهد بطوری که فعّالیت آن حفظ گردیده و خسارات انسانی و مادی ناشی از آن را به حداقل می‌رساند.

۲) **نظام فنی حفاظت از زیرساخت**[3]**:** مجموعه‌ای از الزامات، معیارها، مقرّرات و ضوابط فنّی و تخصصی پدافند غیرعامل که روابط حاکم بر طراحی، ساخت و بهره‌برداری از مراکز زیرساختی کشور را تنظیم می‌کند.

۳) **مصونیّت**[4]**:** سطح مورد انتظار از مصون‌سازی مراکز زیرساختی با تأکید بر تاب‌آوری، آسیب‌ناپذیری و تداوم کارکرد می‌باشد.

---

[1] تعاریف تخصصی مرتبط با الزامات این نظام برگرفته از اسناد علمی است که برخی از آنها در پیوست‌های تخصصی ارائه شده است.

[2] Critical Infrastructure Protection (CIP)

[3] Technical System of Critical Infrastructure Protection (TSOCIP)

[4] Immunization

۴) **مصون‌سازی:** مجموعه اقدامات و تدابیر پدافند غیرعاملی که بکارگیری آنها باعث کاهش عمده آسیب‌پذیری‌ها و یا بی‌اثرسازی تهدیدات بر زیرساخت، جامعه و پیکره کشور، ایجاد پایداری، تاب‌آوری و دستیابی به امنیت کامل در برابر تهدیدات می‌شود.

۵) **سطح‌بندی[5]:** میزان ارزش و اهمّیت مراکز زیرساختی کشور که از منظر پدافند غیرعامل در سطوح حیاتی، حساس، مهم و قابل حفاظت تقسیم‌بندی و تعریف می‌شود.

۶) **درجه‌بندی[6]:** میزان حسّاسیت[7] دارایی‌های مراکز زیرساختی که به لحاظ کارکرد و اهمّیت آنها از منظر پدافند غیرعامل در طیفی از درجات ۱، ۲، ۳ و ۴ قرار می‌گیرند.

۷) **زیرساخت[8]:** به مجموعه‌ای از مراکز و تأسیسات زیربنایی و شریان‌های عمده اطلاق می‌گردد که خدمات و نیازهای ضروری و اساسی کشور را به مردم و سایر مجموعه‌ها ارائه می‌کند. زیرساخت بشرح زیر مشتمل‌بر فرابخش (حوزه)، بخش، زیربخش، دارایی و اجزاء آن می‌باشد.

- **حوزه[9]:** هریک از عناصر اصلی شکل‌گیری زیرساخت‌ها که مطابق طرح راهبردی حفاظت از زیرساخت‌های کشور عبارتند از: انرژی، آب، غذا و کشاورزی، حمل و نقل، بهداشت و سلامت، دفاعی و امنیتی، صنعت، رسانه، هسته‌ای، فضا، جمعیت، حاکمیتی، خدمات ضروری و فوریتی، پولی و مالی، ارتباطات و فناوری اطلاعات.
- **بخش[10]:** آن قسمت از زیرساخت که متناسب با عملکرد و ویژگی‌های خاص خود در تولید محصولات و یا ارائه خدمات ذیل هریک از حوزه‌های با اهمیت کشور قابل تعریف و تفکیک است. به طور مثال بخش‌های برق، نفت و گاز در حوزه انرژی قابل تعریف می‌باشند.
- **زیربخش/مرکز[11]:** مجموعه‌ای از دارایی‌های فیزیکی و غیرفیزیکی هریک از بخش‌ها در زیرساخت که می‌توانند متناسب با حساسیت و درجه اهمّیت خود به عنوان هدف برای دشمن جذاب باشند. از قبیل؛ بندر، فرودگاه، پالایشگاه و ...
- **دارایی[12]:** اجزای فیزیکی و غیرفیزیکی با ارزش مراکز زیرساختی که هرگونه اختلال در عملکرد آنها متناسب با درجه اهمّیت‌شان بر تولید محصول و ارائه خدمت آن مرکز اثر می‌گذارد.

تذکر- در این نظام تمامی الزامات و ملاحظات فنی ارائه شده لایه زیربخش/مرکز و اجزای آن را شامل می‌شود.

۸) **مکان‌یابی:** انجام اقدامات لازم به منظور انتخاب مکانی مناسب مبتنی بر سطح تهدیدات و آسیب‌پذیری‌های مربوطه برای استقرار و احداث مراکز، تأسیسات زیربنایی و شریان‌های عمده می‌باشد.

۹) **وابستگی[13]:** خدمت‌گیری یک طرفه‌ی یک دارایی از سایر دارایی‌های یک مرکز زیرساختی را وابستگی می‌گویند.

۱۰) **وابستگی متقابل / اندرکنش[14]:** عبارت است از ارتباط و وابستگی عملکرد دارایی‌های یک مرکز زیرساختی به یکدیگر که درصورت اختلال در یکی از آنها احتمال ایجاد اختلال در سایر دارایی‌های وابسته به آن وجود دارد.

۱۱) **درجه وابستگی[15]:** میزانی از وابستگی مبتنی بر ویژگی‌های ساختاری یک دارایی در شبکه ارتباطی با سایر دارایی‌ها که در صورت وقوع تهدید/حادثه در عملکرد آن اختلال ایجاد شود.

[5] Classification
[6] Ranking
[7] Criticality
[8] Infrastructure
[9] Sector
[10] Sub-Sector (System)
[11] Sub-System
[12] Asset
[13] Dependency
[14] Interdependency
[15] Degree of dependency

۱۲) **مرکزیت[16]:** جذّابیت یک دارایی برای پذیرش تهدید براساس میزان ارتباطی که در شبکه با سایر دارایی‌ها برقرار می‌کند. مرکزیت می‌تواند در خصوص مکان قرارگرفتن دارایی (گره[17])، نحوه‌ی پیوند و میزان رابطه آن با سایر دارایی‌ها در شبکه مطرح گردد. مرکزیت براساس شاخص‌های درجه، بینابینی و نزدیکی اندازه‌گیری می‌شود.

- **درجه مرکزیت[18]:** مجموع ارتباط یک‌سویه و دوسویه بدون بعد که یک دارایی در شبکه دارا می‌باشد.
- **مرکزیت بینابینی[19]:** جایگاه یک دارایی در درون شبکه زیرساختی برحسب توانایی آن برای ایجاد کوتاه‌ترین مسیر ارتباطی میان سایر دارایی‌ها در شبکه می‌باشد.
- **نزدیکی مرکزیت[20]:** کوتاه‌ترین فاصله میان یک دارایی با سایر دارایی‌ها در شبکه زیرساختی می‌باشد.
- **گام:** فاصله بین دو دارایی در شبکه می‌باشد.
- **مسیر:** هر تعداد گام (فاصله) تعریف شده میان دو دارایی در شبکه را مسیر می‌گویند.
- **مسیر مستقیم:** کوتاه‌ترین مسیر ارتباطی بین دو دارایی در شبکه می‌باشد.

۱۳) **روابط سیستمی زیرساختی:** توسعه مراکز زیرساختی بصورت سیستمی و شبکه‌ای ناشی از روابط درون و برون سیستمی و تعاملات بین آنها که منجر به ایجاد روابطی تحت شبکه از قبیل هم‌افزایی، تضاد، ارتباط و وابستگی متقابل می‌شود.

۱۴) **شبکه زیرساختی درهم تنیده [21]:** مجموعه‌ای از دارایی‌های بهم پیوسته یا درهم تنیده در یک شبکه زیرساختی که عملکرد یکپارچه داشته و خدمات گسترده‌ای را در ارتباط با یکدیگر ارائه می‌دهند.

- **درهم تنیدگی کامل[22]:** نوعی ارتباط سیستمی به هم پیوسته و مستقیم از یک دارایی به کلیه دارایی‌های موجود در یک شبکه زیرساختی که به واسطه آن ارائه خدمات و انجام فعالیت بین کلیه دارایی‌ها صورت گرفته و از ایجاد قطب منحصر به فرد در شبکه جلوگیری می‌کند.
- **درهم تنیدگی بخشی[23]:** نوعی ارتباط سیستمی به هم پیوسته و مستقیم از یک دارایی به برخی از دارایی‌های موجود در یک شبکه زیرساختی که به واسطه آن ارائه خدمات و انجام فعّالیت بین تعدادی از دارایی‌ها صورت گرفته و می‌تواند باعث ایجاد قطب منحصر به فرد در شبکه گردد.
- **قطب[24]:** یک دارایی که بالاترین ارتباط را با سایر دارایی‌ها در شبکه دارد.

شکل ۱– انواع شبکه زیرساختی درهم‌تنیده

الف: درهم‌تنیدگی بخشی **ب:** درهم‌تنیدگی کامل

[16] Centrality
[17] Node
[18] Degree centrality
[19] Betweenness centrality
[20] Closeness centrality
[21] Mesh network
[22] Full Mesh
[23] Partial Mesh
[24] Hub

۱۵) **درجه بیشینه منحصربه‌فرد:** مجموع ارتباط یک‌سویه و دوسویه بدون بُعد یک دارایی که به عنوان یک رأس در شبکه می‌تواند با دیگر دارایی‌های مرکز ایجاد کند.

۱۶) **ضریب خوشه‌بندی[25]:** نسبت تعداد ارتباطات موجود بین یک دارایی با دارایی‌های وابسته به آن به تمام ارتباطات ممکن بین دارایی‌ها می‌باشد.

۱۷) **تاب‌آوری[26]:** توانایی مقاومت مرکز زیرساختی در مقابل یک تغییر ناخواسته یا رویداد اخلال‌گر (قابلیّت جذب)، تطبیق با شرایط جدید (قابلیّت انطباق پذیری) و سرعت بخشیدن به بازیابی پس از اختلال (قابلیّت برگشت‌پذیری) تاب‌آوری گفته می‌شود.

- **ظرفیت جذب:** توانایی یک دارایی برای جذب اثرات ناشی اختلال و به حداقل رساندن پیامدهای آن با کمترین تلاش را ظرفیت جذب می‌گویند.
- **ظرفیت تطبیق‌پذیری:** توانایی یک دارایی برای بهبود و حفظ سطح عملکرد خود (خودسازماندهی) در شرایط حادثه/تهدید را ظرفیت تطبیق‌پذیری می‌گویند.
- **ظرفیت برگشت‌پذیری/بازیابی:** توانایی یک دارایی برای بازگشت به شرایط عملیاتی اولیه قبل از وقوع حادثه/تهدید و ارتقاء توان تولید/ارائه خدمت به نحوی که از پایداری تدوام کارکرد آن اطمینان حاصل گردد را ظرفیت برگشت‌پذیری/بازیابی می‌گویند.

۱۸) **درجه تاب‌آوری:** سطوح مختلفی از تاب‌آوری در مراکز زیرساختی مبتنی بر قابلیت دستیابی به ظرفیت‌های جذب، تطبیق‌پذیری و برگشت‌پذیری را درجه تاب‌آوری می‌گویند.

۱۹) **تداوم کارکرد:** توانایی ادامه تولید محصول یا ارائه خدمت توسط یک مرکز زیرساختی درچارچوب زمانی موردپذیرش، قابل قبول و درحد ظرفیت از پیش تعیین شده، حین و پس از وقوع تهدید یا حادثه، تداوم کارکرد گفته می‌شود.

۲۰) **خدمات زیرساختی:** قابلیت مورد انتظار از کارکرد یک دارایی در مرکز را برای ارائه خدمت یا تولید محصول خدمات زیرساختی می‌گویند که به سطوح زیر تقسیم‌بندی می‌شود:

- **خدمات کلیدی:** سطح مورد انتظار از ارائه خدمات زیرساختی متناسب با نوع دارایی که در مواجهه با حادثه/تهدید، با بکارگیری امکانات و تسهیلات در دسترس بتواند ضمن حفظ تداوم فعّالیت بدون وقفه خود، قابلیت برگشت‌پذیری به حالت عملیاتی را در حداقل زمان ممکن (متناسب با مأموریت آن) داشته باشد.
- **خدمات ضروری:** سطح مورد انتظار از ارائه خدمات زیرساختی متناسب با نوع دارایی که در مواجهه با حادثه/تهدید، ضمن حفظ حداقل سطح تداوم فعّالیت بدون وقفه خود، قابلیت برگشت‌پذیری به حالت عملیاتی را در مدت زمان معین (متناسب با مأموریت آن) به همراه داشته باشد.
- **خدمات لازم:** سطح مورد انتظار از ارائه خدمات زیرساختی متناسب با نوع دارایی که در مواجهه با حادثه/تهدید، قابلیت برگشت‌پذیری به حالت عملیاتی را در زمان قابل قبول (متناسب با مأموریت آن) داشته باشد.

تذکر- زمان برگشت‌پذیری متناسب با نوع خدمات زیرساختی و براساس حفظ سطح رفاه و امنیت جامعه تعیین می‌شود.

۲۱) **جایگزینی:** پیش‌بینی ظرفیت مشابه تطبیق‌پذیر برای اجزای یک دارایی (تأسیسات و تجهیزات آن) به نحوی که در صورت آسیب دیدن آنها امکان استفاده از این ظرفیت وجود داشته و فعّالیت‌های مرکز بی‌وقفه ادامه یابد.

۲۲) **پیامد:** نتیجه وقوع تهدید یا حادثه بصورت ایجاد خسارات و صدمات (با شدت صفر تا صد در صد) همراه با اثرات کوتاه‌مدت، بلندمدت، مستقیم و غیرمستقیم بر اجزای یک دارایی را پیامد می‌گویند.

[25] Clustering
[26] Resiliency

- **پیامد دومینویی**[27]: قابلیت تسرّی و انتقال اختلال از یک دارایی به سایر دارایی‌های وابسته به آن در شبکه در یک فرآیند سری و تکرارپذیر که افزایش شدت خرابی و توقف بخشی از عملکرد را در سایر دارایی‌های شبکه به همراه دارد.
- **پیامد آبشاری**[28]: قابلیت تسرّی و انتقال اختلال از یک دارایی به سایر دارایی‌های وابسته به آن در شبکه در یک فرآیند تصاعدی که افزایش وسعت بالای خرابی و توقف کامل عملکرد را در سایر دارایی‌های شبکه به همراه دارد.
- **پیامد سیستمی**[29]: هریک از پیامدهای دومینویی، آبشاری یا ترکیبی از آن دو را در شبکه زیرساختی، پیامد سیستمی می‌گویند.

۲۳) **خطر**[30]: هرمنبع دارای پتانسیل ایجاد خسارت به نیروی انسانی، اموال و دارایی‌ها را خطر می‌گویند.

۲۴) **مخاطره**[31]: درمعرض خطر قرارگرفتن یک دارایی را مخاطره می‌گویند. به عبارت دیگر وقتی یک خطر از حالت بالقوّه به حالت بالفعل تبدیل شود، مخاطره رخ می‌دهد.

۲۵) **ریسک**[32]: امکان بالقوّه (استعداد) تولید یک نتیجه ناخواسته ناشی از وقوع تهدید یا حادثه، به‌گونه‌ای که می‌توان رتبه آن را برحسب احتمال وقوع و شدّت پیامدهای مرتبط با آن در قالب ریسک قابل قبول، بهینه، نسبی و حداقلی، متناسب با طیف لیکرت[33] برآورد نمود.

۲۶) **آسیب پذیری**[34]: ظرفیت پذیرش خسارات و صدماتی که ناشی از عوامل و پدیده‌های بالقوه(تهدیدات) یا بالفعل خسارت‌زا به نیروی انسانی، تجهیزات و تأسیسات در یک دارایی یا شبکه زیرساختی وارد می‌شود.

۲۷) **تهدیدات درون‌زا**[35]: به تهدیداتی اطلاق می‌گردد که در آن کارکنان یک مرکز زیرساختی یا شبکه‌های همکار آنها اعم از پیمانکاران و سایرین بصورت فردی یا شبکه‌ای، با همکاری یا هدایت عوامل بیگانه، از سطح دسترسی مجاز، دانش و اختیارات خود برای آسیب‌رساندن به آن مرکز استفاده نمایند، این موضوع می‌تواند شامل خسارت به تأسیسات، سیستم‌ها، سامانه‌ها، تجهیزات، کارکردها و فرآیندها (خرابکاری صنعتی) توقف فعّالیت‌های ضروری و یا اقدامات دیگری (صدمه زدن به مأموریت سازمان و منابع) باشد که مرکز را از ادامه ارائه خدمات خود باز می‌دارد.

تذکر- در این نظام، الزامات فنّی مرتبط با تهدیدات درون‌زا صرفاً موضوعات فنّی مرتبط با خرابکاری صنعتی را شامل می‌شود، سایر موارد مرتبط با این موضوع در سایر اسناد ارائه خواهد شد.

۲۸) **آسیب‌پذیری سایبری:** هرنوع ضعف، نقص و عیب موجود در یک دارایی سایبری که قابلیت فعّال شدن تهاجم و یا جنگ سایبری را در قالب پیاده‌سازی تهدیدات سایبری داشته باشد.

۲۹) **هوشمندسازی:** بکارگیری ابزارها و روش‌های فنی و اطلاعاتی (هرگونه ارتباط بین افراد، فرآیندها و سیستم‌ها) جهت تسهیل فعّالیت‌ها، حصول اطمینان از عملکرد صحیح و شتاب بخشیدن به اجرای دقیق، تجزیه‌وتحلیل و پیش‌بینی عمیق عملکردهای زیرساختی و بهره‌برداری حداکثری از خدمات حوزه فناوری اطلاعات در تبدیل دارایی‌های غیرهوشمند به هوشمند را هوشمندسازی می‌گویند.

۳۰) **آمادگی:** مجموعه تدابیر و اقداماتی است که ظرفیّت زیرساخت و دستگاه‌های اجرایی مسئول را برای پاسخ موثّر به حوادث و سوانح ناشی از تهدیدات پایه زیرساختی افزایش می‌دهد بطوری‌که خسارات انسانی و مادی ناشی از آن را به حداقل می‌رساند.

---

[27] Domino effect
[28] Cascading effect
[29] Systematical effect
[30] Hazard
[31] Danger
[32] Risk
[33] Likert Spectrum
[34] Vulnerability
[35] Insider threat

ماده۲– اسناد بالادستی

۱) سیاست‌های کلّی نظام در موضوع پدافند غیرعامل
۲) قانون تشکیل سازمان پدافند غیرعامل کشور
۳) اساسنامه سازمان پدافند غیرعامل کشور
۴) بند ۲۴ سیاست‌های کلّی برنامه پنج‌ساله هفتم توسعه جمهوری اسلامی ایران
۵) بند پ ماده ۱۰۶ و ماده ۱۰۹ برنامه پنج‌ساله ششم توسعه جمهوری اسلامی ایران
۶) ماده ۵۸ قانون احکام دائمی برنامه‌های توسعه کشور
۷) ماده ۲۳ قانون الحاق برخی مواد مقرّرات مالی دولت
۸) آئین‌نامه اجرایی ماده ۳۴ قانون احکام دائمی برنامه‌های توسعه کشور (نظام فنی و اجرایی یکپارچه کشور) مصوّب ۱۴۰۰/۰۲/۰۵
۹) طرح راهبردی حفاظت از زیرساخت‌های کشور- مصوبه شماره۲۳۰۱ مورخ ۱۴۰۱/۰۷/۲۰ کمیته دائمی

ماده۳– هدف

ایجاد نظامی مدوّن و یکپارچه شامل الزامات، ضوابط و مقرّرات به منظور اجرا و پیاده‌سازی طرح راهبردی حفاظت از زیرساخت‌های کشور، در سطوح فنّی و تخصصی برای دستیابی به اهداف زیر:

۱- تعیین معیارها و شاخص‌های فنّی و تخصصی برای اجرای طرح حفاظت از زیرساخت در کشور
۲- استانداردسازی فرآیند تهیه و تدوین مطالعات طرح‌های پدافند غیرعامل مراکز زیرساختی در کشور
۳- تدقیق و تسهیل روابط و تعاملات میان سازمان و دستگاه‌های متولّی راهبری زیرساخت‌های با اهمیت کشور

ماده۴– قلمرو اجرا

مراکز زیرساختی با اهمیت کشور در مراحل پیدایش، مطالعه، طراحی، اجرا و بهره‌برداری در دستگاه‌های اجرایی (موضوع ماده۵ قانون مدیریت خدمات کشوری) و سازمان‌های نیروهای مسلح و مراکز زیرساختی با اهمیت کشور در بخش خصوصی

ماده۵– ساختارهای اجرایی

الف) سطح راهبردی و سیاست‌گذاری

به منظور هدایت، سیاست‌گذاری، برنامه‌ریزی و ایجاد هم‌گرایی، هم‌افزایی، مدیریت هماهنگ و رفع تعارض در راهبری و اجرای الزامات حفاظت از زیرساخت در حوزه‌های کلیدی کشور « **شورای هماهنگی حفاظت از زیرساخت**» با عضویت اشخاص زیر تشکیل می‌شود:

- سازمان پدافند غیرعامل کشور (رئیس شورا)
- وزارتخانه‌های نیرو، نفت، ارتباطات و فناوری اطلاعات، کشور، بهداشت، درمان و آموزش پزشکی، جهاد کشاورزی، دفاع و پشتیبانی ن.م، راه و شهرسازی و اطلاعات (سازمان حراست کل کشور)
- سازمان برنامه و بودجه کشور
- سپاه پاسداران انقلاب اسلامی
- فرماندهی انتظامی جمهوری اسلامی ایران
- معاونت طرح‌ریزی و نظارت فنی سازمان (دبیر شورا)
- و سایر دستگاه‌های اجرایی ذی‌ربط بنا به موضوع

وظایف شورای هماهنگی حفاظت از زیرساخت عبارت است از:

- تعیین خط‌مشی‌ها، سیاست‌ها و برنامه‌های کلان و مشترک در موضوع حفاظت از زیرساخت‌ها

- راهبری پیاده‌سازی طرح راهبردی حفاظت از زیرساخت‌ها در کشور
- هماهنگ‌سازی و هم‌افزایی بین دستگاهی در راستای ارتقاء تاب‌آوری ملّی
- ایجاد هماهنگی و مشارکت موثّر در دستگاه‌های متولّی حوزه‌های با اهمیت در اجرای طرح‌های مشترک حفاظت از زیرساخت و رفع تعارض فیمابین
- اشتراک اطلاعاتی و تعیین اولویت تهدیدات زیرساختی در حوزه‌های با اهمّیت در کشور
- واپایش و نظارت بر وضعیت آمادگی و ارتقاء آن در زیرساخت‌های کشور
- اولویت‌بندی و پیش‌بینی تأمین منابع مالی برای طرح‌های حفاظت از زیرساخت در کشور

تبصره- شورای هماهنگی حفاظت از زیرساخت در سطح معاونین روسای دستگاه‌های اجرایی (معاون وزیر) برگزار می‌گردد.

ب) سطح عملیاتی

به منظور ارتقاء تاب‌آوری، ایجاد هم‌افزایی عملیاتی و مدیریت پیامد ناشی از حادثه/تهدید در جهت مصونیّت و حصول اطمینان از اجرای الزامات حفاظت از زیرساخت در مراکز زیرساختی « **مرکز مدیریت و هماهنگی عملیاتی زیرساخت**» با عضویت اشخاص زیر تشکیل می‌شود:

- سازمان پدافند غیرعامل کشور (رئیس مرکز)
- وزارتخانه‌های نیرو، نفت، ارتباطات و فناوری اطلاعات، کشور، بهداشت، درمان و آموزش پزشکی، جهاد کشاورزی، دفاع و پشتیبانی ن.م، راه و شهرسازی و اطلاعات (سازمان حراست کل کشور)
- سپاه پاسداران انقلاب اسلامی
- فرماندهی انتظامی جمهوری اسلامی ایران
- معاونت اطلاعات و عملیات سازمان (دبیر مرکز)
- مرکز فرماندهی و کنترل سازمان
- قرارگاه ذی‌ربط پدافند غیرعامل کشور متناسب با موضوع
- و نماینده حراست سایر دستگاه‌های اجرایی ذی‌ربط بنا به موضوع

وظایف مرکز مدیریت و هماهنگی عملیاتی زیرساخت عبارت است از:

- رصد، پایش، تشخیص، هشدار و برآورد تهدیدات و مخاطرات در مراکز زیرساختی با اهمّیت کشور
- سازماندهی سامانه فرماندهی و کنترل حوزه عملیاتی حفاظت از زیرساخت
- هدایت، راهبری و نظارت بر طرح‌ریزی، آموزش، تمرین، رزمایش و آمادگی ملّی
- راهبری و نظارت بر مصون‌سازی مراکز زیرساختی با اهمّیت کشور
- مدیریت، کاهش و کنترل پیامدهای ناشی از تهدیدات در مراکز زیرساختی با اهمّیت کشور
- طرح ریزی، هدایت و راهبری اجرای عملیات مقابله و پاسخ در شرایط اضطراری
- اشتراک اطلاعاتی در خصوص تهدیدات و مخاطرات و آسیب‌پذیری‌های زیرساختی بین دستگاه‌ها

تبصره۱- این مرکز در دستگاه‌های دارای مراکز زیرساختی با اهمیت و در استان‌ها و شهرها، سازماندهی، تشکیل و راهبری گردیده و با مرکز مدیریت و هماهنگی عملیاتی زیرساخت در سازمان ارتباط برقرار می‌کند.

تبصره۲- مرکز فرماندهی و کنترل سازمان برابر شرح وظایف مشخص در مصوبه شماره ۸۰۴ کمیته دائمی اقدام می‌کند.

تبصره۳- مدیرکل پدافند غیرعامل دستگاه‌های فوق، موظف به شرکت در جلسات مرکز مدیریت و هماهنگی عملیاتی زیرساخت می‌باشند.

ج) سطح فنّی

به منظور تدوین، تصویب، روزآمدسازی، بررسی، ارزیابی و نظارت بر اعمال مقرّرات و ضوابط فنّی مرتبط با موضوع حفاظت از زیرساخت، « **مرکز تنظیم مقرّرات حفاظت از زیرساخت**» با عضویت اشخاص زیر تشکیل می‌شود:

- رئیس سازمان پدافند غیرعامل (رئیس مرکز)
- رئیس دفتر مقرّرات ملی ساختمان وزارت راه و شهرسازی
- معاون فنی/ رئیس امور نظام فنی و اجرایی، مشاورین و پیمانکاران سازمان برنامه و بودجه کشور
- معاون تدوین و ترویج استاندارد سازمان ملّی استاندارد کشور
- رییس مؤسسه استاندارد دفاعی و صنعتی وزارت دفاع
- رئیس مجتمع پدافند غیرعامل دانشگاه صنعتی مالک اشتر
- رئیس دانشکده پدافند غیرعامل دانشگاه جامع امام حسین (ع)
- دو نفر از اعضای هیئت علمی مرتبط با موضوع با انتصاب توسط رئیس سازمان
- معاون فنی دستگاه‌های اجرایی ذی‌ربط بنا به موضوع
- معاون طرح‌ریزی و نظارت فنی سازمان (دبیر مرکز)
- معاون آموزش و پژوهش سازمان
- رئیس مرکز مطالعات و تدوین آئین‌نامه‌های فنی مهندسی سازمان

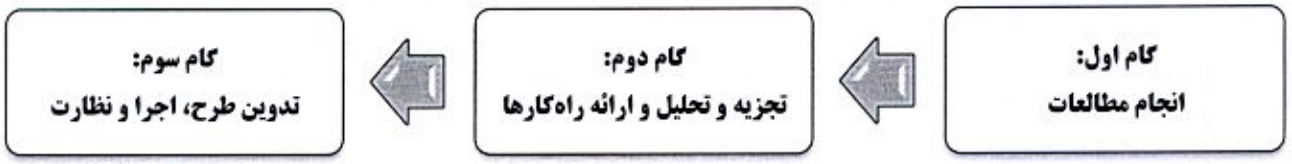
وظایف مرکز مدیریت و هماهنگی عملیاتی زیرساخت عبارت است از:

- تدوین، تولید و به روزرسانی محتوای فنی مقرّرات، الزامات، ضوابط و استانداردهای حفاظت از زیرساخت
- تعیین شاخص‌ها، معیارها، الزامات و ملاحظات فنّی تخصصی حفاظت از زیرساخت
- تدوین دستورالعمل‌ها و بازبینه‌های ارزیابی تخصصی حفاظت از زیرساخت
- بررسی، ارزیابی و اصلاح مقرّرات، اصول، ضوابط و استانداردهای فنی حفاظت از زیرساخت
- تصویب و ابلاغ مقررات، اصول، ضوابط و استانداردهای فنی حفاظت از زیرساخت و نظارت بر اجرای آن
- تشکیل کارگروه‌های فنّی حفاظت از زیرساخت در حوزه‌های تخصصی
- پشتیبانی فنّی تخصصی از شورای هماهنگی حفاظت از زیرساخت
- ایجاد وحدت رویه در تدوین، ارزیابی و تصویب ضوابط فنّی حفاظت از زیرساخت در کشور

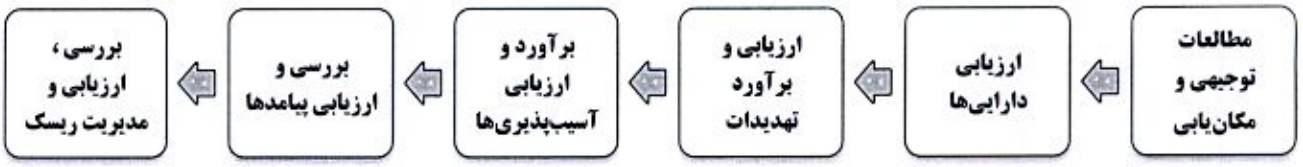
تبصره- مصوبات مرکز تنظیم مقررات حفاظت از زیرساخت، توسط رئیس سازمان ابلاغ می‌شود.

ماده۶- فرآیند اقدامات حفاظت از زیرساخت

این بخش به تبیین فرآیند اقدامات حفاظت از زیرساخت در قالب گام‌های زیر؛ شامل انجام مطالعات، تجزیه و تحلیل و ارائه راهکارها، تدوین طرح‌های عملیاتی، اجرا و نظارت بر پیاده‌سازی آنها در طرح‌های توسعه‌ای مراکز زیرساختی جدید و در حال بهره‌برداری می‌پردازد؛ به همین منظور برای انجام خدمات مطالعه و طراحی توسط مهندسین مشاور ذیصلاح با رویکرد حفاظت از زیرساخت، رئوس اقدامات و مراحل اجرایی این موضوع در قالب اقدامات زیرساختی (گام اول و دوم) و عملیاتی (گام سوم) بشرح زیر پیش‌بینی شده است. لازم به ذکر است در کلیه مراحل، فرایند انجام خدمات تا تدوین جزئیات و نقشه‌های اجرایی ادامه خواهد داشت.



گام اول – انجام مطالعات حفاظت از مراکز زیرساختی



مرحله ۱) مطالعات توجیهی و مکان‌یابی

۱- گردآوری اطلاعات، شناخت اجزا و ابعاد طرح
۲- بررسی، مطالعه و انتخاب مقیاس طرح
۳- ارزیابی و سطح‌بندی مرکز
۴- بررسی گزینه‌های مکان‌یابی
۵- بررسی سناریوهای تهدید دشمن در هر گزینه
۶- بررسی آسیب‌پذیری گزینه‌ها در برابر تهدیدات با احتمال بیشتر
۷- آنالیز ریسک و مقایسه گزینه‌ها از دیدگاه پدافند غیرعامل
۸- پیشنهاد گزینه برتر طرح

مرحله ۲) ارزیابی دارایی‌ها

۱- شناسایی ماهیّت دارایی (فیزیکی، انسانی، سایبری، معنوی و ترکیبی)
۲- شناسایی کارکرد دارایی
۳- شناسایی و تعیین نوع و درجه وابستگی و وابستگی متقابل دارایی
۴- شناسایی مخاطرات دارایی (براساس سطح و شدت خطرزایی)
۵- شناسایی هوشمندی دارایی
۶- شناسایی سلّولی و سیستمی بودن دارایی
۷- تعیین درجه حساسیت دارایی

مرحله ۳) ارزیابی و برآورد تهدیدات

۱- بررسی و توصیف تهدیدات
۲- برآورد تهدیدات
۳- برآورد جذابیت هدف از منظر دشمن
۴- غربال‌گری، تجزیه و تحلیل تهدیدات
۵- تعیین تهدیدات پایه و مبنا
۶- تعیین سناریوی پایه تهدید
۷- شناسایی و انتخاب سلاح معیار تهدید

مرحله ۴) برآورد و ارزیابی آسیب‌پذیری‌ها

۱- بررسی و تعیین نوع و سطح آسیب‌پذیری‌ها
۲- بررسی و تعیین اندرکنش تهدید و آسیب‌پذیری
۳- تجزیه و تحلیل آسیب‌پذیری
۴- تعیین آسیب‌پذیری پایه (تعیین درجه آسیب محتمل)
۵- تعیین آستانه آسیب‌پذیری قابل پذیرش

مرحله ۵) بررسی و ارزیابی پیامدها

۱- تعریف و دسته‌بندی پیامدهای اوّلیه، ثانویه، ... و نهایی
۲- بررسی و مطالعه نوع تخریب (آبشاری، دومینویی، سلّولی)
۳- برآورد شدّت، وسعت و مانایی پیامد
۴- ارزیابی شدّت، وسعت پیامد
۵- اقدامات کنترل، مدیریت و کاهش پیامدها

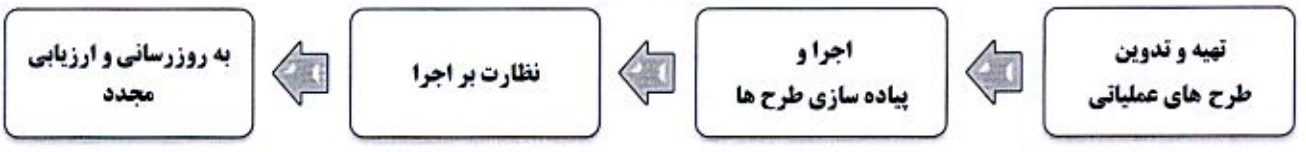
مرحله ۶) بررسی، ارزیابی و مدیریت ریسک

۱- شناسایی و ارزیابی مخاطرات
۲- تعیین شدّت مخاطرات
۳- برآورد و تحلیل میزان، نوع و محل ریسک
۴- تعریف ریسک قابل قبول و راهکارهای کاهش آن

گام دوم –تجزیه و تحلیل و ارائه راهکارها

در طرح‌های توسعه‌ای مراکز جدید ضرورت دارد پس از ارائه راهکارها، جزئیات تهیه شده در نقشه‌های اجرایی قرار گیرد و در مراکز در دست بهره‌برداری پس از ارائه راهکارها، جزئیات مربوطه اجرا و پیاده‌سازی می‌شوند.

گام سوم –تدوین طرح، اجرا و نظارت



مرحله ۱) تهیه و تدوین طرح‌های عملیاتی

۱- طرح پاسخ اضطراری به حوادث و تهدیدات
۲- طرح تضمین و تسهیل تداوم کارکردهای اساسی و بازیابی
۳- طرح ارتقاء تاب‌آوری
۴- طرح کاهش آسیب‌پذیری
۵- طرح بهینه‌سازی وابستگی و وابستگی متقابل
۶- طرح ارزیابی و ارتقاء آمادگی‌های زیرساختی

مرحله ۲) اجرا و پیاده‌سازی

۱- اجرا و پیاده‌سازی طرح‌های عملیاتی

۲- بازخوردگیری، اصلاح نواقص و اشکالات و به روزرسانی طرح‌ها

مرحله ۳) نظارت بر اجرا

۱- اجرای نظارت

۲- احصاء اشکالات و ایرادات اجرایی

۳- ارائه گزارش

مرحله ۴) به‌روزرسانی و ارزیابی مجدد اقدامات

۱- بررسی و برآورد به‌روز تهدیدات

۲- بررسی اندرکنش تهدیدات روزآمد شده و اقدامات لازم

۳- احصاء نواقص، اشکالات و آسیب‌پذیری‌های طرح نسبت به تهدیدات

۴- تهیه و اجرای راهکارهای اصلاحی

تبصره۱- فرایند نظارت در مراحل مطالعه، طراحی، ساخت و بهره‌برداری براساس« نظام نظارت بر طرح‌های حفاظت از زیرساخت» توسط مشاوران حقوقی/حقیقی صلاحیت‌دار پدافند غیرعامل انجام می‌شود.

تبصره۲- در کلیه مراکز زیرساختی ضرورت دارد طرح‌های پدافندی درخصوص حفاظت از مردم، حفاظت فیزیکی مرکز و نیروی انسانی ارائه و پیاده‌سازی شود.

تبصره۳- پس‌ازتولید و ابلاغ استانداردهای پدافند غیرعامل متناسب با الزامات تخصصی حفاظت از زیرساخت دستگاه‌های اجرایی موظف به پیاده‌سازی آنها در مراکز زیرساختی و اخذ گواهی استاندارد پدافند غیرعامل می‌باشند.

ماده۷– تهیه و تدوین طرح‌های عملیاتی

در جهت مصون‌سازی، افزایش آمادگی، ارتقاء تاب‌آوری و اَمن‌سازی مراکز زیرساخت‌های با اهمّیت کشور، گام‌های اجرایی در تهیه و تدوین هریک از طرح‌های جامع عملیاتی پدافندی بشرح زیر می‌باشد:

۱) طرح پاسخ اضطراری به حوادث و تهدیدات زیرساختی

۱- تعیین سطح شرایط اضطراری/بحران متناسب با نوع تهدید/حادثه

۲- بررسی و برآورد سطح خسارت وارده (به مردم، نیروی انسانی، تجهیزات، تأسیسات و سایر)

۳- بکارگیری ظرفیت‌های پیش‌بینی شده برای مقابله با تهدید/حادثه (مدیریت شرایط اضطراری)

۴- سازماندهی و بکارگیری تیم‌های عملیاتی ارزیابی امنیتی، امن‌سازی اضطراری و پاسخ به رخدادهای سایبری

۵- بازیابی اولیه و حفظ سطح خدمات متناسب با سطح‌بندی مرکز

۶- مستندسازی و ارائه گزارش‌ها

۷- اجرای آموزش‌های دوره‌ای برای نیروی انسانی مرکز

۸- طرح‌ریزی رزمایش پاسخ به شرایط اضطراری در مرکز

۹- به‌روز رسانی طرح

۲) طرح تضمین و تسهیل تداوم کارکردهای اساسی و بازیابی

۱- شناسایی مرکز زیرساختی و تعیین عملکردهای کلیدی آن

۲- تعیین سطح تهدیدات و آسیب‌پذیری‌ها
۳- برآورد سطح ریسک
۴- تنظیم برنامه تداوم کارکردهای اساسی متناسب با میزان تقاضا و نیازها ، ظرفیت و توان زیرساخت‌های جایگزین، امکان بازیابی، تعیین حداقل سطح کارکرد، راهکارهای کنترل‌کننده چالش‌ها، مدیریت وکاهش پیامدها و حداکثر مدت زمان اختلال زنجیره ناشی از حادثه/تهدید
۵- تدوین ساختار، تعیین وظایف، پیش‌بینی و تأمین تجهیزات لازم
۶- اجرای آموزش دوره‌ای طرح برای نیروی انسانی مرکز
۷- پیاده‌سازی و اجرای طرح
۸- طرح‌ریزی رزمایش تداوم کارکرد و بازیابی در مرکز
۹- انجام فرآیند بازیابی زنجیره در حین حادثه/تهدید
۱۰- اجرای فرآیند بروزرسانی و اصلاح برنامه تداوم کارکرد و بازیابی پس از وقوع تهدید یا حادثه

۳) طرح ارتقاء تاب‌آوری

۱- شناسایی و ارزیابی تهدیدات و تعیین تهدید مبنا
۲- پیش‌بینی ظرفیت‌های لازم برای ایجاد و ارتقاء آمادگی در برابر تهدید/حادثه
۳- بررسی و ارزیابی میزان قابلیت جذب تنش ناشی از تهدید/حادثه (میزان مقاومت مرکز)
۴- بررسی و ارزیابی ظرفیت‌های بازیابی و بازتوانی مرکز
۵- بررسی و ارزیابی میزان اثرپذیری عملکرد مرکز ناشی از تهدید/حادثه
۶- بررسی و ارزیابی قابلیت‌های تطبیق‌پذیری وضع موجود با شرایط اولیه عملکردی مرکز
۷- ارائه راهکارهای لازم برای ارتقاء تاب‌آوری مرکز زیرساختی
۸- به‌روز رسانی طرح

۴) طرح کاهش آسیب‌پذیری

۱- بررسی و تعیین نوع و سطح آسیب‌پذیری‌ها
۲- تعیین نوع تهدیدات مبتنی بر آسیب‌پذیری‌های موجود
۳- بررسی و تعیین اندرکنش تهدید و آسیب‌پذیری
۴- تجزیه و تحلیل آسیب‌پذیری
۵- تعیین آسیب‌پذیری پایه (تعیین درجه آسیب محتمل)
۶- تعیین آستانه آسیب‌پذیری قابل پذیرش
۷- تولید سناریو و برنامه‌ریزی کاهش تأثیرپذیری
۸- نظارت و کنترل بر کاهش آسیب‌پذیری
۹- مستندسازی آسیب‌پذیری‌ها
۱۰- ارزیابی، بازخورد و به‌روز رسانی طرح

۵) طرح بهینه‌سازی وابستگی و وابستگی‌های متقابل

۱- بررسی ویژگی‌های وابستگی و تعیین نوع آن (درونی و بیرونی)
۲- دسته‌بندی وابستگی‌ها (فیزیکی، جغرافیایی، سایبری و منطقی)

۳- تعیین و بررسی درجه وابستگی دارایی‌ها و تاثیر آن بر عملکرد مرکز
۴- بررسی پیامدهای ناشی از وابستگی و تعیین نوع تخریب
۵- ارائه راهکار بهینه‌سازی وابستگی مبتنی بر نوع ارتباطات (درونی و بیرونی)
۶- به‌روز رسانی طرح

۶) طـرح ارزیابی و ارتقاء آمادگـی‌های زیرساختـی

۱- تهیه و تصویب طرح رزمایش
۲- سازماندهی ساختارها، ظرفیت‌ها، نیروی انسانی و تقسیم کار لازم برابر طرح مصوب شده
۳- تأمین تجهیزات طرح رزمایش
۴- آموزش عمومی و تخصصی نیروهای رزمایش
۵- تمرین و مهارت افزایی
۶- اجرای رزمایش
۷- ارزیابی، بازخورد و اصلاح طرح

۷) طـرح حفاظت از مردم و نیروی انسانی در مراکز زیرساختی

الف- حفاظت از مردم

۱- تعیین محدوده ایمنی برای استقرار مراکز سکونتگاهی در اطراف مراکز
۲- اعلام فوری و هشدار وضعیت اضطراری به مراجع ذیربط پس از وقوع حادثه/تهدید
۳- حفظ حداکثری آرامش و ایجاد امنیت با به کارگیری ظرفیّت‌های انتظامی در زمان وقوع تهدید/حادثه
۴- آموزش عمومی به مردم برای پیشگیری از شدت حادثه/تهدید با همکاری دستگاه‌های ذیربط
۵- برگزاری رزمایش‌های سالانه
۶- ارزیابی اثربخشی اقدامات حفاظت از مردم و به‌روزرسانی طرح

تبصره- تمام مراکز زیرساختی موظفند مبتنی بر شدّت و سطح پیامدهای احتمالی ناشی از وقوع تهدید یا حادثه در آنها، حـریم ایمنی، امنیتی و حفاظتی برای استقرار مراکز سکونتگاهی در مجاورت خود را مشخص و پس از تأیید سازمان بـه ذی‌نفعـان اطلاع‌رسانی نمایند.

ب- حفاظت از نیروی انسانی در مرکز

۱- شناسایی و ارزیابی نیروی انسانی موجود (کارکنان، مراجعین، پیمانکاران) در مرکز
۲- شناسایی ریسک متوجه نیروی انسانی متناسب با نوع شغل و محل فعالیت آنها
۳- پیش‌بینی و طراحی ظرفیت‌های لازم در مرکز جهـت حفاظـت از نیـروی انسـانی (نقـاط امـن، پناهگـاه، اسـکان اضطراری و مانند آن) متناسب با جانمایی تأسیسات و تجهیزات پرخطر در سایت مرکز
۴- پیش‌بینی و تأمین امکانات و تجهیزات حفاظت از نیروی انسانی در شرایط تهدید/حادثه
۵- پیش‌بینی تضمین جبران خسارت (بیمه عمر، بیمه حوادث، بیمه مسئولیت و سایر) در صورت وقوع حادثه/تهدید
۶- آموزش و تمرین طرح تهیه شده و برگزاری رزمایش‌های سالانه
۷- ارزیابی اثربخشی اقدامات حفاظت از نیروی انسانی و به‌روزرسانی طرح

۸) طـرح حفاظت فیزیکی مراکز زیرساختی

۱- شناسایی دارایی‌های مرکز

۲- ارزیابی و درجه‌بندی دارایی‌ها
۳- تعیین نقاط کلیدی و گره‌های اصلی در فرآیند و تعیین جذابیت هدف
۴- حیطه‌بندی امنیتی و تعیین محدوده‌های مجاز دسترسی متناسب با درجه اهمیت دارایی‌ها
۵- پیش‌بینی و بکارگیری تجهیزات و سامانه‌های حفاظت فیزیکی متناسب با ارزش دارایی با لایه‌های انسانی، مهندسی، مکانیکی و سایبری هوشمند
۶- ارزیابی اثربخشی اقدامات حفاظتی و به‌روزرسانی طرح

تذکر۱- در تهیه طرح‌های عملیاتی مراکز زیرساختی رعایت الزامات عمومی مندرج در دستورالعمل شماره ۱۰۲-۰-ث مهرماه ۱۴۰۲ سازمان، مورد تاکید است.

تذکر۲- دستگاه‌های اجرایی در تهیه طرح‌های عملیاتی، رؤس گام‌های فوق را مدنظر قرار داده و متناسب با مأموریت هریک از مراکز زیرساختی، درصورت لزوم، آنها را تکمیل کنند.

تذکر۳- دستگاه‌های متولی راهبری مراکز حیاتی و حساس موظفند طرح‌های عملیاتی مراکز خود را هر ۴ سال یکبار مبتنی بر روند تهدیدات آتی با هماهنگی سازمان به‌روزرسانی کنند.

ماده۸– تهیه و تدوین طرح‌های جامع حفاظت از زیرساخت

الف- طرح جامع موضوعی [۳۶]

به منظور دستیابی به پایداری و تاب‌آوری ملّی و همچنین خدمات رسانی بی‌وقفه به مردم، ضرورت دارد در سطح راهبردی طرح‌های جامع موضوعی در حوزه‌های با اهمّیت کشور از منظر پدافند غیرعامل مورد توجّه و مطالعه قرار گیرند؛ گام‌های اجرایی در تهیه و تدوین این طرح‌ها بشرح زیر است:

۱) شناخت و ارزیابی
۱- شناخت کلی از موضوع و دامنه تأثیر آن
۲- شناخت مأموریت، سیاست‌ها، الزامات و ملاحظات پدافند غیرعامل در موضوع موردنظر
۳- گردآوری و بررسی اسناد (سیاست‌های کلان، برنامه‌های توسعه‌ای، اسناد راهبردی داخلی و خارجی، سند چشم‌انداز، معاهدات و قوانین بین‌المللی و سایر) فرادستی و فرودستی مرتبط با موضوع
۴- بررسی مطالعات موجود مرتبط (داخلی و خارجی)
۵- مطالعات تکمیلی با هدف تبیین اهداف و انتظارات پدافند غیرعامل در موضوع موردنظر

تذکر- قبل از ورود به مرحله بعد لازم است مشاور نتیجه مرحله شناخت و ارزیابی را ارائه و نظر سازمان را دریافت کند.

۲) محیط شناسی
۱- شناخت و ارزیابی تهدیدات و آسیب‌پذیری‌های ملّی (در موضوع مورد نظر)
۲- بررسی چالش‌های اساسی کشور (در موضوع مورد نظر)
۳- بررسی پیشران‌های اساسی کشور (در موضوع مورد نظر)

۳) تدوین راهبردها
۱- ارائه اهداف کلان و چشم‌انداز ملی (در موضوع مورد نظر)
۲- ارائه سیاست‌ها، راهبردها و برنامه‌های کلان موضوعی

[36] Sector Specific Plan (SSP)

۳- ارائه نقشه راه پدافند غیرعامل (در موضوع مورد نظر)
۴- الزامات تحقّق و زمان‌بندی دستیابی به اهداف

ب- طرح جامع بخشی

طرح‌های جامع بخشی یکی از انواع طرح‌های موضوعی حفاظت از زیرساخت است که در سطح عملیاتی متناسب با مأموریت دستگاه‌های اجرایی کشور ذیل هر یک از حوزه‌های با اهمّیت تهیه می‌شوند؛ گام‌های اجرایی در تهیه و تدوین این طرح‌ها بشرح زیر می‌باشد:

۱) محیط شناسی

۱- بررسی گرودارن و ذینفعان بخش (در ارتباط با سایر بخش‌های وابسته به آن)
۲- شناخت مراکز و دارائی‌های با اهمیت بخش (دسته‌بندی و سطح‌بندی)
۳- شناخت و ارزیابی تهدیدات مؤثر بر عملکرد بخش (دسته‌بندی و تعیین تهدید مبنا)
۴- شناخت و ارزیابی آسیب‌پذیری‌های بخش(ذاتی، سیستمی و سایر) و تعیین میزان وابستگی و اندرکنش با سایر بخش‌ها
۵- شناخت، دسته‌بندی و ارزیابی پیامدها (پیامدهای احتمالی اختلال در عملکرد بخش)
۶- بررسی و شناسایی ریسک‌های بخشی
۷- مدیریت ریسک و راهکارهای آن

۲) تدوین راهبردهای بخشی

۱- ارائه اهداف کلان و چشم‌انداز حاکم بر بخش
۲- ارائه سیاست‌ها، راهبردها و برنامه‌های کلان بخشی در راستای برنامه توسعه کشور
۳- بررسی و ارزیابی اثربخشی اقدامات

۳) ارائه الگوی بومی پدافند غیرعامل بخش

۱- ارائه طرح‌های عملیاتی مرتبط با بخش
۲- اولویت‌های تحقیق و توسعه بخشی

تذکر۱- دستگاه‌های اجرایی در تهیه طرح‌های جامع موضوعی و بخشی، رؤس گام‌های فوق را مدنظر قرار داده و درصورت لزوم، آنها را تکمیل کنند.

تذکر۲- طرح‌های جامع موضوعی و بخشی متناسب با برنامه‌های پنج ساله توسعه کشور، هر ۵ سال یکبار مبتنی بر روند تهدیدات آتی با هماهنگی سازمان به‌روزرسانی می‌شوند.

ماده۹- الزامات فنّی

به‌منظور اثربخشی اقدامات، مشارکت ذینفعان و هم‌افزایی بخش‌های فنّی در تهیه طرح‌های حفاظت از زیرساخت و ارتقاء سطح کیفی خدمات پدافند غیرعامل و همچنین تدوین معیارها و شاخص‌های ارزیابی فنّی برای طرح‌های زیرساختی در کشور، دستگاه‌های متولّی مراکز زیرساختی با اهمّیت موظّفند الزامات فنّی زیر را در مراحل طراحی، اجرا و بهره‌برداری از دارایی‌های مراکز خود پیاده‌سازی و اجرا نمایند.

۱) درجه‌بندی دارایی

برای درجه‌بندی دارایی‌های مراکز زیرساختی ضرورت دارد متناسب با ویژگی‌های خاص هر مرکز و اهمّیت آن، مؤلفه‌های ماهیّت، هوشمندی، کارکرد، وابستگی، سیستمی یا غیرسیستمی بودن و خطرزایی نیز مدنظر قرار گیرند. برای

درک بهتر از مفهوم درجه‌بندی دارایی برای هریک از مراکز زیرساختی، راهنمای درجه‌بندی دارایی‌ها توسط سازمان تهیه و ابلاغ می‌گردد.

۲) وابستگی متقابل

الزام۱- مراکز زیرساختی حیاتی با سطح بدون پیامد سیستمی از وابستگی متقابل و تأکید بر حذف حداکثری درجه بیشینه منحصربفرد (حذف حداکثری قطب منحصربفرد) حذف هرگونه وابستگی براساس مرکزیت مسیرهای مستقیم و افزایش ۸۵ درصدی به بالای سطح خوشه‌بندی در دارایی‌های اصلی (درجه ۱ و ۲) طراحی و اجرا شود.

الزام۲- مراکز زیرساختی حساس با سطح بسیار محدود پیامد سیستمی از وابستگی متقابل و تأکید بر حذف حداکثری درجه بیشینه منحصربفرد (حذف حداکثری قطب منحصربفرد) حذف حداکثری وابستگی براساس مرکزیت مسیرهای مستقیم و افزایش ۶۰ درصدی به بالای سطح خوشه‌بندی در دارایی‌های اصلی، طراحی و اجرا گردد.

الزام۳- مراکز زیرساختی مهم با سطح بهینه پیامد سیستمی از وابستگی متقابل و تأکید بر حذف بهینه درجه بیشینه منحصر بفرد (حذف بهینه قطب منحصربفرد)، حذف بهینه وابستگی براساس مرکزیت مسیرهای مستقیم و افزایش ۴۵ درصدی به بالای سطح خوشه‌بندی در دارایی‌های اصلی، طراحی و اجرا گردد.

الزام۴- مراکز زیرساختی قابل حفاظت می‌بایست با سطح قابل قبول پیامد سیستمی از وابستگی متقابل و تأکید بر حذف حداقلی درجه بیشینه منحصربفرد (حذف حداقلی قطب منحصربفرد) نگهداشت قابل قبول وابستگی براساس مرکزیت مسیرهای مستقیم و نگهداشت حداقل ۲۰ درصدی سطح خوشه‌بندی در دارایی‌های اصلی، طراحی و اجرا گردد.

مرکز	درجه بیشینه منحصربفرد	مرکزیت مسیرهای مستقیم	خوشه بندی	سطح پیامد سیستمی
حیاتی	حذف حداکثری	حذف هرگونه وابستگی	حداقل ۸۵ درصد	بدون پیامد
حساس	حذف حداکثری	حذف حداکثری وابستگی	حداقل ۶۰ درصد	بسیار محدود
مهم	حذف بهینه	حذف بهینه وابستگی	حداقل ۴۵ درصد	بهینه
قابل حفاظت	حذف حداقلی	نگهداشت قابل قبول وابستگی	نگهداشت حداقل ۲۰ درصد	قابل قبول

۳) سیستمی و شبکه‌ای

روابط سیستمی و شبکه‌ای در مراکز زیرساختی متناسب با سطح اهمّیت آنها باید به نحوی طراحی گردد که:

الزام۱- مراکز زیرساختی حیاتی از درجه وابستگی حداقلی با نوع ارتباط سیستمی درهم تنیده کامل و قابلیت مورد انتظار کارکرد در ارائه خدمات کلیدی به صورت پایدار و مستمر برخوردار باشند.

الزام۲- مراکز زیرساختی حساس از درجه وابستگی حداقلی با نوع ارتباط سیستمی درهم تنیده کامل و قابلیت مورد انتظار کارکرد در ارائه خدمات کلیدی برخوردار باشند.

الزام۳- مراکز زیرساختی مهم از درجه وابستگی قابل قبول با نوع ارتباط سیستمی درهم تنیده بخشی و قابلیت مورد انتظار کارکرد در ارائه خدمات ضروری برخوردار باشند.

الزام۴- مراکز زیرساختی قابل حفاظت از درجه وابستگی قابل قبول با نوع ارتباط سیستمی درهم تنیده بخشی و قابلیت مورد انتظار کارکرد در ارائه خدمات لازم برخوردار باشند.

مرکز	درجه وابستگی*	ارتباط سیستمی	قابلیت مورد انتظار کارکرد
حیاتی	حداقل وابستگی	درهم تنیده کامل	ارائه خدمات کلیدی
حساس	حداقل وابستگی	درهم تنیده کامل	ارائه خدمات کلیدی
مهم	وابستگی قابل قبول	درهم تنیده بخشی	ارائه خدمات ضروری
قابل حفاظت	وابستگی قابل قبول	درهم تنیده بخشی	ارائه خدمات لازم

* درجه وابستگی بصورت بهینه شده و مبتنی بر طیف لیکرت تعریف گردد.

۴) سایبری

به کارگیری الزامات سایبری در مراکز زیرساختی متناسب با سطح اهمّیت آنها باید به نحوی باشد که:

الزام۱- مراکز زیرساختی حیاتی بصورت آسیب‌ناپذیر سایبری با معماری شبکه مبتنی بر متدولوژی دفاع در عمق، دفاع لایه به لایه، اصل اعتماد صفر، هوشمندسازی بسیار محدود، بومی و امن (حتی‌المقدور بدون هوشمندسازی)، با کارکرد سلولی مستقل از ساختار هوشمند و بصورت موازی با اولویت فرمان دستی با هدف ارائه خدمات کلیدی طراحی و اجرا گردند.

الزام۲- مراکز زیرساختی حساس برخوردار از ذات سایبری مستحکم با معماری شبکه مبتنی بر متدولوژی دفاع در عمق، دفاع لایه به لایه، اصل اعتماد صفر، هوشمندسازی بومی و امن با کارکرد سلولی مستقل از ساختار هوشمند و بصورت موازی با اولویت فرمان دستی با هدف ارائه خدمات کلیدی طراحی و اجرا گردند.

الزام۳- مراکز زیرساختی مهم با حداقل آسیب‌پذیری سایبری ممکن و معماری شبکه مبتنی بر متدولوژی دفاع در عمق، دفاع لایه به لایه، اصل اعتماد صفر، هوشمندسازی آزموده شده و بصورت موازی با اولویت فرمان دستی با هدف ارائه خدمات ضروری طراحی و اجرا گردند.

الزام۴- مراکز زیرساختی قابل حفاظت با حداقل آسیب‌پذیری قابل قبول سایبری و معماری شبکه مبتنی بر متدولوژی دفاع در عمق، دفاع لایه به لایه، هوشمندسازی ایمن و بصورت موازی با اولویت فرمان دستی با هدف ارائه خدمات لازم طراحی و اجرا گردند.

مرکز	پایداری سایبری	نوع هوشمندسازی	نوع فرمان	کارکرد سایبری
حیاتی	آسیب ناپذیر سایبری	بسیار محدود و بومی	با قابلیت فرمان دستی	ارائه خدمات کلیدی
حساس	ذات سایبری مستحکم	هوشمندسازی بومی	با قابلیت فرمان دستی	ارائه خدمات کلیدی
مهم	حداقل آسیب‌پذیری سایبری ممکن	هوشمندسازی آزموده شده	با قابلیت فرمان دستی	ارائه خدمات ضروری
قابل حفاظت	حداقل آسیب‌پذیری قابل قبول سایبری	هوشمندسازی ایمن	با قابلیت فرمان دستی	ارائه خدمات لازم

۵) مدیریت مخاطرات

الف) در مرحله طراحی

در این مرحله، مدیریت مخاطرات در مراکز زیرساختی دارای پتانسیل خطر با پیامد گسترده[37] الزامات زیر پیاده‌سازی می‌شود:

[37] As Low As Reasonably Practicable (ALARP)

الزام۱- مراکز زیرساختی حیاتی برای بدترین سناریو در جهت دستیابی به سطح ایمنی حداکثری با رویکرد حذف/کنترل کامل عامل خطر در تمامی اجزای پرخطر، سطح حفاظتی و امنیتی حداکثری و عدم پذیرش هرگونه ریسک طراحی گردند.

الزام۲- مراکز زیرساختی حساس برای بدترین سناریو در جهت دستیابی به سطح ایمنی حداکثری با رویکرد حذف/کنترل کامل عامل خطر در تمامی اجزای پرخطر، سطح حفاظتی و امنیتی حداکثری و قبول ریسک حداقلی طراحی گردند.

الزام۳- مراکز زیرساختی مهم برای محتمل‌ترین سناریو در جهت دستیابی به سطح ایمنی حداقلی با رویکرد حذف/کنترل نسبی عامل خطر در اجزای با پتانسیل خطر بالا، سطح حفاظتی و امنیتی حداقلی و قبول ریسک نسبی طراحی گردند.

الزام۴- مراکز زیرساختی قابل حفاظت برای محتمل‌ترین سناریو در جهت دستیابی به سطح ایمنی حداقلی با رویکرد حذف/کنترل بهینه عامل خطر در اجزای با پتانسیل خطر بالا، سطح حفاظتی و امنیتی حداقلی و قبول ریسک بهینه طراحی گردند.

مرکز	سناریو/رویکرد طراحی	سطح ایمنی(تجهیزاتی)	حذف/کنترل عامل خطر	سطح حفاظتی- امنیتی	سطح ریسک*
حیاتی	بدترین سناریو	حداکثری	کامل	حداکثری	بدون قبول ریسک
حساس	بدترین سناریو	حداکثری	کامل	حداکثری	قبول ریسک حداقلی
مهم	محتمل‌ترین سناریو	حداقلی	نسبی	حداقلی	قبول ریسک نسبی
قابل حفاظت	محتمل‌ترین سناریو	حداقلی	بهینه	حداقلی	قبول ریسک بهینه

* سطح پذیرش تعریف شده برای ریسک مبتنی بر طیف لیکرت تعریف گردد.

ب) در مرحله بهره‌برداری (عملیات)

در این مرحله، اقدامات مرتبط با مدیریت مخاطرات در زیرساخت‌های دارای پتانسیل خطر با در رعایت الزامات زیر پیاده‌سازی می‌شود:

الزام۱- مراکز زیرساختی حیاتی با ایجاد و پیاده‌سازی ساختار فرماندهی حادثه و اجرای کامل طرح مدیریت ایمنی فرآیند، بدون قبول ریسک از قابلیت پاسخ سریع و فوری به شرایط اضطراری برخوردار باشند.

الزام۲- مراکز زیرساختی حساس با ایجاد و پیاده‌سازی ساختار فرماندهی حادثه و اجرای کامل طرح مدیریت ایمنی فرآیند، با قبول ریسک حداقلی از قابلیت پاسخ سریع و فوری به شرایط اضطراری برخوردار باشند.

الزام۳- مراکز زیرساختی مهم با راه‌اندازی مرکز کنترل شرایط اضطراری و اجرای طرح مدیریت ایمنی فرآیند در بخش‌های دارای پتانسیل خطر، با قبول ریسک نسبی از قابلیت پاسخ نسبی به شرایط اضطراری برخوردار باشند.

الزام۴- مراکز زیرساختی قابل حفاظت با راه‌اندازی مرکز کنترل شرایط اضطراری و اجرای طرح مدیریت ایمنی فرآیند در بخش‌های دارای پتانسیل خطر، با قبول ریسک بهینه از قابلیت پاسخ بهینه به شرایط اضطراری برخوردار باشند.

مرکز	مدیریت و فرماندهی حادثه[38]	طرح مدیریت ایمنی فرآیند[39]	پاسخ	سطح ریسک*
حیاتی	ایجاد و پیاده‌سازی ساختار فرماندهی حادثه	اجرای کامل طرح	سریع و فوری	بدون قبول ریسک
حساس	ایجاد و پیاده‌سازی ساختار فرماندهی حادثه	اجرای کامل طرح	سریع و فوری	قبول ریسک حداقلی
مهم	راه‌اندازی مرکز کنترل شرایط اضطراری	اجرا در بخش‌های دارای پتانسیل خطر	نسبی	قبول ریسک نسبی
قابل حفاظت	راه‌اندازی مرکز کنترل شرایط اضطراری	اجرا در بخش‌های دارای پتانسیل خطر	بهینه	قبول ریسک بهینه

* سطح پذیرش تعریف شده برای ریسک مبتنی بر طیف لیکرت تعریف گردد.

۶) رصد و پایش تهدیدات و آسیب پذیری

رصد و پایش تهدیدات و آسیب‌پذیری در مراکز زیرساختی متناسب با سطح اهمّیت آنها باید به نحوی باشد که:

الزام۱- در مراکز زیرساختی حیاتی، تهدیدات اثرگذار مستقیم هر سه ماه یکبار و تهدیدات با حیطه اثر غیرمستقیم نیز هر شش ماه یکبار احصاء و پایش گردد. این مراکز باید بصورت کامل به سامانه‌های رصد و پایش برخط متصل باشند. آسیب‌پذیری‌ها نیز هر سه ماه یکبار پایش و براساس نوع، اندازه، احتمال وقوع و پیامد، ارزیابی، درجه‌بندی و اندازه‌گیری شوند.

الزام۲- در مراکز زیرساختی حساس، تهدیدات اثرگذار مستقیم بصورت شش ماه یکبار و تهدیدات با حیطه اثر غیرمستقیم نیز هر سال یکبار احصاء و پایش گردد. این مراکز باید بصورت بهینه به سامانه‌های رصد و پایش برخط متصل باشند. آسیب‌پذیری‌ها نیز هر شش ماه یکبار پایش و براساس نوع، اندازه، احتمال وقوع و پیامد، ارزیابی، درجه‌بندی و اندازه‌گیری شوند.

الزام۳- در مراکز زیرساختی مهم، تهدیدات اثرگذار مستقیم و غیرمستقیم هر سال یکبار احصاء و پایش گردد. این مراکز باید بصورت بهینه در خدمات ضروری به سامانه‌های رصد و پایش برخط متصل باشند. آسیب‌پذیری‌ها نیز هر سال یکبار پایش و براساس نوع، اندازه، احتمال وقوع و پیامد، ارزیابی، درجه‌بندی و اندازه‌گیری شوند.

الزام۴- در مراکز زیرساختی قابل حفاظت، تهدیدات اثرگذار مستقیم بصورت سالی یکبار و تهدیدات با حیطه اثر غیرمستقیم نیز هر دو سال یکبار احصاء و پایش گردد. این مراکز باید بصورت حداقلی در خدمات ضروری به سامانه‌های رصد و پایش برخط متصل باشند. آسیب‌پذیری‌ها نیز هرسال یکبار پایش و براساس نوع، اندازه، احتمال وقوع و پیامد، ارزیابی، درجه‌بندی و اندازه‌گیری شوند.

مرکز	رصد و پایش تهدیدات اثرگذار مستقیم	رصد و پایش تهدیدات اثرگذار غیرمستقیم	اتصال به سامانه رصد و پایش برخط تهدیدات	پایش و ارزیابی آسیب‌پذیری‌ها
حیاتی	سه ماه یکبار	شش ماه یکبار	بصورت کامل	سه ماه یکبار
حساس	شش ماه یکبار	سالی یکبار	بصورت بهینه	شش ماه یکبار
مهم	سالی یکبار	سالی یکبار	بصورت بهینه در خدمات ضروری	سالی یکبار
قابل حفاظت	سالی یکبار	دو سال یکبار	بصورت حداقلی در خدمات ضروری	سالی یکبار

[38] Incident Command System (ICS)
[39] Process Safety Management (PSM)

۷) تهدیدات درون‌زا

شرایط مواجهه با تهدیدات درون‌زا در مراکز زیرساختی متناسب با سطح اهمیت آنها باید به نحوی باشد که:

الزام۱- در مراکز زیرساختی حیاتی، سطح صیانت در برابر عامل تهدید درون‌زا با سطح اعتماد صفر، دانش کاملاً محدود شده و دسترسی بسته، میزان در معرض عامل تهدید بودن به صورت حذف کامل جذابیت، سطح قابل قبول پیامد اعمال تهدید به صورت بدون اختلال و سازوکار محافظتی به صورت کاملا آزموده شده با لایه‌بندی کامل حفاظتی می‌باشد.

الزام۲- در مراکز زیرساختی حساس، سطح صیانت در برابر عامل تهدید درون‌زا با سطح اعتماد صفر، دانش محدود شده و دسترسی کنترل شده، میزان در معرض عامل تهدید بودن به صورت حذف جذابیت بدون تأثیر در عملکرد، سطح قابل قبول پیامد اعمال تهدید به صورت بدون اختلال و سازوکار محافظتی به صورت آزموده شده بر پایه اولویت‌بندی با لایه‌بندی کامل حفاظتی می‌باشد.

الزام۳- در مراکز زیرساختی مهم، سطح صیانت در برابر عامل تهدید درون‌زا با سطح اعتماد، دانش و دسترسی کنترل شده، میزان در معرض عامل تهدید بودن به صورت حذف جذابیت با درنظر گرفتن سطح عملکرد، سطح قابل قبول پیامد اعمال تهدید به صورت اختلال در حد قابل تعمیر و بازیابی و سازوکار محافظتی مبتنی بر الگوی تأمین می‌باشد.

الزام۴- در مراکز زیرساختی قابل حفاظت، سطح صیانت در برابر عامل تهدید درون‌زا با سطح اعتماد، دانش و دسترسی کنترل شده، میزان در معرض عامل تهدید بودن به صورت بهینه‌سازی جذابیت، سطح قابل قبول پیامد اعمال تهدید به صورت اختلال در حد قابل تعمیر و بازیابی و سازوکار محافظتی مبتنی بر الگوی تأمین می‌باشد.

مرکز	سطح صیانت در برابر عامل تهدید	در معرض عامل تهدید بودن	سطح قابل قبول پیامد	سازوکار محافظتی
حیاتی	اعتماد صفر دانش کاملاً محدود شده دسترسی بسته	حذف کامل جذابیت	بدون اختلال	کاملا آزموده شده با لایه‌بندی کامل حفاظتی
حساس	اعتماد صفر دانش محدود شده دسترسی کنترل شده	حذف جذابیت بدون تأثیر در عملکرد	بدون اختلال	آزموده شده بر پایه اولویت‌بندی با لایه‌بندی کامل حفاظتی
مهم	اعتماد، دانش و دسترسی کنترل شده	حذف جذابیت با درنظر گرفتن سطح عملکرد	اختلال در حد قابل تعمیر و بازیابی	مبتنی بر الگوی تأمین
قابل حفاظت	اعتماد، دانش و دسترسی کنترل شده	بهینه‌سازی جذابیت	اختلال در حد قابل تعمیر و بازیابی	مبتنی بر الگوی تأمین

۸) ارتقای آمادگی

براساس سطح‌بندی مراکز و سطح پیامد متصور به ازای تهدیدات مرتبط، سطح و میزان آمادگی زیرساختی در آنها به شرح ذیل می‌باشد:

الزام۱- مراکز زیرساختی حیاتی از سطح آمادگی کامل با قابلیت پاسخ سریع و فوری به حادثه/تهدید و آمادگی دائمی ۷*۲۴ فعالیت‌های اصلی در ارائه خدمات زیرساختی برخوردار باشند.

الزام۲- مراکز زیرساختی حساس از سطح آمادگی کامل با قابلیت پاسخ سریع و فوری به حادثه/تهدید و آمادگی دائمی ۷*۲۴ فعالیت‌های اصلی در ارائه خدمات زیرساختی برخوردار باشند.

الزام۳- مراکز زیرساختی مهم از سطح آمادگی هوشیارانه با قابلیت آمادگی برای پاسخ حادثه/تهدید و آمادگی نوبه‌ای ۷*۱۶ فعالیت‌های اصلی در ارائه خدمات زیرساختی برخوردار باشند.

الزام۴- مراکز زیرساختی قابل حفاظت از سطح و قابلیت آمادگی عمومی برای پاسخ حادثه/تهدید و آمادگی نوبه‌ای ۷*۱۶ فعالیت‌های اصلی در ارائه خدمات زیرساختی برخوردار باشند.

توضیح- منظور از آمادگی دائمی۷*۲۴ آمادگی برای ارائه خدمات زیرساختی در طول هفته و بصورت ۲۴ساعته می‌باشد و منظور از آمادگی نوبه‌ای۷*۱۶ آمادگی برای ارائه خدمات زیرساختی در طول ایام هفته و بصورت ۱۶ ساعته می‌باشد.

مرکز	سطح آمادگی	قابلیت مورد انتظار	میزان آمادگی
حیاتی	کامل	پاسخ سریع و فوری به حادثه و تهدید	دائمی ۷*۲۴
حساس	پیشگیرانه	پاسخ سریع و فوری به حادثه و تهدید	دائمی ۷*۲۴
مهم	هوشیارانه	آمادگی برای پاسخ	نوبه‌ای ۷*۱۶
قابل حفاظت	عمومی	آمادگی عمومی	نوبه‌ای ۷*۱۶

۹) تداوم کارکرد

متناسب با سطح اهمیت مراکز زیرساختی ضروریست میزان تداوم کارکرد و پایداری خدمات در آنها به شرح ذیل تأمین و تضمین گردد:

مرکز	حیاتی	حساس	مهم	قابل حفاظت
تداوم کارکرد	خدمات کلیدی	خدمات کلیدی	خدمات ضروری	خدمات لازم

توضیح - منظور از تداوم کارکرد برای ارائه خدمات، حفظ عملکرد مرکز در حین بروز تهدید/حادثه می‌باشد.

۱۰) تاب‌آوری

سطح تاب آوری در مراکز زیرساختی متناسب با ظرفیت مورد انتظار در هریک از آنها باید به نحوی باشد که:

الزام۱- در مراکز زیرساختی حیاتی با تأکید بر ظرفیت جذب حداکثری تنش، ظرفیت تطبیق‌پذیری و جایگزینی کامل، عدم اثرپذیری کلیه خدمات مرکز و برگشت‌پذیری اضطراری، سطح تاب‌آوری درجه۱ تأمین گردد.

الزام۲- در مراکز زیرساختی حساس با تأکید بر ظرفیت جذب متعادل تنش، ظرفیت تطبیق‌پذیری و جایگزینی بالا، عدم اثرپذیری کلیه خدمات مرکز و برگشت‌پذیری اضطراری، سطح تاب‌آوری درجه ۲ تأمین گردد.

الزام۳- در مراکز زیرساختی مهم با تأکید بر ظرفیت جذب محدود تنش، ظرفیت تطبیق‌پذیری و جایگزینی بهینه، عدم اثرپذیری و ظرفیت برگشت‌پذیری با هدف برگشت سریع خدمات ضروری مرکز، سطح تاب‌آوری درجه ۳ تأمین گردد.

الزام۴- در مراکز زیرساختی قابل حفاظت با تأکید بر ظرفیت جذب حداقلی تنش، ظرفیت تطبیق‌پذیری و جایگزینی محدود، ظرفیت برگشت‌پذیری با هدف برگشت سریع خدمات ضروری مرکز، سطح تاب‌آوری درجه ۴ تأمین گردد.

مرکز	ظرفیت جذب	ظرفیت تطبیق‌پذیری و جایگزینی	عدم اثرپذیری	برگشت پذیری
حیاتی	حداکثری	کامل	کلیه خدمات (کلیدی، ضروری، لازم)	اضطراری
حساس	متعادل	بالا	کلیه خدمات (کلیدی، ضروری، لازم)	اضطراری
مهم	محدود	بهینه	خدمات ضروری	خدمات ضروری
قابل حفاظت	حداقلی	محدود	خدمات ضروری	خدمات ضروری

۱۱) مصونیت

سطح مورد انتظار از مصون‌سازی در مراکز زیرساختی پس از پیاده‌سازی الزامات فوق باید به نحوی باشد که:

الزام۱- مراکز زیرساختی حیاتی با تأکیدبر تاب‌آوری، آسیب‌ناپذیری و تداوم کارکرد در ارائه خدمات کلیدی به سطح ۱۰۰ درصدی از مصونیت برسند.

الزام۲- مراکز زیرساختی حساس با تأکیدبر استحکام، حداقل آسیب‌پذیری ممکن و تداوم کارکرد در ارائه خدمات کلیدی به سطح ۷۰ درصدی از مصونیت برسند.

الزام۳- مراکز زیرساختی مهم با تأکیدبر امنیت، حداقل آسیب‌پذیری قابل قبول و تداوم کارکرد در ارائه خدمات ضروری به سطح ۵۰ درصدی از مصونیت برسند.

الزام۴- مراکز زیرساختی قابل حفاظت با تأکیدبر ایمنی، حداقل آسیب‌پذیری قابل قبول و تداوم کارکرد در ارائه خدمات لازم به سطح ۳۰ درصدی از مصونیت برسند.

مرکز	سطح تاب‌آوری [۴۰]	سطح آسیب پذیری[۴۱]	سطح تداوم کارکرد	درصد مصونیت
حیاتی	پایدار	آسیب ناپذیر	خدمات کلیدی	۱۰۰
حساس	مستحکم	حداقل آسیب پذیری ممکن	خدمات کلیدی	۷۰
مهم	امن	حداقل آسیب پذیری قابل قبول	خدمات ضروری	۵۰
قابل حفاظت	ایمن	حداقل آسیب پذیری قابل قبول	خدمات لازم	۳۰

تذکر- تعیین میزان بهینه پیاده‌سازی الزاماتی که در کلیه جداول فوق بعنوان هدف و معیار تعیین شده است با رعایت ملاحظات مهندسی ارزش به دست می‌آید. اگر مبتنی بر شاخص‌های مهندسی ارزش (هزینه- فایده) و سطح تهدید اجرای این الزامات میسر نشود، ضرورت دارد طرح توجیهی میزان دقیق رعایت الزامات در مراکز زیرساختی توسط مشاور طرح تهیه و به تایید سازمان برسد.

ماده۱۰- اقدامات مشترک

دستگاه‌های اجرایی دارای مراکز زیرساختی با اهمّیت در کشور موظّفند:

[۴۰] این عبارات معادل درجه‌های مختلف مصون‌سازی و متناسب با سطح پایداری مورد انتظار از آن در مراکز زیرساختی می‌باشد.
[۴۱] میزان حداقل آسیب‌پذیری مبتنی بر اصل هزینه - فایده استخراج می‌شود.

۱) شورای داخلی حفاظت از زیرساخت را با مسئولیت رئیس کمیته پدافند غیرعامل دستگاه با مشارکت واحدهای حراست و بسیج دستگاه تشکیل داده و گزارش‌های مربوطه را به دبیرخانه شورای هماهنگی حفاظت از زیرساخت مستقر در معاونت طرح‌ریزی و نظارت فنی سازمان ارسال نمایند.

۲) متناسب با درجه اهمّیت مراکز زیرساختی خود و سطح ریسک آن، علاوه بر اولویت‌بندی اقدامات مصون‌سازی مبتنی بر الزامات این نظام، برنامه‌های حفاظت از زیرساخت مستخرجه از آن را نیز به صورت سالانه و بلندمدت تهیه و به سازمان ارائه نماید.

۳) به منظور حصول اطمینان از اثربخشی اقدامات حفاظت از زیرساخت، با سازماندهی تیم‌های عملیاتی در قالب ممیزی‌های داخلی، نظارت لازم را بر پیاده‌سازی و اجرای الزامات این نظام، اعمال نمایند.

۴) دستورالعمل‌های اجرایی موردنیاز حوزه خود را در چارچوب این سند و در قالب برنامه بخشی حفاظت از زیرساخت دستگاه تهیه و پس از تصویب سازمان، اجرا نمایند.

۵) درصورت وقوع تهدید یا حادثه با هماهنگی مرکز مدیریت و هماهنگی عملیاتی زیرساخت، در قالب اطلاع‌رسانی، اعلام وضعیت، اجرای فرمان و انجام هماهنگی نسبت به مدیریت‌صحنه بحران‌ها اقدام نمایند.

۶) درس‌آموخته‌های مربوط به حوادث و تهدیدات زیرساختی حوزه خود را مستندسازی و به مرکز مدیریت و هماهنگی عملیاتی زیرساخت گزارش نمایند تا در انتقال به سایر دستگاه‌ها و به‌روزرسانی دستورالعمل‌ها و الزامات مورد استفاده قرار گیرد.

۷) تجارب حاصل از تهدیدات زیرساختی در سایر دستگاه‌های اجرایی و زیرساخت‌های اصلی را دریافت و نسبت به برگزاری جلسات آموزشی و توجیهی، در دستگاه خود اقدام نمایند.

۸) کمیته تدوین و تنظیم مقررات حفاظت از زیرساخت را با مسئولیت معاون فنی یا مدیرکل پدافند غیرعامل دستگاه تشکیل داده و موضوعات فنی موردنیاز دستگاه که قابلیت تبدیل شدن به مقرّرات و ضوابط فنّی حفاظت از زیرساخت دارند را جهت بررسی به مرکز تدوین و تنظیم مقرّرات حفاظت از زیرساخت ارائه کنند.

۹) برابر نظام آمادگی و رزمایش دستگاه‌های اجرایی در برابر تهدیدات، مصوبه شماره ۲۰۸۸ کمیته دائمی و باهماهنگی سازمان نسبت به برگزاری رزمایش‌های تخصصی حفاظت از زیرساخت در ابعاد مأموریتی خود اقدام نمایند.

۱۰) چنانچه استاندارد پدافند غیرعامل در هریک از موضوعات اصلی حفاظت از زیرساخت تولید گردید نسبت به اجرا و رعایت آن در هریک از مراکز زیرساختی خود اقدام کنند.

۱۱) به صورت فصلی و نوبه‌ای اقدامات انجام شده در قالب این نظام را به سازمان گزارش کنند.

۱۲) نسبت به آموزش، توجیه و توانمندسازی مدیران، کارشناسان و کارکنان زیرمجموعه خود اقدام نمایند.

ماده۱۱– با توجه به تغییرات عناصر محیطی مانند تهدیدات، فناوری‌های بکارگیری شده در زیرساخت‌ها و سایر ملاحظات فنی و مهندسی، برای اجرای بهتر و روزآمدسازی الزامات فنّی تخصصی حفاظت از زیرساخت، دستگاه‌های اجرایی می‌توانند نقطه‌نظرات پیشنهادی و اصلاحی خود را پیرامون این نظام به سازمان اعلام نمایند؛ سازمان با بررسی نظرات دستگاه‌های اجرایی، درصورت نیاز و بعد از ۶ماه، نظام را بازنگری و اصلاح می‌کند.

ماده۱۲– وفق تبصره۱ قانون تشکیل سازمان، مستنکفین از اجرای الزامات و ضوابط این سند در مراکز و دستگاه‌های اجرایی مشمول، علاوه بر جبران خسارات وارد شده، به مجازات موضوع ماده (۵۷۶) کتاب پنجم قانون مجازات اسلامی (تعزیرات و مجازات‌های بازدارنده) مصوب ۱۳۷۵/۳/۰۲ محکوم می‌شوند و چنانچه خسارتی وارد نشده باشد برابر قانون رسیدگی به تخلفات اداری مصوب ۱۳۷۲/۰۹/۰۷ با مستنکف رفتار خواهد شد.

ماده۱۳– سازمان بر حسن اجرای این نظام، نظارت کرده و اجرای آن را سالانه به کمیته‌ی دائمی گزارش کند.

ماده۱۴– این تصویب‌نامه در **چهارده ماده و نه تبصره** در هفتادوهفتمین جلسه کمیته‌ی دائمی به تاریخ بیست و هشتم شهریورماه سال یکهزار و چهارصد و دو هجری شمسی به‌تصویب رسید.

نظام فنی و تخصصی حفاظت از زیرساخت‌های کشور مشتمل بر چهارده ماده و نه تبصره که در تاریخ ۱۴۰۲/۰۶/۲۸ در هفتادو**هفتمین** جلسه کارگروه (کمیته) دائمی پدافند غیرعامل کشور به‌تصویب رسید، به استناد تبصره۱ قانون تشکیل سازمان پدافند غیرعامل کشور و ماده۸ اساسنامه سازمان پدافند غیرعامل کشور مصوّب مقام‌معظّم رهبری(مدظله‌العالی) جهت اجرا ابلاغ می‌گردد./هـ

رئیس ستادکل نیروهای مسلح
و کمیته دائمی پدافند غیرعامل کشور
سرلشکر پاسدار محمّد باقری

فرماندهی کل قوا
جمهوری اسلامی ایران
کمیته دائمی (شورای عالی) پدافند غیرعامل کشور

رونوشت:

رئیس دفتر فرماندهی معظم کل قوا – دفتر رئیس جمهوری اسلامی ایران – دفتر رئیس قوه قضاییه – دفتر رئیس مجلس شورای اسلامی – دفتر معاون اول رئیس‌جمهور– رئیس دفتر رئیس ستاد کل نیروهای مسلح دبیرخانه شورای‌عالی امنیت ملی ج.ا.ا – کلیه وزارتخانه‌ها، سازمان‌ها، موسسات دولتی، نهادهای انقلاب اسلامی و سازمان‌های نیروهای مسلح – سازمان بازرسی کل کشور– دیوان محاسبات کشور– دیوان عدالت اداری– معاونت قوانین مجلس شورای اسلامی – امور تدوین، تنقیح و انتشار قوانین و مقررات – دفتر هیات دولت– روزنامه رسمی جمهوری اسلامی ایران – دبیرخانه شوراهای‌عالی (سلامت و امنیت غذایی، آمایش سرزمین، علوم، تحقیقات و فنآوری (عتف) فضای مجازی، معماری و شهرسازی ایران، هماهنگی ترافیک شهرهای کشور) و دبیرخانه کمیته دائمی پدافند غیرعامل کشور