سازمان حراست کل کشور

وضعیت هشدارهای سایبری و اقدامات ضروری

Cyber Emergency Controls Guideline

سازمان حراست کل کشور

وضعیت هشدارهای سایبری و اقدامات ضروری

(Cyber Emergency Security Controls)

شناسنامه سند

نام سند وضعیت هشدارهای سایبری و اقدامات ضروری

نگارش ۱٫۰

تاریخ صدور ۱۴۰۳/۰۸

آخرین به روز رسانی ۱۴۰۳/۰۸/۰۷

نام فایل SHKK.HF.CECG

شرح سند وضعیت هشدارهای سایبری مبتنی بر شواهد، رویه های اجرایی و اقدامات ضروری به انضمام چک لیست ضروری و ممیزی در هر وضعیت

تهیه شده در اداره کل حفاظت فناوری اطلاعات سازمان حراست کل کشور به همت کمیته سایبری

فهرست مطالب

۱- هدف

با توجه به تهدیدات روزافزون، متنوع و متغیر فضای سایبری، هر روز شاهد حوادث سایبری با درجه‌های ریسک مختلفی هستیم. این حوادث که کانون آن متوجه زیرساخت‌های حیاتی، حساس و مهم کشور است، در زمان‌های خاصی شدت بیشتری می‌یابد که این زمان‌ها را با سطوح هشدار زرد، نارنجی و قرمز مشخص می‌کنیم. از این رو در وضعیت‌های زرد، نارنجی و قرمز نیاز است که اقدامات خاصی صورت گرفته و نهادهای متولی در حالت خاص عملیاتی اقداماتی را با هماهنگی تعریف شده انجام دهند. هدف از تدوین این رویه اجرایی، مشخص کردن اقداماتی است که دستگاه‌ها، می‌بایست در هر یک از وضعیت‌های زرد، نارنجی و قرمز انجام دهند.

لازم به ذکر است که در این سند، اقدامات مرتبط با وضعیت سفید سایبری آورده نشده است و در این راستا، کلیه‌ی خط‌مشی‌ها، دستورالعمل‌ها، الزامات و روش‌های اجرایی که توسط مراجع ابلاغ شده و یا توسط دستگاه تهیه شده است، در وضعیت سفید لازم الاجرا هستند.

۲- دامنه کاربرد

دستگاه‌ها و زیرمجموعه آنها، موظف هستند در زمان اعلام هر یک از وضعیت‌های سایبری زرد، نارنجی یا قرمز، اقدامات مشخص شده در این سند را انجام دهند.

۳- مراجع و اسناد مرتبط

- دستورالعمل‌ها و درس آموخته‌های ابلاغی حراست کل کشور
- استاندارد ISO/IEC 27035:2016 ، مدیریت حوادث امنیت اطلاعات
- استاندارد ISO/IEC 27001:2013
- طرح پاسخگویی به حوادث سایبری، مرکز مدیریت راهبردی افتا، شهریور ۹۸
- الزامات و اقدامات امنیتی جهت پیشگیری و پاسخ به حوادث سایبری، مرکز مدیریت راهبردی افتا، مهر ۱۴۰۰
- طرح پاسخ اضطراری سایبری، قرارگاه پدافند سایبری کشور، مرداد ۹۷
- دستورالعمل عملیاتی پیشگیرانه (اقدامات اساسی) در زمان هشدار سایبری، قرارگاه پدافند سایبری کشور، آبان ۱۴۰۰
- طرح امن سازی زیر ساختهای حیاتی – ابلاغی مرکز مدیریت راهبردی افتا، اسفند ۹۷
- اصول حاکم بر معماری شبکه های سازمانی در زیر ساختهای حیاتی، مرکز ملی فضای مجازی، تیر ۱۴۰۰
- الزامات امنیتی ابلاغی شورای عالی فضای مجازی، خرداد ۹۸
- بایدهای تشدید رصد امنیتی بمنظور کشف و خنثی سازی توطئه دشمن و ایجاد آمادگی همه جانبه برای مواجهه با هر گونه حادثه سایبری، کمیته سایبری قرارگاه ثارالله، آبان ۱۴۰۰

۴- وضعیت‌های هشدار سایبری بر مبنای شواهد

سازمان حراست کل کشور

وضعیت سایبری

:: مدیریت تهدید و آسیب پذیری ::

شرایط احراز وضعیت

وضعیت سبز
- عدم مشاهده موارد مشکوک

وضعیت آبی
- بروز رخداد در سطح بین المللی
- وصول گزارش و اخبار از منابع معتبر و مراجع ذیصلاح
- احتمال التهابات اجتماعی و سیاسی
- سابقه وجود آسیب پذیری مشابه
- منشاء تهدید گروههای هکری بین المللی

وضعیت زرد
- وصول گزارش و اخبار از منابع معتبر و مراجع ذیصلاح
- سابقه وجود آسیب پذیری یکسان
- شکل گیری التهابات اجتماعی و سیاسی
- بروز رخداد در دستگاه های اجرایی کشور
- منشاء تهدید گروههای هکری دارای سابقه تهاجم در کشور

وضعیت نارنجی
- وصول گزارش و اخبار از منابع معتبر و مراجع ذیصلاح
- سابقه وجود آسیب پذیری در محصول یکسان
- خسارت عمده از التهابات اجتماعی و سیاسی
- بروز رخداد در سایر موسسات مشابه
- منشاء تهدید گروههای هکری + نیروهای سایبری کشور متخاصم

وضعیت قرمز
- درگیری مستقیم دستگاه اجرایی با حملات سایبری

سیاست های صیانتی (تدابیر کنترلی)

C0	استمرار فعالیت هـــای عـادی
C1	کاهش تـردد در محیط دستگاه اجرایی
C2	انسداد پورت های سخت افزاری و نرم افزاری
C3	اجـرای سریع شناساگـــر قبلی (YARA)
C4	کاهش پروسس ها در محیط پردازشی
C5	بازگشت پذیـری از طریق Check Point
C6	بازگشت پذیری از طریق Backup
C7	انسداد پورت هـای پر مخاطـره
C8	صدور هشـــدار حفاظتـــی
C9	حداقل کردن زمان اقدامات ریشه ای در SOC
C10	محدویت سرویس در ایران Iran Access
C11	انجام واکنش های حفاظتی تک مرحله ای
C12	لغو ماموریت و مرخصی در فناوری اطلاعات
C13	تشکیل کمیته و کارگروه های مربوطه
C14	ایزوله کردن سامانه های آسیب پذیری
C15	جمع آوری لاگ در بالاترین سطح ممکن
C16	انجام واکنش های حفاظتی دو مرحله ای
C17	تغییر ممنوع NO Change
C18	فارنزیک
C19	کشیک بندی
C20	انجام واکنش های خودکار
C21	انحراف تهاجم

قابلیت هـا

- A.D
- FIM
- PAM
- F.W
- A.V
- M.AV
- WAF
- FAM
- SOAR
- Honey pot
- EDR
- IAM
- DB

۵- تعاریف وضعیت براساس مدیریت ریسک

در این بخش، تعاریف ارائه شده از سطوح هشدار زرد، نارنجی و قرمز، منطبق بر طرح «پاسخ اضطراری سایبری» آورده شده است.

به طور کلی ویژگی‌های هر یک از سطوح هشدار زرد، نارنجی و قرمز، که در واقع مشخص می‌کنند شدت پیامدهای تهاجم سایبری و نیز احتمال وقوع جنگ سایبری در هر یک از این وضعیت ها چه میزان است، در جدول ۱: ویژگی‌های هریک از سطوح هشدار زرد، نارنجی و قرمز آورده شده است.

جدول ۱: ویژگی‌های هریک از سطوح هشدار زرد، نارنجی و قرمز

احتمال وقوع جنگ سایبری / شدت پیامدهای تهاجم سایبری	خیلی غیرمحتمل	غیرمحتمل	ممکن	محتمل	قریب الوقوع
خیلی کم (رویداد)	۰	۱	۲	۳	۴
کم (حادثه امنیتی کوچک)	۱	۲	۳	۴	۵
متوسط (حادثه امنیتی عمده)	۲	۳	۴	۵	۶
زیاد (بحران)	۳	۴	۵	۶	۷
خیلی زیاد (فاجعه)	۴	۵	۶	۷	۸

۰ و ۱ و ۲ = وضعیت سفید = تحت کنترل سایبری

۳ و ۴ و ۵ = وضعیت زرد = اضطرار سایبری (تهدید سایبری)

۶ و ۷ = وضعیت نارنجی = بحران سایبری (نزاع سایبری، تروریسم سایبری، جاسوسی سایبری)

۸ = وضعیت قرمز = جنگ سایبری

همچنین در جدول ۲: ویژگی‌های تهدیدات سایبری در وضعیت زرد، جدول ۳: ویژگی‌های تهدید سایبری در وضعیت نارنجی و جدول ۴: ویژگی‌های تهدید سایبری در وضعیت قرمز، به ترتیب ویژگی‌های تهدیدات سایبری در هر یک وضعیت‌های زرد، نارنجی و قرمز نشان داده شده است.

جدول ۲: ویژگی‌های تهدیدات سایبری در وضعیت زرد

سطح هشدار	وضعیت سایبری	مفهوم	منشاء تهدید سایبری	پیامدهای تهدید سایبری	سطح تهدید سایبری	احتمال وقوع تهدید سایبری	شدت (پیامد) تهدید سایبری
۳	زرد	تهدید سایبری یا اضطرار سایبری	• مجرمین سازمان یافته سایبری • هکرهای دارای انگیزه سیاسی • متصدیان شبکه‌های بات • نویسندگان جاسوس افزار و بدافزار	• نابودی یا تخریب عمده اطلاعات و یا تخریب اطلاعات دارای طبقه‌بندی • ایجاد اختلال گسترده در عملکرد سامانه‌های و شبکه‌ها • دسترسی غیرمجاز به اطلاعات عمده و یا اطلاعات دارای طبقه‌بندی • افشاء اطلاعات عمده یا دارای طبقه‌بندی • دستکاری (تغییر در) اطلاعات عمده یا دارای طبقه‌بندی • ممانعت از ارائه خدمات و انجام وظایف حساس سایبری	• تعداد قابل توجهی دستگاه • بخش قابل توجهی از یک سرمایه ملی سایبری • یک منطقه ویژه یا یک استان	• خیلی غیرمحتمل • غیرمحتمل • ممکن • محتمل • قریب‌الوقوع	• خیلی کم (رویداد) • کم (حادثه امنیتی کوچک) • متوسط (حادثه امنیتی عمده) • زیاد (بحران) • خیلی زیاد (فاجعه)

جدول ۳: ویژگی‌های تهدید سایبری در وضعیت نارنجی

سطح هشدار	وضعیت سایبری	مفهوم	منشاء تهدید سایبری	پیامدهای تهدید سایبری	سطح تهدید سایبری	احتمال وقوع تهدید سایبری	شدت (پیامد) تهدید سایبری
۲	نارنجی	بحران سایبری (مبارزه، ستیز، نزاع سایبری)	• مزدوران سایبری (گروه‌های تحت حمایت پنهان دولت‌ها) • جاسوسان سایبری سرویس‌های امنیتی دولت‌ها • ترورویست‌های سایبری	• صدمه به غرور ملی • ایجاد بحران منطقه‌ای • مخاطره منطقه‌ای برای سلامت ایمنی عمومی • تخریب یا صدمه/ اختلال در سرمایه‌های ملی سایبری در حوزه منطقه‌ای • تخریب یا صدمه/ اختلال در اطمینان یا حساسیت‌های قومی • خسارت شدید اقتصادی	• تعداد زیادی دستگاه • یک سرمایه ملی سایبری • منطقه‌ای (بیش از یک استان)	• ممکن • محتمل • قریب‌الوقوع	• متوسط (حادثه امنیتی عمده) • زیاد (بحران) • خیلی زیاد (فاجعه)

جدول ۴: ویژگی‌های تهدید سایبری در وضعیت قرمز

سطح هشدار	وضعیت سایبری	مفهوم	منشاء تهدید سایبری	پیامدهای تهدید سایبری	سطح تهدید سایبری	احتمال وقوع تهدید سایبری	شدت (پیامد) تهدید سایبری
۱	قرمز	جنگ سایبری	• نیروهای نظامی کشور مهاجم (ارتش سایبری) با سلاح‌های سایبری تحت کنترل یا رها شده توسط این نیروها	• براندازی نظام حاکمیتی یا تهدید فاجعه‌بار امنیت ملی • آغاز همزمان جنگ فیزیکی با زمینه‌سازی و تسهیل شروع جنگ فیزیکی در آینده نزدیک • تخریب یا صدمه فاجعه‌بار به وجهه کشور در سطح بین‌المللی • تخریب یا صدمه فاجعه‌بار به روابط سیاسی و اقتصادی کشور • تلفات انسانی یا مخاطره گسترده برای سلامت و ایمنی عمومی (از طریق ایجاد آلودگی هسته‌ای، شیمیایی یا بیولوژیک) • هرج و مرج و شورش داخلی • اختلال گسترده در اداره امور کشور • تخریب (یا صدمه گسترده به) اطمینان عمومی یا باورهای دینی، ملی و قومی • خسارت شدید به (یا اختلال گسترده در) اقتصاد ملی	• سرمایه‌ای (حداقل دو یا چند سرمایه ملی سایبری) • منطقه‌ای (چندین استان یا منطقه ویژه) • ملی • فراملی	• قریب‌الوقوع	• خیلی زیاد (فاجعه)

۶- رویه اجرایی اقدامات ضروری در هر یک از وضعیت‌های هشدار سایبری

در ادامه اقدامات لازم الاجرا در هر یک از وضعیت‌های هشدار سایبری زرد، نارنجی و قرمز، به تفکیک در سه زیربخش، آورده شده‌اند.

۶-۱- اقدامات ضروری در وضعیت زرد

پشتیبان‌گیری و تأمین افزونگی:

- تهیه نسخه پشتیبان از انواع دارایی‌های اطلاعاتی حیاتی پس از اعلام وضعیت زرد.
- کسب اطمینان از در دسترس بودن و صحت عملکرد فایل‌های پشتیبان تهیه شده.
- بررسی موجودی و آماده‌سازی کاستی های تجهیزات یدک سخت‌افزاری و حصول اطمینان از وجود امکان جایگزینی سریع در شرایط اضطراری.
- حصول اطمینان از وجود افزونگی مناسب در مورد مؤلفه‌های موجود در بخش‌های مختلف معماری اطلاعاتی دستگاه.

تست منابع تغذیه:

- حصول اطمینان از صحت عملکرد در حوزه منابع تغذیه (مانند شارژر، UPS و باطری، منابع تغذیه اضطراری (دیزل ژنراتور) و انواع پست‌های توزیع برق اختصاصی داخل مجموعه، در صورت وجود هر کدام) به محض دریافت وضعیت زرد.

پایش امنیت شبکه:

- تشدید رصد و پایش، تشخیص و هشدار به طوری که حداقل یک نیروی انسانی ۲۴*۷ به صورت On-call بدین منظور معرفی شده باشد.

لاگ‌گیری و فارنزیک:

- اطمینان از فعال بودن انواع مکانیزم‌های لاگ‌گیری بر روی دارایی‌های اطلاعاتی حیاتی برای انجام عملیات فارنزیک در صورت رخداد حادثه.
- بازبینی لاگ‌ها و رخدادهای تجهیزات و تعریف و فعال‌سازی لاگ جدید در صورت نیاز به صورت ماهانه.

صحت عملکرد تجهیزات امنیتی و به‌روزرسانی آن‌ها:

- بررسی صحت عملکرد و به‌روز بودن سامانه‌های امنیتی سایبری مانند انواع سیستم‌های تشخیص و مقابله با نفوذ، دیوارهای آتش شبکه و برنامه‌های کاربردی، آنتی‌ویروس، SIEM و غیره و در صورت لزوم به‌روزرسانی آن‌ها به محض دریافت وضعیت زرد.
- بررسی منظم سایت‌های هشداردهی داخلی مانند سایت مرکز ماهر و مرکز مدیریت راهبردی افتا جهت دریافت انواع اخبار و به‌روزرسانی‌های امنیتی.

- بررسی و اعمال به‌روزرسانی امضاها (Signatures) و پایگاه دانش انواع تجهیزات امنیتی پس از تست از طریق مخازن (Repositories) مورد تأیید
- بررسی وضعیت نصب وصله‌های امنیتی که از طریق مراجع ذی‌صلاح و منابع معتبر اعلام شده‌اند تا در صورت هر گونه کاستی، نصب وصله‌ها سریعاً انجام شود.

آمادگی نیروی انسانی مسئول:

- اطلاع‌رسانی به پرسنل On-call برای آمادگی بیشتر
- اطلاع‌رسانی جامع به کلیه راهبران و مدیران سیستم‌ها و شبکه، برای آمادگی لازم برای حضور در ساعت‌های غیرکاری در محل دستگاه و پرهیز از مرخصی‌های غیرضروری.

کنترل دسترسی و ارتباطات:

- بازنگری، محدودسازی و پایش مرتب سطح دسترسی افراد به دارایی‌های اطلاعاتی حیاتی.
- انجام بررسی در راستای کسب اطمینان از جدا بودن شبکه‌های صنعتی از شبکه‌های داخلی سازمانی و تصمیم‌گیری در مورد نقاط اتصالی موجود در صورت وجود.
- اطمینان از قطع هر گونه دسترسی شبکه صنعتی به اینترنت.
- قطع ارتباط سامانه‌های غیرضروری از اینترنت که در شرایط سفید از طریق اینترنت قابل دسترس هستند.
- بازبینی و اطمینان از صحت عملکرد روش‌هایی مانند Dot1x و Port Security در ورودی شبکه‌های رایانه‌ای.
- محدودسازی دسترسی راه دور به شبکه‌های داخلی از طریق اتصالاتی مانند VPN، RDP، VNC، SSH، Telnet و غیره.
- ایجاد اجبار سیستمی تغییر کلمه عبور اکانت‌های مدیریتی (که برای پیکربندی کل یا بخشی از شبکه و سامانه‌ها و تجهیزات ICT و صنعتی استفاده می‌شوند) و اکانت سامانه‌های کنترلی و پایش حیاتی و حساس، مطابق رویه‌های مربوطه.
- قطع ارتباط از راه دور با IED ها به غیر از پست‌های Unmanned.
- کسب اطمینان از بسته بودن کلیه‌ی پورت‌های USB در محدوده زیرساخت صنعتی.

تشکیل جلسات و گزارش‌دهی:

- تشکیل جلسه کمیته امنیت سایبری دستگاه به محض دریافت اعلام وضعیت زرد و نیز تشکیل منظم جلسات کمیته امنیت سایبری دستگاه به صورت دو هفته یکبار.
- ارسال گزارش هر دو هفته یکبار از دبیرخانه کمیته امنیت سایبری دستگاه به رئیس حراست و کمیته امنیت سایبری.
- ارسال گزارش جلسات کمیته امنیت سایبری دستگاه و کارگروه‌های تخصصی سایبری دستگاه و نیز گزارش اقدامات انجام شده به دبیرخانه کمیته امنیت سایبری و حراست دستگاه
- ارسال گزارش از وقایع سایبری به صورت برخط به دبیرخانه کمیته امنیت سایبری و حراست دستگاه

ممیزی و بازرسی:

- انجام ممیزی و بازرسی‌های امنیت سایبری مطابق با چک‌لیست‌های استاندارد/ابلاغی/بالادستی
- بررسی در دسترس بودن انواع دستورالعمل‌های پاسخگویی به حوادث سایبری و طرح تداوم کسب و کار.
- اطمینان از پیاده‌سازی صحیح آیتم‌های چک لیست بازرسی اضطراری.
- پیگیری و نظارت بر اجرای دستورالعمل‌های سازمان حراست کل کشور، سازمان پدافند غیرعامل و مرکز مرکز مدیریت راهبردی افتا ابلاغ شده از سوی سازمان بالادستی مرتبط
- کلیه‌ی ممیزی‌ها و بازرسی‌های اشاره شده در الزامات، باید تا زمانی که وضعیت زرد است، به صورت دوره‌ای تکرار شود.

فرهنگ‌سازی و آگاهی‌رسانی عمومی:

- اطلاع‌رسانی ورود به وضعیت زرد به نفرات مرتبط.
- انجام آگاهی‌رسانی و اعلام هشدارهای ضروری به کلیه پرسنل (مانند هشدار در مورد عدم بازکردن ایمیل‌های مشکوک، عدم کلیک بر روی لینک‌های غیرضروری، عدم استفاده از تجهیزات ذخیره‌سازی و پردازشی سیار بر روی سیستم‌های کاری و غیره)
- اطلاع رسانی راه‌های ارتباطی با دبیرخانه کمیته امینت سایبری و افراد جانشین ایشان به کلیه پرسنل.

امنیت فیزیکی:

- تشدید حفاظت فیزیکی و مراقبت[1] از مراکز، اتصالات و ارتباطات فیزیکی شبکه‌ای و سایر تجهیزات، دارایی‌های اطلاعاتی و زیرساخت‌های صنعتی، از طریق تخصیص نیروی انسانی برای مراقبت شبانه روزی در کلیه نقاط حساس که دارایی‌های اطلاعاتی حیاتی در آن‌ها مستقرند.
- محدودسازی تردد و لغو بازدیدها و ترددهای غیرضروری و ممانعت از ورود افراد غیر مسئول و فاقد صلاحیت‌های لازم حراستی.
- اعطای مجوز حراستی تردد به نمایندگان سازمان پدافند غیرعامل کشور و مرکز مدیریت راهبردی افتا در صورت نیاز.
- اعطای مجوز حراستی تردد به کارگروه تخصصی سایبری دستگاه بر اساس نیاز.
- بررسی صحت عملکرد سامانه‌های امنیتی فیزیکی مانند دوربین‌های تحت کنترل، قفل‌ها، سامانه‌های BMS و غیره.
- بررسی و بازبینی صحت عملکرد انواع سامانه‌های هشدار مانند SMS، آژیر و غیره.

---

[1] این الزام، به محدوده‌ای از دارایی‌ها که محافظت فیزیکی آن‌ها به واحدهای فناوری اطلاعات و ارتباطات و واحدهای بهره‌برداری بر می‌گردد اشاره دارد. سایر محدوده‌ها که تحت محافظت مستقیم حراست هستند، خارج از این دستورالعمل است و توسط واحد حراست دستگاه‌ها مطابق با دستورالعمل‌های موجود در این حوزه، محافظت می‌شود.

سایر الزامات مرتبط با حراست:

- واحد حراست دستگاه‌ها مطابق دستورالعمل‌های موجود در این حوزه و نیز مواردی که توسط سازمان حراست کل کشور ابلاغ شده است اقدام نمایند.

۶-۲- اقدامات ضروری در وضعیت نارنجی

پشتیبان‌گیری و تأمین افزونگی:

- تهیه نسخه پشتیبان از انواع دارایی‌های اطلاعاتی حیاتی پس از اعلام وضعیت نارنجی.
- تشدید خط‌مشی‌های پشتیبان‌گیری (مانند افزایش تعداد pointهای پشتیبان‌گیری، انجام برخی پشتیبان‌گیری‌ها از نوع full، اطمینان از عدم بازنویسی شدن پشتیبان ها به دلیل نبود ظرفیت کافی، نگهداری تعداد حداقل پشتیبان مربوط به فواصل زمانی مختلف)
- کسب اطمینان از در دسترس بودن و صحت عملکرد فایل‌های پشتیبان تهیه شده.
- بررسی موجودی و آماده‌سازی کاستی های تجهیزات یدک سخت‌افزاری و حصول اطمینان از وجود امکان جایگزینی سریع در شرایط اضطراری.
- حصول اطمینان از وجود افزونگی مناسب در مورد مؤلفه‌های موجود در بخش‌های مختلف معماری اطلاعاتی دستگاه

تست منابع تغذیه:

- حصول اطمینان از صحت عملکرد در حوزه منابع تغذیه (مانند شارژر، UPS و باطری، منابع تغذیه اضطراری (دیزل ژنراتور) و انواع پست های توزیع برق اختصاصی داخل مجموعه، در صورت وجود هر کدام)، به محض دریافت وضعیت نارنجی
- مدیریت ChangeOver با هدف افزایش قابلیت اطمینان تأمین مصارف حیاتی.
- مدیریت فرآیند درخواست و تامین سوخت مورد نیاز دیزل ژنراتور.

پایش امنیت شبکه:

- تشدید رصد و پایش، تشخیص و هشدار به طوری که اولاً: حساسیت سیستم‌های تشخیص، در سخت‌گیرانه‌ترین حالت ممکن خود قرار گیرند و علاوه برهشدارهای Critical، سایر هشدارها نیز اعلام و پیگیری شود و ثانیاً: تنها مبتنی بر تشخیص خودکار و سیستمی نباشند و از طریق تخصیص حداقل یک نیروی انسانی متخصص، مانیتورینگ ۷*۲۴ شبکه صنعتی و ICT صورت پذیرد.

لاگ‌گیری و فارنزیک:

- اطمینان از فعال بودن انواع مکانیزم‌های لاگ‌گیری بر روی دارایی‌های اطلاعاتی حیاتی برای انجام عملیات فارنزیک در صورت رخداد حادثه.
- بازبینی لاگ‌ها و رخدادهای تجهیزات و تعریف و فعال‌سازی لاگ جدید در صورت نیاز به صورت ماهانه.

صحت عملکرد تجهیزات امنیتی و به‌روزرسانی آن‌ها:

- بررسی صحت عملکرد و به‌روز بودن سامانه‌های امنیتی سایبری مانند انواع سیستم‌های تشخیص و مقابله با نفوذ، دیوارهای آتش شبکه و برنامه‌های کاربردی، آنتی‌ویروس، SIEM و غیره و در صورت لزوم به‌روزرسانی آن‌ها، به محض دریافت وضعیت نارنجی
- بررسی منظم سایت‌های هشداردهی داخلی مانند سایت مرکز ماهر و مرکز مدیریت راهبردی افتا جهت دریافت انواع اخبار و به‌روزرسانی‌های امنیتی.
- بررسی و اعمال به‌روزرسانی امضاها (Signatures) و پایگاه دانش انواع تجهیزات امنیتی پس از تست، از طریق مخازن (Repositories) مورد تأیید.
- بررسی وضعیت نصب وصله‌های امنیتی که از طریق مراجع ذی‌صلاح و منابع معتبر اعلام شده‌اند تا در صورت هر گونه کاستی، نصب وصله‌ها سریعاً انجام شود.

آمادگی نیروی انسانی مسئول:

- اطلاع‌رسانی به پرسنل On-call برای آمادگی بیشتر
- اطلاع‌رسانی جامع به کلیه راهبران و مدیران سیستم‌ها و شبکه، برای آمادگی لازم برای حضور در ساعت‌های غیرکاری در محل دستگاه و پرهیز از مرخصی‌های غیرضروری.
- عدم اجازه خروج پرسنل از شهر محل زیرساخت خود تا در صورت فراخوان سریعاً در محل کار حاضر شوند.

کنترل دسترسی و ارتباطات:

- بازنگری، محدوسازی و پایش مرتب سطح دسترسی افراد به دارایی‌های اطلاعاتی حیاتی.
- انجام بررسی در راستای کسب اطمینان از جدابودن شبکه‌های صنعتی از شبکه‌های داخلی سازمانی و تصمیم‌گیری فوری در مورد نقاط اتصالی موجود در صورت وجود.
- اطمینان از قطع هر گونه دسترسی شبکه صنعتی به اینترنت.
- قطع ارتباط سامانه‌های غیرضروری از اینترنت که در شرایط سفید از طریق اینترنت قابل دسترس هستند و بازنگری در لیست سفید ضروری.
- قطع دسترسی کاربران غیر ضروری به سامانه‌ها.
- محدودسازی دسترسی به سامانه‌های ضروری منتشر شده بر روی اینترنت، به IP های کاربران داخل کشور.
- بررسی در راستای کسب اطمینان از جداسازی شبکه‌های داخلی از اینترنت بین‌المللی و اتصال به شبکه ملی اطلاعات.
- بازبینی و اطمینان از صحت عملکرد روش‌هایی مانند Dot1x و Port Security در ورودی شبکه‌های رایانه‌ای.
- در صورت امکان حذف امکان دسترسی راه دور به شبکه صنعتی و محدودسازی دسترسی راه دور به شبکه‌های داخلی ICT از طریق اتصالاتی مانند VPN، RDP، VNC، SSH، Telnet و غیره.

- ایجاد اجبار سیستمی تغییر کلمه عبور اکانت‌های مدیریتی (که برای پیکربندی کل یا بخشی از شبکه و سامانه‌ها و تجهیزات ICT و صنعتی استفاده می‌شوند) و اکانت سامانه‌های کنترلی و پایش حیاتی و حساس، مطابق رویه‌های مربوطه.
- نظارت بر قطع بودن هر گونه ارتباط از راه دور با IED ها به غیر از پست‌های Unmanned.
- بستن کلیه‌ی پورت‌های USB در محدود ICT و کسب اطمینان از بسته بودن کلیه پورت‌های USB در محدوده صنعتی.
- کنترل قرار گرفتن کلید SUB/Scada پست در وضعیت SUB در پست‌های حیاتی و حساس.
- کنترل قرار گرفتن کلید remote/local مربوط به RTU روی حالت local در پست‌های حیاتی و حساس.

فرهنگ‌سازی و آگاهی‌رسانی عمومی:

- اطلاع‌رسانی ورود به وضعیت نارنجی به کلیه پرسنل.
- انجام آگاهی‌رسانی و اعلام هشدارهای ضروری به صورت فوری به کلیه پرسنل (مانند هشدار در مورد عدم بازکردن ایمیل‌های مشکوک، عدم کلیک بر روی لینک‌های غیرضروری، عدم استفاده از تجهیزات ذخیره‌سازی و پردازشی سیار بر روی سیستم‌های کاری و غیره)
- اطلاع رسانی راه‌های ارتباطی با دبیرخانه کارگروه داخلی حوادث و افراد جانشین ایشان به کلیه پرسنل.

تشکیل جلسات و گزارش‌دهی:

- تشکیل جلسه کمیته امنیت سایبری دستگاه به محض دریافت اعلام وضعیت نارنجی و نیز تشکیل منظم جلسات کمیته امینت سایبری دستگاه به صورت هفتگی.
- ارسال گزارش هفتگی از دبیرخانه کمیته امینت سایبری دستگاه به رئیس حراست و کمیته امنیت سایبری.
- ارسال گزارش جلسات کمیته امنیت سایبری دستگاه و کارگروه‌های تخصصی سایبری دستگاه و نیز گزارش اقدامات انجام شده به دبیرخانه کمیته امینت سایبری و حراست دستگاه
- ارسال گزارش از وقایع سایبری به صورت برخط به دبیرخانه کمیته امینت سایبری و حراست دستگاه

ممیزی و بازرسی:

- انجام ممیزی و بازرسی‌های امنیت سایبری مطابق با چک‌لیست‌های استاندارد/ابلاغی/بالادستی
- بررسی در دسترس بودن انواع دستورالعمل‌های پاسخگویی به حوادث سایبری و طرح تداوم کسب و کار.
- اطمینان از پیاده‌سازی صحیح آیتم‌های چک لیست بازرسی اضطراری.
- پیگیری و نظارت بر اجرای دستورالعمل‌های سازمان حراست کل کشور، سازمان پدافند غیرعامل و مرکز مدیریت راهبردی افتا ابلاغ شده از سوی سازمان بالادستی مرتبط
- کلیه‌ی ممیزی‌ها و بازرسی‌های اشاره شده در الزامات، باید تا زمانی که وضعیت نارنجی است، به صورت دوره‌ای تکرار شود.

تعمیرات و نگهداری:

- سنجش میزان ریسک انجام انواع فعالیت‌های تعمیرات، نگهداری، توسعه و بهینه‌سازی و استعلام از مدیریت واحد بهره برداری مربوطه جهت صدور مجوز جهت انجام آن‌ها بر اساس میزان ریسک موجود.

امنیت فیزیکی:

- تشدید حفاظت فیزیکی و مراقبت[1] از مراکز، اتصالات و ارتباطات فیزیکی شبکه‌ای و سایر تجهیزات، دارایی‌های اطلاعاتی و زیرساخت‌های صنعتی، از طریق تخصیص نیروی انسانی برای مراقبت شبانه روزی در کلیه نقاط حساس که دارایی‌های اطلاعاتی حیاتی در آن‌ها مستقرند.
- محدودسازی تردد و لغو بازدیدها و ترددهای غیرضروری و ممانعت از ورود افراد غیر مسئول و فاقد صلاحیت‌های لازم حراستی.
- لغو مجوز پیمانکاران برای تردد و اعطای مجوز دوباره در صورت لزوم.
- اعطای مجوز حراستی تردد به نمایندگان سازمان پدافند غیرعامل و مرکز مدیریت راهبردی افتا در صورت نیاز.
- اعطای مجوز حراستی تردد به کارگروه تخصصی سایبری دستگاه بر اساس نیاز.
- بررسی صحت عملکرد سامانه‌های امنیتی فیزیکی مانند دوربین‌های تحت کنترل، قفل‌ها، سامانه‌های BMS و غیره.
- بررسی و بازبینی صحت عملکرد انواع سامانه‌های هشدار مانند SMS، آژیر و غیره.

سایر الزامات مرتبط با حراست:

- واحد حراست دستگاه‌ها مطابق دستورالعمل‌های موجود در این حوزه و نیزمواردی که توسط سازمان حراست کل کشور ابلاغ شده است اقدام نمایند.

۶-۳- اقدامات ضروری در وضعیت قرمز

پشتیبان‌گیری و تأمین افزونگی:

- تهیه نسخه پشتیبان از انواع دارایی‌های اطلاعاتی حیاتی پس از اعلام وضعیت قرمز
- تشدید خط‌مشی‌های پشتیبان‌گیری (مانند افزایش تعداد pointهای پشتیبان‌گیری، انجام برخی پشتیبان‌گیری‌ها از نوع full، اطمینان از عدم بازنویسی شدن پشتیبان ها به دلیل نبود ظرفیت کافی، نگهداری تعداد حداقل پشتیبان مربوط به فواصل زمانی مختلف)

---

[1] این الزام، به محدوده‌ای از دارایی‌ها که محافظت فیزیکی آن‌ها به واحدهای فناوری اطلاعات و ارتباطات و واحدهای بهره‌برداری بر می‌گردد اشاره دارد. سایر محدوده‌ها که تحت محافظت مستقیم حراست هستند، خارج از این دستورالعمل است و توسط واحد حراست دستگاه‌ها مطابق با دستورالعمل‌های موجود در این حوزه، محافظت می‌شود.

- کسب اطمینان از در دسترس بودن و صحت عملکرد فایل‌های پشتیبان تهیه شده
- بررسی موجودی و آماده سازی کاستی های تجهیزات یدک سخت‌افزاری و حصول اطمینان از وجود امکان جایگزینی سریع در شرایط اضطراری.
- حصول اطمینان از وجود افزونگی مناسب در مورد مؤلفه‌های موجود در بخش‌های مختلف معماری اطلاعاتی دستگاه

تست منابع تغذیه:

- حصول اطمینان از صحت عملکرد در حوزه منابع تغذیه (مانند شارژر، UPS و باطری، منابع تغذیه اضطراری (دیزل ژنراتور) و انواع پست های توزیع برق اختصاصی داخل مجموعه، در صورت وجود هر کدام)، به محض دریافت وضعیت قرمز.
- ایزوله سازی شبکه مرتبط با کنترل و مانیتورینگ تجهیزات تغذیه از سایر شبکه.
- مدیریت ChangeOver با هدف افزایش قابلیت اطمینان تأمین مصارف حیاتی
- مدیریت فرآیند درخواست و تأمین سوخت مورد نیاز دیزل ژنراتور

پایش امنیت شبکه:

- تشدید رصد و پایش، تشخیص و هشدار به طوری که اولاً: حساسیت سیستم‌های تشخیص، در سخت‌گیرانه‌ترین حالت ممکن خود قرار گیرند و علاوه برهشدارهای Critical، سایر هشدارها نیز اعلام و پیگیری شود و ثانیاً: تنها مبتنی بر تشخیص خودکار و سیستمی نباشند و از طریق تخصیص حداقل دو نیروی انسانی متخصص، مانیتورینگ ۲۴*۷ شبکه صنعتی و ICT صورت پذیرد.

لاگ‌گیری و فارنزیک:

- اطمینان از فعال بودن انواع مکانیزم‌های لاگ‌گیری بر روی دارایی‌های اطلاعاتی حیاتی برای انجام عملیات فارنزیک در صورت رخداد حادثه.
- بازبینی لاگ‌ها و رخدادهای تجهیزات و تعریف و فعالسازی لاگ جدید در صورت نیاز به صورت دو هفته یکبار.

صحت عملکرد تجهیزات امنیتی و به‌روزرسانی آن‌ها:

- بررسی صحت عملکرد و به‌روز بودن سامانه‌های امنیتی سایبری مانند انواع سیستم‌های تشخیص و مقابله با نفوذ، دیوارهای آتش شبکه و برنامه‌های کاربردی، آنتی‌ویروس، SIEM و غیره و در صورت لزوم به‌روزرسانی آن‌ها، به محض دریافت وضعیت قرمز.
- بررسی منظم سایت‌های هشداردهی داخلی مانند سایت مرکز ماهر و مرکز مدیریت راهبردی افتا جهت دریافت انواع اخبار و به‌روزرسانی‌های امنیتی.
- بررسی و اعمال به‌روزرسانی امضاها (Signatures) و پایگاه دانش انواع تجهیزات امنیتی پس از تست از طریق مخازن (Repositories) مورد تأیید
- بررسی وضعیت نصب وصله‌های امنیتی که از طریق مراجع ذی‌صلاح و منابع معتبر اعلام شده‌اند تا در صورت هر گونه کاستی، نصب وصله‌ها سریعاً انجام شود.

آمادگی نیروی انسانی مسئول:

- اطلاع رسانی به پرسنل On-call برای آمادگی بیشتر و تشدید قوانین کاری مربوطه در کلیه ساعات شبانه روز در روزهای کاری و تعطیل
- اطلاع رسانی جامع به کلیه راهبران و مدیران سیستم‌ها و شبکه، برای آمادگی لازم برای حضور در ساعت‌های غیرکاری در محل دستگاه و پرهیز از مرخصی‌های غیرضروری.
- لغو هر گونه مرخصی غیرضروری پرسنل و عدم اجازه خروج پرسنل از شهر محل زیرساخت خود تا در صورت فراخوان سریعاً در محل کار حاضر شوند.
- اختصاص اپراتورهای دارای صلاحیت برای پست های بدون اپراتور

کنترل دسترسی و ارتباطات:

- بازنگری، محدوسازی و پایش مرتب سطح دسترسی افراد به دارایی‌های اطلاعاتی حیاتی.
- انجام بررسی در راستای کسب اطمینان از جدابودن شبکه‌های داخلی سازمانی و صنعتی و تصمیم‌گیری فوری در مورد نقاط اتصالی موجود در صورت وجود.
- اطمینان از قطع هر گونه دسترسی شبکه صنعتی به اینترنت.
- قطع ارتباط سامانه‌های غیرضروری از اینترنت که در شرایط سفید از طریق اینترنت قابل دسترس هستند و بازنگری در لیست سفید ضروری.
- بررسی در راستای کسب اطمینان از قطع دسترسی کاربران غیر ضروری به سامانه‌ها.
- محدودسازی دسترسی به سامانه‌های ضروری منتشر شده بر روی اینترنت، به IP های کاربران داخل کشور.
- بررسی در راستای کسب اطمینان از جداسازی شبکه‌های داخلی از اینترنت بین‌المللی و اتصال به شبکه ملی اطلاعات.
- بازبینی و اطمینان از صحت عملکرد روش‌هایی مانند Dot1x و Port Security در ورودی شبکه‌های رایانه‌ای.
- در صورت امکان حذف امکان دسترسی راه دور به شبکه صنعتی و ICT، از طریق اتصالاتی مانند VPN، RDP، VNC، SSH، Telnet و غیره.
- ایجاد اجبار سیستمی تغییر کلمه عبور اکانت‌های مدیریتی (که برای پیکربندی کل یا بخشی از شبکه و سامانه‌ها و تجهیزات ICT و صنعتی استفاده می‌شوند) و اکانت سامانه‌های کنترلی و پایش حیاتی و حساس، مطابق رویه‌های مربوطه.
- نظارت بر قطع بودن ارتباط از راه دور با IED ها به غیر از پست‌های Unmanned.
- کسب اطمینان از بسته بودن کلیه‌ی پورت‌های USB در محدوده صنعتی و ICT.
- قطع نرم افزاری و سخت افزاری سیستم اتوماسیون و DCS پستهای مهم، حیاتی و حساس و بهره برداری از آنها به صورت دستی.
- کنترل قرار گرفتن کلید SUB/Scada پست در وضعیت SUB در کلیه پست‌ها.
- کنترل قرار گرفتن کلید remote/local مربوط به RTU روی حالت local در کلیه پست‌ها.

فرهنگ سازی و آگاهی رسانی عمومی:

- اطلاع رسانی ورود به وضعیت قرمز به کلیه پرسنل
- انجام آگاهی‌رسانی و اعلام هشدارهای ضروری به صورت فوری به کلیه پرسنل (مانند هشدار در مورد عدم بازکردن ایمیل‌های مشکوک، عدم کلیک بر روی لینک‌های غیرضروری، عدم استفاده از تجهیزات ذخیره‌سازی و پردازشی سیار بر روی سیستم‌های کاری و غیره)
- اطلاع رسانی راه‌های ارتباطی با دبیرخانه کارگروه داخلی حوادث و افراد جانشین ایشان به کلیه پرسنل.

تشکیل جلسات و گزارش‌دهی:

-
- تشکیل جلسه کمیته امنیت سایبری دستگاه به محض دریافت اعلام وضعیت قرمز و نیز تشکیل منظم جلسات کمیته امینت سایبری دستگاه به صورت روزانه.
- ارسال گزارش هفتگی از دبیرخانه کمیته امینت سایبری دستگاه به رئیس حراست و کمیته امنیت سایبری.
- ارسال گزارش جلسات کمیته امنیت سایبری دستگاه و کارگروه‌های تخصصی سایبری دستگاه و نیز گزارش اقدامات انجام شده به دبیرخانه کمیته امینت سایبری و حراست دستگاه
- ارسال گزارش از وقایع سایبری به صورت برخط به دبیرخانه کمیته امینت سایبری و حراست دستگاه

ممیزی و بازرسی:

- انجام ممیزی و بازرسی‌های امنیت سایبری مطابق با چک‌لیست‌های استاندارد/ابلاغی/بالادستی بر روی دارایی های اطلاعاتی حیاتی
- بررسی در دسترس بودن انواع دستورالعمل‌های پاسخگویی به حوادث سایبری و طرح تداوم کسب و کار.
- اطمینان از پیاده‌سازی صحیح آیتم‌های چک لیست بازرسی اضطراری.
- پیگیری و نظارت بر اجرای دستورالعمل‌های سازمان حراست کل کشور، سازمان پدافند غیرعامل و مرکز مرکز مدیریت راهبردی افتا ابلاغ شده از سوی سازمان بالادستی مرتبط.
- کلیه‌ی ممیزی‌ها و بازرسی‌های اشاره شده در الزامات، باید تا زمانی که وضعیت قرمز است، به صورت دوره‌ای طبق یک روال چابک تکرار شود.

تعمیرات و نگهداری:

- توقف انواع فعالیت‌های تعمیرات، نگهداری، توسعه و بهینه سازی غیرضروری
- سنجش میزان ریسک انجام انواع فعالیت های تعمیرات، نگهداری، توسعه و بهینه سازی ضروری و استعلام از مدیریت واحد بهره‌برداری مربوطه جهت صدور مجوز جهت انجام آن‌ها، تا با در نظر گرفتن ریسک موجود، تنها فعالیت‌های ضروری که اختلالی در پایداری شبکه ایجاد نمی کنند، صورت پذیرند.

امنیت فیزیکی:

- تشدید حفاظت فیزیکی و مراقبت[1] از مراکز، اتصالات و ارتباطات فیزیکی شبکه‌ای و سایر تجهیزات، دارایی‌های اطلاعاتی و زیرساخت‌های صنعتی، از طریق تخصیص نیروی انسانی برای مراقبت شبانه روزی کلیه نقاط ورودی و سایر نقاط حساس غیر ورودی در محدوده‌ی کلیه دارایی‌ها.
- محدودسازی تردد و لغو بازدیدها و ترددهای غیرضروری و ممانعت از ورود افراد غیر مسئول و فاقد صلاحیت‌های لازم حراستی
- لغو مجوز پیمانکاران برای تردد و اعطای مجوز دوباره در صورت لزوم
- اعطای مجوز تردد به نمایندگان سازمان پدافند غیرعامل و مرکز مدیریت راهبردی افتا در صورت نیاز
- اعطای مجوز تردد به کارگروه داخلی حوادث سایبری دستگاه بر اساس نیاز
- بررسی صحت عملکرد سامانه‌های امنیتی فیزیکی مانند دوربین‌های تحت کنترل، قفل‌ها، سامانه‌های BMS و غیره.
- بررسی و بازبینی صحت عملکرد انواع سامانه‌های هشدار مانند SMS، آژیر و غیره.

سایر الزامات مرتبط با حراست:

- واحد حراست دستگاه‌ها مطابق دستورالعمل‌های موجود در این حوزه و نیزمواردی که توسط سازمان حراست کل کشور ابلاغ شده است اقدام نمایند.

[1] این الزام، به محدوده‌ای از دارایی‌ها که محافظت فیزیکی آن‌ها به واحدهای فناوری اطلاعات و ارتباطات و واحدهای بهره برداری بر می‌گردد، اشاره دارد. سایر محدوده‌ها که تحت محافظت مستقیم حراست هستند، خارج از این دستورالعمل است و توسط واحد حراست دستگاه‌ها مطابق با دستورالعمل‌های موجود در این حوزه، محافظت می‌شود.

گروه اقدامات	اقدامات پیش‌نیاز	انجام شده؟	توضیحات
پیش نیازهای عمومی و مشترک بین چند دسته اقدام شناخت دستگاه و اقدامات اولیه سایبری	۱- شناسایی، تهیه و بروزرسانی لیست دارایی‌های حیاتی و پروتکل ها و سامانه های مجاز و مسئولین و متولیان آنها و مستندات آن ها	☐	
	۲- تشکیل و ساماندهی کمیته و کارگروه (های) تخصصی امنیت سایبری شرکت	☐	
	۳- سفارشی سازی روش اجرایی مدیریت حوادث	☐	
	۴- تشکیل تیم CERT داخلی دستگاه و تکمیل پایگاه دانش و اکسل های پیوست طرح پاسخگویی به حوادث	☐	
	۵- تعیین نقاط point of failure Single و نقاط شکست سامانه های حیاتی	☐	
	۶- تهیه طرح تداوم کسب و کار و بازیابی حادثه و برگزاری مانور	☐	
	۷- تکمیل فرم های اکسل زرد، نارنجی و قرمز و اختصاص نفرات متخصص متناسب با هر فعالیت	☐	
	۸- تهیه لیست پیمانکاران	☐	
	۹- همگام سازی زمان در تمامی تجهیزات و سامانه ها و لاگ های مرتبط با سامانه های حیاتی رعایت شود.	☐	
	۱۰- انجام ارزیابی امنیتی/آزمون نفوذ/ارزیابی آسیب پذیری/تحلیل شکاف دوره ای بر روی دارایی های سایبری	☐	
	۱۱- ضمن توجه در خرید تجهیزات افتایی و فاوایی که دارای مجوز های امنیتی لازم از مرکز افتا هستند، تنها از شرکت های دارای مجوزهای امنیتی لازم از افتا برای دریافت خدمات امن سازی و مشاوره استفاده شود.	☐	
	۱۲- استفاده از پروتکل های امن و ابزار های رمزنگاری برای حفظ محرمانگی داده ها و اطلاعات حساس سامانه های حیاتی در حین انتقال، پردازش و ذخیره سازی	☐	
	۱۳- دسترسی پذیری سامانه ها و سرویس های حیاتی از طریق راهکارهای توزیع بار، HA و ... افزایش یابد.	☐	
	۱۵- تهیه نسخه پشتیبان از انواع دارایی‌های اطلاعاتی حیاتی بر اساس روش اجرایی پشتیبان‌گیری مطمئن	☐	
	۱۶- کسب اطمینان از در دسترس بودن و صحت عملکرد فایل‌های پشتیبان تهیه شده	☐	

	۱۷- تهیه طرح افزونگی دارایی های سایبری در بخش‌های مختلف شرکت و حصول اطمینان از وجود افزونگی مناسب و صحت عملکرد آنها مطابق طرح افزونگی در بازه های زمانی مناسب	☐	
	۱۸- پیش بینی، تهیه و آماده‌سازی تجهیزات یدکی لازم برای عملکرد مناسب فرآیندهای مختلف در شرکت و بازبینی آنها به صورت دوره ای	☐	
	۱۹- پیش بینی و ایجاد سایت پشتیبان و mirror سامانه ها و سیستم ها به صورت off line و ترجیحا در صورت امکان on line	☐	
تست منابع تغذیه و تجهیزات سرمایش تامین برق اضطراری	۲۰- اطمینان از تامین برق اضطراری، UPS(حداقل یک ساعت) و دیزل ژنراتور و سوخت	☐	
	۲۱- وجود دستورالعمل/چک لیست بررسی صحت عملکرد منابع تغذیه و تجهیزات سرمایش و انجام ارزیابی دوره ای در بازهای زمانی مناسب	☐	
	۲۲- مشخص کردن بار مصرفی ضروری	☐	
	۲۳- تدوین فرایند مدیریت درخواست و تأمین سوخت مورد نیاز دیزل ژنراتور	☐	
	۲۴- پیش بینی امکان Change Over بر روی تابلوهای تغذیه مراکز زیرساختی IT و OT	☐	
صحت عملکرد تجهیزات امنیتی و به‌روزرسانی امضاها و قوانین آن‌ها	۲۵- راه‌اندازی، مدیریت و بروزرسانی سامانه‌های تجهیزات امنیتی سایبری و اطمینان از فعال بودن آن ها مطابق روال تعریف شده	☐	
	۲۶- در نظر گرفتن vlan و Zone بندی مناسب و همچنین ارتباط ناحیه DMZ با شبکه داخلی توسط دیوار آتش کنترل شود	☐	
	۲۷- آمادگی جهت راهبردها و تاکتیک های مرتبط با فریب مهاجمین سایبری در راستای ایجاد تاخیر در دستیابی وی به اهداف مورد نظر	☐	
	۲۸- پیکربندی شبکه و اجزای آن به گونه ای پیکربندی شوند که تمام دسترسی ها به شبکه در داخل کشور و از طریق زیرساخت و پهنای باند در اختیار کشور با اولویت شبکه ملی اطلاعات مسیر یابی شود.	☐	
	۲۹- بررسی منظم سامانه جامع مدیریت امنیت سایبری از طریق وب‌سایت‌های هشداردهی داخلی مانند وب‌سایت مرکز	☐	

	ماهر و مرکز مدیریت راهبردی افتا جهت دریافت انواع اخبار و به‌روزرسانی‌های امنیتی حداقل به صورت هفتگی		
	۳۰- بررسی و اعمال به‌روزرسانی امضاها (Signatures) و پایگاه دانش انواع تجهیزات امنیتی پس از تست از طریق مخازن (Repositories) مورد تأیید حداقل به صورت هفتگی	☐	
پایش امنیت شبکه	۳۱- تهیه لیست تجهیزات پایش مورد نیاز و اقدام در جهت رفع کاستی ها	☐	
	۳۲- تهیه دستورالعمل پیکربندی تجهیزات موجود و بازبینی آن ها	☐	
	۳۳- حصول اطمینان از دریافت هشدارهای سیستم ها	☐	
	۳۴- تشکیل تیم پایش شبکه و زیرساخت برای زیرساخت شبکه فناوری اطلاعات و شبکه صنعتی	☐	
لاگ گیری	۳۵- تهیه دستورالعمل لاگ گیری	☐	
	۳۶- مشخص کردن لیست انواع لاگ مورد نیاز بر روی دارایی‌های سایبری حیاتی برای انجام عملیات فارنزیک به ویژه در حوزه های زیر:	☐	
	* ارتباط بین سرورهای فیزیکی و مجازی	☐	
	* دسترسی به سامانه‌ها و تجهیزات در زمان‌های غیر عادی مانند ساعات غیر اداری	☐	
	* دسترسی به پورت‌های ILO، سرویس SSH و دسترسی ریموت	☐	
	* فایل‌های اجرایی در سرورها و کلاینت‌ها مانند فایل‌های دارای پسوند bat،exe و psl	☐	
	* احراز هویت مدیران و کاربران شبکه	☐	
	* کپی برداری و انتقال فایل‌ها	☐	
	* wipe کردن در سامانه‌ها	☐	
	۳۷- فعال سازی مکانیزم‌های لاگ‌گیری و پایش لاگها و بازبینی آنها در بازهای زمانی مناسب	☐	
	۳۸- ذخیره سازی لاگ ها با رعایت اصول امنیتی مانند Signing، Time Stamp، Indexing، در پایگاه داده ایزوله، به صورت امن به مدت حداقل یک سال	☐	
آمادگی نیروی انسانی مسئول	۳۹- تهیه و به‌روزرسانی لیست اطلاعات تماس پرسنل On-call در شرایط اضطراری	☐	
	۴۰- فهرستی از نهادهای ذی صلاح و افراد کلیدی به همراه اطلاعات تماس آن ها، که باید در زمان بحران در دسترس	☐	

	باشند تهیه و در اختیار افراد مجاز قرار گیرد (در لیست مذکور نفر مرتبط با سازمان، در مرکز افتا لحاظ گردد)		
	۴۱- تهیه لیست نیروهای متخصص سامانه‌ها و سرویس‌های زیرساختهای IT و OT و شیفت بندی برای حضور ۲۴ ساعته آنها برای روزهای کاری و غیر کاری در وضعیت هشدار نارنجی و قرمز، به صورتی که تعداد نفرات کافی در محل شرکت حضور داشته باشند	☐	
	۴۲- تعیین لیستی از اماکن، ایستگاه ها و تجهیزات و تعیین سطح کنترل آنها (اتوماتیک، از راه دور، محلی و دستی) برای وضعیت های مختلف هشدار و اختصاص نیروی انسانی برای مواردی که نیاز است در وضعیت هشدار به سطح محلی یا دستی تغییر وضعیت دهند	☐	
کنترل دسترسی و ارتباطات امن	۴۳- تهیه روش های اجرایی مدیریت کلمه عبور و مدیریت هویت و دسترسی ها	☐	
	۴۴- تهیه و به‌روزرسانی لیست سفید (white list) از سامانه‌های ضروری اینترنتی برای وضعیت های مختلف هشدار	☐	
	۴۵- تعیین لیست کاربران ضروری و سطح دسترسی آن ها برای سامانه های مختلف	☐	
	۴۶- تعیین لیست کاربران برای دسترسی و ارتباطات راه دور و اخذ مجوز های لازم برای آنها	☐	
	۴۷- پیاده سازی روش اجرایی دسترسی از راه دور از طریق ارتباطات VPN، RDP، VNC، SSH، Telnet و غیره به شبکه های داخلی	☐	
	۴۸- استفاده از مکانیزم های احراز هویت دو عامله مانند توکن برای اتصال مستقیم به سرورها	☐	
	۴۹- رصد و کنترل کامل دسترسی‌های مدیریتی.	☐	
	۵۰- حصول اطمینان از رها نبودن منابع بلا استفاده (مثلا آدرس های IP تخصیص یافته یا ماشین های مجازی و پایگاه داده‌ها)	☐	
	۵۱- مسدود نمودن تمامی مبادی ورودی و خروجی لبه شبکه به استثناء موارد ضروری و پیاده سازی کنترل‌های تامین کننده سیاست های امنیتی برای موارد ضروری	☐	
	۵۲- ** اطمینان از قطع هر گونه دسترسی شبکه صنعتی به اینترنت	☐	

۵۳- کسب اطمینان از بسته بودن کلیه‌ی پورت‌های USB در محدوده زیرساخت صنعتی و محدود سازی استفاده از پورت های USB در شبکه اداری	☐	
۵۴- جداسازی شبکه‌های داخلی سازمانی و صنعتی و تصمیم‌گیری و کسب مجوز از افتا در مورد نقاط اتصالی ضروری در صورت وجود	☐	
۵۵- اتصال به اینترنت صرفا در قالب یک سرویس در ناحیه Untrusted و به صورت جدا از سایر نواحی شبکه داخلی	☐	
۵۶- بازبینی حساب های کاربران و دسترسی‌های آنها در دوره زمانی معین و مدیریت دسترسی های و حذف دسترسی های غیر ضروری کاربران و همچنین ایجاد سازوکار مناسب برای حراست دستگاه به منظور نظارت و بازبینی دسترسی ها	☐	
۵۷- جلوگیری از حساب کاربری مشترک بین کارشناسان	☐	
۵۸- حذف حسابهای بلا استفاده مانند حساب کارکنان رفته از سازمان	☐	
۵۹- تغییر متناوب و دوره ای گذرواژه های کلیه حساب های کاربری دارای سطح دسترسی بالا در تجهیزات شبکه و سامانه ها با رعایت ملاحظات امنیتی استاندارد	☐	
۶۰- محدودسازی مراجعات و دسترسی‌های غیر ضرور پیمانکاران و افزایش کنترل و نظارت بر اقدامات آنها (لازم به ذکر است هرگونه استفاده از پیمانکاران خارجی در مرحله بهره برداری عملیاتی سامانه ها ممنوع بوده و دسترسی پیمانکاران داخلی بنا بر ضرورت با نظارت و کنترل کامل با مسئولیت پذیری مرجع مشخص انجام شود)	☐	
۶۱- تهیه لیست ارتباطات بیسیم و پیاده سازی و بررسی صحت عملکرد رمزنگاری و احراز هویت در آنها به منظور حفظ محرمانگی و یکپارچگی، حتی الامکان از شبکه بیسیم در سازمان استفاده نشود.	☐	
۶۲- پایش و عدم استفاده از شبکه های مبتنی بر wireless در شبکه ایزوله داخلی و صنعتی	☐	
۶۳- اعمال سیاست های امنیتی برای محدود سازی فعالیت کلاینت ها در ساعات غیر اداری	☐	
۶۴- تعیین الزامات امنیتی جهت استفاده از ابزارهای ذخیره سازی قابل حمل	☐	
۶۵- اعمال رمزنگاری بر روی ترافیک لایه های مختلف شبکه	☐	

	۶۶- حتی الامکان از شبکه بیسیم در سازمان استفاده نشود در غیر این صورت تمهیدات امنیتی مناسب برای امن سازی و مدیریت دسترسی این شبکه ها در نظر گرفته شود.	☐	
	۶۷- ارائه هر سرویس در بستر اینترنت ضمن اینکه باید توسط تجهیزات امنیتی محافظت شوند لذا منوط به انجام آزمون نفوذ و رفع آسیب پذیری های احتمالی گردد. لذا ارائه سرویس حیاتی در بستر اینترنت باید با هماهنگی مرکز افتا صورت پذیرد.	☐	
	۶۸- ضمن ارائه لیست به روز شده از آدرس IPهای معتبر سازمان بر بستر اینترنت و مشخص کردن سرویس های فعال بر روی آن ها و ارسال لیست برای مرکز افتا، فهرست IP های آلوده شناسایی شده و ارتباط سامانه های حیاتی سازمان با آن ها مسدود شود.	☐	
	۶۹- استفاده از سرویس میزبانی خارج از کشور برای تمامی سرویس ها و سامانه های حیاتی غیرمجاز است. (	☐	
	۷۰- رعایت ملاحظات جلوگیری از نشت اطلاعات از جمله تبادل جریان های اطلاعاتی مهم به شکل امن (رمز شده) و با رعایت سیاست گذاری امنیتی	☐	
	۷۱- رصد هر گونه دسترسی مدیریتی به دارایی‌های حیاتی به طور مثال با استفاده از PAM	☐	
جداسازی مناطق امنیتی و مقاوم سازی	۷۲- ایجاد و مقاوم سازی یک شبکه ایزوله برای دسترسی به پورت های مدیریتی سرورها و تجهیزات و محدودسازی دسترسی به این شبکه به مدیران شبکه و دسترسی از طریق کلاینت محلی	☐	
	۷۳- غیر فعال سازی کلیه پورت ها و سرویس های غیر ضروری	☐	
	۷۴- غیر فعال نمودن قابلیت DHCP Client سرور	☐	
	۷۵- محدودسازی دسترسی به پورت های حساس (از جمله سرویسSSH در سرورهای ESX)	☐	
	۷۶- بروز بودن نسخه میان افزار پورت های مدیریتی سرورها از مخازن معتبر محلی	☐	
	۷۷- فعال سازی secure boot در ماشین های مجازی	☐	
	۷۸- بازبینی هرگونه پیکربندی پیش فرض و بررسی نشده تجهیزات و نرم افزارهای مرتبط با سامانه های حیاتی (نظیر سوئیچ، روتر، تجهیزات امنیتی، سیستم عامل، پایگاه داده،	☐	

	سرویس وب و...) و مقاوم سازی آنها مطابق با آخرین راهنماهای امنیتی مربوطه		
	۷۹- وجود روش اجرای/دستورالعمل مدیریت وصله برای تجهیزات سایبری و اجرای منظم آن با رعایت اصول مدیریت تغییرات برای اجرای امن نصب وصله ها و با در نظر گرفتن نصب وصله‌های امنیتی اعلام شده از طریق مراجع ذی‌صلاح و منابع معتبر	☐	
	۸۰- رصد منظم آسیب پذیری های شناخته شده و وصله فوری آنها از مخازن معتبر محلی	☐	
	۸۱- عدم قرارگیری سرویس های پر مخاطره مانند SQL-Server ،SMB،telnet در لبه اینترنت	☐	
	۸۲- استقلال شبکه در خدمات اصلی شبکه و اطمینان از تامین نیازمندی های حیاتی با افزونگی مناسب از جمله خدمات زمانبندی و همزمان سازی و خدمات نام و دامنه	☐	
	۸۳- طراحی امن شبکه با در نظر گرفتن دفاع در عمق و پیاده سازی زونبندی و بخش بندی بین نواحی مختلف شبکه تا انتشار آلودگی و صدمات بین نواحی مختلف محدود شود.	☐	
	۸۴- سرور پایگاه داده از سرور برنامه کاربردی سامانه های حیاتی جدا شده و دسترسی به آن کنترل شود.	☐	
	۸۵- جزیره سازی و مستقل سازی بخش های عملیاتی در شبکه متناسب با موقعیت جغرافیایی، ماموریت سازمان و یا سامانه عملیاتی به طوری که هر بخش توانایی ادامه ماموریت های اصلی خود را بدون اتکا به سایر بخش ها داشته باشد و ارتباطات ضروری بین بخش های توسط تجهیزات امنیتی رصد و کنترل شود.	☐	
	۸۶- مدیریت آسیب پذیری های کشف شده بر روی دارایی های سایبری و رفع آسیب پذیری های شناسایی شده در فرایندهای ارزیابی دوره‌ای دستگاه، ضمن اینکه سامانه های حیاتی خاص سازمان، باید با همکاری مرکز افتا مورد ارزیابی امنیتی قرار گیرند.	☐	
آموزش، فرهنگ سازی، آگاهی رسانی و اطلاع رسانی	۸۷- آموزش، توجیه و آگاهی‌رسانی مستمر امنیت سایبری و شرایط هشدار به کلیه کارکنان	☐	
	۸۸- برنامه ریزی و برگزاری مستمر دوره های امنیتی IT و OT	☐	
	۸۹- تهیه لیست و طبقه بندی کارکنان جهت اطلاع رسانی وضعیتها بر حسب شرایط هشدار سایبری	☐	

	۹۰- تعیین راه ارتباطی کارکنان با تیم CERT و اطلاع رسانی همگانی	☐	
تشکیل جلسات و گزارش‌دهی	۹۱- تهیه فرمت گزارش دهی	☐	
	۹۲- حضور مستمر اعضا کمیته امنیت سایبری نسبت به پایش اوضاع و حصول اطمینان از وجود آمادگی های لازم		
ممیزی و بازرسی	۹۳-تجمیع چک‌لیست‌های امنیتی استاندارد و ابلاغی بالادستی و تهیه چک لیست های ممیزی و ارزیابی داخلی	☐	
	۹۴- انجام ممیزی و ارزیابی داخلی امنیت سایبری مطابق با چک‌لیست‌های تهیه شده به صورت دوره ای	☐	
تعمیرات و نگهداری	۹۵. تهیه و به‌روزرسانی لیست و تناوب انواع فعالیت‌های تعمیرات، نگهداری، توسعه و بهینه‌سازی و مشخص کردن اولویت، میزان ضرورت و میزان تاخیر مجاز هریک	☐	
	۹۶. محاسبه ریسک توقف فعالیت‌های تعمیرات، نگهداری، توسعه و بهینه‌سازی غیرفوری	☐	
امنیت فیزیکی	۹۷- مشخص کردن نقاط حساس محل استقرار دارایی‌های سایبری حیاتی	☐	
	۹۸- مشخص کردن نقاط حساس ورودی و غیر ورودی	☐	حراست
	۹۹- تهیه لیست پیمانکاران داخلی و خارجی شرکت که نیاز به تردد دارند به همراه ساعت و سایر محدودیت های مربوطه	☐	حراست
	۱۰۰- تهیه لیست مجاز تردد همکاران در نقاط حساس به همراه ساعت و سایر محدودیت های مربوطه	☐	حراست
	۱۰۱- استقرار انواع سامانه‌های امنیتی فیزیکی مانند دوربین‌های تحت کنترل، قفل‌ها، سامانه‌های ایمنی، اعلام و اطفای حریق و غیره	☐	حراست
	۱۰۲- استفاده از تجهیزات قابل حمل شامل رسانه های ذخیره ساز، سیار سازمانی و شخصی مدیریت و کنترل شود.	☐	حراست
سایر الزامات مرتبط با حراست	۱۰۳- ** واحد حراست مطابق دستورالعمل‌های موجود در این حوزه و نیزمواردی که توسط سازمان حراست کل کشور ابلاغ شده است اقدام نمایند	☐	حراست
	۱۰۴- ضمن توجه به این موضوع که بهره گیری از افراد دوتابعیتی در امورات مرتنط با امنیت و مشاغل حساس مجاز نیست، لذا اسامی و سمت افراد دو تابعیتی در جایگاه مدیریتی و کارشناسی به حراست سازمان ارسال شود.	☐	حراست
	۱۰۵- حراست زیر ساخت بر روند ورود و خروج نیروها اعم از کادر سازمانی و پیمانکاران که سطح دسترسی بالایی در شبکه دارند کنترل و نظارت جدی داشته باشد.	☐	حراست

گروه اقدامات	اقدامات اجرایی هشدار زرد	وضعیت انجام	مسئول انجام	منابع
پشتیبان‌گیری و تأمین افزونگی	۱- به‌روزرسانی نسخه پشتیبان مطمئن انواع دارایی‌های سایبری حیاتی بصورت آفلاین و آف‌سایت پس از اعلام وضعیت زرد	☐		
	۲- کسب اطمینان از در دسترس بودن و صحت عملکرد فایل‌های پشتیبان تهیه شده	☐		
	۳- بررسی موجودی و آماده سازی تجهیزات یدک سخت‌افزاری و حصول اطمینان از وجود امکان جایگزینی سریع در شرایط اضطراری	☐		
	۴- حصول اطمینان از وجود افزونگی مناسب در مورد مؤلفه‌های سایبری موجود در بخش‌های مختلف.	☐		
	۵- کنترل وضعیت سایت پشتیبان و mirror دارایی‌های سایبری	☐		
تست منابع تغذیه و تجهیزات سرمایش	۶- حصول اطمینان از صحت عملکرد در حوزه منابع تغذیه شامل شارژر، UPS و باطری، منابع تغذیه اضطراری (دیزل ژنراتور) و انواع پست های توزیع برق اختصاصی داخل مجموعه در صورت وجود	☐		
	۷- حصول اطمینان از صحت عملکرد تجهیزات سرمایش مرتبط با دارایی های حیاتی (نظیر اتاق سرور، مراکز داده و ...)	☐		
	۸- مدیریت فرآیند درخواست و تأمین سوخت مورد نیاز دیزل ژنراتور	☐		

صحت عملکرد تجهیزات امنیتی و به‌روزرسانی امضاها و قوانین آن‌ها	۹- بررسی صحت عملکرد و به‌روز بودن سامانه‌های امنیتی شامل انواع سیستم‌های تشخیص و مقابله با نفوذ، دیوارهای آتش شبکه و برنامه‌های کاربردی، آنتی‌ویروس، SIEM و غیره و در صورت لزوم به‌روزرسانی آن‌ها به صورت هفتگی	☐		
	۱۰- بررسی منظم سامانه جامع مدیریت امنیت سایبری از طریق وب‌سایت‌های هشداردهی داخلی مانند وب‌سایت مرکز ماهر و مرکز مدیریت راهبردی افتا جهت دریافت انواع اخبار و به‌روزرسانی‌های امنیتی به صورت روزانه	☐		
	۱۱- بررسی و اعمال به‌روزرسانی امضاها (Signatures) و پایگاه دانش انواع تجهیزات امنیتی پس از تست از طریق مخازن (Repositories) مورد تأیید به صورت روزانه	☐		
پایش امنیت شبکه	۱۲- تشدید رصد و پایش، تشخیص و هشدار و آماده باش نیروهای به صورت on-call	☐		
لاگ گیری	۱۳- اطمینان از فعال بودن انواع مکانیزم‌های لاگ‌گیری بر روی دارایی‌های سایبری حیاتی برای انجام عملیات فارنزیک	☐		
	۱۴- بازبینی لاگ‌ها و رخدادهای بر روی تجهیزات و تعریف و فعال‌سازی لاگ جدید در صورت نیاز وتکرار ماهانه آن در صورت استمرار وضعیت هشدار	☐		

آمادگی نیروی انسانی مسئول	۱۵- اطلاع‌رسانی وضعیت آماده باش به تیم CERT	☐		
	۱۶- اطلاع‌رسانی به پرسنل On-call برای آمادگی بیشتر	☐		
کنترل دسترسی و ارتباطات امن	۱۷- قطع ارتباط سامانه‌های غیرضروری از اینترنت که در شرایط سفید از طریق اینترنت قابل دسترس هستند	☐		
	۱۸- محدودسازی دسترسی راه دور به شبکه‌های داخلی از طریق اتصالاتی مانند VPN، RDP، VNC، SSH، Telnet و غیره و صرفاً بنا بر ضرورت و محدود به محل، زمان و کاربر معین شده	☐		
	۱۹- بازنگری، محدودسازی و پایش مرتب سطح دسترسی افراد به دارایی‌های سایبری حیاتی	☐		
	۲۰- ایجاد اجبار سیستمی تغییر کلمه عبور حساب های کاربری مدیریتی مورد استفاده که برای پیکربندی کل یا بخشی از شبکه و سامانه‌ها و تجهیزات ICT و صنعتی استفاده می‌شوند و حساب‌های کاربری سامانه‌های کنترلی و پایش حیاتی و حساس، مطابق رویه‌های مربوطه	☐		
	۲۱- قطع ارتباط از راه دور با تجهیزات بر اساس سطح کنترل و سطح دسترسی و به غیر از مواردی که اپراتور مستقر ندارند	☐		
	۲۲- انجام بررسی در راستای کسب اطمینان از جدا بودن شبکه‌های داخلی سازمانی و صنعتی و	☐		

	تصمیم‌گیری و کسب مجوز از افتا در مورد نقاط اتصال (در صورت وجود)			
	۲۳- ** اطمینان از قطع هر گونه دسترسی شبکه صنعتی به اینترنت	☐		
	۲۴- بازبینی و اطمینان از صحت عملکرد روش‌هایی مانند Dot1x و Port Security در ورودی شبکه‌های رایانه‌ای	☐		
	۲۵-کسب اطمینان از بسته بودن کلیه‌ی پورت‌های USB در محدوده زیرساخت صنعتی	☐		
	۲۶- محدودیت دسترسی فیزیکی افراد به اماکن حساس مرتبط با سامانه های حیاتی اعمال گردد	☐		
	۲۷- جلوگیری از دسترسی غیرمجاز و دست کاری لاگ های ذخیره شده و نسخه های پشتیبان	☐		
جداسازی مناطق امنیتی و مقاوم سازی	۲۸- ممیزی کلیه اقدامات پیش نیاز توسط تیم فنی بعد از اعلام وضعیت زرد	☐		
آموزش، فرهنگ سازی، آگاهی رسانی و اطلاع رسانی	۲۹- اطلاع‌رسانی ورود به وضعیت زرد به نفرات مرتبط	☐		
	۳۰- انجام آگاهی‌رسانی و اعلام هشدارهای ضروری به کلیه کارکنان شامل هشدار در مورد عدم بازکردن ایمیل‌های مشکوک، عدم کلیک بر روی لینک‌های غیرضروری، عدم استفاده از تجهیزات ذخیره‌سازی و پردازشی سیار بر روی سیستم‌های کاری و غیره	☐		

	۳۱- یادآوری نحوه برقراری ارتباط با تیم CERT به تمام کارکنان	☐		
	۳۲- در صورت بروز هر گونه رخداد غیرطبیعی در شبکه (اعم از سایبری یا غیر سایبری) در اسرع وقت مراتب به سازمان حراست کل کشور گزارش شود	☐		
تشکیل جلسات و گزارش‌دهی	۳۳-تشکیل جلسه کمیته امنیت سایبری و اعلام آماده باش به تیم CERT به محض دریافت اعلام وضعیت زرد و بعد از آن (در صورت نیاز) و نیز تشکیل جلسات تیم CERT حداقل یکبار و بعد از آن (در صورت نیاز)، در ساعات اداری و در صورت نیاز بعد از وقت اداری	☐		
	۳۴- ارسال گزارش بر حسب نیاز توسط فرمانده تیم CERT به رئیس کمیته امنیت سایبری دستگاه	☐		
	۳۵- ارسال گزارش جلسات کمیته امنیت سایبری و تیم CERT و نیز گزارش اقدامات انجام شده به مراجع توسط رئیس کمیته امنیت سایبری	☐		
	۳۶- ارسال گزارش از وقایع سایبری به صورت برخط به تیم CERT مرکزی	☐		
ممیزی و بازرسی	۳۷- انجام ممیزی و بازرسی‌های امنیت سایبری مطابق با چک‌لیست‌های ممیزی و ارزیابی داخلی	☐		
	۳۸- بررسی در دسترس بودن انواع دستورالعمل‌های پاسخگویی به	☐		

	حوادث سایبری و طرح تداوم کسب و کار			
	۳۹- اطمینان از پیاده‌سازی صحیح آیتم‌های چک لیست بازرسی اضطراری	☐		
	۴۰- پیگیری و نظارت بر اجرای دستورالعمل‌های سازمان حراست کل کشور، سازمان پدافند غیرعامل و مرکز مدیریت راهبردی افتا ابلاغ شده توسط سازمان‌های بالادستی	☐		
	۴۱- تکرار ماهانه کلیه‌ی ممیزی‌ها و بازرسی‌های اشاره شده در الزامات، در صورت استمرار وضعیت زرد	☐		
تعمیرات و نگهداری	۴۲- سنجش ریسک هر فعالیت تعمیرات، نگهداری، توسعه و بهینه‌سازی و بررسی و بازنگری لیست با توجه به وضعیت زرد	☐		
امنیت فیزیکی	۴۳- تشدید حفاظت فیزیکی و مراقبت از مراکز، اتصالات و ارتباطات فیزیکی شبکه‌ای و سایر تجهیزات، دارایی‌های اطلاعاتی و زیرساخت‌های صنعتی، از طریق تخصیص نیروی انسانی برای مراقبت شبانه‌روزی در کلیه نقاط حساس محل استقرار دارایی‌های سایبری حیاتی	☐		
	۴۴- محدودسازی تردد و لغو بازدیدها و ترددهای غیرضروری و ممانعت از ورود افراد غیر مسئول و فاقد صلاحیت‌های لازم حراستی.	☐		
	۴۵- درخواست اعطای مجوز تردد به واحد حراست دستگاه ، برای	☐		

	حضور نمایندگان سازمان پدافند غیرعامل کشور و مرکز مدیریت راهبردی افتا در صورت نیاز			
	۴۶- درخواست اعطای مجور تردد به واحد حراست ، برای حضور اعضای تیم CERT در ساعات اداری و غیر اداری	☐		
	۴۷- بررسی صحت عملکرد سامانه‌های امنیتی فیزیکی مانند دوربین‌های تحت کنترل، قفل‌ها، سامانه‌های ایمنی، اعلام و اطفای حریق و غیره	☐		
	۴۸- بررسی و بازبینی صحت عملکرد انواع سامانه‌های هشدار مانند SMS، آژیر و غیره	☐		
سایر الزامات مرتبط با حراست	۴۹- ** واحد حراست مطابق دستورالعمل‌های موجود در این حوزه و نیزمواردی که توسط سازمان حراست کل کشور ابلاغ شده است اقدام نمایند	☐		

گروه اقدامات	اقدامات اجرایی هشدار نارنجی	وضعیت انجام	مسئول انجام	اقدام
پشتیبان‌گیری و تأمین افزونگی	۱- به‌روزرسانی نسخه پشتیبان انواع دارایی‌های سایبری حیاتی بصورت آفلاین و آف‌سایت پس از اعلام وضعیت نارنجی و نگهداری در محیط ایزوله	☐		
	۲- بررسی موجودی و آماده سازی تجهیزات یدک سخت‌افزاری و حصول اطمینان از وجود امکان جایگزینی سریع در شرایط اضطراری	☐		
	۳- حصول اطمینان از وجود افزونگی مناسب در مورد مؤلفه‌های سایبری موجود در بخش‌های مختلف.	☐		
	۴- کنترل وضعیت سایت پشتیبان و Mirror دارایی‌های سایبری	☐		
	۵- تشدید خط مشی‌های پشتیبان‌گیری (مانند افزایش تعداد Pointهای پشتیبان‌گیری، انجام برخی پشتیبان‌گیری‌ها از نوع Full، اطمینان از عدم بازنویسی شدن پشتیبان‌ها به دلیل نبود ظرفیت کافی، نگهداری تعداد حداقل پشتیبان مربوط به فواصل زمانی مختلف)	☐		
تست منابع تغذیه و تجهیزات سرمایش	۶-حصول اطمینان از صحت عملکرد در حوزه منابع تغذیه شامل شارژر، UPS و باطری، منابع تغذیه اضطراری (دیزل ژنراتور) و انواع پست های توزیع برق اختصاصی داخل مجموعه (در صورت وجود)	☐		
	۷- حصول اطمینان از صحت عملکرد تجهیزات سرمایش مرتبط با دارایی های حیاتی (نظیر اتاق سرور، مراکز داده و ...)	☐		
	۸- حصول اطمینان از امکان مدیریت بارهای مصرفی	☐		
	۹- مدیریت فرآیند درخواست و تأمین سوخت مورد نیاز دیزل ژنراتور	☐		

	۱۰- مدیریت Changeover با هدف افزایش قابلیت اطمینان تأمین مصارف حیاتی	☐		
صحت عملکرد تجهیزات امنیتی و به‌روزرسانی امضاها و قوانین آن‌ها	۱۱- بررسی صحت عملکرد و به‌روز بودن سامانه‌های امنیتی شامل انواع سیستم‌های تشخیص و مقابله با نفوذ، دیوارهای آتش شبکه و برنامه‌های کاربردی، آنتی‌ویروس، SIEM و غیره و در صورت لزوم به‌روزرسانی آن‌ها به صورت هفتگی	☐		
	۱۲- بررسی منظم سامانه جامع مدیریت امنیت سایبری از طریق وب‌سایت‌های هشداردهی داخلی مانند وب‌سایت مرکز ماهر و مرکز مدیریت راهبردی افتا جهت دریافت انواع اخبار و به‌روزرسانی‌های امنیتی به صورت روزانه	☐		
	۱۳- بررسی و اعمال به‌روزرسانی امضاها (Signatures) و پایگاه دانش انواع تجهیزات امنیتی پس از تست از طریق مخازن (Repositories) مورد تأیید به صورت روزانه	☐		
پایش امنیت شبکه	۱۴- تشدید رصد و پایش، تشخیص و هشدار با اکتفا نکردن به تشخیص خودکار و سیستمی و افزایش حضور نفرات به دو شیفت و یک شیفت on call با تخصیص حداقل یک نیروی انسانی متخصص برای هر واحد مانیتورینگ شبکه عملیات صنعتی و ICT	☐		
	۱۵-قرار دادن حساسیت سیستم های تشخیص حملات سایبری، در سخت‌گیرانه ترین حالت ممکن	☐		
	۱۶- اعلام و پیگیری همه هشدارها (علاوه برهشدارهای Critical)	☐		
لاگ گیری	۱۷- اطمینان از فعال بودن انواع مکانیزم‌های لاگ‌گیری بر روی دارایی‌های سایبری حیاتی برای انجام عملیات فارنزیک	☐		

	۱۸- بازبینی لاگ‌ها و رخدادهای بر روی تجهیزات و تعریف و فعال‌سازی لاگ جدید در صورت نیاز وتکرار ماهانه آن در صورت استمرار وضعیت هشدار	☐		
آمادگی نیروی انسانی مسئول **آمادگی نیروی انسانی مسئول**	۱۹- اطلاع‌رسانی وضعیت آماده باش به تیم CERT	☐		
	۲۰- اطلاع‌رسانی جامع به کلیه راهبران و مدیران سیستم‌ها و شبکه، برای آمادگی لازم برای حضور در ساعت‌های غیرکاری در محل و پرهیز از مرخصی‌های غیرضروری.	☐		
	۲۱- عدم اجازه خروج از شهر برای نیروهای متخصص مشخص شده در لیست شیفت بندی برای وضعیت هشدار نارنجی و حضور آنها بر اساس برنامه شیفت مشخص شده	☐		
	۲۲- اطلاع‌رسانی به پرسنل On-call برای آمادگی بیشتر	☐		
	۲۳- کاهش سطح کنترل راه دور و اتوماتیک اماکن، ایستگاه ها و تجهیزات بر اساس برنامه مشخص شده و اختصاص اپراتورهای دارای صلاحیت برای اماکن و تجهیزات دارای سطح کنترل محلی یا دستی و بدون اپراتور	☐		
کنترل دسترسی و ارتباطات امن	۲۴- قطع ارتباط سامانه‌های غیرضروری از اینترنت که در شرایط سفید از طریق اینترنت قابل دسترس هستند و بازنگری در لیست سفید ضروری	☐		
	۲۵- در صورت امکان حذف دسترسی راه دور به شبکه صنعتی، از طریق اتصالاتی مانند VPN، RDP، VNC، SSH، Telnet و غیره	☐		
	۲۶- بازنگری، محدودسازی و پایش مرتب سطح دسترسی افراد به دارایی‌های سایبری حیاتی	☐		
	۲۷- ایجاد اجبار سیستمی تغییر کلمه عبور حساب های کاربری مدیریتی مورد استفاده که برای پیکربندی کل یا بخشی از شبکه و	☐		

کنترل دسترسی و ارتباطات امن	سامانه‌ها و تجهیزات ICT و صنعتی استفاده می‌شوند و حساب‌های کاربری سامانه‌های کنترلی و پایش حیاتی و حساس، مطابق رویه‌های مربوطه			
	۲۸- نظارت بر قطع بودن هر گونه ارتباط از راه دور با تجهیزات به غیر از مواردی که اپراتور مستقر ندارند (مثل پست‌های فوق‌توزیع برق بدون اپراتور)	☐		
	۲۹- انجام بررسی در راستای کسب اطمینان از جدا بودن شبکه‌های داخلی سازمانی و صنعتی و تصمیم‌گیری فوری در مورد نقاط اتصالی در صورت وجود	☐		
	۳۰- اطمینان از قطع هر گونه دسترسی شبکه صنعتی به اینترنت	☐		
	۳۱- بازبینی و اطمینان از صحت عملکرد روش‌هایی مانند Dot1x و Port Security در ورودی شبکه‌های رایانه‌ای	☐		
	۳۲-کسب اطمینان از بسته بودن کلیه‌ی پورت‌های USB در محدوده زیرساخت صنعتی	☐		
	۳۳- محدودیت دسترسی فیزیکی افراد به اماکن حساس مرتبط با سامانه های حیاتی اعمال گردد	☐		
	۳۴- جلوگیری از دسترسی غیرمجاز و دست کاری لاگ های ذخیره شده و نسخه های پشتیبان	☐		
	۳۵- محدودسازی دسترسی به سامانه‌های ضروری منتشر شده بر روی اینترنت، به IP های کاربران داخل کشور	☐		
	۳۶- قطع دسترسی کاربران غیر ضروری به سامانه‌ها	☐		
	۳۷- بررسی در راستای کسب اطمینان از جداسازی شبکه‌های داخلی از اینترنت و اتصال به شبکه ملی اطلاعات (اینترانت ملی)	☐		

	۳۸- کنترل عدم امکان انجام تنظیمات تجهیزات صنعتی در واحدهای حساس و حیاتی از راه دور	☐		
جداسازی مناطق امنیتی و مقاوم سازی	۳۹- ممیزی کلیه اقدامات پیش نیاز توسط تیم فنی بعد از اعلام وضعیت نارنجی	☐		
آموزش، فرهنگ سازی، آگاهی رسانی و اطلاع رسانی	۴۰- اطلاع‌رسانی ورود به وضعیت نارنجی به نفرات مرتبط	☐		
	۴۱- انجام آگاهی‌رسانی و اعلام هشدارهای ضروری به کلیه کارکنان شامل هشدار در مورد عدم بازکردن ایمیل‌های مشکوک، عدم کلیک بر روی لینک‌های غیرضروری، عدم استفاده از تجهیزات ذخیره‌سازی و پردازشی سیار بر روی سیستم‌های کاری و غیره	☐		
	۴۲- یادآوری نحوه برقراری ارتباط با تیم CERT به تمام کارکنان	☐		
	۴۳- در صورت بروز هر گونه رخداد غیرطبیعی در شبکه (اعم از سایبری یا غیر سایبری) در اسرع وقت مراتب به سازمان حراست کل کشور گزارش شود	☐		
تشکیل جلسات و گزارش‌دهی	۴۴- تشکیل جلسه کمیته امنیت سایبری و تیم CERT دستگاه به محض دریافت اعلام وضعیت نارنجی و نیز تشکیل جلسات تیم CERT بر حسب نیاز، حداقل به صورت هفتگی جهت انجام و نظارت بر اقدامات در وضعیت هشدار نارنجی سایبری	☐		
	۴۵- ارسال گزارش بر حسب نیاز توسط فرمانده تیم CERT به رئیس کمیته امنیت سایبری	☐		
	۴۶- ارسال گزارش جلسات کمیته امنیت سایبری و تیم CERT دستگاه به مراجع توسط رئیس کمیته امنیت سایبری	☐		
	۴۷- ارسال گزارش از وقایع سایبری به صورت برخط به تیم CERT مرکزی	☐		

ممیزی و بازرسی	۴۸- انجام ممیزی و بازرسی‌های امنیت سایبری مطابق با چک‌لیست‌های ممیزی و ارزیابی داخلی	☐		
	۴۹- بررسی در دسترس بودن انواع دستورالعمل‌های پاسخگویی به حوادث سایبری و طرح تداوم کسب و کار	☐		
	۵۰- اطمینان از پیاده‌سازی صحیح آیتم‌های چک لیست بازرسی اضطراری	☐		
	۵۱- پیگیری و نظارت بر اجرای دستورالعمل‌های سازمان حراست کل کشور، سازمان پدافند غیرعامل و مرکز مدیریت راهبردی افتا ابلاغ شده توسط سازمان‌های بالادستی	☐		
	۵۲- تکرار کلیه‌ی ممیزی‌ها و بازرسی‌های اشاره شده در الزامات، هر دو هفته یکبار در صورت استمرار وضعیت نارنجی	☐		
تعمیرات و نگهداری	۵۳- توقف انواع فعالیت‌های تعمیرات، نگهداری، توسعه و بهینه سازی غیرفوری	☐		
	۵۴- سنجش میزان ریسک انجام انواع فعالیت های تعمیرات، نگهداری، توسعه و بهینه سازی ضروری و استعلام از مدیریت واحد بهره‌برداری مربوطه جهت صدور مجوز جهت انجام آن‌ها تا با در نظر گرفتن ریسک موجود (تنها فعالیت‌های ضروری که اختلالی در پایداری شبکه ایجاد نمی کنند، صورت پذیرند.)	☐		
امنیت فیزیکی	۵۵- تشدید حفاظت فیزیکی و مراقبت از مراکز، اتصالات و ارتباطات فیزیکی شبکه‌ای و سایر تجهیزات، دارایی‌های اطلاعاتی و زیرساخت‌های صنعتی، از طریق تخصیص نیروی انسانی برای مراقبت شبانه‌روزی در کلیه نقاط حساس محل استقرار دارایی‌های سایبری حیاتی	☐		
	۵۶- محدودسازی تردد و لغو بازدیدها و ترددهای غیرضروری و ممانعت از ورود افراد	☐		

	غیر مسئول و فاقد صلاحیت‌های لازم حراستی.			
	۵۷- درخواست اعطای مجوز تردد به واحد حراست، برای حضور نمایندگان سازمان پدافند غیرعامل کشور و مرکز مدیریت راهبردی افتا در صورت نیاز	☐		
	۵۸- درخواست اعطای مجور تردد به واحد حراست، برای حضور اعضای تیم CERT و کارکنان On Call و شیفت‌بندی شده، در ساعات اداری و غیر اداری	☐		
	۵۹- بررسی صحت عملکرد سامانه‌های امنیتی فیزیکی مانند دوربین‌های تحت کنترل، قفل‌ها، سامانه‌های ایمنی، اعلام و اطفای حریق و غیره	☐		
	۶۰- بررسی و بازبینی صحت عملکرد انواع سامانه‌های هشدار مانند SMS، آژیر و غیره	☐		
سایر الزامات مرتبط با حراست	۶۱- واحد حراست مطابق دستورالعمل‌های موجود در این حوزه و نیزمواردی که توسط سازمان حراست کل کشور ابلاغ شده است اقدام نمایند	☐		

گروه اقدامات	اقدامات اجرایی هشدار قرمز	وضعیت انجام	مسئول انجام
پشتیبان‌گیری و تأمین افزونگی	۱- به‌روزرسانی نسخه پشتیبان انواع دارایی‌های سایبری حیاتی بصورت آفلاین و آف‌سایت پس از اعلام وضعیت قرمز و نگهداری در محیط ایزوله	☐	
	۲- بررسی موجودی و آماده سازی تجهیزات یدک سخت‌افزاری و حصول اطمینان از وجود امکان جایگزینی سریع در شرایط اضطراری	☐	
	۳- حصول اطمینان از وجود افزونگی مناسب در مورد مؤلفه‌های سایبری موجود در بخش‌های مختلف دستگاه .	☐	
	۴- کنترل وضعیت سایت پشتیبان و mirror دارایی‌های سایبری	☐	
	۵- تشدید خط‌مشی‌های پشتیبان‌گیری (مانند افزایش تعداد Pointهای پشتیبان‌گیری، انجام برخی پشتیبان‌گیری‌ها از نوع full، اطمینان از عدم بازنویسی شدن پشتیبان‌ها به دلیل نبود ظرفیت کافی، نگهداری تعداد حداقل پشتیبان مربوط به فواصل زمانی مختلف)	☐	
تست منابع تغذیه و تجهیزات سرمایش	۶- حصول اطمینان از صحت عملکرد در حوزه منابع تغذیه شامل شارژر، UPS و باطری، منابع تغذیه اضطراری (دیزل ژنراتور) و انواع پست های توزیع برق اختصاصی داخل مجموعه (در صورت وجود)	☐	
	۷- حصول اطمینان از صحت عملکرد تجهیزات سرمایش مرتبط با دارایی های حیاتی (نظیر اتاق سرور، مراکز داده و ...)	☐	
	۸- حصول اطمینان از امکان مدیریت بارهای مصرفی	☐	
	۹- مدیریت فرآیند درخواست و تأمین سوخت مورد نیاز دیزل ژنراتور	☐	

	۱۰- مدیریت Changeover با هدف افزایش قابلیت اطمینان تأمین مصارف حیاتی	☐	
	۱۱- حذف دسترسی Remote به زیرساخت کنترل و مانیتورینگ تجهیزات تغذیه به طوریکه امکان قطع و وصل منابع تغذیه وجود نداشته باشد.	☐	
صحت عملکرد تجهیزات امنیتی و به‌روزرسانی امضاها و قوانین آن‌ها	۱۲- بررسی صحت عملکرد و به‌روز بودن سامانه‌های امنیتی شامل انواع سیستم‌های تشخیص و مقابله با نفوذ، دیوارهای آتش شبکه و برنامه‌های کاربردی، آنتی‌ویروس، SIEM و غیره و در صورت لزوم به‌روزرسانی آن‌ها به صورت هفتگی	☐	
	۱۳- بررسی منظم سامانه جامع مدیریت امنیت سایبری از طریق وب‌سایت‌های هشداردهی داخلی مانند وب‌سایت مرکز ماهر و مرکز مدیریت راهبردی افتا جهت دریافت انواع اخبار و به‌روزرسانی‌های امنیتی به صورت روزانه	☐	
	۱۴- بررسی و اعمال به‌روزرسانی امضاها (Signatures) و پایگاه دانش انواع تجهیزات امنیتی پس از تست از طریق مخازن (Repositories) مورد تأیید به صورت روزانه	☐	
پایش امنیت شبکه	۱۵- تشدید رصد و پایش، تشخیص و هشدار با اکتفا نکردن به تشخیص خودکار و سیستمی و افزایش حضور نفرات به دو شیفت و یک شیفت on call با تخصیص حداقل یک نیروی انسانی متخصص برای هر واحد مانیتورینگ شبکه عملیات صنعتی و ICT	☐	
	۱۶-قرار دادن حساسیت سیستم های تشخیص حملات سایبری، در سخت‌گیرانه ترین حالت ممکن	☐	
	۱۷- اعلام و پیگیری همه هشدارها (علاوه برهشدارهای Critical)	☐	

لاگ گیری	۱۸- اطمینان از فعال بودن انواع مکانیزم‌های لاگ‌گیری بر روی دارایی‌های سایبری حیاتی برای انجام عملیات فارنزیک	☐	
	۱۹- بازبینی لاگ‌ها و رخدادهای تجهیزات و تعریف و فعالسازی لاگ جدید در صورت نیاز و تکرار دو هفته یکبار آن در صورت استمرار وضعیت هشدار	☐	
آمادگی نیروی انسانی مسئول **آمادگی نیروی انسانی مسئول**	۲۰. اطلاع‌رسانی وضعیت آماده باش به تیم CERT	☐	
	۲۱. اطلاع‌رسانی جامع به کلیه راهبران و مدیران سیستم‌ها و شبکه، برای آمادگی لازم برای حضور در ساعت‌های غیرکاری در محل دستگاه و پرهیز از مرخصی‌های غیرضروری.	☐	
	۲۲. عدم اجازه خروج از شهر برای نیروهای متخصص مشخص شده در لیست شیفت بندی برای وضعیت هشدار قرمز و حضور آنها بر اساس برنامه شیفت مشخص شده	☐	
	۲۳- ابلاغ on call بودن به کارکنان مسئول پشتیبانی سیستم های IT و OT	☐	
	۲۴. اطلاع‌رسانی به پرسنل On-call برای آمادگی بیشتر و تشدید قوانین کاری مربوطه در کلیه ساعات شبانه روز در روزهای کاری و تعطیل.	☐	
	۲۵. کاهش سطح کنترل راه دور و اتوماتیک اماکن، ایستگاه ها و تجهیزات بر اساس برنامه مشخص شده و اختصاص اپراتورهای دارای صلاحیت برای اماکن و تجهیزات دارای سطح کنترل محلی یا دستی و بدون اپراتور	☐	
	۲۶- قطع ارتباط سامانه‌های غیرضروری از اینترنت که در شرایط سفید از طریق اینترنت قابل دسترس هستند و بازنگری در لیست سفید ضروری	☐	

کنترل دسترسی و ارتباطات امن	۲۷- در صورت امکان حذف دسترسی راه دور به شبکه صنعتی، از طریق اتصالاتی مانند VPN، RDP، VNC، SSH، Telnet و غیره	☐	
	۲۸- بازنگری، محدودسازی و پایش مرتب سطح دسترسی افراد به دارایی‌های سایبری حیاتی	☐	
	۲۹- ایجاد اجبار سیستمی تغییر کلمه عبور حساب های کاربری مدیریتی مورد استفاده که برای پیکربندی کل یا بخشی از شبکه و سامانه‌ها و تجهیزات ICT و صنعتی استفاده می‌شوند و حساب‌های کاربری سامانه‌های کنترلی و پایش حیاتی و حساس، مطابق رویه‌های مربوطه	☐	
	۳۰- نظارت بر قطع بودن هر گونه ارتباط از راه دور با تجهیزات به غیر از مواردی که اپراتور مستقر ندارند	☐	
	۳۱- انجام بررسی در راستای کسب اطمینان از جدا بودن شبکه‌های داخلی سازمانی و صنعتی و تصمیم‌گیری فوری در مورد نقاط اتصالی در صورت وجود	☐	
	۳۲- ** اطمینان از قطع هر گونه دسترسی شبکه صنعتی به اینترنت	☐	
	۳۳- بازبینی و اطمینان از صحت عملکرد روش‌هایی مانند Dot1x و Port Security در ورودی شبکه‌های رایانه‌ای	☐	
	۳۴-کسب اطمینان از بسته بودن کلیه‌ی پورت‌های USB در محدوده زیرساخت صنعتی	☐	
	۳۵- محدودیت دسترسی فیزیکی افراد به اماکن حساس مرتبط با سامانه های حیاتی اعمال گردد	☐	

	۳۶- جلوگیری از دسترسی غیرمجاز و دست کاری لاگ های ذخیره شده و نسخه های پشتیبان	☐	
	۳۷- محدودسازی دسترسی به سامانه‌های ضروری منتشر شده بر روی اینترنت، به IP های کاربران داخل کشور	☐	
	۳۸- قطع دسترسی کاربران غیر ضروری به سامانه‌ها	☐	
	۳۹- بررسی در راستای کسب اطمینان از جداسازی شبکه‌های داخلی از اینترنت و اتصال به شبکه ملی اطلاعات (اینترانت ملی)	☐	
	۴۰- کنترل عدم امکان انجام تنظیمات تجهیزات صنعتی در واحدهای حساس و حیاتی از راه دور	☐	
جداسازی مناطق امنیتی و مقاوم سازی	۴۱- ممیزی کلیه اقدامات پیش نیاز توسط تیم فنی بعد از اعلام وضعیت قرمز	☐	
آموزش، فرهنگ سازی، آگاهی رسانی و اطلاع رسانی	۴۲. اطلاع‌رسانی ورود به وضعیت قرمز به نفرات مرتبط	☐	
	۴۳. انجام آگاهی‌رسانی و اعلام هشدارهای ضروری به صورت فوری به کلیه کارکنان شامل هشدار در مورد عدم بازکردن ایمیل‌های مشکوک، عدم کلیک بر روی لینک‌های غیرضروری، عدم استفاده از تجهیزات ذخیره‌سازی و پردازشی سیار بر روی سیستم‌های کاری و غیره	☐	
	۴۴. اطلاع‌رسانی و یادآوری راه‌های ارتباطی با نماینده تیم CERT دستگاه و افراد جانشین ایشان به کلیه کارکنان.	☐	
	۴۵- در صورت بروز هر گونه رخداد غیرطبیعی در شبکه (اعم از سایبری یا غیر سایبری) در اسرع وقت مراتب به سازمان حراست کل کشور گزارش شود	☐	

تشکیل جلسات و گزارش‌دهی	۴۶- تشکیل جلسه کمیته امنیت سایبری و تیم CERT دستگاه به محض دریافت اعلام وضعیت قرمز و نیز تشکیل جلسات تیم CERT حداقل به صورت روزانه جهت انجام و نظارت بر اقدامات در وضعیت هشدار قرمز سایبری	☐	
	۴۷- ارسال گزارش روزانه توسط فرمانده تیم CERT دستگاه به رئیس کمیته امنیت سایبری دستگاه	☐	
	۴۸- ارسال گزارش جلسات کمیته امنیت سایبری و تیم CERT دستگاه و نیز گزارش اقدامات انجام شده به تیم CERT مرکزی و مراکز امنیت سایبری (حراست، افتا، پدافند و ماهر) توسط رئیس کمیته امنیت سایبری دستگاه	☐	
	۴۹- ارسال گزارش از وقایع سایبری به صورت برخط به تیم CERT مرکزی	☐	
ممیزی و بازرسی	۵۰- انجام ممیزی و بازرسی‌های امنیت سایبری مطابق با چک‌لیست‌های ممیزی و ارزیابی داخلی	☐	
	۵۱- بررسی در دسترس بودن انواع دستورالعمل‌های پاسخگویی به حوادث سایبری و طرح تداوم کسب و کار	☐	
	۵۲- اطمینان از پیاده‌سازی صحیح آیتم‌های چک لیست بازرسی اضطراری	☐	
ممیزی و بازرسی	۵۳- پیگیری و نظارت بر اجرای دستورالعمل‌های سازمان حراست کل کشور، پدافند غیرعامل و مرکز مدیریت راهبردی افتا ابلاغ شده توسط سازمان‌های بالادستی	☐	
	۵۴- تکرار کلیه‌ی ممیزی‌ها و بازرسی‌های اشاره شده در الزامات، بصورت هفتگی با یک روال چابک در صورت استمرار وضعیت قرمز	☐	

تعمیرات و نگهداری	۵۵- توقف انواع فعالیت‌های تعمیرات، نگهداری، توسعه و بهینه سازی غیرفوری	☐	
	۵۶- سنجش میزان ریسک انجام انواع فعالیت های تعمیرات، نگهداری، توسعه و بهینه سازی ضروری و استعلام از مدیریت واحد بهره‌برداری مربوطه جهت صدور مجوز جهت انجام آن‌ها تا با در نظر گرفتن ریسک موجود (تنها فعالیت‌های ضروری که اختلالی در پایداری شبکه ایجاد نمی کنند، صورت پذیرند.)	☐	
امنیت فیزیکی	۵۷- تشدید حفاظت فیزیکی و مراقبت از مراکز، اتصالات و ارتباطات فیزیکی شبکه‌ای و سایر تجهیزات، دارایی‌های اطلاعاتی و زیرساخت‌های صنعتی، از طریق تخصیص نیروی انسانی برای مراقبت شبانه‌روزی در کلیه نقاط حساس محل استقرار دارایی‌های سایبری حیاتی	☐	
	۵۸- محدودسازی تردد و لغو بازدیدها و ترددهای غیرضروری و ممانعت از ورود افراد غیر مسئول و فاقد صلاحیت‌های لازم حراستی.	☐	
	۵۹- درخواست اعطای مجوز تردد به واحد حراست دستگاه ، برای حضور نمایندگان سازمان پدافند غیرعامل کشور و مرکز مدیریت راهبردی افتا در صورت نیاز	☐	
	۶۰- درخواست اعطای مجور تردد به واحد حراست دستگاه، برای حضور اعضای تیم CERT و کارکنان On Call و شیفت‌بندی شده، در ساعات اداری و غیر اداری	☐	
	۶۱- بررسی صحت عملکرد سامانه‌های امنیتی فیزیکی مانند دوربین‌های تحت کنترل، قفل‌ها، سامانه‌های ایمنی، اعلام و اطفای حریق و غیره	☐	
	۶۲- بررسی و بازبینی صحت عملکرد انواع سامانه‌های هشدار مانند SMS، آژیر و غیره	☐	

	۶۳- لغو مجوز پیمانکاران برای تردد، غیر از نفرات عضو تیم CERT و اعطای مجوز به صورت موردی	☐	
سایر الزامات مرتبط با حراست	۶۴- ** واحد حراست دستگاه‌ها مطابق دستورالعمل‌های موجود در این حوزه و نیزمواردی که توسط سازمان حراست کل کشور ابلاغ شده است اقدام نمایند	☐	

فرم ارزیابی FRM-HF-CH03v1

نام دستگاه: نام وزارتخانه : نام دستگاه هماهنگ کننده: نام دستگاه همکار:

عناوین و شاخص های مورد بررسی	عدم درک ضرورت	درک ضرورت	اقدامات پراکنده	اقدامات نظام مند	توضیحات
الزامات مراجع					
۱-۱- طرح تداوم کسب وکار دستگاه و اجرای مانور (پدافند)					
۱-۲- شناسایی آسیب پذیری ها و اقدامات جهت رفع آنها (افتا)					
۱-۳- تشکیل کمیته و کارگروه های تخصصی حراست (فارنزیک و..)					
۱-۴- ایجاد پرونده سایبری حراستی					
کمیته امنیت و ممیزی					
۲-۱- گزارش جلسات کمیته امنیت سایبری و تیم CERT					
۲-۲- تجمیع چک‌لیست‌های امنیتی استاندارد و ابلاغی بالادستی					
۲-۳- انجام ممیزی و ارزیابی داخلی امنیت سایبری					
۲-۴- پیگیری و نظارت بر اجرای دستورالعمل‌های مراجع					
کنترل دسترسی و ارتباطات امن					
۳-۱- بازنگری، محدودسازی و پایش سطح دسترسی					
۳-۲- ممنوعیت هرگونه دسترسی از راه دور به سامانه ها					
۳-۳- جداسازی شبکه‌های داخلی سازمانی و صنعتی					
۳-۴- قطع هر گونه دسترسی شبکه IT و OT به اینترنت					
۳-۵- قطع دسترسی کاربران غیر ضروری به سامانه‌ها					
۳-۶- سیاستگذاری تغییر کلمه عبور سامانه ها و تجهیزات					
۳-۷- ممنوعیت پیمانکاران خارجی					
مقاوم سازی و پایش شبکه					
۴-۱- رصد و پایش، تشخیص و هشدار و آماده باش نیروهای شبکه					
۴-۲- غیر فعال سازی کلیه پورت ها و سرویس های غیر ضروری					
۴-۳- مدیریت وصله با رعایت اصول مدیریت تغییرات					
۴-۴- بازبینی هرگونه پیکربندی پیش فرض					
۴-۵- مدیریت آسیب پذیری های کشف شده					
تجهیزات امنیتی و ثبت وقایع					
۵-۱- رصد و پایش هرگونه دسترسی مدیریتی به دارایی‌های حیاتی					
۵-۲- مدیریت و بروزرسانی تجهیزات امنیتی					
۵-۳- فعال بودن مکانیزمهای لاگ‌گیری					
پشتیبان گیری و افزونگی					
۶-۱- سایت پشتیبان و mirror سامانه ها					
۶-۲- افزونگی دارایی های سایبری					
۶-۳- تهیه پشتیبانگیری مطمئن از سامانه ها					
۶-۴- عملکرد منابع تغذیه مراکز داده (ژنراتور)					
آمادگی نیروی انسانی					
۷-۱- تهیه و غربالگری لیست نیروهای متخصص					
۷-۲- اعلام وضعیت آماده باش به تیم CERT					
۷-۳- اطلاع‌رسانی جامع به کلیه راهبران سیستمها (هشدارها)					
آموزش و اطلاع رسانی					
۸-۱- آموزش، توجیه و آگاهی‌رسانی مستمر امنیت سایبری					
۸-۲- آگاهی رسانی و اعلام هشدارهای ضروری					
۸-۳- گزارش رخدادهای سایبری به مراجع					
امنیت فیزیکی					
۹-۱- تهیه لیست پیمانکاران داخلی و خارجی					
۹-۲- محدودسازی تردد و لغو بازدیدها و ترددهای غیرضروری					
۹-۳- بررسی عملکرد سامانههای امنیتی فیزیکی و هشدار					
۹-۴- مدیریت و کنترل تجهیزات قابل حمل الکترونیکی					

نتایج ارزیابی

مهمترین نقاط قوت و ضعف ارزیابی:

مهمترین نیازمندی ها در شرایط بحران:

نام و نام خانوادگی ارزیابان، حاضرین و امضاء: