وزارت نیرو
کارگروه تخصصی امنیت سایبری

سند راهنمای شرح خدمات

پروژه‌های امنیت سایبری حوزه OT

نوع مدرک: سند راهنما **شناسه:** ECS-MOE-G-OT Projects RFP-V1.0

نسخه: ۱,۰ **طبقه‌بندی:** مهم **تاریخ آخرین اصلاح:** ۱۴۰۳/۰۹/۲۰

	تهیه	بازنگری	تایید و تصویب کنندگان
رکن نظام‌نامه	کمیته امنیت سایبری سامانه های صنعتی شرکت مدیریت منابع آب ایران	کارگروه خدمات تخصصی امنیت سایبری	کارگروه تخصصی امنیت سایبری وزارت نیرو
سمت	دبیر کمیته	رئیس کارگروه	روسای کارگروه
نام	سیف الله آقابیگی	دولت جمشیدی	آزرم دهستانی- سیف الله آقابیگی
تاریخ	۱۴۰۳/۰۹/۲۰	۱۴۰۳/۰۹/۲۰	۱۴۰۳/۰۹/۲۰
امضا			

جمهوری اسلامی ایران
وزارت نیرو
کارگروه تخصصی
امنیت سایبری

جدول سوابق تغییرات

شماره نسخه	تاریخ بازنگری	شرح تغییرات
۱,۰	۱۴۰۳/۰۹/۲۰	تهیه نسخه اولیه مستند

فهرست مطالب

عنوان **صفحه**

۱-هدف و دامنه کاربرد

صنعت آب و برق کشور، به عنوان دو زیرساخت حیاتی که سایر زیرساخت‌های کشور به آنها وابسته هستند و مخاطره سایبری برای این دو زیرساخت، موجب بروز پیامدهایی مانند به مخاطره افتادن و وقفه در عملیات سایر بخش‌های کشور خواهد شد، نیاز به توجه و تمرکز ویژه‌ای به منظور ارتقاء امنیت سایبری در حوزه عملیات و زیرساخت‌های صنعتی دارند.

در راستای پاسخگویی به این نیاز، و براساس تاکیدات بخشنامه ارتقا امنیت سایبری حوزه OT، شرکت‌ها بایستی متناسب با ارکان اجرایی، زیرساختی و فنی تعیین شده در آن بخشنامه، نسبت به تصویب نقشه راه ارتقای امنیت سایبری و سپس برنامه‌ریزی پروژه‌های مورد نیاز ذیل نقشه راه اقدام نمایند. سند پیش‌رو، جهت ارائه راهنما برای تعریف شرح خدمات مشاوران پروژه‌های ارتقای امنیت سایبری حوزه OT تدوین شده و حداقل اقلام خدمتی مورد انتظار که در هر نوع پروژه باید توسط مشاور ارائه شود را تشریح می‌نماید.

علاوه بر این، لازم است کلیه فعالیت‌های مرتبط با تدوین نقشه راه و اجرای پروژه‌های ارتقای امنیت سایبری ذیل نقشه راه، توسط کمیته راهبری امنیت سایبری شرکت مادر تخصصی مربوطه در حوزه‌های زیر مورد بررسی و تأیید قرار گیرد:

- انجام تحلیل شکاف، ارائه نقشه راه و برنامه زمان‌بندی اجرای فعالیت‌ها متناسب با وضع موجود، نیازها و بودجه
- بررسی دلایل انتخاب انواع استانداردها، چهارچوب‌ها، متدولوژی‌ها برای اجرای هر بخش از هر یک از انواع پروژه‌ها
- تعیین شاخص‌های موفقیت هر فعالیت، هر پروژه و کل نقشه راه و گزارش‌دهی مستمر در خصوص میزان ارتقا در هریک از شاخص‌ها
- تحلیل قیمت و ارزش گذاری پروژه و تعیین وزن اقلام خروجی و نتایج پروژه
- نظارت کلان بر پروژه‌ها و ارائه نقطه‌نظرات در خصوص جامعیت، کفایت و دقت خروجی‌ها و نتایج فنی، فرایندی و مستندات تعریف شده برای پروژه
- زمان‌بندی و اولویت‌دهی انجام فعالیت‌ها و تصویب زمانبندی اجرایی
- ممیزی نهایی پروژه و تأیید دریافت خروجی‌های پروژه

موارد مطرح شده جهت تائید توسط کمیته راهبری امنیت سایبری شرکت مادر تخصصی، می‌تواند بر اساس مستندات (خط مشی، روش اجرایی و دستورالعمل) ابلاغی وزارت نیرو و مستقیماً از طریق نماینده(ها)ی کمیته راهبری انجام شود یا

مشاور تعیین شده از سوی کمیته راهبری امنیت سایبری شرکت مادر تخصصی تحت عنوان مشاور راهبری، مسئولیت اقدامات فوق را بر عهده بگیرد. لازم است صلاحیت مشاور راهبری منتخب برای هر شرکت مادر تخصصی، به تایید کارگروه تخصصی امنیت سایبری وزارت نیرو برسد.

به‌طور کلی هدف اصلی این سند، ارائه راهنما به کلیه شرکت‌ها در راستای تدوین شرح خدمات انواع پروژه‌های امنیت سایبری حوزه OT جهت واگذاری به شرکت‌ها در قالب مشاور اجرایی می‌باشد.

محدوده اجرای این سندِ راهنما، ستاد وزارت نیرو، شرکت‌های مادرتخصصی و زیرمجموعه و سازمان‌های تابعه (ساتبا، سازمان توسعه و بهره‌برداری فناوری‌های نوین آب‌های جوّی و ساتکاب) و موسسات آموزشی و پژوهشی وابسته به وزارت نیرو که دارای زیرساخت‌های فناوری عملیاتی (OT) هستند یا در این حوزه، وظایف و مسئولیت‌هایی برای آنها تعیین شده است را در برمی‌گیرد و کلیه این شرکت‌ها لازم است حداقل‌های عنوان شده در این سند را در پروژه‌های برون‌سپاری امنیت سایبری حوزه OT خود منظور نمایند.

۲-مسئولیت‌ها

- مسئولیت تصویب و ابلاغ این سند راهنما بر عهده کارگروه تخصصی امنیت سایبری وزارت نیرو است.
- مسئولیت پشتیبانی اجرای این سند در هر شرکت و در حوزه ستادی وزارت نیرو بر عهده کمیته راهبری امنیت سایبری می‌باشد.
- مسئولیت اجرای این سند در هر شرکت بر عهده کارگروه(های) تخصصی مرتبط و مسئولیت اجرای آن در حوزه ستادی وزارت نیرو بر عهده مدیر کل دفتر مدیریت بحران و پدافند غیرعامل ستاد وزارت نیرو می‌باشد.
- مسئولیت نظارت بر نحوه اجرای این سند در کلیه شرکت‌ها بر عهده واحد حراست و امور محرمانه (حفاظت فناوری اطلاعات) شرکت و نظارت عالیه بر عهده معاون حفاظت فناوری اطلاعات حراست وزارت نیرو می‌باشد.

۳-مراجع و اسناد مرتبط

- طرح امن‌سازی زیرساخت‌های حیاتی در قبال حملات سایبری، ابلاغی مرکز مدیریت راهبردی افتا - سال ۱۳۹۷
- طرح پاسخ اضطراری سایبری در حوزه انرژی (CERP)، ابلاغی قرارگاه پدافند سایبری سازمان پدافند غیرعامل کشور - مرداد ۱۳۹۷

جمهوری اسلامی ایران
وزارت نیرو
کارگروه تخصصی
امنیت سایبری

- طرح پاسخگویی به حوادث سایبری، ابلاغی مرکز مدیریت راهبردی افتا – شهریور ۱۳۹۸
- صورتجلسه بررسی و تعیین ساختار امنیت سایبری وزارت نیرو به شماره ۹۹/۲۶۶۰۹/۵۵۰ د مورخ ۱۳۹۹/۰۵/۰۶
- نظام‌نامه امنیت سایبری وزارت نیرو به شماره ۹۹/۳۵۷۱۱/۵۰/۱۰۰ مورخ ۱۳۹۹/۰۹/۱۱
- مصوبه جلسه بیست و سوم شورای اجرایی فناوری اطلاعات کشور ابلاغی طی نامه شماره ۱/۱۰۰۲۲ مورخ ۱۴۰۱/۰۱/۲۷
- بخشنامه شماره ۳۸۷۵۶۳ مورخ ۹۹/۱۱/۰۵ سازمان اداری و استخدامی کشور خطاب به دستگاه‌های اجرایی، موضوع ماده ۲۹ قانون برنامه توسعه ششم
- مستند «روش اجرایی پاسخگویی به حوادث سایبری» ابلاغی وزارت نیرو طی نامه شماره ۱۴۰۰/۴۷۴۱۷/۵۵۰ مورخ ۱۴۰۰/۱۰/۲۵
- مستند «اقدامات اساسی امن‌سازی اضطرارای در زیرساخت‌های کشور»، ابلاغی قرارگاه پدافند سایبری سازمان پدافند غیرعامل کشور – مرداد ۱۴۰۱
- ابلاغیه «سیاست‌های و الزامات فناوری اطلاعات و امنیت سایبری وزارت نیرو» به امضای وزیر نیرو، طی نامه شماره ۱۴۰۲/۴۳۱۶۸/۵۰/۱۰۰ مورخ ۱۴۰۲/۰۸/۲۷
- استانداردها و راهنماهای بین‌المللی امنیت فناوری عملیاتی (OT) :

  – IEC 62443 series, Industrial Communication Networks - networks and system security
  – IEC 62351 series, Power systems management and associated information exchange – Data and communications security
  – NIST 800-82, Guide to Operational Technology (OT) Security
  – NIST 7628, Guidelines for Smart Grid Cybersecurity
  – NERC CIP, Reliability Standards for the Bulk Electric Systems of North America
  – ISO/IEC 27019, Information technology ssecurity techniques- Information Security Controls for the Energy Utility Industry
  – IEEE 1686, IEEE Standard for Intelligent Electronic Devices Cyber Security Capabilities
  – C2M2 , Cybersecurity Capability Maturity Model, DOE (v2.1 June 2022)
  – CSF, NIST Cybersecurity Framework v2.0 (February 2024)

جمهوری اسلامی ایران
وزارت نیرو
کارگروه تخصصی
امنیت سایبری

۴- تعاریف

- **مشاور راهبری:** به نمایندگی و یا در کنار کارفرمای اصلی پروژه‌ها، به انجام فعالیت‌هایی که از جنس تحلیل شکاف، تدوین نقشه راه، تعیین چهارچوب و متدولوژی مربوط به انجام فعالیت‌ها، راهبری فنی، مدیریتی و نظارتی هستند، می‌پردازد.
- به‌منظور ایجاد یکپارچگی و هم‌افزایی، کارگروه تخصصی امنیت سایبری وزارت نیرو، طی مشارکت نمایندگان کلیه شرکت‌های مادر تخصصی در حوزه‌های آب و برق و مرکز تخصصی امنیت سایبری پژوهشگاه نیرو، نقش تدوین چهارچوب‌ها، روش‌های اجرایی، دستورالعمل‌ها و متدولوژی‌های کلان را ایفا می‌نماید. شرکت‌های مادر تخصصی می‌توانند جهت مدیریت و راهبری یکپارچه‌ی انجام فعالیت‌های ارتقای امنیت سایبری و ارزیابی مربوطه در محدوده کاری خود، از مشاور راهبری استفاده نمایند.
- **مشاور اجرایی:** منظور شرکتی است که یک یا چند پروژه تعریف شده در حوزه امنیت سایبری OT ، به آن شرکت واگذار شده است و از نظر شرایط عمومی و تخصصی، صلاحیت لازم برای انعقاد قرارداد را متناسب با الزامات و نقطه‌نظرات ارائه شده توسط نماینده کمیته راهبری امنیت سایبری شرکت/سازمان مربوطه، دارا است.
- **حوزه‌ها یا مراکز** OT **:** کلیه حوزه‌های کاری صنعت آب و برق که بر روی عملیات اصلی این صنعت و ارائه خدمات آب و برق اثرگذار هستند به عنوان حوزه‌های OT یا مراکز OT مدنظر می‌باشند که شامل و نه محدود به موارد زیر می‌باشند:
  - مرکز دیسپاچینگ ملی کشور، انواع نیروگاه‌های برق حرارتی، برق-آبی، تجدیدپذیر و تولید پراکنده، شبکه انتقال برق کشور، پست برق در سطح انتقال (۴۰۰ و ۲۳۰ کیلوولت)، پست برق در سطح فوق‌توزیع (۱۳۲ و ۶۳ کیلوولت)، مرکز دیسپاچینگ انتقال و فوق‌توزیع، شبکه توزیع برق کشور، سیستم کنترل و اتوماسیون شبکه توزیع برق، سامانه‌های اندازه‌گیری هوشمند انرژی، کنتورهای تبادلی، بازار برق و غیره.
  - انواع سدها و منابع آبی، شبکه انتقال آب، ایستگاه‌های پمپاژ آب، تلمبه‌خانه‌ها، شبکه آبیاری و زهکشی و غیره.
  - شبکه تامین، تصفیه و توزیع آب، شبکه تجمیع و تصفیه فاضلاب و غیره.

۵- تشریح روش اجرایی

با بررسی انواع استانداردها، چارچوب‌ها، مدل‌های بلوغ و به‌روش‌های حوزه امنیت سایبری، ابلاغیه‌های ارگان‌های بالادستی، انواع فعالیت‌ها و اقدامات اصلی که لازم است در راستای ارتقای امنیت سایبری در حوزه OT برنامه‌ریزی و

پیاده‌سازی شوند مشخص شده و پس از آن، فعالیت‌های استخراج شده گروه‌بندی گردید و در نهایت گروه اقدامات کلان حوزه امنیت سایبری مشخص شد. هر کدام از این گروه اقدامات کلان یا مجموعه‌ای از آن‌ها را می‌توان در قالب پروژه‌هایی تعریف و اجرایی نمود.

در این راستا، با بررسی اسناد مهم مرتبط، از جمله ISO/IEC 62443-3-3، NIST 800-82، C2M2، IEC 62351، NIST CSF، NISTIR 7628، ISO/IEC 27019 و NERC CIP، گروه اقدامات زیر اهم دسته فعالیت‌هایی که باید در حوزه OT صورت پذیرد:

۱. مدیریت دارایی‌های سایبری و ارتباطی، و فرایندهای عملیاتی
۲. حاکمیت امنیت سایبری
۳. مدیریت امنیت منابع انسانی و کاربری امن
۴. ممیزی و بازرسی
۵. ارزیابی امنیتی
۶. امن‌سازی و مدیریت آسیب‌پذیری و وصله‌های امنیتی
۷. مدیریت ریسک سایبری
۸. مدیریت زنجیره تامین
۹. مدیریت هویت و کنترل دسترسی
۱۰. امنیت فیزیکی
۱۱. آموزش و آگاهی‌رسانی
۱۲. امنیت داده
۱۳. استقرار انواع تجهیزات و سامانه‌های امنیتی
۱۴. مدیریت لاگ و پایش امنیت سایبری و اشتراک‌گذاری اطلاعات
۱۵. پاسخ به حوادث سایبری و تشکیل تیم CSIRT
۱۶. تداوم کسب و کار
۱۷. پشتیبان‌گیری

جمهوری اسلامی ایران
وزارت نیرو
کارگروه تخصصی
امنیت سایبری

۱۸. نگهداری، تعمیرات و افزونگی دارایی‌های سایبری

۱۹. مدیریت و کنترل رسانه‌های قابل حمل

در ادامه، به منظور ارائه راهنمایی برای تعریف شرح خدمات مشاوران/پیمانکاران اجرای پروژه‌ها به ازای هر یک از گروه اقدامات فوق، حداقلِ فعالیت‌ها و اقلام خدمتی که باید در شرح خدمات هر نوع پروژه متناظر با هر گروه اقدام صورت پذیرد، در ۱۹ زیربخش تشریح شده است.

لازم به ذکر است که در راستای برون‌سپاری پروژه‌های مرتبط با هر یک از گروه اقدامات فوق، ممکن است برای هر گروه اقدام، چندین پروژه با شرح خدمات، اهداف و محدوده‌های متفاوت در بازه‌های زمانی مختلف تعریف شود و یا در حالتی دیگر، انجام فعالیت‌های مرتبط با چندین گروه اقدام از فهرست فوق، در قالب یک پروژه تجمیع شود. هر کدام از دو حالت فوق، مشکلی ندارد و قابل اجرا است و این سند، از این منظر محدودیتی تعیین نمی‌کند. به عبارت دیگر، لزومی به وجود تناظر یک به یک بین تعداد پروژه‌ها و تعداد گروه اقدامات فوق، وجود ندارد.

در مورد تقدّم و تأخّر کلّی بین گروه اقدامات و فعالیت‌های ذیل آن‌ها نمی‌توان نسخه واحدی ارائه داد که برای همه مراکز OT دقیق باشد و از همین منظر است که تأکید شده که شرکت‌ها بایستی متناسب با ارکان اجرایی، زیرساختی و فنی بخشنامه OT، نسبت به تدوین نقشه راه ارتقای امنیت سایبری بر اساس نتایج تحلیل شکاف و سپس برنامه‌ریزی پروژه‌های مورد نیاز ذیل نقشه راه اقدام نمایند. ولی نکته‌ای که می‌توان به صورت عمومی برای همه شرکت‌ها و مراکز OT آن‌ها توصیه کرد، این است که از بین ۱۹ گروه اقدام عنوان شده، سه گروه اقدام «مدیریت دارایی‌های سایبری و ارتباطی، و فرایندهای عملیاتی»، «حاکمیت امنیت سایبری» و «مدیریت ریسک سایبری»، باید به عنوان گروه اقدامات اولویت اول برنامه‌ریزی شوند و خروجی انجام آن‌ها، با توجه به ماهیت‌شان، تقدّم و تأخّر سایر فعالیت‌ها را با رویکرد پوشش ریسک‌های با درجه خطر بالاتر، مشخص می‌نماید. در واقع با انجام این سه گروه اقدام، به عنوان مهم‌ترین دستاوردها، اولاً شناخت درستی از دارایی‌های سایبری و معماری ارتباطی و فرایندهای مراکز OT به دست می‌آید، ثانیاً، مسئولیت‌ها به درستی تبیین و مسائل مرتبط با فرایندهای تصویب پروژه‌ها و تخصیص بودجه مربوطه شفاف می‌شود و در نهایت به کمک نتایج ارزیابی ریسک، فعالیت‌های ذیل ۱۶ گروه اقدام دیگر به صورت موازی برنامه‌ریزی و اجرا می‌شوند تا برنامه مواجهه با ریسک‌های با درجه خطر بالاتر، سریع‌تر اجرایی شود.

۵-۱- مدیریت دارایی‌های سایبری و ارتباطی، و فرایندهای عملیاتی

- مشخص کردن نقش‌ها، سمت‌ها و شرح وظایف مرتبط با اجرای مدیریت دارایی‌های سایبری
- سفارشی‌سازی سند ابلاغی وزارت نیرو مرتبط با مدیریت دارایی‌ها و ارتباطات سایبری
- شناسایی فرایندهای اصلی یا سرویس‌های کسب و کاری کل محدوده
- استخراج معماری اطلاعاتی و ارتباطی کل محدوده
- سفارشی‌سازی قالب دارایی‌های سایبری ابلاغی وزارت نیرو در صورت نیاز برای کلیه‌ی دارایی‌های سایبری (شامل و نه محدود به: انواع سخت‌افزارها مانند سرور، روتر و سوئیچ، تجهیزات امنیتی، توکن، دیتادیود، هارد، ماشین‌های مجازی، پایگاه‌های داده، سرویس‌های شبکه و امنیت، نرم‌افزارها، PC ها و لپ تاپ‌های کاربران، تجهیزات مخابراتی، زیرساخت‌های اندازه‌گیری پیشرفته، انواع مکان‌های فیزیکی مانند اتاق سرور و اتاق کنترل مرکزی و جانبی، اتاق کابینت، اتاق EWS، تجهیزات واحد برق، رله، درایو، بریکر، اسکادا، PLC، DCS، سیستم‌های کنترل صنعتی، سیستم‌های کنترل قطع اضطراری، آنالایزرها، HMI، تجهیزات UPS، سوئیچ‌های صنعتی، کنتور، پرسنل و .....)
- جمع‌آوری دارایی‌های سایبری و تکمیل کردن کل فیلدها و پارامترهای شناخت و تحلیل امنیت مرتبط با هر دارایی
- سفارشی‌سازی سند ابلاغی وزارت نیرو مرتبط با طبقه‌بندی دارایی‌های سایبری
- انجام طبقه‌بندی دارایی‌های سایبری
- سفارشی‌سازی سند ابلاغی وزارت نیرو مرتبط با امحا دارایی‌های سایبری
- ایجاد ساز و کار امحا دارایی‌های سایبری مطابق با سند تهیه شده
- سفارشی‌سازی سند ابلاغی وزارت نیرو مرتبط با فرمول ارزش‌گذاری دارایی‌های سایبری
- انجام ارزش‌گذاری دارایی‌های سایبری
- جاری‌سازی کل فرایندهای تدوین شده در شرکت

۵-۲- حاکمیت امنیت سایبری

فعالیت‌های مرتبط با این گروه اقدام (حاکمیت امنیت سایبری) عمدتاً از جنس راهبری و مدیریت کلان امنیت سایبری در محدوده کل شرکت است و ریزفعالیتی برای مشاور اجرایی، تعریف نمی‌شود.

جمهوری اسلامی ایران
وزارت نیرو
کارگروه تخصصی
امنیت سایبری

۵-۳- مدیریت امنیت منابع انسانی و کاربری امن

- مشخص کردن نقش‌ها، سمت‌ها و شرح وظایف مرتبط با عملیاتی کردن روش اجرایی مدیریت امنیت منابع انسانی در حین جذب، طول مدت زمان همکاری، جابجایی یا انفصال
- سفارشی‌سازی سند ابلاغی وزارت نیرو مرتبط با امنیت منابع انسانی
- جاری‌سازی کل فرایند و روش اجرایی تدوین شده و ایجاد و به جریان انداختن کلیه فرم‌ها و سیستم‌های مورد نیاز
- سفارشی‌سازی سند خط‌مشی کاربری امن (AUP) ابلاغ شده توسط وزارت نیرو و همراهی در انتشار آن در کل سازمان
- بازبینی و به‌روزرسانی سند NDA کارکنان در صورت لزوم

۵-۴- ممیزی و بازرسی

- مشخص کردن انواع بازرسی‌ها و ممیزی‌های دوره‌ای
- تدوین یا سفارشی‌سازی یا به‌روزرسانی چک‌لیست‌های فنی و پرسش‌نامه‌های تخصصی بازرسی و ممیزی دوره‌ای
- سفارشی‌سازی سند ابلاغی وزارت نیرو مرتبط با انجام ممیزی داخلی
- جاری‌سازی کل فرایندهای تدوین شده به صورت سیستمی
- انجام ممیزی‌ها یا بازرسی‌هایی که در محدوده شرح کار به مشاور/پیمانکار سپرده می‌شود و ارائه گزارش تفصیلی مدیریتی و فنی کلیه عدم انطباق‌ها به تفکیک نوع عدم انطباق و برنامه‌ریزی ممیزی یا بازرسی مجدد

۵-۵- ارزیابی امنیتی

- تهیه یا سفارشی‌سازی قالب سند شناخت محدوده، برای ارزیابی امنیتی
- انجام فاز شناخت به صورت کامل و تکمیل کردن قالب اسناد شناخت برای کلیه محدوده مشخص شده برای ارزیابی امنیتی
- به‌روزرسانی و سفارشی‌سازی اسناد متدولوژی ارزیابی امنیتی برای انواع دارایی‌های سایبری یا زیرساخت شبکه و سرویس‌دهی
- تهیه انواع موارد تست (Test Caseها)، چک‌لیست‌ها، پرسشنامه‌های فنی، ابزارها و روال‌های ارزیابی مرتبط با انواع ارزیابی امنیتی (تست نفوذ جعبه سفید، جعبه خاکستری، جعبه سیاه، ارزیابی آسیب‌پذیری (V.A.)، مصاحبه، بازدید میدانی، ممیزی پیکربندی، بازبینی کد و غیره) روی انواع دارایی‌های سایبری یا زیرساخت شبکه OT و سرویس‌دهی

- دریافت تأییدیه فاز شناخت و روال‌های انجام ارزیابی روی کل محدوده
- انجام ارزیابی امنیتی مطابق محدوده مشخص شده و روال‌های تأیید شده به طوری که هر ارزیابی، حداقل شامل موارد زیر باشد:
  - گزارش تفصیلی
  - توضیحات و تشریح موارد آسیب‌پذیری/عدم انطباق
  - مراجع و در صورت امکان کد مربوط به موارد آسیب‌پذیری/عدم انطباق،
  - شواهد موارد آسیب‌پذیری/عدم انطباق
  - رتبه‌بندی شدّت خطر بر اساس روش رتبه‌بندی تأیید شده، برای موارد آسیب‌پذیری/عدم انطباق
  - راهکار پیشنهادی رفع آسیب‌پذیری، برای موارد آسیب‌پذیری/عدم انطباق
- برنامه‌ریزی برای ارزیابی مجدد و انجام آن بعد از اعلام رفع آسیب‌پذیری یا عدم انطباق کشف شده
- تهیه گزارش مدیریتی نهایی از هر ارزیابی و کل ارزیابی‌های انجام شده

۵-۶- امن‌سازی و مدیریت آسیب‌پذیری و وصله‌های امنیتی

- سفارشی‌سازی سند ابلاغی وزارت نیرو مرتبط با انجام امن‌سازی
- تهیه دستورالعمل‌های امن‌سازی به تفکیک نوع دارایی
- سفارشی‌سازی سند ابلاغی وزارت نیرو مرتبط با انجام مدیریت آسیب‌پذیری و وصله‌های امنیتی
- تهیه دستورالعمل‌های مدیریت آسیب‌پذیری و وصله به تفکیک دسته دارایی‌های سایبری
- به‌روزرسانی چک‌لیست‌های امن‌سازی ابلاغی وزارت نیرو مطابق با محدوده پروژه امن‌سازی بر اساس مراجع معتبر از جمله CIS، STIGs و Vendor و تجربه مشاور
- انجام ممیزی وضعیت امن‌سازی و ارائه راهنمای نحوه امن‌سازی به تفکیک دارایی‌های سایبری محدوده پروژه
- ارائه سند معماری امن با در نظر گرفتن الزامات جداسازی حداکثری شبکه OT از سایر شبکه‌ها و استخراج LOM مربوط به امن‌سازی
- اجرای امن‌سازی دارایی‌های سایبری در صورت درخواست کارفرما و بعد از تأیید روش امن‌سازی ارائه شده
- اجرایی نمودن کل فرایندهای تدوین شده برای مدیریت آسیب‌پذیری و وصله

جمهوری اسلامی ایران
وزارت نیرو
کارگروه تخصصی
امنیت سایبری

۵-۷- مدیریت ریسک سایبری

- مشخص کردن نقش‌ها، سمت‌ها و شرح وظایف مرتبط با مدیریت ریسک امنیت سایبری حوزه OT
- تهیه سند شناخت و Context شامل شناخت اهداف امنیت سایبری و استراتژی‌ها و مأموریت‌ها، فرایندها، عوامل داخلی و خارجی، نقاط قوت و ضعف و فرصت‌ها و تهدیدها، ذینفعان و نیازمندی‌ها و انتظارات ایشان
- شناخت محدوده و نهایی‌سازی آن مطابق قالب مشخص شده و دریافت تأییدیه آن
- سفارشی‌سازی سند ابلاغی وزارت نیرو مرتبط با متدولوژی مدیریت ریسک سایبری شامل فرمول‌های ارزیابی ریسک
- انجام آموزش‌های مدیریت ریسک به کل افراد محدوده پروژه، در سطوح مختلف
- انجام یا بازبینی ارزش‌گذاری دارایی‌ها
- به‌روزرسانی فهرست آسیب‌پذیری‌های بالقوه
- احصا آسیب‌پذیری‌ها به‌تفکیک دارایی‌های محدوده مدنظر
- به‌روزرسانی فهرست تهدیدات
- ارزیابی احتمال وقوع تهدیدات به تفکیک دارایی‌های محدوده مدنظر
- به‌روزرسانی سناریوهای ریسک
- ارزیابی ریسک
- تعیین ریسک‌های غیرقابل پذیرش و استراتژی‌های برخورد با هر کدام
- تهیه اسناد RTP(Risk Treatment Plan) و SOA(Statement of Applicability)
- برنامه‌ریزی و اجرایی نمودن اقدامات RTP مطابق نظر کارفرما
- انجام ممیزی داخلی بعد از اعلام رفع ریسک‌ها
- ارائه گزارش بازبینی مدیریتی

۵-۸- مدیریت زنجیره تامین

- مشخص کردن نقش‌ها، سمت‌ها و شرح وظایف مرتبط با اجرای روش اجرایی مدیریت زنجیره تأمین در کل شرکت با تمرکز بر حوزه OT

- سفارشی‌سازی سند ابلاغی وزارت نیرو مرتبط با مدیریت زنجیره تأمین در حوزه OT و تهیه دستورالعمل‌های مربوطه
- اجرایی نمودن کل فرایند و دستورالعمل تدوین شده
- تهیه لیست تأمین‌کنندگان فعلی و بالقوه
- تهیه لیست سیاه تأمین‌کنندگان
- بررسی و ارزیابی فرایندهای مدیریت زنجیره تأمین در محدوده OT و ارائه سند نقاط ضعف و ریسک‌های موجود و راهکارهای پیشنهادی
- بازبینی و به‌روزرسانی NDA پیمانکاران در صورت لزوم

۵-۹- مدیریت هویت و کنترل دسترسی

- مشخص کردن نقش‌ها، سمت‌ها و شرح وظایف مرتبط با مدیریت هویت و کنترل دسترسی
- سفارشی‌سازی سند ابلاغی وزارت نیرو مرتبط با مدیریت هویت و دسترسی
- تهیه دستورالعمل مدیریت هویت و دسترسی به تفکیک هر دارایی سایبری در محدوده پروژه شامل نحوه اعطای دسترسی بر اساس اصل حداقل دسترسی، نحوه لغو دسترسی، نحوه و بازه‌ی زمانی بازبینی دسترسی‌ها و غیره
- سفارشی‌سای خط مشی کلمات عبور در صورت نیاز به تفکیک دارایی
- جاری‌سازی کل فرایندها و دستورالعمل‌های تدوین شده مطابق محدوده پروژه
- انجام بازبینی کل دسترسی‌ها بر روی دارایی‌های سایبری هدف پروژه
- سفارشی‌سازی سند ابلاغی وزارت نیرو در حوزه دسترسی از راه دور
- پیاده‌سازی PAM در صورت صلاحدید کارفرما
- سفارشی‌سازی سند ابلاغی وزارت نیرو در حوزه محافظت از نشت اطلاعات
- پیاده‌سازی DRM در صورت صلاحدید کارفرما
- بازبینی وضعیت توکن‌های مورد استفاده موجود
- پیاده‌سازی SSO در صورت صلاحدید کارفرما

جمهوری اسلامی ایران
وزارت نیرو
کارگروه تخصصی
امنیت سایبری

۵-۱۰- امنیت فیزیکی

- مشخص کردن نقش‌ها، سمت‌ها و شرح وظایف مرتبط با امنیت فیزیکی
- سفارشی‌سازی سند ابلاغی وزارت نیرو مرتبط با امنیت فیزیکی
- بازنگری و سفارشی‌سازی چک لیست‌های ارزیابی امنیت فیزیکی
- انجام ارزیابی وضعیت امنیت فیزیکی و ارائه گزارش تفصیلی و راهکارهای پیشنهادی
- مشاوره پیاده‌سازی امنیت فیزیکی در محدوده‌ی مشخص شده، شامل اتاق سرور، محیط پیرامونی، درب‌های ورودی و غیره، از نظر مسائل مختلف مانند پایش با دوربین، کنترل ورود/خروج، اطفای حریق، مقابله با لرزه، محافظت در برابر آب و رطوبت و غیره

۵-۱۱- آموزش و آگاهی‌رسانی

- مشخص کردن نقش‌ها، سمت‌ها و شرح وظایف مرتبط با آموزش و آگاهی‌رسانی
- سفارشی‌سازی سند ابلاغی وزارت نیرو مرتبط با نقشه راه آموزش امنیت سایبری برای حوزه OT
- تهیه دستورالعمل آموزش، برگزاری دوره‌های آموزشی و انجام پایش‌های مرتبط با اثربخشی آموزش‌ها
- تهیه دستورالعمل آگاهی‌رسانی شامل کلیه رسانه‌ها و انواع محتوای آگاهی‌رسانی
- اجرای آگاهی‌سانی امنیت سایبری مطابق دستورالعمل مشخص شده
- برگزاری حداقل یک دوره آگاهی‌رسانی عمومی و یک دوره آگاهی‌رسانی مدیریتی امنیت سایبری برای حوزه OT

۵-۱۲- امنیت داده

- مشخص کردن نقش‌ها، سمت‌ها و شرح وظایف مرتبط با محافظت از داده‌ها متناسب با فعالیت‌های مشخص شده در روش‌های اجرایی و دستورالعمل‌های مرتبط با این حوزه
- مشخص کردن انواع رمزنگاری، امضای دیجیتال یا درهم‌سازی مورد نیاز به تفکیک انواع اقلام اطلاعاتی مرتبط با دارایی‌های سایبری و بسترهای ارتباطی
- بازبینی وضعیت زیرساخت مدیریت کلید و گواهی‌های دیجیتال مورد استفاده و ارائه راهکار اصلاحی
- انجام تغییرات مرتبط با فعال‌سازی رمزنگاری یا امضای دیجیتال برای هر کدام از دارایی‌های سایبری محدوده‌ی مدنظر

- سفارشی‌سازی سند ابلاغی وزارت نیرو در رابطه با محافظت از نشت اطلاعات
- پیاده‌سازی DLP در صورت صلاحدید کارفرما
- پیاده‌سازی SSM/HSM در صورت نیاز کارفرما

۵-۱۳- استقرار انواع تجهیزات و سامانه‌های امنیتی

- مشخص کردن نقش‌ها، سمت‌ها و شرح وظایف مرتبط با تأمین و راه‌اندازی تجهیزات و سامانه‌های امنیتی
- سفارشی‌سازی سند ابلاغی وزارت نیرو مرتبط با معماری شبکه اطلاعاتی سازمان برای حوزه OT
- پیشنهاد جانمایی استقرار و مشخصات کلیه‌ی تجهیزات و سامانه‌های امنیتی بر اساس اصل دفاع در عمق با در نظر گرفتن نیازمندی‌های .H.A و افزونگی در کلیه لایه‌ها و دریافت تأییدیه
- ارائه مشاوره در تأمین تجهیزات و سامانه‌های مورد نیاز بر اساس اولویت و ارجاع کار توسط کارفرما
- راه‌اندازی تجهیزات و سامانه‌های امنیتی تأمین شده به درخواست کارفرما و انجام پیکربندی دقیق و آزمون عملکرد تجهیز یا سامانه و تهیه سند نگهداری و راهنمای بهره‌برداری

۵-۱۴- مدیریت لاگ و پایش امنیت سایبری و اشتراک‌گذاری اطلاعات

- مشخص کردن نقش‌ها، سمت‌ها و شرح وظایف مرتبط با مدیریت لاگ و پایش و اشتراک‌گذاری
- سفارشی‌سازی سند ابلاغی وزارت نیرو مرتبط با مدیریت لاگ
- سفارشی سند ابلاغی وزارت نیرو در حوزه پایش امنیت سایبری
- تهیه دستورالعمل‌های مرتبط با مدیریت لاگ و پایش امنیت سایبری (SOC)
- جاری‌سازی کل فرایندها و دستورالعمل‌های تدوین شده
- فعال‌سازی لاگ به ازای هر دارایی سایبری و ارسال آن یا راه‌اندازی Agentهای جمع‌آوری و ارسال لاگ
- راه‌اندازی سامانه مدیریت لاگ و SIEM
- استقرار تیم پایش طبق نیازمندی ۷*۲۴ یا ۸*۵ با پایش خودکار خارج از زمان کاری
- به‌روزرسانی مستمر قوانین تشخیص
- راه‌اندازی هوش تهدیدات

۵-۱۵- پاسخ به حوادث سایبری و تشکیل تیم CSIRT

- مشخص کردن نقش‌ها، سمت‌ها و شرح وظایف مرتبط با پاسخگویی به حوادث
- سفارشی‌سازی سند ابلاغی وزارت نیرو در حوزه پاسخ‌گویی به حوادث سایبری
- انجام پیش‌نیازهای درج شده در روش اجرای پاسخگویی به حوادث سایبری در شرکت‌های زیرمجموعه
- تهیه سیستم مدیریت دانش و مستندات
- ایجاد ارتباطات موردنیاز برای ارجاع کارهای پی‌جویی جرم (Forensic) به یک مرکز متخصص در این حوزه

۵-۱۶- تداوم کسب و کار

- مشخص کردن نقش‌ها، سمت‌ها و شرح وظایف مرتبط با تداوم کسب و کار
- سفارشی‌سازی سند ابلاغی وزارت نیرو در حوزه تداوم کسب و کار و فرمول‌های مربوطه
- انجام تحلیل BIA و شناسایی فرایندهای حیاتی و کلیدی
- انجام ارزیابی ریسک با رویکرد BCP
- تهیه طرح تداوم کسب و کار و بازیابی از فاجعه به ازای هر دارایی حیاتی و کلیدی شامل فعال‌سازی استراتژی‌ها و راهکارهایی که قبل از بروز اختلال، در طول اختلال و پس از آن باید به کار گرفته شوند
- تهیه سناریوهای مانور مطابق با تعداد توافق شده با کارفرما
- تهیه فرم‌های مرتبط با انجام مانور و گزارش‌دهی نهایی آن
- راهبری اجرای نمونه‌هایی از مانور مطابق نظر کارفرما به صورت دورِ میزی یا میدانی

۵-۱۷- پشتیبان‌گیری

- مشخص کردن نقش‌ها، سمت‌ها و شرح وظایف مرتبط با پشتیبان‌گیری
- سفارشی‌سازی روش اجرای ابلاغی وزارت نیرو در حوزه پشتیبان‌گیری OT
- جاری‌سازی روش اجرایی پشتیبان‌گیری
- تکمیل فرم پشتیبان‌گیری ابلاغی وزارت نیرو یا نسخه سفارشی‌سازی شده آن برای کلیه دارایی‌های سایبری که نیاز به پشتیبان‌گیری دارند

جمهوری اسلامی ایران
وزارت نیرو
کارگروه تخصصی
امنیت سایبری

- اجرای پشتیبان‌گیری مطابق با فرم تکمیل شده
- اجرای تست بازیابی نسخه‌های پشتیبان تهیه شده

۵-۱۸- نگهداری، تعمیرات و افزونگی دارایی‌های سایبری

- مشخص کردن نقش‌ها، سمت‌ها و شرح وظایف مرتبط با نگهداری، تعمیرات و افزونگی دارایی‌های سایبری
- سفارشی‌سازی روش اجرایی نگهداری و بازبینی دوره‌ای (PM) حوزه OT ابلاغی وزارت نیرو
- تدوین دستورالعمل‌های تعمیرات و تأمین افزونگی دارایی‌های سایبری با در نظر گرفتن مسائل امنیت سایبری
- جاری‌سازی فرایندهای تدوین شده در این حوزه

۵-۱۹- مدیریت و کنترل رسانه‌های قابل حمل

- مشخص کردن نقش‌ها، سمت‌ها و شرح وظایف مرتبط با مدیریت و کنترل رسانه‌های قابل حمل
- سفارشی‌سازی روش اجرایی ابلاغی وزارت نیرو در حوزه امنیت رسانه‌های قابل حمل
- جاری‌سازی فرایندهای تدوین شده در این حوزه
- نصب و راه‌اندازی نرم‌افزار MDM در صورت درخواست کارفرما بر روی دارایی‌های اطلاعاتی امکان‌پذیر مانند لپ‌تاپ پیمانکاران

۶-بازنگری

سند پیش‌رو در دوره‌های زمانی دو ساله یا در صورت بروز تغییراتی که بر آن تأثیرگذار باشند، به‌منظور تضمین تناسب با نیازمندی‌های امنیتی وزارت نیرو، مورد بازبینی و در صورت نیاز، مورد «تجدیدنظر» و «بازنگری» قرار خواهد گرفت.

جمهوری اسلامی ایران
وزارت نیرو
کارگروه تخصصی
امنیت سایبری

پیوست شماره ۱: گردآورندگان سند

تهیه مدرک

مسئولیت	نام و نام خانوادگی	عنوان	شرکت
راهبری	سیف‌الله آقابیگی	مدیر کل دفتر مدیریت بحران و پدافند غیر عامل و دبیر کمیته امنیت سایبری سامانه‌های صنعتی	شرکت مدیریت منابع آب ایران
برنامه‌ریزی و هماهنگی	فربد استیری	مشاور مدیر عامل	شرکت مدیریت منابع آب ایران
همکار مشارکت‌کننده	حسین تاج‌بخش	رئیس گروه پدافند غیرعامل	شرکت مدیریت منابع آب ایران
همکار مشارکت‌کننده	داود خطیب	رئیس گروه نظارت مالی	شرکت مدیریت منابع آب ایران
همکار مشارکت‌کننده	سعید منصوری	رئیس گروه حفاوا حراست شرکت مدیریت منابع آب ایران	شرکت مدیریت منابع آب ایران
همکار مشارکت‌کننده	محسن افشردی	کارشناس شبکه و بسترهای ارتباطی	شرکت مدیریت منابع آب ایران
همکار مشارکت‌کننده	تورج متینی	کارشناس پدافند غیر عامل	شرکت مدیریت منابع آب ایران
همکار مشارکت‌کننده	محمد جنتی‌پور	رئیس گروه امنیت سامانه های صنعتی	شرکت آب و برق خوزستان
همکار مشارکت‌کننده	محمدرضا ایستان	مدیر پروژه امنیت سایبری و پدافند غیر عامل	شرکت توسعه منابع آب و نیروی ایران
همکار مشارکت‌کننده	وحید کریمی‌فر	مدیر امور نگهداری، تعمیرات و بهره‌برداری در معاونت بهره‌برداری	شرکت توسعه منابع آب و نیروی ایران
همکار مشارکت‌کننده	مریم شبرو	معاون مرکز نوآوری و توسعه فناوری اطلاعات و ارتباطات و امنیت سایبری	پژوهشگاه نیرو
همکار مشارکت‌کننده	تینا تعویذی	مشاور مرکز نوآوری و توسعه فناوری اطلاعات و ارتباطات و امنیت سایبری	پژوهشگاه نیرو

بازنگری مدرک

مسئولیت	نام و نام خانوادگی	عنوان	شرکت
راهبری	دولت جمشیدی	رئیس کارگروه خدمات تخصصی امنیت سایبری	پژوهشگاه نیرو
برنامه‌ریزی و هماهنگی	مریم شبرو	معاون مرکز فناوری اطلاعات و ارتباطات و امنیت سایبری	پژوهشگاه نیرو
همکار مشارکت‌کننده	امیرعباس گل‌گذار	رئیس گروه زیرساخت، شبکه و امنیت اطلاعات دفتر فناوری اطلاعات و امنیت فضای مجازی	وزارت نیرو
همکار مشارکت‌کننده	مریم عامری	کارشناس دفتر مدیریت بحران و پدافند غیرعامل	وزارت نیرو
همکار مشارکت‌کننده	تینا تعویذی	مشاور مرکز نوآوری و توسعه فناوری اطلاعات، ارتباطات و امنیت سایبری	پژوهشگاه نیرو

تایید و تصویب مدرک

مسئولیت	نام و نام خانوادگی	عنوان	شرکت
راهبری	آزرم دهستانی منفرد	مدیر کل دفتر فناوری اطلاعات و امنیت فضای مجازی	وزارت نیرو
راهبری	سیف‌الله آقابیگی	مدیر کل دفتر مدیریت بحران و پدافند غیرعامل	وزارت نیرو
همکار مشارکت‌کننده	حسن مهربانی	معاون فناوری اطلاعات حراست	وزارت نیرو
همکار مشارکت‌کننده	امیرعباس گل‌گذار	رئیس گروه زیرساخت، شبکه و امنیت اطلاعات دفتر فناوری اطلاعات و امنیت فضای مجازی	وزارت نیرو
همکار مشارکت‌کننده	مرتضی بیگلری	رئیس گروه پدافند غیرعامل دفتر مدیریت بحران و پدافند غیرعامل	وزارت نیرو
همکار مشارکت‌کننده	مریم عامری	کارشناس دفتر مدیریت بحران و پدافند غیرعامل	وزارت نیرو
همکار مشارکت‌کننده	حبیب قراگوزلو	مشاور مدیرعامل و نماینده کارگروه امنیت انتقال	شرکت مادر تخصصی توانیر
همکار مشارکت‌کننده	حامد احمدی	مدیر کل دفتر هوشمندسازی و فناوری‌های نوین توزیع و نماینده کارگروه امنیت توزیع	شرکت مادر تخصصی توانیر
همکار مشارکت‌کننده	حمید مرادی غیاث‌آبادی	سرپرست معاونت مخابرات و نماینده کارگروه امنیت اسکادا انتقال و مخابرات – شرکت مدیریت شبکه برق ایران	شرکت مدیریت شبکه برق ایران
همکار مشارکت‌کننده	محمد اسدنژاد	معاون مدیرکل دفتر فنی تولید	شرکت مادرتخصصی تولید نیروی برق حرارتی
همکار مشارکت‌کننده	مصطفی محمدی	رئیس گروه انرژی و سامانه‌های کنترل	شرکت مهندسی آب و فاضلاب کشور
همکار مشارکت‌کننده	فربد استیری	مشاور مدیرعامل	شرکت مدیریت منابع آب ایران
همکار مشارکت‌کننده	حسین تاج‌بخش	مدیر گروه پدافند غیرعامل	شرکت مدیریت منابع آب ایران
همکار مشارکت‌کننده	وحید کریمی‌فر	مدیر امور نگهداری، تعمیرات و بهره‌برداری در معاونت بهره‌برداری	شرکت توسعه منابع آب و نیروی ایران
همکار مشارکت‌کننده	محمد جنتی‌پور	رئیس گروه امنیت سایبری	شرکت آب و برق خوزستان
همکار مشارکت‌کننده	محسن کشاورز	مدیر کل دفتر توسعه مدیریت و فناوری اطلاعات	سازمان انرژی‌های تجدیدپذیر و بهره‌وری انرژی برق (ساتبا)
همکار مشارکت‌کننده	دولت جمشیدی	رئیس مرکز نوآوری و توسعه فناوری اطلاعات و ارتباطات و امنیت سایبری	پژوهشگاه نیرو

جمهوری اسلامی ایران
وزارت نیرو
کارگروه تخصصی
امنیت سایبری