جمهوری اسلامی ایران
وزارت نیرو

نظام‌نامه

امنیت سایبری وزارت نیرو

معاونت تحقیقات و منابع انسانی

دفتر فناوری اطلاعات و آمار

پاییز ۹۹

جمهوری اسلامی ایران
وزارت نیرو

فناوری اطلاعات و آمار

نظام نامه امنیت سایبری وزارت نیرو

مقام تصویب کننده : وزیر نیرو

دریافت کنندگان سند جهت اجرا:

-کلیه معاونت‌ها و دفاتر مستقل حوزه ستادی وزارت نیرو---------- □

-کلیه شرکت‌های مادرتخصصی و زیرمجموعه ---------- □

- ساتبا، کلیه موسسات و مراکز آموزشی و پژوهشی وابسته وزارت نیرو---------- □

-دفتر فناوری اطلاعات و آمار---------- □

- دفتر توسعه مدیریت و تحول اداری---------- □

اسناد مرتبط:

- طرح امن‌سازی زیرساخت‌های حیاتی در قبال حملات سایبری ابلاغ شده توسط مرکز مدیریت راهبردی افتای ریاست جمهوری در سال ۱۳۹۷
- مستند Essential Body of Knowledge (EBK) مرتبط با امنیت سایبری از وزارت انرژی (DOE) ایالات متحده ۲۰۱۳
- سری استانداردهای امنیت سامانه‌های کنترل صنعتی ISA/IEC ۶۲۴۴۳
- سری استانداردهای مدیریت امنیت اطلاعات ISO/IEC ۲۷۰۰۰
- صورتجلسه بررسی و تعیین ساختار امنیت سایبری وزارت نیرو به شماره ۹۹/۲۶۶۰۹/۵۵۰ د مورخ ۹۹/۰۵/۰۶

فهرست

عنوان **صفحه**

مقدمه

با توجه به اهمیت نقش و جایگاه امنیت سایبری برای مقابله با تهدیدات و حملات مختلف پیش‌روی سامانه‌های مورد استفاده در وزارت نیرو و مسئولیت این وزارتخانه در قبال مواجهه با چالش‌های امنیتی، استفاده از نیروهای متخصص در این حوزه و ارائه ساختار امنیتی بهینه و کارآمد در این زمینه ضروری است. همچنین عدم وجود نظامی هماهنگ و یکپارچه در برنامه‌ریزی و اجرای اقدامات امنیتی، به عنوان یک نقطه ضعف اساسی در حفظ امنیت تلقی شده و به همین دلیل نیاز به یک چارچوب حاکمیت امنیت سایبری مؤثر در هر سازمانی وجود دارد تا به تصمیم‌گیرندگان سازمان در فهم جامع و دقیق امنیت کمک نموده و به‌طور کامل و شفاف، همراه با کاهش ناهماهنگی در وظایف و نقش‌ها و تفکیک آنها به مدیریت و اجرای کامل امنیت در سطح کلیه واحدهای وزارت نیرو (حوزه ستادی، فناوری اطلاعات و ارتباطات و صنعتی زیرمجموعه) منتج گردد.

۱- اهداف

نظام‌نامه امنیت سایبری در حوزه‌های فناوری اطلاعات، ارتباطات و سامانه‌های صنعتی وزارت نیرو به تبیین شرح وظایف و مسئولیت‌ها برای نقش‌های تعریف‌شده می‌پردازد. این مستند جهت آشنایی و تعیین نحوه عملکرد مسئولان و کارشناسان وزارت نیرو، شرکت‌های مادرتخصصی، شرکت‌های زیرمجموعه و مراکز و مؤسسات آموزشی و پژوهشی وابسته به وزارت نیرو با نظام مدیریت امنیت سایبری وزارت نیرو در هر دو حوزه «فناوری اطلاعات و ارتباطات» و «سامانه‌های صنعتی» مطابق با استانداردهای بین‌المللی تدوین شده است.

۲- محدوده اجرا

محدوده اجرای این نظام‌نامه حوزه ستادی وزارت نیرو، شرکت‌های مادرتخصصی، شرکت‌های زیرمجموعه و مراکز و مؤسسه‌های آموزشی و پژوهشی وابسته به وزارت نیرو بوده و شامل کلیه زیرساخت‌های صنعتی و فناوری اطلاعات و ارتباطات می‌باشد.

۳- مسئولیت‌ها

الف- مسئولیت اجرای این نظام‌نامه در حوزه ستادی وزارت نیرو و نظارت عالیه بر اجرای آن در زیر مجموعه، بر عهده دفتر فناوری اطلاعات و آمار وزارت نیرو، در شرکت‌های مادرتخصصی و زیرمجموعه بر عهده مدیران‌عامل مربوطه و ساتبا، مراکز و مؤسسات آموزشی و پژوهشی وابسته به وزارت نیرو بر عهده رئیس سازمان/ مرکز/ مؤسسه است.

ب- مسئولیت نظارت بر حسن اجرای موارد مرتبط با تامین امنیت اطلاعات، در کلیه شرکت‌ها بر عهده واحدهای حراست و امور محرمانه (حفاظت فناوری اطلاعات) و نظارت عالیه بر عهده مرکز حراست وزارت نیرو می‌باشد.

ج- مسئولیت اجرای رزمایش‌های سایبری مطابق اسناد بالادستی برعهده دفتر مدیریت بحران و پدافند غیرعامل شرکت‌ها و نظارت عالیه بر عهده دفتر مدیریت بحران و پدافند غیرعامل وزارت نیرو می‌باشد.

٤- اصول و ساختار

٤-١- تعاریف

٤-١-١- امنیت سایبری

امنیت سایبری به معنای حفاظت از انواع دارایی‌های اطلاعاتی نرم‌افزارها، سخت افزارهای مربوط به فناوری اطلاعات و ارتباطات و سامانه‌های صنعتی (آب و برق)، شبکه‌های ارتباطی و غیره، در برابر افشا، تغییر و دستکاری، از بین رفتن و یا از دسترس خارج شدن عمدی یا غیر عمدی است.

٤-١-٢- سازمان

منظور از سازمان، کلیه واحدهای تابعه وزارت نیرو، اعم از حوزه ستادی، شرکت‌های مادرتخصصی، شرکت‌های زیرمجموعه (وابسته و مستقل) و مراکز و مؤسسات مرتبط است.

٤-١-٣- محدوده

محدوده امنیت سایبری در این نظام‌نامه شامل تمام حوزه‌های سه‌گانه وزارت نیرو و کلیه زیرساخت‌ها و سامانه‌های صنعتی و فناوری اطلاعات و ارتباطات آن‌ها می‌باشد.

٤-١-٤- مدل بلوغ امنیت سایبری

مدل بلوغ امنیت سایبری، مدلی منطبق با "طرح امن سازی زیرساخت‌های حیاتی در قبال حملات سایبری" است که توسط مرکز مدیریت راهبردی افتای ریاست جمهوری در سال ۱۳۹۷ تدوین و ابلاغ گردیده است و متناسب با نیاز مجموعه از سایر مدل‌های بلوغ به عنوان مکمل استفاده خواهد شد.

۲-٤- اصول

اصول حاکم بر امنیت سایبری به شرح زیر است:

۱-۲-٤- محرمانگی: جلوگیری از دسترسی غیرمجاز به اطلاعات

دسترسی به محتوای اطلاعات بطوریکه، در سه حالت استراحت، انتقال و پردازش اطلاعات، بجز توسط افراد، موجودیت‌ها و فرآیندهای مجاز، امکان‌پذیر نباشد.

۲-۲-٤- یکپارچگی یا صحت: جلوگیری از دستکاری و اصلاحات غیرمجاز و تغییر در محتوای اطلاعات، اجرای فعالیت‌ها و سرویس‌ها

یکپارچگی اطلاعات و سرویس‌های موجود باید هم درون هر یک از شرکت‌ها و سازمان‌های وزارت نیرو و هم ما بین آن‌ها برقرار باشد تا از افزونگی داده، چندگانگی اطلاعات مبهم و غیرشفاف جلوگیری شود و شرایط، جهت تبادل آنلاین اطلاعات بین سطوح مختلف فراهم گردد.

۳-۲-٤- دسترس‌پذیری: دسترسی به داده‌ها و سرویس‌ها توسط افراد مجاز در زمان و مکان مجاز

اصل دسترس‌پذیری، ویژگی در دسترس و قابل استفاده بودن داده، سرویس و سامانه در هنگام درخواست توسط یک موجودیت مجاز در مکان و زمان مجاز است. سامانه در دسترس یعنی هر زمان که کاربر خدمتی را درخواست کند، سامانه آن خدمت را ارائه دهد.

٤-۲-٤- انکارناپذیری یا پذیرش مسئولیت: جلوگیری از انکار فعالیتی که رخ داده و ادعای به وقوع پیوستن آنچه رخ نداده است

انکارناپذیری یا پذیرش مسئولیت، قابلیتی است برای اثبات اینکه فعالیت یا رخدادی به وقوع پیوسته است، به طوری که این رخداد یا فعالیت نتواند در آینده انکار شود. انکارناپذیری در واقع یک خدمت امنیتی است که عدم انکار نادرست فعالیت‌ها در یک ارتباط را حفاظت می‌کند.

۵-۲-٤- مدیریت مخاطره: درک جامع از وضعیت امنیت سایبری در سازمان بر مبنای مخاطرات موجود و تهدیدات متصور و اتخاذ تصمیم‌های امنیت سایبری مبتنی بر نتایج ارزیابی مخاطره

فرآیندی است که در آن مخاطره، شناسایی، تحلیل و ارزیابی‌شده و گام‌های کاهش مخاطره تا رسیدن به سطح قابل قبول برداشته می‌شود. مدیریت مخاطره باید مبتنی بر درک جامعی از وضعیت امنیت سایبری ساختار و منابع سازمان باشد. به‌عبارت‌دیگر، امنیت سایبری با روش‌های مدیریت مخاطره فراگیر ترکیب شود. رویکرد مدیریت مخاطره باید به‌عنوان فرآیندی برای تعادل بین اقدامات و هزینه‌های اقتصادی جهت محافظت از اطلاعات و سامانه‌ها پیاده‌سازی و بکار گرفته شود.

٦-۲-٤- ارزیابی و بهبود مستمر: بهبود مستمر در سیستم و فرآیندهای امنیت سایبری سازمان بر اساس ارزیابی‌های دوره‌ای

به منظور برقراری راهبرد امنیتی مقاوم لازم است که چرخه بهبود مستمر (طراحی، اجرا، بررسی و اقدام) امنیت مرتب تکرار شود. به این منظور باید فعالیت‌های مرتبط با امنیت سایبری در وزارت نیرو در کلیه سطوح قابل اندازه‌گیری، پایش و سنجش بوده و نتایج حاصل از ارزیابی در جهت بهبود وضعیت، مورد تحلیل قرار گیرد و به واحدهای مرتبط، جهت اقدامات اصلاحی بازخورد گردد. همچنین می‌بایست آموزش‌های امنیتی در سه سطح فرهنگ‌سازی و آگاهی بخشی، آموزش و کسب مهارت درنظر گرفته شود.

۳-٤- سطوح نظام امنیت سایبری

از آنجایی‌که نظام امنیت فضای سایبری، باید به‌گونه‌ای طراحی گردد که سه فعالیت سیاست‌گذاری، نظارت و استقرار امنیت را پوشش دهد، لذا این نظام در سه سطح حاکمیت، مدیریت و اجرا در نظر گرفته شده است.

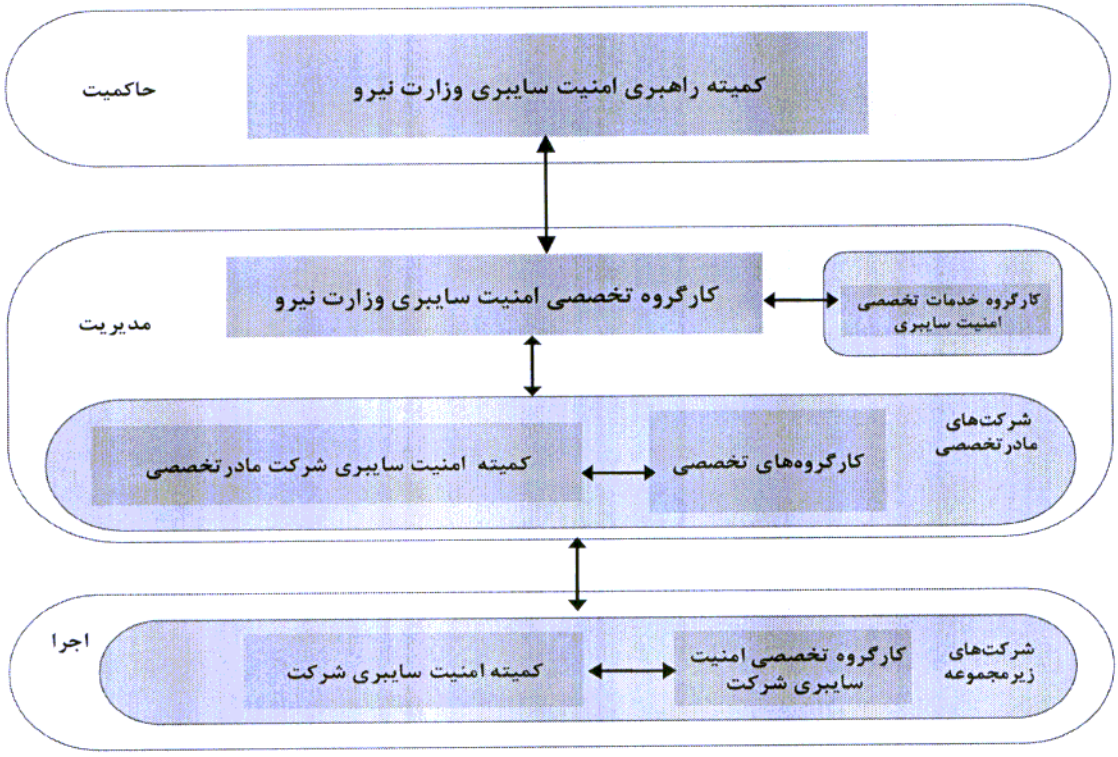
الف) حاکمیت: در این سطح، اهداف، سیاست‌ها و جهت‌گیری‌های کلان، مقررات نظام، اولویت‌ها و استراتژی‌های امنیتی تعیین گردیده و بر اجرای آن‌ها نظارت می‌گردد. مهم‌ترین کارکردهای سطح حاکمیت، سیاست‌گذاری و جهت‌دهی است.

ب) مدیریت: در این سطح به‌منظور تبدیل اهداف، سیاست‌ها و جهت‌گیری‌های کلان، اولویت‌ها و استراتژی‌های کلان امنیتی به اولویت‌ها و استراتژی‌های خرد، سازوکارها، استانداردها، رویه‌ها و چارچوب‌های مرتبط، تدوین و تصویب می‌گردد و زمینه‌های لازم برای عملیاتی شدن نظام امنیت سایبری در سطح شرکت‌های زیرمجموعه فراهم می‌گردد. کارکرد سطح مدیریت شامل استانداردسازی و تسهیل‌گری است.

ج) اجرا: در این سطح بر اساس سازوکارها، استانداردها، رویه‌ها و چارچوب‌های مرتبط، اقدامات لازم به‌منظور حصول اطمینان از به‌کارگیری نیروی انسانی دارای صلاحیت حرفه‌ای، نظارت بر پیاده‌سازی و اجرای لایه‌های مختلف امنیت، پیمایش و سنجش و ارزیابی امنیت سایبری صورت می‌گیرد. مهم‌ترین کارکرد سطح اجرا شامل پیاده‌سازی، سنجش و ارزیابی است. ارزیابی امنیت سایبری با مدیریت "کمیته امنیت فضای سایبری شرکت‌های مادرتخصصی" در سطح شرکت‌های زیرمجموعه صورت می‌پذیرد.

٤-٤- ارکان نظام امنیت سایبری

ارکان نظام امنیت سایبری در سطح حاکمیت شامل کمیته راهبری امنیت سایبری وزارت نیرو، در سطح مدیریت شامل کارگروه تخصصی امنیت سایبری وزارت نیرو، کارگروه خدمات تخصصی امنیت سایبری، کمیته‌های امنیت سایبری و کارگروه‌های تخصصی آن در شرکت‌های مادرتخصصی و در سطح اجرا شامل کمیته‌های امنیت سایبری شرکت‌های زیرمجموعه و کارگروه تخصصی آن‌ها است. نحوه چیدمان و ارتباط بین این ارکان در شکل ۱ ارائه شده است.



شکل ۱- ارکان نظام امنیت سایبری وزارت نیرو

٤-٥- شرح وظایف و اعضا

اعضای ارکان نظام امنیت سایبری و شرح وظایف به شرح زیر می‌باشد.

٤-٥-١- کمیته راهبری امنیت سایبری وزارت نیرو

اعضای کمیته راهبری امنیت سایبری به شرح زیر می‌باشد:

۱. وزیر نیرو (رئیس)
۲. مدیرکل دفتر فناوری اطلاعات و آمار وزارت نیرو (دبیر)
۳. مدیران عامل شرکت‌های مادرتخصصی
۴. رئیس مرکز حراست وزارت نیرو
۵. مدیرکل دفتر مدیریت بحران و پدافند غیرعامل وزارت نیرو
۶. نمایندگان مرکز ملی فضای مجازی، مرکز مدیریت راهبردی افتای ریاست جمهوری و سازمان پدافند غیرعامل کشور (عضو مدعو)

کمیته راهبری در سطح حاکمیت و سیاستگذاری عمل نموده و شرح وظایف آن به شرح زیر است:

الف – تبیین و ابلاغ خط‌مشی‌های کلان امنیت سایبری صنعت آب و برق

ب – تصویب و ابلاغ اهداف، شاخص‌ها و الزامات کلان امنیت سایبری صنعت آب و برق

پ – تصویب، ابلاغ و پایش برنامه‌های کلان راهبری و اجرایی (نقشه راه) امنیت سایبری صنعت آب و برق

ت – هدایت کلان سیستم مدیریت امنیت سایبری جهت دستیابی به اهداف امنیتی در وزارت نیرو

ث – تصویب سیاست‌های تأمین و جذب منابع و متوازن‌سازی سرمایه‌گذاری امنیت سایبری در حوزه‌های مختلف و همسوسازی با اولویت‌های امنیت سایبری

ج – تصویب استراتژی‌ها و ساختارهای لازم برای مدیریت و ترویج فرهنگ امنیت سایبری در وزارت نیرو

چ – تصویب استانداردهای موردنیاز امنیت سایبری

ح – ارائه گزارش اقدامات انجام شده در خصوص ابلاغیه‌ها و درخواست‌های گزارش‌های دوره‌ای ارگان‌های ذیربط و نهادهای امنیتی

- جلسات کمیته راهبری امنیت سایبری وزارت نیرو به‌صورت دوره‌ای حداقل سه ماهه (یا در صورت بروز موارد اضطراری به صورت فوق العاده) تشکیل می‌گردد.

۲-۵-٤- کارگروه تخصصی امنیت سایبری وزارت نیرو

اعضای کارگروه تخصصی امنیت سایبری وزارت نیرو به شرح زیر می‌باشد:

۱. مدیرکل دفتر فناوری اطلاعات و آمار وزارت نیرو (رئیس)
۲. مسئول امنیت سایبری دفتر فناوری اطلاعات و آمار (دبیر)
۳. مدیران‌کل دفاتر فناوری اطلاعات شرکت‌های مادرتخصصی
۴. معاون حفاظت فناوری اطلاعات مرکز حراست وزارت نیرو
۵. معاون دفتر مدیریت بحران و پدافند غیر عامل وزارت نیرو
۶. نماینده معاونت‌های تخصصی (آب و برق) وزارت نیرو
۷. رئیس کارگروه خدمات تخصصی امنیت سایبری
۸. روسای کارگروه‌های تخصصی شرکت‌های مادرتخصصی (مدعو)
۹. مشاور امنیت کارگروه (مدعو)

کارگروه تخصصی در حوزه راهبری اجرا عمل نموده و شرح وظایف آن به شرح زیر می‌باشد:

الف– تهیه پیش‌نویس خط‌مشی‌ها، اهداف، شاخص‌ها و الزامات کلان امنیت سایبری صنعت آب و برق

ب – تدوین پیش‌نویس اولویت‌ها و برنامه‌های اجرایی امنیت سایبری (نقشه راه)

پ – نظارت بر تدوین، پایش و به‌روزرسانی برنامه‌های راهبردی و عملیاتی امنیت سایبری در وزارت نیرو

ت - تصویب آیین‌نامه‌ها و دستورالعمل‌های کلان، عمومی یا مشترک حوزه‌های مختلف امنیت سایبری صنعت آب و برق

ث - بررسی درخواست‌ها و صدور مجوزهای دسترسی و تبادل اطلاعات بین شرکت‌های زیرمجموعه صنعت آب و برق و یا با سایر دستگاه‌ها

ج - تعیین، تصویب، ابلاغ معیار و شاخص‌های ارزیابی امنیت سایبری صنعت آب و برق و ممیزی و نظارت کلان بر اجرای آن‌ها

چ - تدوین سیاست‌های تأمین و جذب منابع و متوازن‌سازی سرمایه‌گذاری در حوزه مختلف امنیت سایبری و یکسوسازی با اولویت‌های امنیت سایبری

ح - پیشنهاد ساختار و چارت سازمانی مورد نیاز جهت دستیابی به اهداف امنیتی در وزارت نیرو و پیشنهاد نقش‌ها، مسئولیت‌ها و مهارت‌های تخصصی مورد نیاز متولیان فعالیت‌های مختلف در حوزه امنیت سایبری و هماهنگی جهت اخذ مجوزهای لازم

خ - تدوین فرآیند و تعیین چارچوب گزارش‌دهی، جمع‌آوری و تحلیل گزارشات وضعیت و حوادث امنیت سایبری شرکت‌های مادرتخصصی و تصمیم‌گیری در خصوص روش‌ها و راهکارهای بهبود امنیت

د - تصمیم‌گیری در خصوص نیازمندی‌های ساختاری، آزمایشگاهی و آموزشی کمیته‌های امنیت سایبری شرکت‌های مادرتخصصی و ارجاع آن‌ها به کارگروه خدمات تخصصی امنیت سایبری.

ذ - نظارت عالیه بر ارائه کلیه خدمات کارگروه خدمات تخصصی امنیت سایبری

ر - بررسی نامه‌های راهبردی و عملیاتی امنیت سایبری در وزارت نیرو ارائه شده توسط کمیته‌های امنیت سایبری شرکت‌های مادرتخصصی و ارائه گزارش به کمیته راهبری امنیت سایبری وزارت نیرو جهت تصویب نهایی

ز - پیگیری و تجمیع گزارشات اقدامات انجام شده وضعیت امنیت سایبری به صورت دوره‌ای و موردی جهت ارائه به کمیته راهبری وزارت نیرو و سایر نهادهای بالادستی

ژ - مدیریت کلان آموزش و فرهنگ‌سازی، پژوهش و توسعه فناوری در حوزه امنیت سایبری صنعت آب و برق

- جلسات کارگروه تخصصی امنیت سایبری وزارت نیرو حداقل به‌صورت دو هفته یک‌بار (ماهانه دو بار) یا بنا بر ضرورت تشکیل می‌گردد.
- ارتباط میان این کارگروه تخصصی در وزارت نیرو با کمیته‌های تخصصی و اجرایی و همچنین کمیته‌های امنیت سایبری شرکت‌های مادرتخصصی و بالعکس، از طریق دبیرخانه کارگروه تخصصی امنیت سایبری صورت می‌پذیرد.
- دبیرخانه کمیته راهبری امنیت سایبری و کارگروه تخصصی امنیت سایبری، دفتر فناوری اطلاعات و آمار وزارت نیرو بوده و وظایف زیر را بر عهده دارد:

الف - تعیین دستور جلسات و پیگیری برگزاری جلسات کمیته راهبری امنیت سایبری و کارگروه تخصصی امنیت سایبری وزارت نیرو

ب - پیگیری اجرای مصوبات کمیته راهبری امنیت سایبری و کارگروه تخصصی امنیت سایبری وزارت نیرو

پ - مدیریت ارجاع موارد مصوبه کمیته راهبری امنیت سایبری و کارگروه تخصصی امنیت سایبری وزارت نیرو

ت - مدیریت ارجاع مصوبات ابلاغی در سطح وزارت نیرو از طریق کمیته‌های امنیت شرکت‌های مادرتخصصی

ث- دریافت گزارش‌های دوره‌ای از کمیته‌های امنیت شرکت‌های مادرتخصصی و تحویل به کارگروه تخصصی امنیت سایبری جهت تحلیل و ارائه بازخورد در جلسات کارگروه تخصصی

ج - جمع‌آوری اولویت‌ها و برنامه‌های اجرایی امنیت سایبری (نقشه راه) ارائه شده توسط کمیته‌های شرکت مادرتخصصی و تحویل به کارگروه خدمات تخصصی امنیت سایبری جهت یکپارچه سازی و تهیه پیش‌نویس‌های ذیربط

چ - جمع‌آوری آیین‌نامه‌ها و دستورالعمل‌های کلان، عمومی یا مشترک حوزه‌های مختلف امنیت سایبری، ارائه شده توسط کمیته‌های امنیت سایبری شرکت‌های مادرتخصصی و تحویل به کارگروه خدمات تخصصی امنیت سایبری جهت یکپارچه‌سازی و تهیه پیش نویس‌های مربوطه

۳-۵-٤- کارگروه خدمات تخصصی امنیت سایبری

اعضای کارگروه خدمات تخصصی امنیت سایبری به شرح زیر می‌باشد:

۱. رئیس مرکز توسعه فناوری امنیت سایبری پژوهشگاه نیرو (رئیس)
۲. معاون مرکز توسعه فناوری امنیت سایبری پژوهشگاه نیرو (دبیر)
۳. نماینده کارگروه تخصصی امنیت سایبری وزارت نیرو
۴. مدیر طرح دستیابی به دانش فنی فناوری‌های امنیتی صنعت برق
۵. مدیر طرح توسعه زیرساخت‌های ارزیابی امنیت سامانه‌های کنترل صنعتی
۶. مدیر طرح توسعه زیرساخت‌های امنیت سامانه‌های کنترل صنعتی
۷. مدیر طرح توسعه پژوهش، آموزش و فرهنگ‌سازی امنیت سایبری
۸. مدیر طرح تدوین الزامات و دستورالعمل‌های امنیت سایبری
۹. نمایندگان کارگروه‌های تخصصی شرکت‌های مادرتخصصی (مدعو)
۱۰. مسئول حفاظت فناوری اطلاعات پژوهشگاه نیرو

شرح وظایف کارگروه خدمات تخصصی امنیت سایبری به شرح ذیل می‌باشد:

الف - یکپارچه‌سازی و تهیه پیش‌نویس اولویت‌ها و برنامه‌های اجرایی امنیت سایبری صنعت آب و برق (نقشه‌راه) و ارسال آن به کارگروه تخصصی امنیت سایبری وزارت نیرو

ب - تهیه پیش‌نویس آیین‌نامه‌ها و دستورالعمل‌های کلان، عمومی یا مشترک حوزه‌های مختلف امنیت سایبری، ارائه شده توسط کمیته‌های امنیت سایبری شرکت‌های مادرتخصصی و تحویل به کارگروه تخصصی امنیت سایبری جهت تصویب

پ - بررسی گزارش‌های دوره‌ای "کمیته‌های امنیت سایبری شرکت‌های مادرتخصصی"و ارائه گزارش تحلیلی به کارگروه تخصصی امنیت سایبری وزارت نیرو جهت تصمیم‌گیری در خصوص روش‌ها و راهکارهای بهبود

ت - ارائه خدمات پژوهشی و فناوری در حوزه‌های مختلف امنیت سایبری بر مبنای اسناد بالادستی، استانداردها، به‌روش‌ها، دستورالعمل‌ها و سوابق و تجربیات موجود در داخل و خارج از کشور بر حسب نیاز کارگروه تخصصی امنیت سایبری وزارت نیرو

ث - شناسایی و تدوین استانداردها، دستورالعمل‌ها و پروتکل‌های موردنیاز با هماهنگی کارگروه تخصصی امنیت سایبری وزارت نیرو

ج - تهیه شاخص‌ها و معیارهای نظارتی و ارزیابی در اندازه‌گیری ورودی‌ها، فرآیندها و یا پیامدها بر اساس وظایف کارگروه‌های مختلف امنیت و ارائه آن به کارگروه تخصصی امنیت سایبری وزارت نیرو

چ - ارائه خدمات تخصصی ارزیابی امنیتی شرکت‌ها از منظر ارتقای امنیت سایبری و سطح بلوغ امنیتی و تدوین شیوه‌نامه اجرای ارزیابی و نحوه‌ی ارائه گزارش‌های تحلیلی و مدیریتی به تشخیص کارگروه تخصصی امنیت سایبری وزارت نیرو

ح - تهیه گزارش‌های انحراف از اجرای برنامه‌ها و الزامات امنیت سایبری و ارائه به کارگروه تخصصی امنیت سایبری وزارت نیرو

خ - ارائه خدمات تخصصی - مدیریتی جهت تجهیز و راه‌اندازی زیرساخت‌های امنیت سایبری مورد نیاز صنعت آب و برق

د - ارائه خدمات تخصصی تجهیز و راه‌اندازی آزمایشگاه‌های ارزیابی امنیتی و پایلوت‌های آزمایشگاهی جهت اجرای مانور سایبری و ارائه خدمات مورد نیاز صنعت آب و برق به تشخیص کارگروه تخصصی امنیت سایبری وزارت نیرو

ذ - ارائه خدمات تخصصی توسعه فناوری‌های موردنیاز جهت ارتقای امنیت سایبری در وزارت نیرو و شرکت‌های زیرمجموعه به تشخیص کارگروه تخصصی امنیت سایبری وزارت نیرو

ر - ارائه خدمات تخصصی آموزشی و فرهنگ‌سازی امنیت سایبری به تشخیص کارگروه تخصصی امنیت سایبری وزارت نیرو

ز - ایجاد پایگاه‌های دانش مورد نیاز و شبکه‌های متخصصین امنیت سایبری در حوزه‌های تخصصی وزارت نیرو

- جلسات کارگروه خدمات تخصصی امنیت سایبری به‌صورت حداقل دو هفته یک‌بار (ماهانه دو بار) یا بنا بر ضرورت تشکیل می‌گردد.

٤-٥-٤- کمیته امنیت سایبری شرکت‌های مادرتخصصی

اعضای کمیته امنیت سایبری شرکت‌های مادرتخصصی به شرح زیر می‌باشند:

۱. مدیرعامل شرکت مادرتخصصی (رئیس کمیته)
۲. مدیرکل دفتر فناوری اطلاعات شرکت مادرتخصصی (دبیر)
۳. معاونت تخصصی ذیربط
۴. رؤسای کارگروه‌های تخصصی
۵. مدیرکل حراست شرکت مادرتخصصی
۶. مدیرکل دفتر مدیریت بحران و پدافند غیر عامل شرکت مادرتخصصی
۷. نمایندگان وزارت نیرو (حراست، پدافند و معاونت تخصصی)
۸. مشاور امنیت حوزه تخصصی شرکت مادرتخصصی
۹. رئیس کارگروه خدمات تخصصی امنیت سایبری (مدعو)

کمیته امنیت سایبری شرکت‌های مادرتخصصی در سطح مدیریت اجرا و هماهنگی و نظارت بوده و شرح وظایف آن به شرح زیر می‌باشد:

الف - تبیین خط‌مشی‌های کلان امنیت سایبری در حوزه تخصصی شرکت/ سازمان بر اساس سیاست‌های ابلاغی کمیته راهبری امنیت سایبری وزارت نیرو

ب - تصویب و ابلاغ خط مشی‌های سازمان و شرکت‌های زیرمجموعه در حوزه‌های مدل بلوغ امنیت سایبری

پ - تصویب و ابلاغ خط‌مشی‌ها، برنامه‌ها، فرآیندها و دستورالعمل‌های اجرایی در حوزه‌های مختلف مدل بلوغ امنیت سایبری

ت - بررسی طرح و برنامه، تامین منابع و تخصیص بودجه و نظارت بر اجرای فعالیت‌های کارگروه‌های تخصصی و شرکت‌های زیرمجموعه در حوزه‌های مختلف بلوغ امنیت سایبری

ث - پایش و برنامه‌ریزی جهت بهبود مستمر در حوزه‌های مختلف مدل بلوغ امنیت سایبری

ج - پیشنهاد سیاست‌های کلان امنیت فضای تولید و تبادل اطلاعات در حوزه‌کاری شرکت مادرتخصصی به وزارت نیرو

چ - ارائه برنامه راهبردی به کمیته راهبری امنیت سایبری وزارت نیرو

ح - تجمیع، بررسی و تصویب برنامه عملیاتی سالانه جهت شرکت‌های زیرمجموعه

خ - اتخاذ تدابیر برای استفاده از منابع مشترک (مانند زیرساخت‌های ارتباطی، مراکز داده و ...) در راستای ارتقای امنیت سایبری صنعت آب و برق

د - ایجاد هم‌افزایی و هماهنگی با کلیه عوامل درونی و بیرونی صنعت آب و برق

ذ - حفظ یکپارچگی طرح‌ها و برنامه‌های کلیه حوزه‌های تخصصی در راستای ارتقای امنیت

ر - برنامه‌ریزی کلان و حمایت برای آموزش و فرهنگ‌سازی، پژوهش و توسعه فناوری در حوزه امنیت سایبری حوزه تخصصی شرکت/ سازمان

ز - دریافت تحلیل گزارشات وضعیت و حوادث امنیت سایبری کارگروه‌های تخصصی و شرکت‌های زیرمجموعه و تصمیم‌گیری در خصوص روش‌ها و راهکارهای بهبود ارایه شده

ژ - تعیین ساختار و چارت سازمانی مورد نیاز جهت دستیابی به اهداف امنیتی در حوزه تخصصی شرکت/ سازمان و تعیین نقش‌ها، مسئولیت‌ها و مهارت‌های تخصصی مورد نیاز متولیان فعالیت‌های مختلف در حوزه امنیت سایبری

س - تدوین گزارش‌های دوره‌ای و موردی در خصوص وضعیت و حوادث امنیت سایبری جهت ارائه به کمیته راهبری وزارت نیرو و پاسخگویی به نهادهای بالادستی مرتبط با حوزه کاری امنیت سایبری

- جلسات کمیته امنیت سایبری شرکت‌های مادرتخصصی باید به‌صورت دوره‌ای حداقل دوماهه (یا در صورت بروز موارد اضطراری) تشکیل گردد و صورتجلسات برای دبیر کمیته راهبری امنیت سایبری (مدیرکل دفتر فناوری اطلاعات و آمار) وزارت نیرو ارسال گردد.

ارتباط میان این کمیته با کارگروه تخصصی امنیت سایبری وزارت نیرو و کارگروه‌های تخصصی شرکت مادرتخصصی از طریق دبیرخانه کمیته امنیت سایبری شرکت مادرتخصصی صورت می‌پذیرد. دبیرخانه کمیته امنیت سایبری شرکت‌های مادرتخصصی در دفتر فناوری اطلاعات آن شرکت/ سازمان بوده و وظایف زیر را بر عهده دارد:

الف - تعیین دستور جلسات و پیگیری برگزاری جلسات کمیته امنیت سایبری

ب - پیگیری اجرای مصوبات کمیته امنیت سایبری

پ - مدیریت ارجاع موارد مصوبات کارگروه‌های تخصصی امنیت سایبری شرکت‌های مادرتخصصی

ت - جمع‌آوری گزارش‌های وضعیت و حوادث امنیت سایبری از کارگروه‌های تخصصی و کمیته‌های امنیت شرکت‌های زیرمجموعه بصورت دوره‌ای و موردی

ث - جمع‌آوری برنامه‌ها و طرح‌های امنیت سایبری تهیه شده در کارگروه‌های تخصصی شرکت‌های مادرتخصصی جهت تصمیم‌گیری در کمیته امنیت سایبری

ج - جمع‌آوری گزارش پیشرفت پروژه‌ها و طرح‌های امنیت سایبری تهیه شده در کارگروه‌های تخصصی جهت جمع‌بندی و تصمیم‌گیری در کمیته امنیت سایبری

چ - ایجاد هماهنگی بین کارگروه‌های تخصصی

تبصره: حضور مدیر دفتر حراست و امور محرمانه به همراه معاون حفاظت فناوری اطلاعات شرکت/ سازمان در جلسات کمیته امنیت سایبری شرکت/ سازمان الزامی است.

۵-۵-٤- کارگروه‌های تخصصی امنیت سایبری شرکت‌های مادرتخصصی

اعضای کارگروه‌های تخصصی امنیت سایبری شرکت‌های مادرتخصصی به شرح زیر می‌باشد:

۱. بالاترین مقام شرکت در زمینه تخصصی کارگروه (رئیس)
۲. مسئول امنیت در زمینه تخصصی کارگروه (دبیر)
۳. سه الی هفت نماینده تخصصی منتخب از شرکت‌های زیرمجموعه
۴. معاون / مسئول حفاظت فناوری اطلاعات دفتر حراست شرکت مادرتخصصی (مدعو)
۵. نماینده واحد بحران و پدافند غیرعامل شرکت مادرتخصصی (مدعو)
۶. مشاور امنیت حوزه تخصصی کارگروه (مدعو)

کارگروه‌های تخصصی امنیت شرکت‌های مادرتخصصی در سطح اجرا بوده و شرح وظایف آن به شرح زیر می‌باشد:

الف - تدوین خط‌مشی‌های سازمان و شرکت‌های زیرمجموعه در حوزه های مدل بلوغ امنیت سایبری

ب - تدوین و اولویت‌بندی برنامه‌ها، فرآیندها و دستورالعمل‌های اجرایی در حوزه‌های مختلف مدل بلوغ امنیت سایبری با همکاری شرکت‌های زیرمجموعه

پ - تعیین و اولویت بندی منابع و بودجه مورد نیاز برای اجرای فعالیت‌ها در حوزه‌های مختلف مدل بلوغ امنیت سایبری

ت - شناسایی نیازمندی‌های حوزه‌های مختلف مدل بلوغ امنیت سایبری و مستندسازی و ارائه گزارش به کمیته امنیت سایبری شرکت مادرتخصصی

ث - بررسی، جمع‌بندی و تأیید اولیه طرح‌ها و برنامه‌های شرکت‌ها و ارائه به کمیته برای تأیید نهایی و پایش مستمر اجرای آن‌ها

ج - تدوین برنامه عملیاتی سالانه و ارائه به کمیته امنیت سایبری شرکت مادرتخصصی

چ - ارزیابی و ممیزی شرکت‌های زیرمجموعه بر اساس مصوبات و خط‌مشی‌های کمیته راهبری امنیت سایبری وزارت نیرو و کمیته امنیت سایبری شرکت مادرتخصصی در تمامی حوزه‌های مدل بلوغ امنیت سایبری

ح - نظارت بر تجهیز و راه‌اندازی زیرساخت‌های مورد نیاز حوزه تخصصی کارگروه بر اساس مصوبات کمیته امنیت سایبری شرکت مادرتخصصی

خ - تدوین برنامه‌های آموزشی، آگاهی‌رسانی و فرهنگ‌سازی در تمامی حوزه‌های مدل بلوغ امنیت سایبری

د - ایجاد سازوکارهای لازم برای اجرای برنامه‌های مدل بلوغ امنیت سایبری

ذ - ارائه آمار، اطلاعات و گزارش‌های دوره‌ای و موردی از عملکرد و اقدامات به کمیته امنیت سایبری شرکت مادرتخصصی

ر - اتخاذ تدابیر لازم جهت اقدامات ضربتی مورد نیاز در چارچوب وظایف محوله و منطبق با سیاست‌های ابلاغی وزارت نیرو

- جلسات کارگروه‌های تخصصی امنیت شرکت‌های مادرتخصصی باید به‌صورت دوره‌ای حداقل ماهانه (یا در صورت بروز موارد اضطراری) تشکیل گردد و صورتجلسات برای دبیر کمیته امنیت سایبری شرکت مادرتخصصی ارسال گردد.

٦-٥-٤-کمیته امنیت سایبری شرکت‌های زیرمجموعه

اعضای کمیته امنیت سایبری شرکت‌ها به شرح زیر می‌باشد:

۱. مدیرعامل (رئیس)
۲. مدیر دفتر فناوری اطلاعات (دبیر)
۳. کلیه معاونین حوزه‌های تخصصی شرکت
۴. مدیر دفتر حراست و امور محرمانه شرکت
۵. مسئول مدیریت بحران و پدافند غیرعامل شرکت

کمیته امنیت سایبری شرکت‌های زیرمجموعه در سطح اجرا بوده و شرح وظایف آن به شرح زیر می‌باشد:

الف - تصویب و ابلاغ خط مشی‌های شرکت در حوزه‌های مدل بلوغ امنیت سایبری براساس اهداف و برنامه‌های کمیته امنیت سایبری شرکت مادرتخصصی

ب - تصویب و ابلاغ برنامه ها، فرآیندها و دستورالعمل‌های اجرایی شرکت در حوزه‌های مختلف مدل بلوغ امنیت سایبری

پ - پیشنهاد پیش‌نویس سیاست‌ها، دستورالعمل‌ها، پیوست‌های امنیتی به شرکت مادرتخصصی

ت - تعیین ساختار و چارت سازمانی مورد نیاز جهت دستیابی به اهداف امنیتی در حوزه تخصصی شرکت و تعیین نقش‌ها، مسئولیت‌ها و مهارت‌های تخصصی مورد نیاز متولیان فعالیت‌های مختلف در حوزه امنیت سایبری

ث- ارائه آمار، اطلاعات و گزارش‌های دوره‌ای و موردی از عملکرد و اقدامات به شرکت مادرتخصصی

ج- تصویب برنامه عملیاتی سالانه و ارائه به کمیته امنیت سایبری شرکت مادرتخصصی

چ - مدیریت ریسک و ارزیابی وضعیت زیر ساخت کلیه سامانه‌ها بویژه صنعتی، محاسبه مخاطرات ناشی از نقض‌های امنیتی و ارائه طرح براساس تحلیل هزینه-فایده جهت ارتقای امنیت.

ح- اتخاذ تدابیر لازم جهت ترویج فرهنگ امنیت فضای سایبری و ارتقای سطح آموزش، آگاه‌سازی و دانش افزایی مدیران، صاحبان مشاغل حساس و کارکنان شرکت در خصوص تهدیدات سایبری.

خ- نظارت و پایش بر حسن اجرا و پیاده‌سازی کلیه دستورالعمل‌ها و ضوابط و الزامات حفاظتی و همسوسازی برنامه‌های عملیاتی و اولویت‌ها با شاخص‌ها و معیارهای ابلاغی از سوی بالادست.

د-نظارت برعملکرد کارگروه ذیل کمیته امنیت شرکت و صدور احکام مربوطه.

- جلسات کمیته امنیت سایبری شرکت‌ها باید به‌صورت دوره‌ای حداقل دوماهه (یا در صورت بروز موارد اضطراری) تشکیل گردد و صورتجلسات برای دبیر کمیته امنیت سایبری شرکت مادرتخصصی ارسال گردد.

تبصره: شرکت‌های مادرتخصصی بدون زیرمجموعه، مراکز و موسسه‌های آموزشی و پژوهشی وابسته و ساتبا بصورت مستقیم با کارگروه تخصصی امنیت سایبری وزارت نیرو مرتبط بوده و صورتجلسات خود را برای دبیر کارگروه ارسال نمایند.

ارتباط میان این کمیته با کمیته امنیت سایبری شرکت مادرتخصصی و کارگروه تخصصی شرکت از طریق دبیرخانه کمیته امنیت سایبری شرکت صورت می‌پذیرد. دبیرخانه کمیته امنیت سایبری در دفتر فناوری اطلاعات آن شرکت بوده و وظایف زیر را بر عهده دارد:

الف – تعیین دستور جلسات و پیگیری برگزاری جلسات کمیته امنیت سایبری شرکت‌های مادرتخصصی

ب – پیگیری اجرای مصوبات کمیته امنیت سایبری شرکت‌های مادرتخصصی

پ – جمع‌آوری گزارشات وضعیت و حوادث امنیت سایبری از کارگروه تخصصی بصورت دوره‌ای و موردی

ت – جمع‌آوری برنامه‌ها و طرح‌های امنیت سایبری تهیه شده در شرکت جهت تصمیم‌گیری در کمیته

ث – جمع‌آوری گزارش پیشرفت پروژه‌ها و طرح‌های امنیت سایبری شرکت جهت جمع‌بندی و تصمیم‌گیری در کمیته

تبصره: حضور مدیر دفتر حراست و امور محرمانه شرکت به همراه مسئول حفاظت فناوری اطلاعات شرکت در جلسات کمیته سایبری شرکت الزامی است.

۷-۵-٤- کارگروه تخصصی امنیت سایبری شرکت‌ها

اعضای کارگروه تخصصی امنیت سایبری شرکت‌ها به شرح زیر می‌باشد:

۱. مدیر دفتر فناوری اطلاعات و ارتباطات (رئیس)
۲. مسئول امنیت سایبری فناوری اطلاعات و ارتباطات (دبیر)
۳. نمایندگان از تمامی حوزه‌های تخصصی و عملیاتی
۴. مسئول/ کارشناس حفاظت فناوری اطلاعات حراست
۵. مسئول مدیریت بحران وپدافند غیر عامل

کارگروه تخصصی امنیت سایبری شرکت‌ها در سطح اجرا بوده و شرح وظایف آن به شرح زیر می‌باشد:

الف - تهیه پیش‌نویس سیاست‌ها، دستورالعمل‌ها، پیوست‌های امنیتی جهت پیشنهاد به کمیته امنیت سایبری شرکت

ب - تدوین خط‌مشی‌های شرکت در حوزه های مدل بلوغ امنیت سایبری با پوشش‌دهی کامل خط مشی ابلاغی شرکت مادرتخصصی مربوطه

پ - بررسی کفایت برنامه‌ها، فرآیندها و دستورالعمل‌های ابلاغی بالادست بر اساس شرایط اختصاصی شرکت و تهیه موارد تکمیلی در صورت نیاز

ت - اولویت‌بندی و نظارت بر اجرای برنامه‌ها، فرآیندها و دستورالعمل‌های مصوب کمیته امنیت سایبری شرکت

ث - تعیین و احراز اصالت و نقش‌ها متناسب با برنامه‌ها و خط‌مشی های ابلاغ شده

ج - تدوین برنامه عملیاتی سالانه و ارائه به کمیته امنیت سایبری شرکت

چ - ارائه آمار، اطلاعات و گزارش‌های دوره‌ای و موردی از عملکرد و اقدامات به کمیته امنیت سایبری شرکت

ح - ایجاد نظام پایش، پیش‌گیری، آمادگی، مقابله و امداد رخدادهای امنیتی در شرکت و تدارک فرآیند مدیریت بحران هنگام وقوع رخدادهای امنیتی در حوزه‌های اداری و صنعتی.

خ - تدارک پیوست‌های امنیتی و بررسی طرح‌ها و پروژه‌های اجرایی شرکت جهت ارتقای ضریب امنیت در حوزه‌های امنیت فضای سایبری شرکت

د - پایش مستمر زنجیره تأمین و بررسی سخت افزارها، نرم‌افزارها و زیرساخت‌های مورد نیاز در حوزه امنیت سایبری قبل از شروع فرآیند خرید

ذ - تدوین و نظارت بر الزامات امنیتی برون‌سپاری فعالیت‌های حوزه فناوری اطلاعات و صنعتی

ر - برآورد بودجه مورد نیاز طرح‌ها و پروژه‌های امنیت در حوزه‌های اداری و صنعتی و پیشنهاد به کمیته جهت تصویب

ز - ارسال صورتجلسات کارگروه تخصصی امنیت سایبری شرکت‌ها برای دبیر کمیته امنیت سایبری آن شرکت

- جلسات کارگروه تخصصی امنیت سایبری شرکت‌ها باید به‌صورت دوره‌ای حداقل ماهانه (یا در صورت بروز موارد اضطراری) تشکیل گردد و صورتجلسات برای دبیر کمیته امنیت سایبری شرکت مادرتخصصی ارسال گردد.

تبصره: اعضاء و ساختار کمیته و کارگروه‌های تخصصی امنیت سایبری ساتکاب، ساتبا و موسسات و مراکز آموزشی و پژوهشی وابسته به تشخیص مدیرعامل/رئیس مربوطه سازماندهی می‌گردد.

۵- بازنگری

این نظام‌نامه 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، توسط دفتر فناوری اطلاعات و آمار وزارت نیرو مورد " تجدیدنظر " و "بازنگری " قرار خواهد گرفت.

٦- کنترل سند:

۱- صدور سند

سند با ضوابط آیین‌نامه تولید، بهره‌برداری و بازنگری اسناد اداری مطابقت دارد. نام و نام خانوادگی کنترل‌کننده: **مرتضی بخشایش** سمت: **مدیر کل دفتر توسعه مدیریت و تحول اداری**	مهر و امضا جمهوری اسلامی ایران وزارت نیرو معاونت تحقیقات و منابع انسانی دفتر توسعه مدیریت و تحول اداری ۹۹/۸/۱۸

۲-دریافت سند و کنترل‌های لازم

نام سازمان: ..... تاریخ دریافت سند: ..... سند از نظر شکلی (تعداد اوراق، خوانایی و ... کامل است. * سند در فرم‌های مربوطه ثبت گردید. * اسناد منسوخ و یا بی اعتبار مرتبط ابطال گردید. نام و نام خانوادگی کنترل‌کننده: .....سمت:.....	مهر و امضاء

۳- بهره برداری

نام واحد سازمانی: ..... * دریافت سند تاریخ: ..... * خاتمه دوره اجرا تاریخ : ..... نام و نام خانوادگی دریافت‌کننده: ..... سمت:	مهر و امضا

۴- ابطال سند

این سند در تاریخ : ..... به استناد: .....ابطال گردید. نام و نام خانوادگی ابطال‌کننده: ..... سمت:	مهر و امضا

۷- پدیدآورندگان (نسخه اولیه)

ردیف	شرکت	نام و نام خانوادگی
۱	وزارت نیرو	**آزرم دهستانی منفرد**- مدیر کل دفتر فناوری اطلاعات و آمار **حسین دانش آرا**- معاون مدیر کل دفتر فناوری اطلاعات و آمار **مهتاب قائمی**- کارشناس زیر ساخت، شبکه و امنیت اطلاعات **محسن کشاورز**- کارشناس امنیت صنعتی
۲	شرکت توانیر	**محمد حسن متولی زاده- مدیر عامل** **امیره نیکخواه** - مدیر کل دفتر دفتر فناوری اطلاعات، ارتباطات و آمار **محمد مهدی عابدی**- کارشناس توسعه سیستم‌های نرم افزار
۳	شرکت مهندسی آب و فاضلاب کشور	**حمیدرضا جانباز- مدیرعامل** **شهریار بهارلویی**- مدیر کل دفتر فناوری اطلاعات و توسعه دولت الکترونیک **سعید رضا رحیمیان**- رئیس گروه امنیت و شبکه
۴	شرکت مدیریت منابع آب	**قاسم نقی زاده خامسی - مدیرعامل** **سید حسن مهدوی فر** - مدیر کل دفتر فناوری اطلاعات، توسعه مدیریت و تحول اداری **سودابه حجت الاسلامی** – رئیس گروه فناوری اطلاعات **محسن افشردی**- کارشناس شبکه و بسترهای ارتباطی
۵	شرکت تولید نیروی برق حرارتی	**محسن طرز طلب- مدیر عامل** **سید محسن ابطحی نژاد** - مدیر کل دفتر فناوری اطلاعات، توسعه و زیر ساخت **غلامعلی عرب‌شاهان** – کارشناس شبکه و امنیت
۶	سازمان انرژی‌های تجدید پذیر و بهره وری انرژی برق (ساتبا)	**محمد ساتکین- معاون وزیر و رئیس سازمان** **غلامرضا کبریایی** - مدیرکل توسعه مدیریت و فناوری اطلاعات **سید محسن زمزمیان**- رئیس گروه فناوری اطلاعات
۷	شرکت مدیریت ساخت و تهیه کالا آب و برق (ساتکاب)	**محمد ولی علاء الدینی- مدیر عامل** **داود ابهت** - مشاور فن آوری و هوشمند سازی **داود منوچهری**- کارشناس سخت افزار و امنیت
۸	پژوهشگاه نیرو	**دولت جمشیدی** - سرپرست مرکز توسعه فناوری اطلاعات، ارتباطات و تجهیزات صنعت برق **صوفیا آهنج**- معاون مرکز توسعه فناوری اطلاعات، ارتباطات و تجهیزات صنعت برق **سحر راکعی**- مدیر پروژه مرکز توسعه فناوری اطلاعات، ارتباطات و تجهیزات صنعت برق
۹	وزارت نیرو	**حمید محسنی** – رئیس مرکز حراست **محمد خورشیدی**- معاون حفاظت فناوری اطلاعات IT **حسن مهربانی** – رئیس اداره امنیت شبکه‌ها
۱۰	وزارت نیرو	**میثم جعفرزاده** – مدیر کل دفتر مدیریت بحران و پدافند غیر عامل **جلال جهانبخشی** – معاون مدیر کل دفتر مدیریت بحران و پدافند غیر عامل
۱۱	مشاور دفتر فناوری اطلاعات و آمار	**محمدعلی محمدی حاجی** **علیرضا جالینوس**