وزارت ارتباطات و فناوری اطلاعات
سازمان فناوری اطلاعات ایران

مرکز مدیریت، توسعه و اعتاربخشی
نظام ملی مدیریت امنیت اطلاعات

توصیه نامه ایمن سازی ساختارها و سامانه های فناوری اطلاعات

توصیه نامه شماره ۷ :سیاست های امنیتی

نوع سند	توصیه نامه
سطح دستیابی سند	عمومی
سطح امنیتی سند	عادی
اولویت سند	خیلی فوری
تاریخ ارائه سند	تیر ۹۰
نگارش سند	۱
تعداد صفحات	۱۱
مؤلف/مؤلفین سند	سازمان فناوری اطلاعات ایران
کد سند	R90040107

هدف:

هدف از تدوین این توصیه نامه اطمینان از توجه راهبردی سازمان به امنیت فناوری اطلاعات و اهتمام مدیریت ارشد به تامین ضروریات ساختاری آن و تدوین اسناد راهبرد ی مربوط شامل سند خط مشی، سند تعیین قلمرو (حوزه) پیاده سازی و سند سیاستگذاری مدیریت امنیت اطلاعات می باشد.

ضرورت:

تامین امنیت فعالیت های پردازش اطلاعات اعم از جمع آوری ، تولید، تصحیح، پردازش، ذخیره سازی، تهیه نسخ پشتیبان، انتشار، انتقال و حذف یا معدوم کردن داده ها به عنوان یکی از وظایف اصلی سازمان ها پذیرفته شده است. این کار باید به صورت یک فعالیت ساختار یافته و منظم به اجراء گذاشته شود. بنابراین می بایست ساز و کار لازم برای آن در نظر گرفته شود. تصمیم گیری، هدف گذاری و اهتمام مدیریت ارشد سازمان به تعیین روش ها و تامین منابع، اولین قدم در این راه بوده و به دنبال آن لازم است این عزم و اهتمام به اطلاع آحاد پرسنل سازمان رسیده و رئوس گامهای چگونگی نیل به اهداف بیان شود.

اسناد راهبردی شامل سند خط مشی مدیریت امنیت اطلاعات، سند تعیین قلمرو پیاده سازی سامانه مدیریت امنیت اطلاعات و سند سیاست گذاری مدیریت امنیت اطلاعات به ترتیب مبین موارد زیر می باشند:

- اهتمام مدیریت به ایجاد ساختار مدیریتی تامین امنیت.
- حوزه جغرافیایی و عملیاتی تحت پوشش سامانه مدیریت امنیت اطلاعات.
- سیاستهای عمده ای که لازم است رعایت شوند.

الزامات:

- مسئولیت تهیه و اعلام خط مشی مدیریت امنیت اطلاعات، تعیین قلمرو (حوزه) پیاده سازی سامانه مدیریت امنیت اطلاعات، سیاستگذاری کلان و پیگیری اجرای مفاد این اسناد توسط کلیه آحاد بر عهده بالاترین مقام اجرایی سازمان می باشد.

- لازم است سند خط مشی مدیریت امنیت اطلاعات و سند تعیین قلمرو پیاده سازی سامانه مدیریت امنیت اطلاعات با توجه به نوع ، ماهیت خدمات پردازشی و حوزه ارا ئه خدمات سازمان تدوین گردد. (الگوی معرفی شده در ضمیمه همین توصیه نامه را می توان به عنوان راهنما مورد استفاده قرار داد)

- اسناد فوق باید به نحو مناسب به اطلاع کلیه آحاد سازمان، ارباب رجوع، مشتریان، طرف های اداری- تجاری و سایر گروه های ذینفع رسانده شود. اسناد موضوع این توصیه نامه در سازمان هایی که مورد مراجعه عموم هستند و یا ماهیت نظامی و امنیتی ندارند و لازم است سیاست های آن از طرف مراجعه کنندگان غیر وابسته رعایت شوند نباید دارای طبقه بندی محرمانه، سری و نظایر آن باشند.

- متن اسناد باید گویا، صریح، خلاصه، کافی و تفسیر ناپذیر باشد.

- هنگام تدوین اسناد باید به نکات زیر توجه کرد:

  - متن سند بدون استفاده از توضیحات غیر ضروری تدوین شده باشد.
  - اجرای مفاد سند عملی و امکان پذیر باشد.
  - حجم مطالب مندرج در متن سند خط مشی به نحوی باشد که بتوان آن را به سادگی در تابلو اعلانات، سایت اطلاع رسانی الکترونیک و یا پوسترهای اطلاع رسانی درج و آگهی نمود.

- در متن سند خط مشی باید به رئوس و راهبردهای اصلی در نظر گرفته شده برای پیاده سازی مدیریت امنیت اطلاعات اشاره شود.
- از آنجا که سامانه مدیریت امنیت اطلاعات در جهت استانداردسازی فعالیت های مدیریت امنیت اطلاعات پیاده سازی می شود، لازم است در متن سند خط مشی به استاندارد مرجع اشاره شود.
- لازم است مدیر ارشد در متن سند به تعهد خود به پیاده سازی سامانه مدیریت امنیت اطلاعات و اهتمام به پشتیبانی از اهداف و روش های تبیین شده در سند خط مشی از طریق ایجاد ساختارهای مناسب لازم و تأمین و تخصیص بودجه اشاره نماید.
- در متن سند باید به انجام ممیزی سامانه مدیریت امنیت اطلاعات اشاره شود.
- لازم است اسناد موضوع این توصیه نامه به امضاء بالاترین مقام اجرایی سازمان برسد.

- در سند تعیین قلمرو باید بصورت مشخص به مکان ها و خدماتی که در حوزه اجرای سیستم مدیریت امنیت اطلاعات قرار می گیرند اشاره شود. (فهرست مکان ها، خدمات، تجهیزات، نرم افزارها، بانک های اطلاعاتی و سایر دارایی ها یا منابع اطلاعاتی که باید در حوزه اجرای سامانه مدیریت امنیت اطلاعات قرار گیرند در اولین جلسه کمیته امنیت اطلاعات سازمان استخراج شده و برای تصویب به بالاترین مقام اجرایی نهاد بهره بردار پیشنهاد می شود.)

- کلیه فعالیت های مدیریت امنیت اطلاعات باید به نحوی برنامه ریزی و اجراء شود که محدوده تعیین شده در سند تعیین قلمرو را بطور کامل پوشش دهد.

– در سند سیاست‌گذاری لازم است رئوس تدابیر لازم برای حفاظت از دارایی‌های اطلاعاتی در اختیار سازمان در مقابل تمام تهدیدهای موجود، اعم از درون یا برون سازمانی و تصادفی یا عمدی، مربوط به حوزه (قلمرو) پیاده سازی معین شده باشد. این تدابیر حداقل باید موارد زیر را تامین نماید:

– از اطلاعات در برابر دسترسی‌های غیرمجاز حفاظت به عمل آید.

– محرمانگی اطلاعات رعایت گردد.

– اطلاعات به هیچ وجه نزد افراد غیرمجاز، چه به صورت ناخواسته و یا با قصد قبلی و یا در اثر کم توجهی به رعایت اصول مربوط، افشاء نگردد.

– جامعیت اطلاعات از طریق حفاظت از آن در مقابل تغییرات ناخواسته یا غیرمجاز، تضمین گردد.

– اطلاعات در زمان مورد نیاز در اختیار افراد مجاز قرار داده شود.

– کلیه قوانین کشوری (یا بین المللی پذیرفته شده در کشور) و مقررات سازمانی در زمینه تبادل و پردازش اطلاعات و یا استفاده از دارایی‌های اطلاعاتی رعایت گردد.

– طرح پیوستگی عملیات، تهیه شده و به طور دائم به هنگام‌سازی شود و در زمان‌های مناسب تحت آزمایش قرار گیرد.

– آموزش‌های لازم در زمینه حفظ امنیت اطلاعات به کلیه پرسنل شرکت داده شود.

– کلیه موارد نقض امنیت اطلاعات و یا نقاط ضعفی که ممکن است در آینده از آنها برای نقض امنیت اطلاعات سوء استفاده شود شناسایی و گزارش شده و پیگیری بعدی در مورد نحوه مقابله با آنها به مورد اجراء گذاشته شود.

- اسناد موضوع این توصیه نامه باید در فواصل زمانی مناسب (که در سند سیاستگذاری نباید بیش از سه سال باشد) مورد بازنگری قرار گیرد.

فرآیند:

مراحل تهیه سازی این توصیه نامه به شرح زیر است:

ابتدا سند خط مشی باید توسط مدیریت ارشد تهیه و تصویب شده و به اطلاع آحاد سازمان برسد. هرچند مشاوره گرفتن از منابع خارج از سازمان می تواند سودمند باشد اما متن سند خط مشی باید راساً توسط مدیریت ارشد درک و دیکته شده باشد تا از تعهد و اهتمام مدیریت به اجرای آن اطمینان حاصل شود.

در تهیه سند تعیین قلمرو باید از کمک کارشناسی افراد خبره درون سازمان استفاده شود. هدف اصلی از سند تعیین قلمرو، تعیین مرزهای پیاده سازی سامانه مدیریت امنیت اطلاعات است. این مرز باید به سهولت و به طور کامل قابل تشخیص باشد. رعایت خط مشی و سیاستگذاری مدیریت امنیت اطلاعات برای تمام دارایی های اطلاعاتی که درون مرزهای این قلمرو قرار می گیرند ضروری است.

سند سیاستگذاری مدیریت امنیت اطلاعات سند ی است که چگونگی به کارگیری رهنمودهای بیان شده سند خط مشی را در قلمرو پیاده سازی سامانه بیان می دارد. این سند به عنوان سند واسط بین سندهای سیاستگذاری اجرایی امنیت اطلاعات و سند خط مشی می باشد. باید به تفاوت بین سند سیاستگذاری مدیریت امنیت اطلاعات و سندهای سیاستگذاری اجرایی امنیت اطلاعات توجه داشت. سند سیاستگذاری اجرایی امنیت اطلاعات سندی است که روش های امن استفاده از یک یا چند دارایی اطلاعاتی خاص یا

فرآیند را بیان می کند و ممکن است به ازای یک یا چند دارایی یا فرآیند، یک سند تدوین و به اجراء گذاشته شود.

ضمیمه ۱

سند راه‌نمای (خط مشی) مدیریت امنیت اطلاعات

{**سازمان**} که ماموریت {**مأموریت اصلی سازمان**} را به عهده دارد این سند راهبردی را به عنوان خط مشی مدیریت امنیت اطلاعات خود منتشر نموده است.

این {**نهاد**} با توجه به مأموریت خود و بر اساس راهبردها و راهکارهای مندرج در قانون برنامه پنجم توسعه اقتصادی، اجتماعی و فرهنگی جمهوری اسلامی ایران و سند راهبردی نظام جامع فناوری اطلاعات کشور و سند راهبردی امنیت فضای تولید و تبادل اطلاعات کشور، بهره گیری از فناوری های برتر روز و امن سازی فعالیت های مرتبط با آن را در دستور کار خود قرار داده است.

{**سازمان**} بر این اعتقاد است که اطلاعات و کانال های ارتباطی یکی از با ارزش ترین دارایی های وی است و باید در چهارچوب قوانین و مقررات کشور جمهوری اسلامی ایران از آن محافظت بعمل آید و به این منظور استاندارد {**نام مدل استاندارد انتخابی**} را به عنوان مرجع اجرایی و مدیریتی خود برگزیده است.

مهمترین راهبردهای این {**نهاد**} در حفظ امنیت اطلاعات عبارتند از:

- ***حفاظت از محرمانگی اطلاعات برای جلوگیری از افشای غیر مجاز اطلاعات***
- ***حفظ جامعیت و صحت اطلاعات برای جلوگیری از تغییرات غیر مجاز***
- ***حفظ دسترسی پذیری اطلاعات جهت دسترسی سریع و آسان مراجع مجاز به اطلاعات در مواقع نیاز***

بنابر راهبردهای فوق {**سازمان**} خود را ملزم به انجام موارد ذیل می داند:

- ***استقرار نظام مدیریت امنیت اطلاعات و ارزیابی مستمر آن***
- ***فرهنگ سازی، اطلاع رسانی و آموزش لازم در خصوص حفاظت از امنیت اطلاعات به کاربران***
- ***تشکیل نهادهای پشتیبان نظام مدیریت امنیت اطلاعات شامل کمیته امنیت اطلاعات، نهاد متصدی حفظ امنیت اطلاعات و گروه مقابله با شرایط اضطراری و تامین نیازهای آن***
- ***تدوین طرح مقابله با بحران و تأمین ابزار و ساختار مورد نیاز جهت اجرای آن در مواقع ضروری***

{**بالاترین مقام اجرایی**} ضمن ارزیابی و بازنگری این نظام مدیریتی بصورت دوره ای همواره بر پیشبرد و بهبود آن اهتمام داشته و از تمامی همکاران عزیز انتظار دارد با همدلی صمیمانه در راستای مدیریت امنیت اطلاعات، بهبود امنیت داده ها، اطلاعات، سیستم ها و شبکه های پردازشی، همت گمارند.

{عنوان بالاترین مقام اجرایی}

نام : .....

امضاء : .....

ضمیمه ۲

سند تعیین قلمرو و حوزه پیاده سازی

سامانه مدیریت امنیت اطلاعات

به موجب این سند مقرر می گردد نظام مدیریت امنیت اطلاعات در حوزه های جغرافیایی و عملیاتی زیر و در خصوص کلیه فعالیت های مرتبط با جمع آوری، پردازش، نگهداری و ارسال داده ها و اطلاعات در مکان های زیر پیاده سازی شود:

۱- پردیس مرکزی {**سازمان**}

۲- ساختمان های (یا سایت های) واقع در {**آدرس محل**}

۳- دارایی های اطلاعاتی متعلق به {**سازمان**} مستقر در {**آدرس محل های نگهداری که مالکیت یا اداره آنها به عهده سازمان نمی باشد**}

۴- .....

۵- .....

همچنین کلیه خدمات قابل ارائه از طریق سیستم های پردازشی زیر باید با توجه به الزامات نظام مدیریت امنیت اطلاعات ارائه گردند:

۱ -.....

۲ -.....

۳ -.....

۴ -.....

{**فهرست فوق باید شامل کلیه پردازش ها و خدماتی باشد که توسط سازمان از طریق سیستم های رایانه ای ارائه می گردند از قبیل :**

- **نظام اتوماسیون اداری و کنترل های داخلی**
- **سیستم دریافت و ثبت تقاضانامه ها مثل تقاضای ثبت سفارش، موافقت نامه اصولی، پروانه ساختمان، ....**
- **سیستم های صدور مدارک یا مجوز مانند گواهینامه رانندگی، پروانه بهره برداری و .....**
- **سیستم های پیگیری مکاتبات یا مراسلات که از طریق کد های پیگیری عمل می کنند.**
- **سایر سیستم های کاربردی اداری، تجاری**
- **بانک های اطلاعاتی سرویس دهنده به سیستم های فوق**
- **کلیه سیستم های مدیریت، راهبری، کنترل، نظارت و پشتیبانی شبکه های رایانه ای**

}

به علاوه نظام مدیریت امنیت برای حفاظت از دارایی های اطلاعاتی زیر به کار گرفته خواهد شد:

- اطلاعاتی که حقوق مالکیت معنوی آن متعلق به {**سازمان**} می باشد.
- اطلاعات مربوط به مشتریان یا ارباب رجوع
- اطلاعات مربوط به نمایندگان، پیمانکاران یا طرف های اداری و تجاری
- نیروی انسانی در اختیار