وزارت ارتباطات و فناوری اطلاعات
سازمان فناوری اطلاعات ایران

مرکز مدیریت، توسعه و اعتباربخشی
نظام ملی مدیریت امنیت اطلاعات

توصیه نامه ایمن سازی ساختارها و سامانه های فناوری اطلاعات

توصیه نامه شماره ۱۲ : امنیت فیزیکی

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	۱۳
مؤلف/مؤلفین سند	سازمان فناوری اطلاعات ایران
کد سند	R90040412

هدف:

هدف از تدوین این توصیه نامه بیان لزوم حفظ امنیت محیطی و فیزیکی دارایی های اطلاعاتی و منابع انسانی از طریق ایجاد محیطی امن برای نگهداری اطلاعات، دارایی های اطلاعاتی و تجهیزات مهم بوسیله ایجاد موانع، دیوارها یا حصارهای مناسب و مستحکم و نظارت وکنترل بر نقاط ورود به محوطه های تحت کنترل یا مالکیت و ارائه راهکارها و روش های مناسب جهت امن سازی اتاق ها، دفاتر، امکانات و تجهیزات پردازشی و نگهداری دارایی های اطلاعاتی برای حفظ امنیت محیطی و پیرامونی می باشد.

ضرورت:

سخت افزارها علاوه بر آنکه در مقابل حمله های رایانه ای آسیب پذیر هستند مثل هر دارایی دیگری در مقابل تهدید های محیطی نیز آسیب پذیرند. اگر بیگانه یا افراد فاقد مجوز بتوانند وارد محل نگهداری دارایی های اطلاعاتی شوند ممکن است تجهیزات را تخریب یا سرقت نموده یا داده ها را دستکاری نمایند. علاوه بر آن، تهدیدات محیطی مثل زلزله و رانش زمین، سیل یا آب گرفتگی، صاعقه و آتش سوزی و یا گرما یا سرمای بیش ازحد که دارای ماهیت طبیعی هستند می توانند سامانه های اطلاعاتی را تحت تاثیر قرار دهند. در این حالت منابع انسانی نیز در معرض تهدید قرار می گیرند.

تهدیدات محیطی از دو عامل طبیعی و انسانی سرچشمه می گیرند. عوامل طبیعی معمولاً دارای حوزه اثر بسیار گسترده می باشند و به زیرساخت ها و منابع انسانی ضربه می زنند. همچنین اگر عامل تهدید، عامل انسانی باشد و روش عملکرد آن برنامه ریزی شده باشد، نتایج فعال شدن آن بسیار خطرناک خواهد بود.

بنابراین حفظ امنیت محیطی و فیزیکی به خصوص در سازمان هایی که به ارائه خدمات عمومی می پردازند و یا زیرساخت های ارائه خدمات را مدیریت یا راهبری می نمایند ضروری است.

الزامات:

- مسئولیت تعریف مرزهای فیزیکی و محدوده هر یک از دفاتر، اتاق ها و مکان های ارائه خدمات رایانه‌ای به عهده نهاد متصدی فناوری اطلاعات می باشد.

- درانتخاب تجهیزات مناسب برای کنترل مبادی ورود و خروج لازم است به سطح بندی و الزامات تعیین شده از سوی سازمان پدافند غیر عامل توجه شود.

- لازم است درمورد ورود به نواحی دارای طبقه بندی محرمانه به ترتیب کنترل های اضافی از قبیل کنترل شناسه کاربری و کلمه عبور، کنترل نشانه[1] های سخت افزاری و یا کنترل عوامل بیومتری بکار گرفته شود، به علاوه در نواحی خیلی محرمانه از روش تایید دسترسی توسط مقام بالاتر نیز استفاده شود.

- لازم است نقاط و درهای ورودی به نواحی امنیتی طبق دستورالعمل‌های تهیه شده توسط مدیریت حراست تحت مراقبت و حفاظت قرار گیرد.

- لازم است افرادی که از مکان های امن بازدید می کنند همراهی یا تایید شوند و زمان ورود و خروجشان ثبت گردد. فقط افراد مجاز می توانند به مکان هایی که از نظر مدیریت سازمان مکان های خاص تلقی می شوند دسترسی داشته باشند.

- لازم است ابزار مدیریت تجهیزات کنترل دسترسی مانند چاپگرهای کارت های الکترونیکی عکسدار فقط در اختیار افراد مجاز بوده وکلیه دسترسی ها ثبت شود.

[1]- Token

- لازم است رویه های تعاملی و برخورد مناسب با افرادی که هویت آن ها غیر قابل شناسایی و تشخیص است تنظیم و به اجرا گذاشته شود.

- لازم است رویه های کنترل بازدیدکنندگان و میهمانان مراجعه کننده به محوطه های پردازش اطلاعات یا محل نصب تجهیزات مسیریابی یا سوئیچینگ یا ترمینال های مخابراتی به درستی انتخاب، تنظیم و اجراء شود.

- لازم است افراد مجاز از مقررات و الزامات امنیتی محیط آگاهی داشته و رویه های اضطراری را نیز به یاد داشته باشند.

- لازم است دسترسی به اطلاعات حساس و تجهیزات پردازش اطلاعات فقط برای افراد مجاز تعریف شود. افراد موظفند هنگام کار در محوطه پردازش اطلاعات از لباس فرم و کارت شناسایی قابل رویت استفاده نمایند.

- لازم است رویه های جلوگیری از دسترسی افراد به تجهیزات پردازش اطلاعات، خارج از ساعات کاری مجاز، به درستی تنظیم و به کار گرفته شود.

- افراد حراست باید متناسب با اهمیت مکانی که از آن حفاظت می نمایند، آمادگی جسمانی یا تجهیزاتی لازم را داشته باشند تا با افرادی که به تنهایی یا به صورت گروهی قصد ورود بدون مجوز را دارند، مقابله نمایند.

- لازم است مجوزهای دسترسی به مناطق امن مرتباً بازنگری شوند.

- استفاده از مکانیزم هایی که مانع از ورود خودروهای غیر مجاز می شوند در مراکز حساس و حیاتی ضروری است.

- در محیط های بسته، لازم است مرزهای فیزیکی بصورت کامل از کف تا سقف از مصالح مستحکم و متناسب با اهمیت سطح طبقه بندی محیط تحت حفاظت ایجاد شود.

- لازم است پیوستگی مرزهای فیزیکی و یا موانع ایجاد شده جهت محدود کردن محیط، به طور کامل رعایت شود به طوری که امکان نفوذ به محیط تحت حفاظت، از هیچ یک از نقاط (بخصوص نقاطی که نوع مرز تغییر می کند، مثل نقاط اتصال فنس به دیوار یا تغییر روش حفاظت از مشاهده بصری به حفاظت الکترونیکی) وجود نداشته باشد.

- لازم است کانال های آب و راه های آب زیرزمینی مثل کاریز و مسیرهای رودخانه های فصلی که از داخل محوطه تحت نظارت می گذرد کنترل شود تا از ورود افراد غیرمجاز از این گونه مسیرها جلوگیری به عمل آید.

- در مراکز داده (سازمان های) حساس و حیاتی لازم است سقف ها و کف ها از جنس بتنی و فولادی ساخته شود تا در برابر آتش، وزن زیاد و ریزش مقاوم باشد.

- باید توجه شود که اندازه، حجم و محل قرار گرفتن گیاهان، درختان و گلها به نحوی باشد که نتوان با استفاده از آنها به محوطه تحت حفاظت نفوذ کرد.

- تصمیم گیری در مورد کفایت مکانیزم های بکار گرفته شده در ورودی نواحی امن یا بکارگیری مکانیزم های اضافی بنا به مورد، به عهده کمیته امنیت اطلاعات است.

- لازم است هر یک از اتاق ها، دفاتر، امکانات و تجهیزات جانبی مربوط به ساختمان ها با توجه به نواحی امنیتی تعریف شده و مطابق با الزامات آن امن سازی شود.

- بمنظور احتراز از شکست های امنیتی ناشی از نفوذ افراد غیرمجاز به دفاتر و اتاق ها، لازم است دستورالعمل ها وشیو ه های تایید شده بطور صحیح اجرا شود و نظارت کامل بر اجرا به عمل آید.

- لازم است فهرست افرادی که مجاز به تردد در یک اتاق، دفتر یا محوطه هستند تهیه و در محل مناسب نصب شود و یا به سهولت در دسترس افراد مجاز قرار گیرد.

- در مراکز حساس و حیاتی لازم است اتاق ها، دفاتر و راهروها بطور دائم توسط دوربین های مدار بسته و سیستم مانیتورینگ تحت کنترل و نظارت قرار گیرد.

- دیوار اتاق ها، مراکز اصلی پردازش یا ذخیره اطلاعات و یا محل استقرار تجهیزات ارتباطی در مراکز حساس و حیاتی باید از نوع بتنی ضخیم بوده و نسبت به نفوذ رطوبت، صوت، ارتعاشات و امواج الکترومغناطیسی عایق‌بندی شده باشد. همچنین دیوارها باید مجهز به سیستم های امنیتی هشدار دهنده مانند سیستم کنترل دما، فشار و ضربه باشند.

- در صورت وجود پنجره در اتاق های محل نگهداری تجهیزات پردازشی و دارایی های اطلاعاتی طبقه‌بندی شده، لازم است پنجره ها دارای حفاظ بوده و همچنین در صورت لزوم از شیشه های نشکن و عایق در مقابل نفوذ رطوبت، صدا و ارتعاشات استفاده شود.

- بمنظور نگهداری و محافظت از رسانه های ذخیره سازی و نگهداری اطلاعات اعم از اطلاعات چاپی مانند فرم‌ها، نامه ها، مستندات مختلف و تمام مواردی که به ثبت می رسد و نیز داده های اطلاعاتی ثبت

شده بر روی میکروفیلم، رسانه های مغناطیسی، دیسک های نوری، دیسک های سخت، دیسک های فشرده نوری، فلاپی و ... باید از گاوصندوق های مخصوص نگهداری این دارایی ها با قفل‌های رمزی، کارت خوان یا بیومتری[1] استفاده شود.

- به عنوان یک قاعده عمومی، سرورهای شبکه نباید در اتاق افراد خاص مثلا اتاق مدیر بخش قرار گیرد. برای سرورها باید اتاق های جداگانه و امنی در نظر گرفته شود. تردد به این اتاق ها باید تحت کنترل بوده و فقط افراد مجاز بتوانند به سهولت به این تجهیزات و امکانات پشتیبانی آنها دسترسی داشته باشند.

- در مراکز حساس و حیاتی لازم است اتاق ها، دفاتر و راهروها بطور دائم توسط دوربین های مدار بسته و سیستم مانیتورینگ تحت کنترل و نظارت قرار گیرند.

- محل قرار گرفتن کامپیوتر باید حتی الامکان در جایی باشد که افراد غیرمجاز قادر نباشند صفحه نمایش و صفحه کلید آن را مشاهده نمایند. رعایت این اصل در خصوص تجهیزات و دارایی‌هایی که برای دسترسی به اطلاعات دارای طبقه بندی به کار می روند الزامی است.

- تجهیزات مناسب ردیابی و کنترل نفوذ بر اساس استانداردهای حرفه ای باید نصب شده و مرتباً آزمایش گردند. این تجهیزات باید کلیه درها، پنجره ها و منافذ احتمالی را که هنگام دسترسی غیرمجاز ممکن است مورد استفاده قرار گیرند پوشش دهد. همه مکان های خلوت باید بوسیله سیستم تشخیص نفوذ فیزیکی تحت کنترل قرار گرفته و از پوشش حفاظتی مناسب برای اتاق کامپیوتر و تجهیزات مخابراتی استفاده شود.

[1] - Biometry

- تجهیزات پشتیبانی مانند دستگاه فتوکپی یا فکس باید به نحوی درمنطقه امن پیش بینی شود که نیازی به خارج کردن اطلاعات نباشد. به منظور بالا بردن امنیت و حفظ اطلاعات باید از خارج شدن بدون کنترل منابع ذخیره اطلاعا ت و ورود افراد غیرمجاز به اتاق ها و دفاتر محل نگهداری دارایی های اطلاعاتی دارای طبقه بندی جلوگیری بعمل آید.

فرآیند:

توجه به حساسیت عملکرد و تنش پذیری در مقابل تهدیدات و طبقه بندی دارایی های اطلاعاتی اولین گام در ایجاد امنیت محیطی و فیزیکی می باشد. باید توجه داشت که سطح اهمیت هر مکان یا ناحیه، حداقل معادل بالاترین سطح امنیت تجهیزات یا منابع مستقر در آن می باشد.

به منظور مدیریت بهتر، تجهیزات پردازشی و دارایی های اطلاعاتی دارای طبقه بندی حفاظتی یکسان را باید در اتاق ها و دفاتر با طبقه بندی یکسان نگهداری کرد تا بطور مناسب و در حد مطلوب محافظت از آنها به عمل آید. قرار دادن دارایی های اطلاعاتی دارای طبقه بندی حفاظتی متفاوت در یک مکان می تواند باعث نقض محرمانگی یا عدم رعایت سطح طبقه بندی تخصیص داده شده به دارایی مورد نظر شود، زیرا ممکن است افرادی که دارای سطح دسترسی به طبقه بندی رده پایین باشند بتوانند به بهانه کار با دارایی های اطلاعاتی مربوط به خود، به دارایی های اطلاعاتی دارای رده حفاظتی بالاتر دسترسی پیدا کنند.

توضیحات:

کنترل ورود و خروج مهم ترین و کاراترین مکانیزم حفاظتی در امنیت فیزیکی و جلوگیری از پیامدهای دسترسی فیزیکی به سخت‌افزار، نرم‌افزار و دارایی های اطلاعاتی می باشد. مناطق امن باید بوسیله تجهیزات مناسب کنترل ورود و خروج محافظت شود به نحوی که فقط افراد مجاز قادر به عبور از دروازه های دسترسی به این مناطق باشند. به منظورایجاد سطح بندی مناسب در این دستورالعمل بهتر است به دو عامل اصلی طبقه بندی اطلاعات و دارایی های اطلاعاتی در داخل سازما ن و دسته بندی سازمان پدافند غیرعامل برای مراکز، سازمان ها و نهادهای کشوری توجه شود. از نظر سازمان پدافند غیرعامل سه نوع سطح بندی مهم، حساس و حیاتی در نظر گرفته شده که برای آگاهی بیشتر در خصوص این نوع سطح بندی لازم است به مستندات منتشر شده یا رهنمودهای اختصاصی آن سازمان مراجعه شود. برای سهولت در عملیات امن‌سازی، سطح بندی سه گانه زیر بر اساس طبقه بندی داخلی نهاد تحت حفاظت و دسته بندی سازمان از دیدگاه پدافند غیرعامل پیشنهاد می شود :

		دسته بندی سازمان پدافند غیر عامل		
		مهم	حساس	حیاتی
طبقه‌بندی اطلاعات و دارایی‌های اطلاعاتی در سازمان	عادی	سطح یک	سطح یک	سطح دو
	محدود	سطح یک	سطح دو	سطح دو
	محرمانه	سطح دو	سطح دو	سطح سه
	خیلی محرمانه	سطح دو	سطح سه	سطح سه

(جدول سطح بندی عملیات امن سازی)

در یک طرح نمونه امنیتی برای بالا بردن قابلیت اطمینان که طبعاً با بالا رفتن هزینه نیز همراه خواهد شد از دور افتاده‌ترین وکم اهمیت ترین نقاط سازمان گرفته تا نواحی مرکزی و حساس از روش های متفاوتی استفاده می گردد. استفاده از روش های ترکیبی در نقاط ورودی، موجب افزایش ضریب اطمینان در این نقاط خواهد شد. همچنین بکارگیری روش های متفاوت امنیتی برای سطوح داخلی به طور قابل ملاحظه ای ظرفیت های امنیتی را در سطوح بالاتر ارتقا خواهد داد، زیرا سطح بالاتر نه تنها توسط ساز وکار حفاظتی متعلق به خود بلکه به واسطه بررسی هایی محافظت می گردد که در لایه های بیرونی انجام می شود.

بعضی از دستگاه های کنترل دسترسی برای مثال کارت خوان و اسکنر بیومتریک می توانند اطلاعات مربوط به رخدادهای دسترسی را ضبط و ثبت نمایند. چنانچه به این تجهیزات قابلیت کار در شبکه نیز افزوده شود می توان این اطلاعات را با هدف ممیزی تردد و مانیتورینگ، کنترل عملکرد ماشین‌ها و افراد، تعریف کد دسترسی برای اشخاص خاص در اوقات خاص و همچنین اعلام اخطار و اطلاع از تلاش های تکراری ناموفق برای عبور از یک دروازه امنیتی بکار گرفت و یا از طریق شبکه به یک سیستم مدیریت دسترسی راه دور انتقال داد. جهت حفاظت از نقاط ورودی و دروازه های ارتباطی بین محیط های دارای کاربری متفاوت می توان از روش های زیر برای سطوح مختلف بهره برد:

۱- محیط های سطح یک

- دراین سطح از کنترل بمنظور جلوگیری از ورود افراد غیر مجاز استفاده از کلید و قفل معمولی و یا غیر قابل کپی الزامی است.

۲- محیط های سطح دو

- استفاده از قفل و کلیدهای الکترونیکی خودکفا(بدون اتصال به سیستم مرکزی کنترل دسترسی) بر روی درهای ورودی به عنوان مکانیزم حداقلی الزامی است. در این قفل ها باید از مکانیزم UPT و در مناطق حساس تر از مکانیزم UPTB استفاده شود.
- به منظور نظارت بر ورود افراد، درهای ورود باید مجهز به سیستم مانیتورینگ باشند.
- بمنظور جلوگیری از حمل اشیا غیر مجاز استفاده از دروازه های بازرسی الزامی است.

۳- محیط های با طبقه بندی سطح سه

- استفاده از قفل و کلیدهای الکترونیکی شبکه ای (متصل به سیستم مرکزی کنترل دسترسی) روی درهای ورودی الزامی است. درهای ورود باید مجهز به مکانیزم ممیزی[1] باشند. در این قفل ها باید از مکانیزم UPTB1 و در مناطق حساس تر از مکانیزم UPTB1+ استفاده شود.
- کلیه درها باید توسط دوربین های مدار بسته کنترل شود و برق اضطراری برای دوربین‌ها در نظر گرفته شود.
- همچنین برای حفاظت از دوربین ها باید آنها را در محفظه های ضد حریق و ضد ضربه قرار داد. در صورتی که امکان ورود از پنجره وجود داشته باشد لازم است مکانیزم های حفاظتی کامل (تشخیص نفوذ فیزیکی) در مورد آن بکار گرفته شود.
- بمنظور جلوگیری از ورود و خروج اشیا غیرمجاز، استفاده از دروازه های بازرسی فیزیکی یا تصویر برداری معمولی و یا مادون قرمز و یا X-Ray الزامی است.

[1] - Auditing

با توجه به دسته بندی در نظر گرفته شده بر اساس طبقه بندی حفاظتی مکان ها و دارایی های اطلاعاتی در اختیار سازمان و رهنمودهای سازمان پدافند غیر عامل می توان از مکانیزم های مختلفی جهت کنترل دسترسی استفاده نمود.

بطور کلی مکانیزم های کنترل دسترسی را می توان به صورت زیر (به ترتیب اهمیت) فهرست نمود (علائم مقابل هر مکانیزم به عنوان علامت اختصاری به کار گرفته شده است):

- کنترل عادی و یا شناسایی توسط نفر [N]
- استفاده از شناسه کاربری و کلمه عبور به منظور اثبات هویت ادعا شده (شناسه کاربری) از طریق آنچه که به وی تخصیص داده شده است (کلمه عبور)[UP]
- استفاده از شناسه کاربری و کلمه عبور همراه با نشانه سخت افزاری[1] به منظور جلوگیری از سواستفاده از کلمه عبور توسط دیگران [UPT]
- استفاده از روش فوق (UPT) همراه علائم حیاتی و یا زیست سنجی[2] به منظور جلوگیری از سوء استفاده از کلمه عبور و استفاده غیرمجاز از نشانه سخت افزاری [UPTB]
- استفاده از روش فوق (UPTB) به علاوه تایید مقام بالاتر به منظور اطمینان از مجاز بودن فرد به دسترسی در زمان های خاص یا تحت شرایط خاص [+UPTB]

[1] - Token
[2] - Biometrics

- استفاده از روش فوق (UPTB+) به علاوه همراهی توسط یک نفر دیگر به منظور جلوگیری از سوءاستفاده شخص از اختیاراتش [UPTB+1]

با توجه به تعریف های فوق مکانیزم های شش گانه کنترل دسترسی به شرح جدول زیر پیشنهاد می شود:

		سطح بندی سازمان پدافند غیر عامل		
		مهم	حساس	حیاطی
طبقه بندی حفاظتی اطلاعات/دارایی های اطلاعاتی/مکان ها	عادی	N	UP	UPT
	محدود	UP	UPT	UPTB
	محرمانه	UPT	UPTB	UPTB1
	خیلی محرمانه	UPTB	UPTB1	UPTB1+

با مقایسه این جدول و جدول ارائه شده در ابتدای این توصیه نامه (سطح بندی سه گانه) مکانیزم های قابل استفاده در هر یک از سطوح عبارتند از:

سطح حفاظتی	مکانیزم های کنترل دسترسی قابل استفاده
سطح یک	کنترل عادی یا استفاده از شناسه کاربری و کلمه عبور(UP)
سطح دو	استفاده از شناسه کاربری و کلمه عبور و یا کنترل بیومتریک(UPT/UPTB)
سطح سه	استفاده از شناسه کاربری و کلمه عبور، همراه کنترل بیومتریک و تایید مقام بالاتر و یا همراهی توسط یک نفر دیگر(UPTB+/UPTB+1)

(جدول نگاشت مکانیزم های کنترل دسترسی و سطح حفاظتی)

به عبارت دیگر برای انتخاب ساده تر مکانیزم کنترل دسترسی می توان ابتدا سطح حفاظتی مورد نظر برای دارایی های اطلاعاتی را (با استفاده از نظر افراد خبره یا مشاوران سازمان) تعیین نمود و سپس یکی از مکانیزم های کنترل دسترسی متناظر با آن را مورد استفاده قرار داد.