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 ۹ : قوانین استفاده از کامپیوتر

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	۷
مؤلف/مؤلفین سند	سازمان فناوری اطلاعات ایران
کد سند	R90040409

هدف:

هدف از تدوین این توصیه نامه بیان لزوم استفاده کنترل شده از دارایی های اطلاعاتی (بر اساس روش های از پیش تاییدشده) به منظور کاهش زیان‌ها و یا تبعات امنیتی ناشی از بهره برداری نادرست از دارایی های اطلاعاتی می باشد.

ضرورت:

بدیهی است تحمیل بار بیش از حد ظرفیت به هر ابزار می تواند یکی از دو پیامد خرابی ابزار و یا کاهش کیفیت خروجی را به دنبال داشته باشد. علاوه بر آن شرایط کار هر ابزار نیز تابع محدودیت های مختلف از قبیل درجه حرارت، رطوبت، ارتعاش، میدان مغناطیسی یا الکتریکی و مشابه آن می باشد. دارایی های اطلاعاتی نیز دارای این محدودیت ها می باشند. یکی دیگر از خصوصیات اغلب دارایی های اطلاعاتی، سهولت به کارگیری آنها در کاربرد های مختلف (مثلاً شخصی یا اداری) می باشد. اطلاعات ذخیره شده در رسانه های الکترونیکی قابلیت انتقال آسان از یک مکان به مکان دیگر را داشته و در صورت دسترسی داشتن به ابزار مناسب، به راحتی قابلیت تغییر، حذف و یا جعل را دارند.

به دلایل فوق و بسیاری دلایل دیگر که اشاره به آنها در این زمان نمی گنجد، ضروری است استفاده از دارایی های اطلاعاتی و داده های موجود در آنها تحت کنترل کامل باشد و این دارایی ها بر اساس روش های قابل پذیرش و از پیش تایید شده مورد استفاده قرار گیرند.

الزامات:

- مسئولیت تدوین شرایط و نحوه استفاده قابل پذیرش از دارایی های اطلاعاتی به عهده متصدی یا تحویل گیرنده یا مالک همان دارایی اطلاعاتی می باشد. شرایط تدوین شده باید به اطلاع کاربران رسانده شود.
- قوانین کشوری و مقررات سازمانی باید به عنوان اولین منبع استخراج نحوه استفاده قابل پذیرش از تجهیزات رایانه ای مورد توجه قرارگیرند. بنابراین لازم است کلیه قوانین و مقرراتی که مستقیماً در ارتباط با بهره برداری از این تجهیزات وضع شده، شناسایی گردیده و یک نسخه از انها در دسترس باشد.
- اگر ارائه خدمات رایانه ای به نحوی است که عبور داده از مرزهای کشوری را ضروری می سازد باید به قوانین یا محدودیت های بین المللی مربوط به پردازش یا انتقال داده یا ارائه خدمات رایانه‌ای در کشورهای محل عبور یا پردازش داده توجه شود. (به علت متفاوت بودن سیستم های قضایی ممکن است انتقال برخی داده ها یا استفاده از برخی الگوریتم های رمزنگاری در بعضی کشورها جرم محسوب شود)
- کلیه بهره برداران از دارایی های اطلاعاتی باید بر اساس شرایط تعیین شده از دارایی های اطلاعاتی استفاده نمایند.
- لازم است نحوه استفاده قابل پذیرش از دارایی های اطلاعاتی براساس نتایج حاصل از عملکرد سامانه مورد بازنگری و تصحیح قرار گیرد.

- استفاده صحیح از یک دارایی اطلاعاتی بدین معنی است که باید بهره برداری از آن در جهت اهداف تعیین شده سازمان صورت پذیرد و کمترین مخاطرات را برای دارایی های اطلاعاتی و فرآیندهای سازمانی ایجاد نماید.
- نحوه استفاده قابل پذیرش از دارایی ها علاوه بر ملاحظات امنیتی باید مواردی همچون شرایط تعیین شده توسط سازنده یا تامین کننده، شرایط محیطی محل استفاده، نحوه استفاده صحیح و شرایط پس از بهره برداری از دارایی ها را نیز بیان کند.
- لازم است جهت استفاده از کلیه تجهیزات پردازشی یا دارایی های اطلاعاتی مندرج در فهرست دارایی های اطلاعاتی، مجوزهای بهره برداری (بر اساس روال مدون صدور مجوز استفاده از دارایی های اطلاعاتی) اخذ گردد.
- لازم است کلیه افراد قبل از استفاده از دارایی های اطلاعاتی دارای طبقه بندی حفاظتی، توافق نامه حفظ محرمانگی (و یا سند مشابهی که شرایط بهره برداری از دارای های اطلاعاتی دارای طبقه بندی به روشنی در آن شرح داده شده باشد) را پذیرفته و امضاء نموده باشند.
- لازم است واحد امنیت اطلاعات یا مرکز حراست فناوری اطلاعات یا نهاد جایگزین آن با تعامل با مالکان و متصدیان دارایی های اطلاعاتی، شرایط و ضوابط دسترسی افراد به دارایی ها و شرایط اختصاصی مد نظر قسمت مربوطه را اخذ و در دستورالعمل اختصاصی بهره برداری از هر دارایی اطلاعاتی لحاظ نمایند. (نحوه استفاده و شرایط خاص مالکان / متصدیان دارایی های اطلاعاتی).

- نحوه استفاده و دسترسی به دارایی های اطلاعاتی پیرو سیاست های کنترل دسترسی سازمان بوده و در صورت بیان شرایط دیگر مبنی بر اخذ مجوز خاص، این مجوزها باید اخذ و رعایت گردد.
- لازم است رویدادها و یا موارد استفاده ناصحیح از دارایی ها توسط متصدیان/مالکین دارایی ها، ممیزان امنیت و یا مراجع و افرادی که نظارت بر بهره برداری امن از دارایی های اطلاعاتی را ب ر عهده دارند، طبق فرم های گزارش/ ثبت رخداد مکتوب شده و به واحد امنیت اطلاعات یا مرکز حراست فناوری اطلاعات یا نهاد جایگزین آن اعلام گردد.
- برای تعیین شرایط قابل پذیرش استفاده باید از نتایج حاصل از شناخت سازمان و تحلیل (ارزیابی ریسک) نیز استفاده شود.
- شرایط نگهداری و تعمیرات دارایی های اطلاعاتی سخت افزاری نیز باید به عنوان بخشی از شرایط نحوه استفاده قابل پذیرش لحاظ شود.
- نصب اصلاحیه ها و به هنگام سازی نرم افزارها نیز باید به عنوان بخشی از شرایط نحوه استفاده قابل پذیرش لحاظ شود.
- استفاده شخصی از دارایی های اطلاعاتی سخت افزاری یا نرم افزارهای تحت مالکیت یا در اختیار سازمان ممنوع است. نگهداری اطلاعات شخصی در رایانه های سازمانی حتی الامکان باید ممنوع باشد. اگر مدیریت سازمان بخواهد این ممنوعیت را نادیده بگیرد اولاً باید مسؤولیت آن را به عهده بگیرد و ثانیاً باید فضای مجزایی به این کار اختصاص داده شده و از طریق مکانیزم های کنترل

دسترسی، به طور کامل کنترل گردد. در این صورت لازم است به پیامدهای قانونی ناشی از نقض حریم خصوصی افراد توجه شود.

- هنگام تعیین شرایط قابل پذیرش بهره برداری باید به تجهیزات خارج از سازمان توجه خاص نمود. تجهیزاتی که خارج از دید روزمره تحویل گیرنده آن می باشند از این قبیل محسوب می شوند و به عنوان تجهیزات بدون مراقب لحاظ می شوند. به عنوان مثال سایت های مخابراتی خارج از سازمان، تجهیزات موجود در کانال های مخابراتی و داکت ها (زیرزمینی یا درون ساختمان)، خودپردازها یا دستگاه های فروش خودکار نصب شده در مکان های عمومی و تجهیزات امانی نصب شده در مکان های خارج از سازمان نمونه هایی از این تجهیزات هستند.
- آزمایش نرم افزارهای جدید قبل از نصب در محیط عملیاتی، باید به عنوان یکی از شرایط اصلی تعیین شود. تخریب اطلاعات ناشی از عملکرد بد نرم افزار یا عدم انطباق فرمت اطلاعات می تواند نتایج غیرقابل جبرانی در پی داشته باشد.
- در بهره برداری تخصصی از نرم افزارها و سخت افزارها، آموزش و میزان مهارت کاربر باید به عنوان شرایط بهره برداری لحاظ شود. در صورتی که آموزش کاربران امکان پذیر نباشد (مثلاً ارائه خدمات در وب یا مکان های در دسترس عموم)،صدور مجوز بهره برداری فقط باید پس از اطمینان از محدویت کامل دارایی اطلاعاتی به کاربرد مورد نظر صادر شود. یعنی واسط ارتباطی کاربر یا حدود دسترسی به نحوی تنظیم شده باشد که انجام هیچ فعالیتی بجز فعالیت خاص در نظر گرفته شده برای ابزار امکان پذیر نباشد.

- تجهیزات بدون مراقب نباید امکان دسترسی ممتاز به دارایی های اطلاعاتی را ایجاد نمایند مگر آنکه زمان، حدود و مدت آن از قبل تعیین شده و به اطلاع تحویل گیرنده یا مالک تجهیزات هدف رسیده باشد.
- نحوه و ترتیب از سرویس خارج کردن دارایی های اطلاعاتی باید به عنوان بخشی از شرایط نحوه بهره برداری از دارایی اطلاعاتی معین شده باشد. در صورتی که دارایی اطلاعاتی دارای نقش کلیدی در ارائه خدمات باشد روش از سرویس خارج کردن آن باید مدون شده و در مانورهای طرح پیوستگی عملیات تمرین شود.

فرآیند:

هنگام تعیین شرایط استفاده قابل پذیرش برای هر دارایی اطلاعاتی باید در خصوص مکتوب بودن یا شفاهی بودن دستورالعمل مربوط تصمیم گیری کرد. به طور کلی این شرایط را می توان به دو دسته شرایط عمومی و شرایط اختصاصی کار با هر دارایی اطلاعاتی تقسیم کرد.

شرایط اختصاصی کار باید مکتوب بوده و به امضای بهره بردار برسد. به علاوه اگر غفلت یا استفاده نادرست موجب نقض مقررات یا قوانینی گردد که پیگرد انضباطی یا قضایی به دنبال داشته باشد، این موضوع باید به اطلاع بهره بردار برسد و اطمینان حاصل شود بهره بردار موضوع را (در حد متعارف) درک کرده است.

شرایط عمومی استفاده قابل پذیرش را می توان در قالب جلسات توجیهی یا اطلاعیه به کاربران خارج از سازمان اعلام نمود. اما در مورد کاربران درون سازمان باید این کار را در قالب ابلاغیه هنگام استخدام یا تغییر در شرایط کاری (تغییر پست، تغییر شغل و یا تغییر در روش یا تجهیزات) به اطلاع افراد رساند.

نتایج حاصل از ارزیابی ریسک مهمترین منبع تعیین شرایط نحوه استفاده قابل پذیرش را تشکیل می دهد. علاوه بر آن شرایط عملکرد تعیین شده توسط سازنده یا تامین کننده سخت افزار یا نرم افزار یا خدمات، راهنمای مهم دیگر تعیین شرایط می باشد.

شرایط استفاده قابل پذیرش شرایط ثابتی نیست و با توجه به پیشرفت فناوری یا تغییر در محیط عملیاتی سازمان قابل تغییر می باشند. این شرایط را می توان بر اساس نتایج حاصل از ممیزی، بازنگری های دوره‌ای، ارزیابی مجدد ریسک، نتایج حاصل از مانورها و یا تجربه تغییر داد.