وزارت ارتباطات و فناوری اطلاعات

وزارت ارتباطات و فناوری اطلاعات
سازمان فناوری اطلاعات ایران

توصیه نامه ایمن سازی ساختارها و سامانه های فناوری

اطلاعات و ارتباطات

توصیه نامه شماره ۱: تهیه نسخه پشتیبان و بازگشت به آخرین وضعیت صحیح قبلی

نوع سند	توصیه نامه
سطح دستیابی سند	عمومی
سطح امنیتی سند	عادی
اولویت سند	خیلی فوری
تاریخ ارائه سند	آذرماه ۸۹
نگارش سند	۱
تعداد صفحات	۶
مؤلف/مؤلفین سند	سازمان فناوری اطلاعات
کد سند	R018909

هدف:

هدف از تدوین این توصیه نامه بیان ضرورت و چگونگی تهیه نسخه پشتیبان از داده‌ها و اطلاعات تحت مالکیت آن دستگاه می‌باشد.

ضرورت:

بازگرداندن نسخه پشتیبان قابل اعتماد، آخرین راهکار پاسخگویی به حوادث و رخدادهای رایانه ایی اعم از خرابی یا عملکرد نادرست سخت افزار یا نرم افزار، اشتباه کاربر و یا حمله های عمدی یا غیر عمدی رایانه‌ای یا هر حادثه دیگر منجر به تخریب داده ها می باشد. بنابراین تهیه نسخه پشتیبان قابل بازگرداندن یکی از الزامات تامین امنیت در سامانه های فناوری اطلاعات می باشد.

الزامات:

- لازم است مسئولیت تهیه نسخه پشتیبان از داده ها و اطلاعات دارایی های اطلاعاتی الکترونیکی موجود در فهرست دارایی های اطلاعاتی الکترونیکی و اطمینان از صحت روش تهیه و جامعیت نسخه پشتیبان، بر عهده تحویل گیرنده، متصدی و یا مالک همان دارایی اطلاعاتی الکترونیکی قرار گیرد. این مسئولیت قابل انتقال به غیر نمی باشد و به صورت سلسله مراتبی مدیران فرد مربوط نیز ضامن تهیه نسخه پشتیبان می باشند. وجود سامانه خودکار و یا متمرکز تهیه نسخه پشتیبان رافع مسئولیت هیچیک از افراد مسئول تهیه نسخه پشتیبان نمی باشد.

- لازم است از کلیه داده‌های الکترونیک اعم از بانک‌های داده و اطلاعات، نرم‌افزارهای کاربردی، فایل‌های پیکربندی، سیستم عامل‌ها، فایل‌های داده، ابزارهای سیستم و غیره، نسخه پشتیبان قابل اعتماد تهیه شده و در محلی امن نگهداری شود.

- لازم است نسخه پشتیبان در بازه‌های زمانی مشخص یا بلافاصله پس از هرگونه اعمال تغییرات در نرم‌افزارها یا فایل‌های داده به صورت خودکار یا توسط اپراتور به‌هنگام‌سازی شود.

- لازم است در مورد ایجاد نسخه پشتیبان داده‌ها و اطلاعات به حجم، طبقه‌بندی و نوع اطلاعات و نوع فایل توجه و از ابزار مناسب مورد نیاز هر کدام و الگوریتم های مستحکم رمزنگاری (در صورت نیاز) استفاده شود.

- لازم است کفایت، صحت و سلامت نسخه‌های پشتیبان تهیه شده مورد بررسی و کنترل مداوم قرار داشته باشد.

- لازم است فرم های لازم (مانند فرم درخواست تهیه نسخه پشتیبان، فرم خلاصه اطلاعات نسخه پشتیبان، فرم کنترل صحت و ...) طراحی و تدوین شده و به صورت نظام مند مورد استفاده قرار گیرد.

- لازم است هنگام تولید یا خرید نرم‌افزارهای جدید، روش تهیه نسخه پشتیبان از اطلاعات نیز مورد توجه قرار گرفته و از وجود و صحت آن اطمینان حاصل شود.

- سلسله مراتب بازیابی نسخه پشتیبان باید به نحوی باشد که از تخریب اطلاعات به دلیل عدم تطابق اطلاعات بازیابی شده با اطلاعات اصلی ایمن باشد.

- متصدی یا مسئول تهیه نسخه پشتیبان موظف است به طور دوره‌ای چک لیست لوازم و ابزار رسانه‌های مورد نیاز برای پشتیبان‌گیری را بررسی و در صورت کمبود اقدامات لازم جهت تأمین آنها را انجام دهد.

- تهیه، ارسال، جابجایی، حمل و نقل نسخ پشتیبان دارائی‌های اطلاعاتی باید تحت کنترل کامل قرار داشته باشد.

- در صورت مشاهده هرگونه اشکال در تهیه پشتیبان یا صحت داده، افراد یا واحدهای ذیربط موظف به اعلام موضوع بصورت کتبی به کمیته امنیت اطلاعات می‌باشند.

- در صورت وجود مسئول تهیه نسخه پشتیبان، این شخص موظف است برنامه‌های مناسب برای نگهداری نسخ پشتیبان را تدوین و به تأیید مدیر واحد امنیت اطلاعات برساند. در هر صورت وجود چنین شخصی رافع مسئولیت سایر افراد در تهیه نسخه پشتیبان از داده ها و اطلاعات در اختیار خود نمی باشد.

- لازم است سوابق تهیه نسخه پشتیبان به طور کامل ثبت و نگهداری شود. متصدی مربوطه باید بر تغییر سطوح دسترسی افراد به نسخ پشتیبان نظارت داشته باشد.

فرآیند:

مراحل انجام این توصیه نامه به شرح زیر می باشد:

۱- در ابتدا طرح تهیه نسخه پشتیبان تهیه شده و بهمراه الزامات امنیتی آن تدوین شود. در این طرح بایستی به دسته بندی سازمان از دیدگاه پدافند غیرعامل و طبقه بندی حفاظتی سازمان توجه شود. همچنین ارزش و اهمیت اطلاعات از دیگر مواردی است که در تدوین این طرح باید مدنظر قرار

گیرد. در صورتی که سازمان دارای الزامات اختصاصی باشد الزامات مورد نظر به الزامات بیان شده در این سند افزوده خواهد شد.

۲- در مرحله بعد باید کلیه مکانیزم ها، امکانات و تجهیزات مورد نیاز اعم از فضا، سخت افزارها و نرم افزارهای مورد نیاز و متناسب با طرح و الزامات تدوین شده تامین شود. همچنین فرم های مربوط به این فرآیند نیز در این مرحله تهیه گردد.

۳- پس از تامین موارد فوق، طرح تدوین شده پیاده سازی گشته، الزامات امنیتی به اجرا گذاشته شده، نسخه پشتیبان تهیه و از صحت آن اطمینان حاصل گردد.

۴- در صورت قابل قبول بودن نسخه تهیه شده اگر نسخ پشتیبانی وجود داشته باشند که مورد نیاز نباشند (مثلاً از نظر زمانی دارای ارزش نباشند) و یا نامعتبر باشند (بعنوان مثال دارای نقصان باشند) باید از بین برده شده و امحاء شوند.

۵- در صورتی که کلیه الزامات روش مدون پشتیبان گیری (بیان شده در این سند و الزامات اختصاصی سازمان) برآورده شده باشد بایستی کلیه اقدامات لازم برای نگهداری و حفاظت از نسخ تهیه شده متناسب با الزامات امنیت فیزیکی پیرامونی انجام شود.

تعاریف:

دارایی‌های اطلاعاتی الکترونیکی:

داده‌های دیجیتالی یا الکترونیکی، به عنوان مثال بانک‌های اطلاعات، سیستم عامل، برنامه‌های کاربردی، فایل‌های پیکربندی تجهیزات و ... .

تحویل گیرنده، متصدی و یا مالک همان دارایی اطلاعاتی الکترونیکی:

برای اطمینان از بهره برداری در شرایط قابل پذیرش دارایی های اطلاعاتی الکترونیکی، لازم است هر دارایی اطلاعاتی الکترونیکی به طور صریح و واضح به یک فرد از آحاد سازمان سپرده شود. این فرد باید در مورد نحوه بهره برداری امن از دارایی اطلاعاتی الکترونیکی تحت مسئولیت خود آموزش دیده باشد. به علاوه لازم است ابزار و اختیارات لازم برای حفاظت از دارایی اطلاعاتی الکترونیکی در اختیار وی گذارده شود.

همچنین لازم است برای جلوگیری از ناهماهنگی در تعامل با دارایی های اطلاعاتی الکترونیکی و پیشگیری از تبعات و آسیب پذیری های ناشی از آن، متصدی یا تحویل گیرنده دارایی اطلاعاتی الکترونیکی در موارد زیر به عنوان مرجع اصلی محسوب شده و نظرات وی در اولویت قرار گیرد:

- تعیین طبقه بندی حفاظتی دارایی اطلاعاتی الکترونیکی
- تعریف سیاست ها و مکانیزم های کنترل دسترسی
- تایید فرم های درخواست دسترسی