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 ۱۰ : حفاظت از اطلاعات

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	R90040410

هدف:

هدف از تدوین این توصیه نامه بیان لزوم رعایت الزامات امنیتی در ایجاد و بکارگیری رویه‌های مدیریت و نگهداری اطلاعات (جمع‌آوری، نگهداری، ذخیره‌سازی و بازخوانی) برای حفاظت در برابر افشاء غیرمجاز یا استفاده نابجا از اطلاعات و همچنین طبقه بندی اطلاعات جهت حفاظت مؤثر از دارایی های اطلاعاتی فهرست شده در فهرست موجودی دارایی های اطلاعاتی و حفاظت از اطلاعات شخصی افراد می باشد.

ضرورت:

داده‌ها و اطلاعات با توجه به نیاز و اهداف سازمانی (یا شخصی) جمع آوری می‌شود و لازم است با توجه به ماهیت و اهمیت آن به صورت صحیح طبقه‌بندی شود. برای نگهداری صحیح اطلاعات ابتدا بایستی شناخت کاملی از آن به دست آید؛ بدین معنا که ابتدا باید با توجه به نیازها، اهداف و سیاست‌های سازمان، اطلاعات مورد نظر شناسایی شوند. پس از شناسایی اطلاعات، ماهیت و اهمیت آن، باید برای تضمین حفاظت و استفاده صحیح از اطلاعات تدابیری اندیشیده شود. به عبارت دیگر باید نگهداری و بهره برداری از اطلاعات بر اساس رویه های امن انجام شود. استفاده امن از اطلاعات به ویژه در خصوص اطلاعات حیاتی سازمان و اطلاعات شخصی افراد، اهمیت بیشتر پیدا می کند.

الزامات:

- لازم است نحوه جمع‌آوری، کسب و دسته‌بندی اطلاعات منطبق بر نیازهای از پیش تعیین شده باشد.

- پس از تولید اطلاعات باید آنها را به شکل صحیح طبقه‌بندی کرده و سطح دسترسی هر دسته از اطلاعات به دقت مشخص شود.

- لازم است رسانه های ذخیره اطلاعات طبقه‌بندی شده با علامت‌ها و برچسب‌های لازم علامت گذاری شوند به نحوی که به آسانی قابل تشخیص باشند.

- برای انجام عمل طبقه‌بندی بایستی معیارهای از پیش تعیین شده و غیرقابل تفسیر مورد استفاده قرار گیرد.

- برای پردازش اطلاعات باید به سطح طبقه‌بندی هر دسته از اطلاعات توجه کرد و اطلاعات با هر سطح طبقه‌بندی فقط به افرادی که اجازه دسترسی به آن سطح را دارا هستند تحویل داده شود.

- باید توجه داشت که سطح طبقه‌بندی اطلاعات پس از پردازش در چه درجه‌ای است و اگر پردازش موجب تولید اطلاعاتی با سطح طبقه‌بندی سخت گیرانه‌تر شود باید الزامات مدیریت آن دسته از اطلاعات رعایت گردد.

- لازم است صحت اطلاعات پس از پردازش و قبل از عمل ذخیره‌سازی به دقت مورد بررسی قرار گیرد که در آن مقادیر غیر منطقی (به عنوان مثال مقادیر عددی به جای نام یا نام خانوادگی یا بستانکاری برای مقادیر دارای ماهیت بدهکار) وجود نداشته باشد. خصوصاً برای مراکز حساس یا حیاتی این عمل بایستی با دقت بیشتری انجام شود تا مبادا اطلاعات نادرستی وارد سیستم شود.

- بعد از اتمام مراحل پردازش بایستی اطمینان حاصل شود که تغییرات در تمامی نسخه‌های موجود اطلاعات اعمال شود.

- پردازش اطلاعات می‌تواند باعث ایجاد اطلاعات جدید شود، در این صورت بایستی اطلاعات جدید مجدداً طبقه‌بندی و علامت گذاری شود. پس از انجام پردازش اطلاعات باید دقت داشت اگر بین اطلاعات جدید با اطلاعات قبلی ناهماهنگی وجود دارد جایگزینی اطلاعات به درستی انجام شود.

- اطلاعات باید برای ذخیره‌سازی در محل امن قرار گیرد به طوری که دسترسی به آنها برای افراد غیرمجاز امکان‌پذیر نباشد.

- برای اطمینان از عدم لطمه ناخواسته به اطلاعات باید از آنها نسخه پشتیبان تهیه شود.

- بایستی از اطلاعات در مقابل تهدیدات ناشی از حوادث طبیعی و غیرطبیعی بر اساس سطح حساسیت سازمان (طبق دسته بندی سازمان پدافند غیرعامل) تا آنجا که ممکن است محافظت شود.

- در مراکز حساس و حیاتی، محل نگهداری اطلاعات باید در مقابل بلایایی از قبیل سیل، زلزله، آتش‌سوزی، انفجار، اغتشاشات اجتماعی و مانند آن کاملاً ایمن باشد.

- بعد از استفاده کامل از اطلاعات و اطمینان از عدم نیاز همیشگی به اطلاعات باید اطلاعات به صورت کامل از بین برده شود.

- دستورالعمل طبقه بندی که نحوه تعیین اهمیت، اولویت و درجه بندی حفاظتی هر دسته از دارایی های سازمان را بیان می دارد باید مدون شده و به اطلاع بخشهای مختلف سازمان رسانده شود.

- لازم است نکات مربوط به تعداد طبقه های تعریف شده و مزایای حاصل از آن به دقت تحت نظر قرار گیرد و در صورت تعریف عناوین مشابه با سایر سازمان ها، تفاوت ها و جزئیات تمایز این عناوین به اطلاع تمامی قسمت ها برسد.

- هر قسمت موظف است تا تمامی دارایی های اطلاعاتی حوزه خود را طبقه بندی نموده و در فرم شناسنامه دارایی های اطلاعاتی ذکر نماید. این طبقه بندی باید مورد بررسی و تائید واحد امنیت اطلاعات یا مرکز حراست فناوری اطلاعات یا نهاد جایگزین آن قرار گیرد.

- لازم است طبقه بندی اطلاعاتی دارایی ها (به جز دارایی های دارای طبقه بندی عادی) در برچسب های قابل رویت درج و نصب گردد.

- لازم است بعد از طبقه‌بندی، هر طبقه و دسته را با نشانه‌ها و رنگهای مشخص علامت‌گذاری کرد تا به سادگی قابل شناسایی بوده و از افشای سهوی اطلاعات محرمانه جلوگیری شود. این عملیات بایستی با دقت کامل توسط افراد مطمئن انجام شود.

- طبقه بندی دارایی ها ممکن است پس از گذشت زمان تغییر نمایند. لذا لازم است تا طی زمانبندی مناسبی که توسط واحد امنیت اطلاعات یا مرکز حراست فناوری اطلاعات صورت می پذیرد، (حداکثر در بازه های زمانی یکساله) مورد بازبینی قرار گیرند.

- مسئولیت حفاظت از دارایی های طبقه بندی شده بر عهده متصدی یا مالک دارایی اطلاعاتی بوده و قابل تفویض به غیر نمی باشد. همچنین این فرد موظف است تا آموزشها و آگاهی های لازم در خصوص حفاظت از دارایی های اطلاعاتی طبقه بندی شده را به مجموعه تحت مدیریت خود منتقل نماید.

- بهره برداری و نگهداری دارایی های طبقه بندی شده باید بگونه ای باشد که امنیت دارایی ها را مد نظر قرار دهد لذا لازم است موارد مندرج در خصوص نحوه استفاده قابل پذیرش از دارایی ها ی اطلاعاتی رعایت شود.

– در تعریف طبقه بندی و شیوه های حفاظتی باید نکات مربوط به نحوه کنترل دسترسی، اشتراک گذاری، نگهداری و انهدام یا امحاء دارایی های اطلاعاتی مشخص شده باشد.

– اطلاعات شخصی افراد حداقل باید دارای طبقه بندی خیلی محرمانه باشد.

– داده های موجود در بانک های اطلاعاتی دارای طبقه بندی بالاتر از عادی باید رمزنگاری شوند.

– لازم است برای هر دسته از اطلاعات دارای طبقه بندی، زمان نگهداری معینی در نظر گرفته شود و در پایان زمان نگهداری، در خصوص تمدید نگهداری، تغییر طبقه بندی و یا امحاء اطلاعات تصمیم گیری شود.

– معمولاً هر دسته از اطلاعات دارای یک تاریخ انقضاء می‌باشد و لذا بایستی بعد از گذشت مدتی نسبت به به روز رسانی یا امحاء اطلاعات اقدام کرد. بازه به روز رسانی با توجه به ماهیت اطلاعات و هدف از نگهداری آنها تعیین می شود و مدت نگهداری تابع مقررات بایگانی اسناد می باشد.

– تدوین روال های امحاء اطلاعات نیز الزامی است و باید به عنوان بخشی ضروری از مدیریت امنیت اطلاعات مورد توجه قرار گیرد.

فرآیند:

بر اساس الگوی مدیریت امنیت اطلاعات، امنیت دارای سه ویژگی محرمانگی، جامعیت و دسترسی پذیری است. رویه های حفاظت از اطلاعات باید به نحوی تنظیم شود که این ویژگی ها را رعایت نماید. البته

بدیهی است که در هر سازمان و با توجه به ماهیت وجودی سازمان، ممکن است یکی از ویژگی های فوق برجستگی پیدا کند. در هر حال ویژگی محرمانگی نباید در هیچ حالتی نادیده گرفته شود.

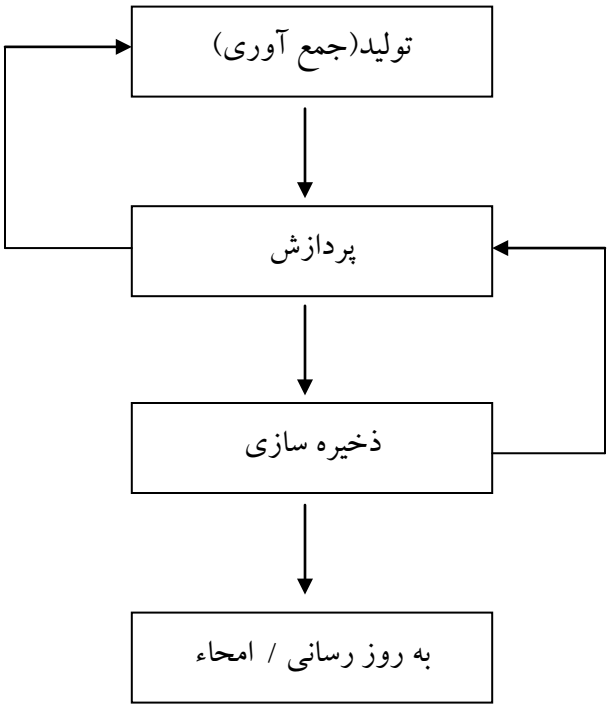
در تعیین طبقه بندی و روال های حفاظت از اطلاعات می توان از الگوی زیر استفاده نمود:

- روال طبقه بندی اطلاعات باید مکتوب شود و یا از روال معرفی شده توسط مراجع بالادستی استفاده شود.
- برای کلیه دارایی های اطلاعاتی مندرج در فهرست دارایی های اطلاعاتی که پر اهمیت یا پر ریسک هستند باید روال(های) حفاظتی خاص نوشته شود. این روال(ها) می تواند به تفکیک دارایی ها بوده و یا برای هر دسته از تجهیزات یک روال تدوین شود.
- هنگام تدوین روال مربوط به داده ها و اطلاعات شخصی یا حریم خصوصی افراد، به قوانین کشوری ناظر بر حفظ حریم خصوصی اشخاص توجه شود.
- اجرای روال(ها) از طریق ثبت وقایع و ممیزی، تحت کنترل و بازنگری قرار گیرد.

نکات فوق حداقل مواردی است که باید در طبقه بندی حفاظتی اطلاعات مورد توجه قرار گیرد. بدیهی است اجرای فرآیندهای موجود در سازمانها (با لحاظ کردن ماهیت الکترونیکی داده ها) مورد انتظار است.

توضیحات:

مفهوم اطلاعات را می توان از دیدگاه دیگری تحت عنوان چرخه عمر اطلاعات مورد توجه قرار داد. در این دیدگاه بیشتر توجه به مراحل جمع آوری، پردازش و ذخیره‌سازی داده ها و اطلاعات از لحظه ایجاد تا زمان امحا می‌باشد. این چرخه در شکل بعدی نمایش داده شده است.



چرخه عمر اطلاعات (داده)