فن آوری اطلاعات

بخش دوازدهم

مدیریت پرونده های الکترونیکی

INFORMATION TECHNOLOGY

PART 12

ELECTRONIC RECORDS MANAGEMENT

بخش تحقیق وتوسعه

زمستان ۱۳۸۳

RAH SHAHR

۷۴

Architects, Urban Design, Hydraulics & Energy Consultants گروه مهندسین مشاور معمار و شهرساز، عمران آب و انرژی

فن‌آوری اطلاعات (Information Technology)

بخش دوازدهم: مدیریت پرونده های الکترونیکی Electronic Records Management - Part 12

به کوشش:
مازیار دباغ، روزبه علی‌بیک، وحید نصیری، مرتضی امیرمیران، الهام هراتی، دلنواز موبدپور و ساناز سیدموسوی (مهندسین مشاور فن‌آوری اطلاعات، مدیریت و آموزش ره‌پردا)

حروفچینی کامپیوتری: بخش حروفچینی ره‌شهر

چاپ و صحافی: چاپ شهر

فهرست مطالب

عنوان **صفحه**

پیشگفتار

بوجود آمدن مفهوم دولت الکترویک موجب بروز تغییرات وسیعی در سازمان‌ها و مراکز دولتی و نحوه ارتباطات داخلی و خارجی آنها گردیده ، ساختار سازمان‌ها را دگرگون ساخته، موجب حذف مشاغل و پست‌های سازمانی و پیدایش مشاغل و پست‌های سازمانی جدید گشته است.

از جمله تغییرات بوجود آمده در سازمان‌ها بعد از بکارگیری دولت الکترونیک؛ تغییر در نحوه تولید، نگهداری و مدیریت اسناد و مدارک دولتی است. پیش از آغاز فعالیت دولت الکترونیک، بیشتر سازمان‌های دولتی بر نگهداری از مدارک بصورت فیزیکی و چاپ نمودن پرونده‌های الکترونیکی آنها بر روی کاغذ تکیه می‌نمودند و از سیستم‌های بایگانی، مدیریت و نگهداری اسناد به روش فیزیکی استفاده می‌نمودند.

بوجود آمدن شکل جدیدی از ارائه خدمات دولتی به شرکت‌ها و شهروندان با استفاده از فن‌آوری اطلاعات، باعث ایجاد پرونده‌های الکترونیکی گردید. این بسته به اهمیت و اطلاعات موجود در آنها ممکن است در یک یا چند سازمان دولتی مورد پردازش قرار گیرند. این امر سبب گردیده است تا مدیریت موثر پرونده‌های الکترونیکی بعنوان یکی از عوامل پشتیبانی کننده دولت‌های الکترونیکی مطرح شود.

یکی از مهمترین موضوعات موجود در مدیریت پرونده‌های الکترونیکی، بررسی صحت و جلوگیری از ایجاد تغییرات در محتوای آنها می‌باشد. با توجه به این نیاز، تا کنون اقدامات بسیار گسترده‌ای در این زمینه توسط سازمان‌های دولتی در سراسر جهان صورت گرفته است که در نتیجه آنها، سیستم‌های بسیار کاملی برای کنترل این مورد ابداع گردیده‌اند. این سیستم‌ها بدلیل پیچیدگی و گران قیمت بودن تنها در مواردی که اطلاعات بسیار حیاتی بوده و ایجاد تغییرات خواسته و ناخواسته در آنها منجر به ضایعات قابل توجهی می‌گردد، مورد استفاده قرار می‌گیرند.

در این مجموعه ابتدا به مفاهیم کلی مدیریت پرونده‌های الکترونیکی و خط‌مشی‌های مورد استفاده در آن پرداخته شده است. سپس سیستم‌های دریافت، ضبط و ایجاد پرونده‌های الکترونیکی معرفی گردیده‌اند. در مرحله بعد نکات مربوط به نگهداری پرونده‌های الکترونیکی معرفی گردیده‌اند و در انتها نیز اصول نگهداری یک سیستم پرونده‌های الکترونیکی ایمن و قابل اطمینان، بیان شده است.

این نشریه در ادامه ۱۱ نشریه قبلی فن‌آوری اطلاعات – که با موضوعات "مفاهیم کلی فن‌آوری اطلاعات"، "مدیریت فن‌آوری اطلاعات"، "تجارت الکترونیک"، "امنیت در تجارت الکترونیکی"، "تجارت بی‌سیم"، "بازاریابی الکترونیکی"، "شهرداری الکترونیکی"، "آموزش الکترونیکی"، "آموزش الکترونیکی (بخش دوم)"، "سیستم‌های اطلاعات مدیریتی ساختمان (مفاهیم و کاربردها)" و "دانشگاه الکترونیکی" تهیه شده‌اند، با همت مهندسین مشاور ره‌پردا که یکی از مشاورین متخصص در زمینه IT از گروه مهندسین مشاور ره‌شهر می‌باشد، با موضوع "مدیریت پرونده‌های الکترونیکی" منتشر می‌گردد. امید است این مجموعه بتواند آشنائی مقدماتی و اطلاعات پایه‌ای در این زمینه در اختیار خوانندگان محترم قرار دهد.

سعید شهیدی

مدیر بخش تحقیق و توسعه

مقدمه

یکی از نکاتی که در پیاده‌سازی دولت الکترونیکی از اهمیت بسیار زیادی برخوردار است، مدیریت پرونده‌های الکترونیکی (e-Records Management) می‌باشد. برای راه‌اندازی دولت الکترونیکی ابتدا باید یک بستر مناسب در سازمان های دولتی برای استفاده و مدیریت پرونده‌های الکترونیکی که برای مستندسازی و هدایت مبادلات (transactions) دولت الکترونیکی بکار می‌رود، ایجاد شود. پیاده‌سازی یک سیستم مناسب مدیریت پرونده‌های الکترونیکی نیازهای فوق را برآورده ساخته، و علاوه بر آن دارای مزایای زیر می‌باشد:

- ایجاد و مدیریت پرونده‌های الکترونیکی دقیق و قابل استناد
- حصول اطمینان از پذیرش قانونی پرونده‌های الکترونیکی
- کاهش هزینه‌های بازیابی (retrieval) اطلاعات
- کاهش اتکا بر اطلاعات کاغذی (paper records) و مشکلات بایگانی اسناد فیزیکی
- حصول اطمینان از دسترسی طولانی مدت به پرونده‌های الکترونیکی قانونی، فرهنگی، مدیریتی و تاریخی که دارای ارزش ماندگار هستند.

در قسمت اول این نشریه در مورد مفاهیم کلیدی مدیریت پرونده‌های الکترونیکی به بحث پرداخته و راهنمایی‌های کلی در مورد چگونگی مدیریت پرونده‌های الکترونیکی جهت حصول اطمینان از صحت، عدم تغییر، قابلیت دسترسی و بایگانی شدن مطمئن آنها ارائه شده است. در قسمت‌های دوم تا چهارم راهکارهایی در مورد موضوعات زیر ارائه شده است:

- دریافت (receiving)، ضبط (capturing) و ایجاد پرونده‌های الکترونیکی
- حفظ، قابل دسترس بودن، صحت و کامل بودن پرونده‌های الکترونیکی
- ایجاد یک سیستم پرونده‌های الکترونیکی دارای امنیت بالا، قابل اتکا و قابل اعتماد

در آخر هر یک از این بخش‌ها اقدامات لازم برای سازمان‌های دولتی جهت نگهداری پرونده‌های الکترونیکی با امنیت بالا، دارای صحت و قابل دسترسی آورده شده است. مطالب ارائه شده در این قسمت‌ها فنی نبوده و بجای آن بر دست‌یافتن به خروجی‌های مشخص یا عملکردهای استاندارد تمرکز شده است. راه‌حل‌های نگهداری بلندمدت

اطلاعات باید مستقل از محیط های نرم‌افزاری باشد زیرا استانداردها و قالب‌های اینگونه محیط ها در طول زمان نگهداری اطلاعات تغییر خواهند نمود.

در انتهای هر بخش خط‌مشی‌ها، فرآیندها و اقدامات فیزیکی و فن آورانه‌ای که می‌توانند در رسیدن به خروجی‌های مناسب موثر واقع شوند، ارائه شده گردیده‌اند.

روزبه علی‌بیک

مدیر بخش فن‌آوری اطلاعات و ارتباطات

مشاوره مدیریت، آموزش و فن‌آوری ره‌پردا

بوجود آمدن شکل جدیدی از ارائه خدمات دولتی به شرکت‌ها و شهروندان بـا اسـتفاده از فـن‌آوری اطلاعـات، موجب تولید پرونده‌های الکترونیکی می‌گردد که ممکن است در یک یا چند سازمان دولتی مورد پردازش قرار گیرند. اینگونه پرونده‌ها در فعالیت‌های روزمره کلیه سازمان‌های دولتی ایجاد می‌گردند. بعلاوه نوآوری‌های صورت گرفته در روش‌های کاری، فعالیت‌های مبتنی بر دانش (knowledge based activities) و استفاده کـاربردی از اطلاعـات، موجب تولید پرونده‌های الکترونیکی پیچیده می‌گردند که تنها با اسـتفاده از روش‌هـای الکترونیکـی قابـل مـدیریت هستند.

مدیریت موثر پرونده‌های الکترونیکی یکی از عوامل پشتیبانی کننده دولت‌های الکترونیک می‌باشد که مزایـای زیر را در سیستم‌های دولت الکترونیک به‌همراه دارد:

- همکاری موثر، تبادل اطلاعات و قابلیت عملکرد مشترک بین سازمان‌های دولتی
- تعیین خط مشی‌ها بر اساس تجربیات کسب شده با استفاده از ارائه اطلاعـات صـحیح و قابـل اطمینـان از اقدامات انجام گرفته و تصمیمات اتخاذ شده در گذشته
- مدیریت دانش در کلیه سازمان‌های دولتی بوسیله ارائه اطلاعات قابل اطمینان در هنگام نیاز

پیش از آغاز فعالیت دولت‌های الکترونیک، بیشتر سازمان‌های دولتی (که البته هنوز هم اکثر آنها اینکار را انجام می‌دهند.) بر نگهداری مدارک بصورت فیزیکی و چـاپ نمـودن پرونـده‌هـای الکترونیکـی آن بـر روی کاغـذ تکیـه می‌نمودند. با گسترش روش‌های الکترونیکی انجام کارها و پیچیده‌تر شدن آنها، چنین سیستم‌هـایی کـارایی خـود را کاملاً از دست می‌دهند. برای مثال:

- کارکنان، ذخیره‌سازی و چاپ مدارک مهمی را فراموش می‌نمایند
- e-mail ها بدون هیچگونه ذخیره‌سازی اولیه از روی سرور حذف می‌گردند
- مدارک مربوط به وب سایت و اینترانت (بویژه تاریخ نگارش آنها) بطور مناسبی کنترل نمی‌گردند
- تمامی خصوصیات فایل‌های چندرسانه‌ای بصورت فیزیکی قابل نگهداری نیستند

عدم موفقیت در مدیریت پرونده‌های الکترونیکی و تبادل آنها بعنوان مدارک رسمی سازمانی، به معنی از بین رفتن فرصت‌های مناسب زیادی برای بکارگیری اطلاعات مورد نیاز برای پشتیبانی از روش‌های جدید کاری در جهت دسترسی سریعتر به اطلاعات به روز و دارای کیفیت بالا می‌باشد. پرونده‌های الکترونیکی باید با ابزار الکترونیکی مدیریت گردند تا بتوان از مزایای دولت الکترونیک بیشترین بهره را کسب نمود. این مزایا عبارتند از:

- توسعه و نگهداری بهینه‌تر اطلاعات سازمانی
- ایجاد همکاری بین گروه‌های کاری و سازمانی
- ایجاد بستر لازم برای ارتقاء سطح کارمندان عادی به کارکنان حرفه‌ای
- دسترسی وسیعتر به اطلاعات سازمانی
- ارتقاء سطح خدمات عمومی و کیفیت آنها
- مدیریت اطلاعات بصورت یک دارایی که منجر به جمع‌آوری، توزیع و به اشتراک گذاری بهتر آنها می‌گردد
- ارتقاء سطح یادگیری و دانش سازمانی
- کاهش هزینه فرآیندهای کاری
- قابلیت واکنش سریع به تغییرات

۱) مفاهیم کلی و خط‌مشی‌ها

۱-۱) ارزیابی و مشخص نمودن مسائل ویژه قانونی، تجاری و سایر مواردی که به کاربرد پرونده‌های الکترونیکی مربوط می‌شوند.

ایجاد، قالب‌بندی (format) و مدیریت اطلاعات، غالباً براساس الزامات قانونی، نیازهای کاری و تجارب گذشته شکل می‌گیرند. هنگامی‌که مسئولان سازمان‌های دولتی قصد استفاده از پرونده‌های الکترونیکی را دارند، باید روش‌های کنونی نگهداری اطلاعات خود را ارزیابی نمایند تا مشخص شود که بر چه اساسی استوار می‌باشد:

- الزامات قانونی که باید در خط‌مشی‌ها، رویه‌ها و فن‌آوری‌های مورد استفاده در مدیریت پرونده‌های الکترونیکی لحاظ گردند.
- نیازهای تجاری که باید سازماندهی شده و در عین حال در حین پیاده‌سازی سیستم پرونده‌های الکترونیکی، قابل اصلاح یا جایگزینی باشند.
- روش‌های قدیمی مدیریت اطلاعات کاغذی که در هنگام پیاده‌سازی سیستم پرونده‌های الکترونیکی قابل حذف شدن هستند.

بمنظور راه اندازی سیستم در کوتاه‌ترین زمان ممکن جهت تعیین نیازمندی های مربوط به پرونده‌های الکترونیکی مسئولان سازمان‌ها برای پیاده‌سازی سیستم پرونده‌های الکترونیکی، باید از مشاورین متخصص در این زمینه استفاده نمایند.

۱-۲) اقدامات پایه‌ای مدیریت پرونده‌های الکترونیکی در مورد ارزش اطلاعات

دقیقاً مانند اطلاعات کاغذی، پرونده‌های الکترونیکی که یک سازمان دولتی ایجاد یا دریافت می‌نماید همگی دارای ارزش یکسان نیستند. هرچند تمامی اطلاعات دولتی باید به خوبی نگهداری شوند، میزان فعالیت‌ها و منابعی که یک سازمان دولتی برای مدیریت و نگهداری این اطلاعات صرف می‌نماید و شامل پرونده‌های الکترونیکی نیز می‌باشد، باید با ارزشی که اطلاعات مذکور برای سازمان‌های دولتی و شهروندان دارد، سازگار باشد. استفاده از مدیریت ریسک در این فرآیند می‌تواند مفید واقع شود. مدیریت ریسک نیازمند به موارد زیر است :

تحلیل ریسک‌های موجود، بررسی ارتباط آنها با مزایای ایجاد شده توسط سیستم، طراحی و تعیین فعالیت‌های جایگزین در هنگام بروز مشکل در فرآیند اصلی و پیاده‌سازی اقداماتی که به بهترین نحو ریسک‌های موجود را تحت

کنترل قرار می‌دهند. در هنگام استفاده از مدیریت ریسک در پرونده‌های الکترونیکی، مسائل زیر باید مورد بررسی قرار گیرند:

- اگر اطلاعاتی مفقود شده و یا غیرقابل دسترسی گردد، چه تاثیری بر روی عملکردهای سازمان خواهد داشت؟
- آیا درصورت مفقود شدن اطلاعات، سازمان یا دیگران دچار ضررهای مادی می‌گردند؟
- احتمال اینکه قانون خاصی در مورد اطلاعات بکار رفته وجود داشته باشد، به چه میزان است؟
- آیا اطلاعات برای مدت زمان طولانی مورد نیاز می‌باشند؟
- آیا اطلاعات موجود دارای ارزش فرهنگی یا تکنولوژیکی خاصی می‌باشند؟

مسئولان سازمان‌های دولتی باید توجه داشته باشند که میزان دستیابی به خروجی‌های مشخص شده در این خط‌مشی‌ها و اقداماتی که جهت رسیدن به آنها انجام می‌شوند، یک تصمیم‌گیری تجاری هستند که به ارزش اطلاعات مورد استفاده سازمان‌های دولتی و شهروندان، میزان خسارتی که در اثر فقدان آن اطلاعات ایجاد می‌شود و هزینه‌ای که برای برطرف نمودن این ریسک لازم است، بستگی دارد.

۳-۱) تمرکز بر روی سیستم و فرآیندهای کاری که منجربه ایجاد پرونده‌های الکترونیکی می‌گردند

قابلیت اطمینان و دقت فرآیندها و رویه‌هایی که برای ایجاد، ضبط و نگهداری پرونده‌های الکترونیکی مورد استفاده قرار می‌گیرند، برای نشان دادن اصالت، یکپارچگی و امنیت آنها حیاتی می‌باشد. این عوامل از فرمت یا محیط‌های پرونده‌های الکترونیکی یا فن‌آوری‌های ویژه‌ای که برای ایجاد و نگهداری آنها مورد استفاده قرار می‌گیرند بسیار مهمتر هستند. سازمان‌های دولتی اگر انتظار دارند که پرونده‌های الکترونیکی آنها در فرآیندهای قانونی یا سایر مسائل مورد پذیرش قرار گیرند، باید این فرآیندها و رویه‌ها را تعیین، تعریف و مستندسازی نمایند.

٤-۱) توجه به اهمیت آموزش

آموزش در نگهداری مناسب سیستم ایجاد و نگهداری پرونده‌های الکترونیکی توسط پرسنل بسیار مهم می‌باشد. با توجه به اینکه مسائل مدیریتی "منحصربفرد" (Unique Management) پرونده‌های الکترونیکی برخاسته از ضعف محیط‌های ذخیره‌کننده آنها و نیاز به وجود پلت‌فرم‌های تکنولوژیکی جهت دستیابی و استفاده از

این مدارک می‌باشد، اطمینان از آگاهی مسئولان دولتی از این مسائل مدیریتی بسیار مهم و قابل‌توجه است. مسئولان دولتی همچنین باید از مسئولیت‌های خود در قبال مدیریت پرونده‌های الکترونیکی آگاه بوده و به دقت وظایف خود را به انجام رسانند تا اطمینان حاصل شود که پرونده‌های الکترونیکی آنها در فرآیندهای قانونی قابل قبول بوده و در مدت نگهداری قانونی آنها، قابل دسترسی می‌باشند.

۲) دریافت، ضبط و ایجاد پرونده‌های الکترونیکی

سیستم‌هایی که یکی از عملکردهای سازمان را کنترل می‌نمایند باید قادر به ضبط یا ایجاد اطلاعات به شکل‌های مورد نیاز، که شامل محتویات اطلاعاتی و سایر موارد مورد نیاز (از قبیل صدور مجوز، حک تاریخ، امضاء الکترونیکی) هستند، باشند. همچنین در هنگام ضبط اطلاعات باید مشخصه‌ای برای آنها تعیین شود تا قابلیت دسترسی به آنها ایجاد شود. در دریافت و ارسال پرونده‌های الکترونیکی، باید اقدامات لازم جهت جلوگیری از دسترسی افراد غیرمجاز به پرونده‌های الکترونیکی و ایجاد هرگونه آسیب احتمالی صورت گیرد. عدم توانایی در انجام اینکار ممکن است باعث به خطر افتادن صحت و یکپارچگی اطلاعات شود.

۱-۲) ایجاد یا ضبط یک داده برای هر یک از مبادلات تجاری بگونه‌ای که با تمام الزامات قانونی یا سایر الزاماتی که مربوط به ساختار، محتویات و تاریخ تهیه یا ضبط اطلاعات می‌باشند، دارای مطابقت باشد.

ایجاد و مستندسازی رویه‌ها و فرآیندهای مشخص برای ایجاد، دریافت، پردازش و ذخیره‌سازی پرونده‌های الکترونیکی: در این خط‌مشی‌ها و رویه‌ها باید یک فرمت قابل قبول برای ضبط اطلاعات و یک نقطه خاص که مبادلات در آن به پایان رسیده و اطلاعات با ایمنی کامل ذخیره شوند، تعیین گردد.

برگزیدن وسیله‌ای جهت دریافت اطلاعات: سازمان‌های دولتی باید وسیله‌ای را جهت دریافت پرونده‌های الکترونیکی انتخاب نمایند. یک "وسیله" ممکن است به معنی یک سرور ویژه، یک آدرس e-mail یا یک وب سایت باشد.

۲-۲) مشخص نمودن ارسال کننده پرونده‌های الکترونیکی و حصول اطمینان از عدم تغییر آن

تعیین خط‌مشی‌ها و رویه‌هایی جهت تعیین هویت (Authenticate) ارسال کننده اطلاعات و تعیین یکپارچگی هر یک از انواع پرونده‌های الکترونیکی:

این خط‌مشی‌ها و رویه‌ها، صحت و یکپارچگی انواع مختلف پرونده‌های الکترونیکی را که توسط یک سازمان دولتی دریافت می‌شود تعیین می‌نمایند. این خط‌مشی‌ها باید بر اساس خطرات بالقوه و هزینه‌هایی که بر اثر آسیب‌دیدن یا از بین رفتن اطلاعات، عدم توزیع مناسب و به خطر افتادن آنها ایجاد می‌شوند، تعیین گردند. سازمان‌های دولتی همچنین باید خط‌مشی‌هایی را در مورد اینترنت و e-mail مطابق با ساختار سازمانی ایجاد و پیاده‌سازی نمایند.

تعیین اقدامات محفوظ برای تبادل پرونده‌های الکترونیکی که حفظ یکپارچگی اطلاعات در حین ارسال و پردازش در آن مد نظر قرار گرفته شده باشند:

این اقدامات با توجه به میزان ریسک، نیازهای کاری و فن‌آوری مورد استفاده، متفاوت خواهند بود. برای مثال به موارد زیر توجه نمایید:

- زیرساخت کلیدی عمومی (Public Key Infrastructure- PKI) که یک رمزگذاری (Encryption) بسیار پیشرفته و قدرتمند را برای مبادلات دارای ریسک زیاد فراهم می‌سازد و از امضای الکترونیکی و سایر اقدامات امنیتی که در زیر شرح داده شده‌اند، پشتیبانی می‌نماید.
  - از استاندارد Secure Sockets Layer (SSL) اغلب برای نرم‌افزارهای کاربردی تحت وب استفاده می‌شود. هرچند نرم‌افزارهای مرورگر وب باید دارای PKI باشند.
  - نرم‌افزارهای مربوط به e-mail نیز اغلب از انواع نامه‌های اینترنتی دارای امنیت بالا (S/MIME) استفاده می‌نمایند.
- حفظ حریم شخصی (Pretty Good Privacy-PGP) تکنیکی است که برای ارسال پیام‌ها با امنیت بالا با استفاده از بسته‌های کدگذاری ویژه استفاده می‌شود.
- شبکه اختصاصی مجازی (Virtual Private Network-VPN) :

از این شبکه برای برقراری روابط کاری مستمر بین چندشعبه از یک شرکت استفاده می گردد و دراین نـوع شبکه ها باید دو طرف مبادلـه کننـده اطلاعـات ازتکنولـوژی مـشابهی اسـتفاده نماینـد معمـولا شـرکتهاو سازمانهای بزرگ مانند بانکها که دارای چندین شعبه هستند و باید اطلاعات زیادی بین مراکز مختلف انهـا رد و بدل شود از این روش استفاده می‌نمایند. البته برای استفاده از این تکنولوژی دو طـرف مبادلـه کننـده اطلاعات باید از تجهیزات تولید شده توسط یک کمپانی واحد استفاده نمایند.

تکنیک‌های ویژه‌ای را می‌توان بصورت مجزا یا در ارتباط با فن‌آوری‌های اشاره شده در بالا برای کنترل اینکه آیا پرونده‌های الکترونیکی تغییر داده شده‌اند یا خیر، بکار برد. این تکنیک‌ها می‌توانند شامل انجام اقدامات ساده‌ای از قبیل ارائه یک رسید و کپی از مدرک دریافت شده به ارسال کننده، استفاده از تکنیک‌های مرسوم پردازش اطلاعات از قبیل کنترل و ویرایش فایل‌ها و استفاده از فن‌آوری Hashing به همان صورتیکه در فن‌آوری امضای الکترونیکی مورد استفاده قرار می‌گیرند و به راحتی تغییرات ایجاد شده در اطلاعات را تشخیص می‌دهند، باشند.

تعیین اقداماتی برای تعیین هویت ارسال کننده اطلاعات بر اساس خطرات بالقوه و الزامات قانونی:

ممکن است این اقدامات مطابق با نوع مبادلات صورت گرفته و نیازهای ویژه کاری تغییر پیدا کنند. برای مثال در بعضی از مبادلات نیازی به تعیین هویت نیست. بطور کلی برای احراز هویت شناسه کاربری با استفاده از رمز عبور منحصر به فرد و شماره‌های تعیین هویت (PIN) صورت می‌گیرد. استفاده از اطلاعات منحصر به فرد ویژه (برای استفاده از نام یک فامیل دور) می‌تواند دقت تعیین هویت را بالا ببرد. هر چند برای تعیین هویت در ارسال اطلاعات بسیار مهم می‌توان از روش‌های مانند امضای الکترونیکی، تشخیص صدا، نحوه امضاء نمودن هر فرد و غیره استفاده نمود.

تعیین اقداماتی برای ثبت تاریخ و زمان دریافت اطلاعات:

ثبت و نگهداری این اطلاعات برای بسیاری از مبادلات دولتی بسیار مهم می‌باشد و این اطلاعات با استفاده از یک سیستم دریافت کننده خودکار ضبط می‌گردد. اطلاعات مربوط به دریافت اطلاعات (Receipt Information)، باید به نحوی به اطلاعات دریافت شده مرتبط شود همانطوریکه یک مهر تاریخ بر روی اطلاعات کاغذی دریافت شده زده خواهد شد. برای اطلاعاتی که دارای اهمیت بالایی هستند، می‌توان از روش‌های ویژه تاریخ و ساعت‌گذاری

الکترونیک بر روی اطلاعات استفاده نمود یا اینکار را به یک سازمان ثالث و بی‌طرف واگذار نمود. ساعت‌گذاری مطمئن، یکی از دیگر ویژگی‌هایی است که در یک PKI وجود دارد.

تایید دریافت اطلاعات:

در برخی از فرآیندهای تجاری یا الزامات قانونی لازم است که دریافت مدارک تایید شوند. این تاییدیه ممکن است با توجه به نوع کاربرد آن مدرک حالت‌های مختلفی داشته باشد. برای مثال برای مدارکی که در نرم‌افزارهای کاربردی تحت شبکه ارسال می‌گردند می‌توان از یک صفحه که در آن ارسال یا تبادل اطلاعات، تایید شده و یک شماره برای ایجاد قابلیت ردیابی صادر شده است، استفاده نمود. برای محیطهای با امنیت بالا، ارسال یک تاییدیه جداگانه با استفاده از یک ساختار جداگانه پیشنهاد می‌گردد. برای مثال تایید دریافت نشانی پستی یک شخص را می‌توان با استفاده از یک پایگاه داده خارجی (خارج از برنامه کاربردی) و ارسال یک تاییدیه برای وی انجام داد.

۳-۲) مشخص نمودن هر یک از اطلاعات به شکل منحصر به فرد

تعیین روشی برای مشخص نمودن منحصر به فرد هر یک از اطلاعات:

حداقل اطلاعات لازم برای مشخص نمودن پرونده‌های الکترونیکی عبارتند از:

- نام یا شماره مشخص
- خصوصیات ایجاد کننده اطلاعات، مرجع اطلاعات یا مالک آن (واحد سازمانی)
- تاریخ و زمان دریافت یا ایجاد اطلاعات
- استفاده از اندیس برای متمایز نمودن نسخه‌های مختلف اطلاعات
- تاریخ ایجاد اخرین تغییر در اطلاعات

۳) نگهداری پرونده‌های الکترونیکی به‌شکل کامل، صحیح و قابل دسترسی

سازمان‌های دولتی برای برآورده ساختن الزامات قانونی تعیین شده یا نیازهای کاری و مدیریتی، لازم است پرونده‌های الکترونیکی خود را نگهداری نمایند. پرونده‌های الکترونیکی با الزامات نگهداری طولانی مدت یا دائمی باید بگونه‌ای نگهداری شوند که قابل دسترسی و استفاده بوده و در صورت نیاز قابل انتقال به آرشیو نگهداری

اطلاعات مرکزی باشند. سایر پرونده‌های الکترونیکی باید مطابق رویه‌های قانونی که اجازه امحاء اطلاعات را می‌دهند، از بین برده شوند.

۱-۳) حفظ یکپارچگی پرونده‌های الکترونیکی در هنگام ضبط یا ایجاد، بگونه‌ای که بصورت یک واحد مستقل قابل دسترسی، نمایش و سازماندهی باشند.

تعیین خط‌مشی‌های مدیریت پرونده‌های الکترونیکی برای ذخیره نمودن و مدیریت اطلاعات:

این خط‌مشی‌ها باید نکات زیر را پوشش دهند:

- *توصیف اینکه کدام دسته از پرونده‌های الکترونیکی تحت پوشش قرار می‌گیرند:* پرونده‌های الکترونیکی باید به انواع یا گروه‌های مختلفی که با یک روش یکنواخت قابل مدیریت باشند، تقسیم شوند. برای مثال اطلاعات ممکن است بر اساس فعالیت تجاری که باعث ایجاد آنها شده‌است (مثلاً صدور مجوز فعالیت تجاری، قوانین مربوط به محیط زیست و ...) یا بر اساس جنس آنها (اطلاعات مالی، مدارک مربوط به مشتریان، مدارک مربوط به سیستم‌های کیفیت و ...) طبقه‌بندی شوند. بعضی از اطلاعات ممکن است برای بعضی از عملکردهای سازمانی حیاتی‌تر باشند یا احتمال نیاز به آنها در اقدامات قانونی زیاد باشد یا اگر از بین رفته یا برای دیگران قابل دسترسی گردند، موقعیت سازمان به خطر افتد. چنین اطلاعاتی باید از سازماندهی مناسب‌تر و قویتری برخوردار بوده و دارای سیستم‌های محافظتی پیشرفته‌ای باشند، هرچند حتی در شرایطی که خط‌مشی‌های نگهداری اطلاعات وجود دارد، اغلب نحوه نگهداری پرونده‌های الکترونیکی را پوشش نمی‌دهند.
- *تعیین استانداردهایی برای فرمت فایل‌ها:* خط‌مشی‌هایی باید یکی از انواع تاییدشده فرمت فایل‌ها را به هر یک از انواع اطلاعات تخصیص دهند. برای نگهداری و نمایش تمامی اطلاعاتی که بر روی یک سیستم رایانه‌ای ذخیره می‌شوند، به نرم‌افزار خاصی نیاز می‌باشد. این نرم‌افزار به علت پیاده‌سازی نسخه‌های جدید اطلاعات یا بدلیل تغییر در سیستم‌های نرم‌افزاری و سخت‌افزاری همواره دستخوش تغییر خواهد بود. یک خط‌مشی تعیین کننده انواع فرمت‌های تایید شده برای ذخیره اطلاعات، انتقال اطلاعات را تسهیل نموده و نگهداری صحیح و بلندمدت اطلاعات را تضمین خواهد نمود.

- *تعیین شرح وظایف برای مسئولان مدیریت اطلاعات:* برای تهیه یک رویه موثر بمنظور نگهداری اطلاعات، لازم است که شرح وظایفی برای پیاده‌سازی اجزاء مختلف آن تعیین شود. در مورد پرونده‌های الکترونیکی، این وظایف بین اعضای گروه برنامه‌نویسی و گروه فنی که صرفاً برای راه‌اندازی سیستم‌های مدیریت پرونده‌های الکترونیکی فعالیت می‌نمایند، تقسیم می‌گردند.
- *تهیه رویه‌هایی برای ذخیره‌سازی و مدیریت پرونده‌های الکترونیکی جهت حصول اطمینان از قابلیت دسترسی به آنها در تمام طول مدت نگهداری.* (قسمت ۱-۴ را نیز ملاحظه نمایید.)
- *ایجاد سیستم‌های ذخیره‌سازی یا طبقه‌بندی اطلاعات که قادر به حفظ یکپارچگی هستند و قابلیت دسترسی به اطلاعات را فراهم نمایند:* هنگامیکه پرونده‌های الکترونیکی ایجاد و ضبط می‌گردند، لازم است در محیط‌های کنترل شده‌ای که یکپارچگی و صحت آنها حفظ می‌شود، نگهداری گردند. بعلاوه پرونده‌های الکترونیکی باید بگونه‌ای ذخیره شوند که از هرگونه تغییر یا تصحیح غیرقانونی آنها جلوگیری شده یا درصورت عدم امکان جلوگیری، این تغییرات شناسایی گردند. نرم‌افزارهای مدیریت مستندات یا مدیریت دانش، در حال حاضر قابل تهیه و استفاده می‌باشند.

۲-۳) نگهداری پرونده‌های الکترونیکی به گونه ای که توسط مراجع قانونی قابل دسترس باشند.

به منظور اینکه پرونده‌های الکترونیکی نگهداری شده در کوتاهترین زمان در مواقع مورد نیاز توسط مراجع قانونی در دسترس باشند، باید موارد زیر تدوین و در نظر گرفته شوند :

تهیه و استفاده از برنامه‌های نگهداری و ارائه پرونده‌های الکترونیکی مطابق الزامات موجود در قوانین دولتی:

بطور کلی در ساختار دولت الکترونیک برنامه‌های اجرایی تهیه می‌گردند که تمامی وظایف سازمان‌های دولتی مرکزی و سازمان‌های محلی در آن مشخص شده‌اند. سازمان‌های دولتی می‌توانند بر اساس وظایف و فعالیت‌های منحصر بفرد خود، برنامه‌های اجرایی را مطابق با رویه‌های سازمانی موجود تهیه نمایند. یک نهاد مستقل و سازمان‌یافته می‌تواند به سازمان‌های مختلف دولتی در تهیه این برنامه‌های اجرایی و تفسیر صحیح برنامه‌های کلی اعلام شده کمک کند. ممکن است این مساله در حالت استفاده از اطلاعات کاغذی در دستورالعمل‌های نگهداری اطلاعات مشخص شده باشد. البته حتی درصورت وجود چنین دستورالعمل‌هایی، اغلب مشاهده می‌شود که به پرونده‌های الکترونیکی اشاره‌ای نشده است.

تعیین استانداردهای فنی و زیرساخت‌های فن‌آوری مورد قبول و بکارگیری آنها:

استانداردهای منتخب معمولاً مطابق مشخصه‌های تعیین شده توسط سازمان‌های استاندارد ملی و بین‌المللی می‌باشند. استانداردها، به اشتراک گذاری و دسترسی به پرونده‌های الکترونیکی را تسهیل می‌نمایند.

نگهداری از پرونده‌های الکترونیکی بصورت محافظت شده (رمزدار) در مواقعی‌که خطرات امنیتی وجود دارند:

پرونده‌های الکترونیکی گاهی اوقات به دلایل امنیتی بر روی شبکه یا در حین جابجایی رمزگذاری می‌شوند. اطلاعات بسیار حساس، از قبیل آنهایی که حاوی اطلاعات شخصی مهم می‌باشند، ممکن است تا مدت‌های طولانی بصورت محافظت شده نگهداری گردند. البته لازم به ذکر است که از دست رفتن یا خراب شدن کلید رمزگشایی به معنی از بین رفتن دسترسی به اطلاعات رمزگذاری شده خواهد بود. به همین دلیل سازمان‌های دولتی باید از نگهداری پرونده‌های الکترونیکی بصورت رمزگذاری شده غیر از مواقعی که مسائل امنیتی چنین اقداماتی را ایجاب می‌کند، خودداری نمایند. اقدامات امنیتی سیستم که در بخش ۴ (نگهداری یک سیستم پرونده‌های الکترونیکی ایمن، قابل اعتماد و قابل اتکا) توضیح داده شده‌اند می‌تواند برای حفاظت اکثر پرونده‌های الکترونیکی که توسط سازمان‌های دولتی نگهداری می‌شوند، مفید واقع شود.

تهیه راه‌حل‌هایی برای نگهداری اطلاعات که به بهترین نحو نیازمندی‌های نگهداری پرونده‌های الکترونیکی را برآورده می‌سازند:

تمام راه‌حل‌های نگهداری اطلاعات، باید مدت زمانی را که اطلاعات باید نگهداری گردند مشخص نماید. برای مثال، اطلاعاتی که برای مدت زمان کوتاهی نگهداری می‌گردند (۳–۶ سال) همیشه باید در سیستمی که در آن ایجاد یا ضبط شده‌اند، نگهداری شوند. هرچند تمام راه‌حل‌هایی که ارائه می‌گردند باید مسائل زیر را پوشش دهند:

- *حفظ عملکرد صحیح پرونده‌های الکترونیکی به میزان مورد نیاز:* بسیاری از پرونده‌های الکترونیکی درصورتیکه نتوانند به‌همانگونه که در فضای کاری اصلی خود کاربرد داشتند (برای مثال قابلیت پردازش یا جستجو)، عملکرد مناسبی از خود نشان دهند، معنا و قابلیت استفاده خود را از دست خواهند داد. پس ابتدا باید مشخص شود که آیا حفظ عملکرد پرونده‌های الکترونیکی نگهداری شده ضروری می‌باشد یا خیر. اگر حفظ آن ضروری تشخیص داده شد، اطلاعات مربوطه باید بگونه‌ای ذخیره شوند که توسط فن‌آوری‌های موجود قابل پردازش و استفاده باشند.

- *حفظ ساختار و ارتباط میان اجزاء پرونده‌های الکترونیکی:* برای آشکار شدن عملکرد برخی از پرونده‌های الکترونیکی لازم است که تمامی ساختارها و روابط موجود بین اجزای آن در طول نگهداری آن، حفظ گردند. برای مثال، شاید لازم باشد حلقه‌های ارتباطاتی (link) فایل‌های ویدیویی یا فایل‌هایی که خود قسمتی از یک فایل چند رسانه‌ای می‌باشند، برای تمام مدتی که فایل اصلی نگهداری می‌شود، حفظ شوند.

ایجاد راه‌حل‌هایی که با کمترین دخالت نیروی انسانی قابل اجراء باشند:

هر قدر که یک راه‌حل مکانیزه‌تر باشد، کمتر به نیروی انسانی وابسته بوده و در نتیجه کارایی آن افزایش می‌یابد، بنابراین احتمال پیاده‌سازی آن افزایش می‌یابد.

ایجاد راه‌حل‌هایی که مستقل از محیط‌های نرم‌افزاری بوده و از نظر فن‌آوری خنثی هستند:

راه‌حل‌های نگهداری بلندمدت اطلاعات باید مستقل از محیط‌های نرم‌افزاری باشند زیرا استانداردها و قالب‌های اینگونه محیط‌ها در طول زمان نگهداری اطلاعات تغییر خواهند نمود. این راه‌حل‌ها باید بگونه‌ای طراحی شوند که اطلاعات در طول زمان نگهداری، قابل دسترسی و استفاده باشند.

تعیین الزامات نگهداری بلندمدت اطلاعات:

برخی از پرونده‌های الکترونیکی باید بصورت دائمی یا طولانی مدت نگهداری شوند و سیستم طراحی شده باید بگونه‌ای باشد که قابلیت دسترسی همیشگی به آنها را فراهم سازد. متاسفانه هیچ راه‌حل ساده فنی برای نگهداری بلندمدت پرونده‌های الکترونیکی وجود ندارد البته رویکردهایی برای حل این مشکل وجود دارد. هزینه‌ها و فوایددر هر یک از این رویکردها باید مطابق با نیازهای دسترسی داخلی و خارجی به اطلاعات سنجیده شوند. رویکردهای مختلف حفظ دسترسی طولانی مدت یا دائمی به پرونده‌های الکترونیکی، در زیر توضیح داده شده‌اند.

انتقال سیستم (Migration):

انتقال سیستم یکی از رایج‌ترین راه‌حل‌های پیشنهادی برای نگهداری پرونده‌های الکترونیکی می‌باشد. برای این کار لازم است که مدیر یک سیستم ثبت خودکار اطلاعات، پرونده‌های الکترونیکی را از سیستم خود به یک سیستم پیشرفته‌تر منتقل نماید، البته پیش از آنکه سیستم اصلی از دور خارج و غیر قابل استفاده گردد. این انتقال باید

بصورت مرحله به مرحله با استفاده از یک سیستم تناوبی و ارتقای نرم‌افزاری صورت گیرد. این رویکرد در حقیقت نوعی استراتژی است که در ارتباط با نگهداری پرونده‌های الکترونیکی تحت یک فرمت استاندارد استفاده می‌شود.

- *ذخیره نمودن پرونده‌های الکترونیکی تحت یک فرمت استاندارد:* استفاده از فرمت‌های استاندارد (پایگاه‌های داده رابطه‌ای، ASCII، PDF ، Unicode ، SGML و غیره) به کاهش دادن نرخ از دور خارج شدن فن‌آوری و نیاز به انتقال کمک می‌کند هرچند این رویکرد یک راه‌حل همیشگی نمی‌باشد زیرا استانداردها در طول زمان تغییر کرده یا جایگزین می‌گردند.
- *کپسوله‌سازی(Encapsulation – تلفیق داده‌ها با داده‌های دیگر):* کپسوله‌سازی به روش ضبط شکل و کارکرد اصلی اطلاعات به همراه Metadata (اطلاعات مربوط به اطلاعات) مورد نیاز بصورت یک شیء دیجیتالی، تحت یک فرمت قابل ارائه (Portable Format) اطلاق می‌شود. کپسوله‌سازی، انتقال سیستم را با استفاده از فرمت‌های استاندارد ترکیب می‌نماید.
- *تبدیل اطلاعات به صورت‌های دیگر:* تبدیل پرونده‌های الکترونیکی خروجی از رایانه به صورت‌های با دوام از قبیل کاغذ یا میکروفیلم تقریباً آسان است. پرونده‌های الکترونیکی را می‌توان بر روی کاغذ چاپ نمود یا بطور مستقیم و از طریق یک خروجی مخصوص بر روی یک میکروفیلم ذخیره کرده و در نهایت آن کاغذ یا میکروفیلم را به عنوان نسخه پشتیبان نگهداری نمود. این راه‌حل تنها زمانی مفید و قابل استفاده خواهد بود که تمام متادیتای مورد نیاز در محیط خروجی قابل ضبط بوده و هیچ نیاز بحرانی به دسترسی و استفاده از آن اطلاعات به شکل الکترونیکی وجود نداشته باشد.
- *شبیه‌سازی فن‌آوری‌های قدیمی:* شبیه‌سازی عبارت است از استفاده از نرم‌افزار و سخت‌افزار بگونه‌ای که یک فن‌آوری رایانه‌ای بتواند شبیه به یک فن‌آوری رایانه‌ای دیگر عمل نماید. این راه‌حل این امکان را فراهم می‌سازد که علیرغم اینکه سخت‌افزار و نرم‌افزارهای مورد استفاده با گذشت زمان تغییر می‌نمایند، پرونده‌های الکترونیکی با فرمت اصلی خود قابل نگهداری باشند. پیاده‌سازی فن‌آوری شبیه‌سازی برای سیستم‌های توسعه یافته، بسیار پیچیده و گران‌قیمت می‌باشد. تحقیقات بر روی این راه‌حل هنوز ادامه دارد.

۳-۳) جستجو و بازیابی پرونده‌های الکترونیکی در شرایط عادی در طول مدت نگهداری از اطلاعات

توسعه و استفاده از قابلیت‌های مناسب جستجو و بازیابی پرونده‌های الکترونیکی که در طول مدت نگهداری ممکن است برای مقاصد کاری قانونی مورد نیاز باشند:

این مساله باید شامل بازیابی اطلاعات در طول زمانی که اطلاعات در یک محیط near line (مانند CD ROM یا DVD ROM) یا offline قرار دارد، باشد. استفاده از چنین قابلیتی نیازمند به اندیس‌گذاری کامل و ابزار جستجوی مناسب خواهد بود.

۴-۳) تهیه نسخه‌های معتبر از پرونده‌های الکترونیکی و ارائه آنها تحت فرمت‌های قابل استفاده (مانند کپی فیزیکی برای مقاصد کاری و تمامی نیازهای عمومی)

ایجاد یا بازنگری رویه‌های دسترسی و حفاظت از حریم شخصی افراد برای پرونده‌های الکترونیکی:

چنین رویه‌هایی باید با الزامات تعیین شده توسط سازمان‌های دولتی و الزامات ویژه سایر ارگان‌های مرتبط همخوانی داشته باشند.

ایجاد روش‌هایی برای ایجاد دسترسی عمومی به پرونده‌های الکترونیکی با حفظ حریم شخصی افراد و محرمانه بودن اطلاعات:

هنگامی‌که سیستم‌ها طراحی می‌شوند، سازمان‌های دولتی باید روش‌هایی برای نحوه دسترسی که شامل مسائل مربوط به دسترسی عمومی به پرونده‌های الکترونیکی و محرمانه ماندن اطلاعات می شود را تدوین نمایند. نیازهای دسترسی عمومی به پرونده‌های الکترونیکی باید با توجه به الزامات موجود در سازمان‌های دولتی در رابطه با حفظ حریم شخصی و محرمانه ماندن اطلاعات، سنجیده شوند. به همین دلیل سازمان‌های دولتی باید تمامی اطلاعات خصوصی افراد را محرمانه نگهداشته و ابزاری خودکار برای جدا نمودن اطلاعات محرمانه از سایر پرونده‌های الکترونیکی پیش از انتشار عمومی آنها، ایجاد نمایند.

جمع‌آوری و استفاده از اطلاعات شخصی:

استفاده از اطلاعات شخصی جمع‌آوری شده، ذخیره و منتشر شده توسط دولت، غیر از مواقعی که اشخاص دانسته به این کار مبادرت می‌نمایند، می‌تواند حقوق افراد در زمینه محرمانه بودن اطلاعات خصوصی را شدیداً به مخاطره بیاندازد.

الف) اطلاعات خصوصی افراد باید:

- تنها در مواقعی جمع‌آوری و استفاده گردند که در قانون بطور ویژه اشاره شده یا برای مقاصد قانونی مورد نیاز باشند.
- تنها در راستای *اهداف* تعیین شده یا در ارتباط با آنها مورد استفاده قرار گیرد.
- تنها مواقعی مورد *استفاده* قرار گیرند که از دقت و به‌روز بودن آنها اطمینان حاصل شده باشد.
- بطور حفاظت شده نگهداری شوند.
- تنها به مدتی که لازم است نگهداری شده و سپس از بین برده شوند.

ب) بحثی که امروزه مطرح است، موضوع فروش و انتشار اطلاعات خصوصی برای مقاصد مالی می‌باشد. تمام قوانین دولت مرکزی و فرمانداری‌های محلی می‌توانند بر روی خط‌مشی‌ها تعیین شده و اقدامات صورت گرفته در خصوص حل این مساله، تاثیر بسزایی داشته باشند. متعاقباً مسئول مسائل قانونی سازمان می‌تواند از آخرین تغییرات ایجاد شده در قوانین مرتبط با این مسائل اطلاع حاصل نماید.

پ) توانایی برای ذخیره‌سازی و بازیابی الکترونیکی اطلاعات و اطلاعات جمعی(Aggregate Information) نگرانی‌های جدیدی در مورد احتمال دسترسی غیرمجاز به اطلاعات خصوصی افراد و استفاده از آنها ایجاد می نماید.

ت) سازمان‌هایی که اطلاعات خصوصی افراد را جمع‌آوری، نگهداری و استفاده می‌نمایند باید اقدامات احتیاطی برای جلوگیری از استفاده نادرست این اطلاعات را بعمل آورند. در واقع یک سازمان با قرار دادن اطلاعات خصوصی افراد در دسترس عموم، باعث ایجاد تعرض بدون مجوز به حریم شخصی آنها می‌شود.

ث) شماره ملی افراد، شماره حساب‌های بانکی و شماره کارت‌های اعتباری هرکسی باید محرمانه باشد و می‌بایست از تمامی مدارکی که به نحوی ممکن است در معرض مشاهده عموم قرار گیرد، خارج شوند. سازمان‌های دولتی باید با استفاده از قوانین دولتی منع کننده، از انتشار اطلاعات خصوصی افراد، در برابر وقوع چنین اتفاقاتی جلوگیری نمایند.

ج) این الزام باید توسط قانون بر سازمان‌های دولتی اعمال گردد،بدین ترتیب که اطلاعات خصوصی افراد نباید بدون اجازه رسمی آنها مورد استفاده قرار گیرد.

ایجاد امکان دسترسی به پرونده‌های الکترونیکی به شکلی که کاربر ترجیح می‌دهد:

بعضی از افراد به فن‌آوری مورد نیاز برای استفاده از پرونده‌های الکترونیکی دسترسی ندارند یا شکل کاغذی آن را ترجیح می‌دهند. در برخی از قوانین مدیریت پرونده‌های الکترونیکی، سازمان‌های دولتی ملزم به ایجاد دسترسی به این مدارک بصورت کاغذی به هنگام اعلام نیاز شهروندان، می‌باشند. البته بدین معنی نیست که سازمان‌های دولتی باید نسخه‌های کاغذی پرونده‌های الکترونیکی را نگهداری نمایند، بلکه به این معنی است که تمامی این سازمان‌ها باید دارای توانایی فنی برای ایجاد نسخه‌های آنها به هر دو حالت الکترونیکی و فیزیکی می‌باشند.

٤) نگهداری یک سیستم پرونده‌های الکترونیکی ایمن و قابل اطمینان

پذیرش پرونده‌های الکترونیکی برای اهداف قانونی، ممیزی و سایر موارد، مشروط به تصدیق اعتبار و صحت آنها می‌باشد که با اثبات قابلیت اعتماد سیستمی که آنها را ایجاد می‌نماید، مشخص می‌شود. سیستم‌هایی که اینگونه مدارک را ایجاد می‌نمایند باید توانایی آن را داشته باشند که این کار در سیر طبیعی کسب و کار نیز با دقت بالا و صرف مدت زمان کمی به انجام رسد. پیشنهادات زیر می‌توانند به متولیان نگهداری از مدارک در راستای تلاش برای نگهداری پرونده‌های الکترونیکی معتبر و قابل اعتمادی که به راحتی برای اهداف فوق‌الذکر مورد استفاده قرار می‌گیرند، یاری رسانند.

١-٤) حصول اطمینان از عملکرد صحیح، قابل اعتماد و پایدار سیستم در سیر طبیعی کسب و کار

تعریف و مستندسازی خط‌مشی‌ها و فرآیندهای مدیریت سیستم:

خط‌مشی‌ها و فرآیندهای نوشته شده برای هر سیستم باید دارای شرایط زیر باشند:

- توصیف روش‌های *مورد* استفاده برای ایجاد، اصلاح، تکثیر و از بین بردن مدارک
- تعریف نقش و *مسئولیت* افرادی که درگیر تهیه، نگهداری و از بین بردن مدارک می‌باشند
- فراهم ساختن بستر لازم برای کنترل کیفیت، رفع مشکلات و تعریف فرآیندهایی برای برخورد با فعالیت‌هایی که ممکن است در معرض اقدامات ناصحیح قرار گیرند
- نشان دادن اهداف و کاربردهای سیستم
- به روز بودن و قابلیت دسترسی آسان

تعیین نقش‌ها و مسئولیت‌های مدیریت سیستم و جاری ساختن اصول تفکیک وظایف (Separation of Duties)، که پس از تهیه خطمشی انجام می‌گیرند:

تفکیک وظایف به جدا ساختن نقش‌ها و مسئولیت‌ها بگونه‌ای که یک فرد نتواند به یک فرآیند حساس آسیب برساند، گفته می‌شود. برای مثال در سیستم‌های مالی، هیچ فردی نباید به تنهایی قادر باشد یک فقره چک صادر نماید، بلکه بجای آن یک نفر باید درخواستی برای پرداخت پول صادر نموده و فرد دیگری این پرداخت را تایید نماید. مثال دیگر اینکه باید اطمینان حاصل نمود که حتماً بیش از یک نفر مسئولیت پاک نمودن فایل‌های الکترونیکی منسوخ شده را عهده دار باشد.

تهیه و تدوین فرآیندهای حل مشکلات شامل گزارش‌دهی حوادث و فرآیندهای پاسخگویی به آنها:

این‌فرایندهاتضمین کننده تشخیص مشکلات سیستمی و رسیدگی به آنها می باشند، از این رو برطرف شدن مشکلات را تسریع می بخشند همچنین این فرآیندها به همراه ثبت عملکردهای سیستم و یک سیستم پشتیبانی می‌توانند در جلوگیری از به مخاطره افتادن یکپارچگی سیستم و پرونده‌های الکترونیکی آن، در برابر مشکلات بسیار موثر باشند.

سنجش کارایی سیستم شامل قابلیت اطمینان نرم‌افزار و سخت‌افزار:

استفاده از سیستمهای نرم افزاری و سخت افزاری قابل اعتماد بر روی صحت و یکپارچگی پرونده‌های الکترونیکی تاثیر بسزائی دارند. عدم عملکرد صحیح تجهیزات می‌تواند به ایجاد تغییر در محتویات پرونده‌های الکترونیکی منجر شود. اگر تجهیزات پردازش اطلاعات و نرم‌افزارهایی که برای ایجاد و ذخیره‌سازی پرونده‌های الکترونیکی موجود هستند قابل اطمینان نباشند، ممکن است یکپارچگی پرونده‌های الکترونیکی به مخاطره بیفتد. یکپارچگی پرونده‌های الکترونیکی را می‌توان با استفاده از روش‌های زیر بهبود بخشید:

- آزمودن مستمر نرم‌افزار و *سخت‌افزار* به همراه انجام فعالیت‌های مرتبط با نگهداری آنها مطابق با توضیحات سازنده
- نگهداری مستندات مرتبط با *تدارک*، نصب و نگهداری نرم‌افزار و سخت‌افزار

- نگهداری سوابق مربوط به *عملکردهای* سیستم و تهیه برنامه‌های زمانبندی برای مستند سازی قابلیت اطمینان و کارایی سیستم

سازمان‌های دولتی باید یک ارزیابی (ممیزی) فنی خارجی برای سیستم‌هایی که دارای خطرپذیری بالایی می‌باشند، در نظر گیرند. یک ارزیابی مستقل از چنین سیستم‌هایی می‌تواند قابلیت اعتماد سیستم و پرونده‌های الکترونیکی که توسط آن ایجاد می‌شوند را مستند نموده و اطمینان افکار عمومی به آنها را افزایش دهد.

نگهداری نتایج ممیزی عملکردهای سیستم:

نتایج ممیزی درصورتیکه با فرآیندها و ابزارهای مناسبی همراه شود می‌تواند در به انجام رساندن تعداد زیادی از اهداف امنیتی شامل مواردی از قبیل مسئولیت‌پذیری فردی، ترمیم مشکلات، ردیابی نفوذ به سیستم و تشخیص مشکلات ، کمک نماید. نتیجه ممیزی باید دارای اطلاعات کافی در مورد مشکلات به وجود آمده و عامل ایجاد کننده آنها باشد. همچنین می‌توان از آن در مستند نمودن قابلیت اعتماد و اطمینان یک سیستم و یکپارچگی پرونده‌های الکترونیکی ذخیره شده در سیستم، استفاده نمود. در صورت امکان، نتایج ممیزی باید توسط سیستمی که وظایف دریافت، پردازش و نگهداری مدارک را عهده‌دار می‌باشد، بصورت اتوماتیک ایجاد شود. تمامی مدارک مربوط به ممیزی‌ها باید مطابق با برنامه دولتی نگهداری مدارک، نگهداری شوند.

ارائه آموزش و پشتیبانی کافی برای حصول اطمینان از اینکه کاربر فرآیندهای سیستم را به درستی پیاده‌سازی خواهد نمود:

برنامه‌های رسمی آموزش و پشتیبانی، برای حصول اطمینان از اینکه پرسنل به خوبی از رویه‌ها و فرآیندها آگاهی داشته و آنها را پیاده‌سازی می‌نمایند، هستند. تهیه دستورالعمل‌هایی برای وارد نمودن، پردازش و بازیابی اطلاعات، آموزش پرسنل را پشتیبانی می‌کند و تلاش‌های صورت‌گرفته سازمان در زمینه آموزش پرسنل را مستندسازی می‌نماید. تهیه مستنداتی که نشان‌دهنده اعمال نظارت کافی از سوی سازمان بر روی استفاده صحیح و نگهداری پرسنل از سیستم باشد نیز، به جلوه دادن عملکرد صحیح سازمان بر اساس فرآیندهای تعریف شده کمک خواهد نمود. همچنین توصیه می‌شود که مدارک حضور پرسنل در کلاس‌های آموزشی و گواهی‌های پایان دوره آنها، نگهداری گردند.

۲-٤) حفاظت از پرونده‌های الکترونیکی برای حفظ قابلیت بازیابی سریع و دقیق آنها در طول نگهداری

تهیه یک برنامه عملکرد در هنگام بحران(Contingency Plan) شامل تهیه نسخه پشتیبان از اطلاعات، بازسازی پس از بحران (Disaster Recovery) و عملیات اضطراری:

برنامه عملکرد در هنگام بحران، می‌تواند به سازمان‌های دولتی در بازگشت به فعالیت‌های عادی خود پس از بروز یک بحران کمک نماید. این برنامه باید شامل نحوه تهیهBackup از اطلاعات و بازیابی آنها برای جلوگیری از، نابودشدن پرونده‌های الکترونیکی باشد.

ایجاد کنترل‌های لازم بر روی دقت و صحت ورود و خروج اطلاعات:

دقت و صحت ورودی و خروجی یک سیستم برای نشان دادن یکپارچگی و صحت پرونده‌های الکترونیکی که توسط آن سیستم ایجاد می‌گردد بسیار حیاتی می‌باشد.

پیاده‌سازی سیستم‌های کنترل کننده رسانه (Media):

شامل اقدامات مختلفی از قبیل نگهداری و طبقه‌بندی استاندارد گزارش پیگیری‌ها و اعمال کنترل‌های فیزیکی و فنی لازم بر روی دیسکت‌ها، Tapeها و سایر رسانه‌ها می‌باشد. میزان کنترل رسانه‌ها به پارامترهای مختلفی بستگی دارد که عبارتند از نوع اطلاعات، کمیت رسانه‌ها و خصوصیات فضای کاربری. رسانه‌هایی که برای ذخیره سازی پرونده‌های الکترونیکی حساس یا دارای خطرپذیری بالا استفاده می‌شوند، نیاز به کنترل بیشتری نسبت به سایر رسانه‌ها دارند.

تهیه نسخه پشتیبان بر طبق روال‌های از پیش تعیین شده:

بسیار مهم است که از نرم‌افزارها و اطلاعات به ویژه اگر اطلاعات مربوط به پرونده‌های الکترونیکی باشد، نسخه پشتیبان تهیه نمود. تناوب تهیه نسخه پشتیبان به میزان تغییرات صورت گرفته بر روی اطلاعات و اهمیت آنها بستگی دارد. مشاوره لازم باید به مدیران برنامه‌های نرم‌افزاری برای تعیین یک برنامه مناسب جهت تهیه نسخه پشتیبان از نرم‌افزارهای مورد استفاده، ارائه شود. نسخه‌های پشتیبان باید برای تعیین قابلیت کاربرد آنها و ذخیره شدن در مکانی مناسب و دور از سیستم در هنگام وقوع بحران، مورد بررسی قرار گیرند

۳-٤) محدود نمودن دسترسی به سیستم برای افراد مجاز و برای مقاصد مجاز

ایجاد کنترل‌های امنیتی فیزیکی و محیطی:

تهدیدهای فیزیکی و محیطی می‌توانند بر روی پرونده‌های الکترونیکی تاثیرگذار باشند، بخصوص مدارکی که در محیط‌های فیزیکی شکننده ذخیره می‌گردند. برنامه امنیتی یک سازمان باید دسترسی فیزیکی و شرایط محیطی مناسب در فضای کاری، مراکز اطلاعاتی یا اتاق‌هایی که حاوی سخت‌افزار (از قبیل سرورهای LAN)، سیم‌کشی اصلی، خدمات پشتیبانی (شبکه اصلی برق)، محل نگهداری از نسخه‌های پشتیبان و بسیاری از عناصر دیگر می‌باشند، را تعریف کند. در این برنامه همچنین باید نحوه برخورد با مشکلاتی از قبیل آتش‌سوزی، خرابی تجهیزات و بوجود آمدن مشکل در ساختار معین شود.

ایجاد بستر مناسب برای تعیین و کنترل هویت:

اقدامات فنی برای جلوگیری از ورود افراد غیر مجاز (یا فرآیندهای غیرمجاز) وجود دارد که باید انجام شود. این اقدامات نه تنها در مبادلاتی که بر روی شبکه انجام می‌شوند بسیار ملموس هستند بلکه همانگونه که در بالا نیز بحث گردید، در مدیریت سیستم‌ها و حصول اطمینان از امنیت پرونده‌های الکترونیکی نیز بسیار حائز اهمیت هستند. سیستم‌ها باید قادر باشند تا کاربران را با استفاده از یک شناسه کاربری (ID) منحصر به فرد، شناسایی و تفکیک نموده و هر فعالیت موجود در سیستم را به یک کاربر خاص با استفاده از شناسه کاربری مرتبط سازد. شناسه‌های کاربری تنها باید به کاربران فعال مجاز، اختصاص یافته باشند. تعیین هویت یکی از ابزاری است که صحت هویت یک کاربر را کنترل می‌نماید. بطور کلی سه روش برای تعیین هویت یک کاربر وجود دارد که می‌توانند بصورت جداگانه یا ترکیبی مورد استفاده قرار گیرند:

- *استفاده از مشخصه‌ای که تنها یک فرد از آن اطلاع دارد:* یک رمز (بعنوان مثال یک کلمه عبور، شماره مشخصه فردی یا یک کلید رمزنگاری)
- *استفاده از چیزی که منحصراً در مالکیت یک فرد قرار دارد:* یک نشانه (برای مثال کارت‌های هوشمند)
- *استفاده از خصوصیات فردی:* ویژگی‌هایی از قبیل اثر انگشت و خصوصیات صدا

ایجاد سیستم کنترل دسترسی:

دسترسی به توانایی انجام کاری با استفاده از رایانه اتلاق می‌شود. سیستم‌های کنترل دسترسی ابزار سیستمی هستند که دسترسی با استفاده از آنها مجاز یا ممنوع می‌گردد. در این سیستم‌ها می‌توان سطح دسترسی هر گروه از کاربران به هر گروه از اطلاعات موجود بر روی شبکه‌های رایانه‌ای را از پیش تعیین نمود. بطور کلی سازمان‌ها باید رویه سیستم دسترسی خود را بر اساس اصل کمترین مزیت (Least Privilege) تعریف نمایند. کمترین مزیت به ارائه امکانات به کاربران تنها هنگامی که دسترسی به سیستم برای انجام فعالیت‌های رسمی آنها ضروری باشد، اتلاق می‌شود. برای مثال متصدیان وارد نمودن اطلاعات احتیاجی به استفاده از گزارش‌های تحلیلی از پایگاه داده‌های خود ندارند. سازمان‌ها باید دسترسی به منابع خود را بر اساس معیارهای زیر کنترل نمایند:

- *شناسه کاربری:* برای حفظ شرایط پاسخگویی فردی
- *نقش‌ها:* کارهای محول شده به هر یک از کاربران
- *موقعیت:* بر اساس واحدهای سازمانی یا بصورت فیزیکی
- *زمان:* محدود نمودن دسترسی به ساعاتی از روز یا روزهایی از هفته. برای مثال استفاده از فایل‌های شخصی محرمانه تنها باید در طول ساعت کار اداری مجاز باشد.
- *مبادلات:* دسترسی به یک فایل بخصوص که تنها باید در طول یک فرآیند خاص مجاز باشد. به کاربری که بر روی چنین فایل‌هایی کار می‌کند یک دسترسی خواندن اطلاعات داده شده که پس از اتمام آن فرآیند خاص، این دسترسی نیز قطع می‌شود.

ایجاد مکانیزم‌های کنترل دسترسی از بیرون:

این مکانیزم‌ها در حقیقت ابزاری برای کنترل نمودن تعاملات بین سیستم و افراد، سیستم و خدمات خارجی می‌باشند. هنگامی که کنترل دسترسی ایجاد می‌گردد، سازمان باید مکانیزم‌های زیر را بکار گیرد:

- *رمزگذاری:* با استفاده از یک کلید رمزگشای مناسب می‌توان اطلاعات رمزگذاری شده را باز و استفاده نمود.
- *گذرگاه‌های ایمن (Secure Gateways) یا Firewallها :* گذرگاه‌های ایمن، دسترسی بین دو شبکه، که اغلب بین یک شبکه خصوصی و یک شبکه بزرگ‌تر می‌باشد را فیلتر می‌نمایند.

- *تعیین هویت بر اساس میزبان (Host) کاربر:* این نوع تعیین هویت بجای اینکه هویت خود کاربر را کنترل نماید، اجازه دسترسی را براساس هویت میزبانی که دسترسی از طرف کاربران مربوط به آن درخواست شده است صادر می‌نماید. بسیاری از برنامه‌های کاربردی تحت شبکه که امروزه استفاده می‌شوند از این نوع تعیین هویت برای تعیین مجاز بودن دسترسی استفاده می‌نمایند.

دستورالعمل ایجاد امنیت، صحت، یکپارچگی و قابلیت دسترسی پرونده‌های الکترونیکی

قوانین عمومی تعیین و ارزیابی الزامات قانونی، کاری و سایر الزاماتی که در مورد پرونده‌های الکترونیکی مصداق پیدا می‌نمایند، تعیین اقدامات لازم برای مدیریت پرونده‌های الکترونیکی، براساس ارزش آنها، توجه خاص بر روی سیستم‌ها و فرآیندهای کاری که پرونده‌های الکترونیکی ایجاد می‌نمایند، آموزش بسیار ضروری می‌باشد.	
دریافت، ضبط و ایجاد پرونده‌های الکترونیکی	
خروجی‌ها	**پیاده‌سازی و راه‌اندازی**
ایجاد یا ضبط یک مدرک الکترونیکی برای هر یک از مبادلات کاری که با تمامی الزامات قانونی و سایر الزامات مربوط به ساختار، محتویات و زمان ایجاد یا ضبط مدرک الکترونیکی دارای مطابقت می‌باشند.	تهیه و مستند نمودن رویه‌ها و فرآیندهایی برای دریافت، ایجاد، پردازش و بایگانی نمودن پرونده‌های الکترونیکی انتخاب تجهیزات دریافت اطلاعات
تعیین هویت ارسال کننده پرونده‌های الکترونیکی و حصول اطمینان از اینکه در آنها تغییراتی داده نشده است.	تعیین خط‌مشی‌ها و فرآیندهایی برای تعیین هویت ارسال کننده مدرک الکترونیکی و مشخص نمودن یکپارچگی هر یک از انواع آنها مشخص نمودن اقداماتی برای ایجاد امنیت در هنگام ارسال پرونده‌های الکترونیکی، از قبیل حفظ یکپارچگی مدارک در حین ارسال یا پردازش آنها تعیین اقداماتی برای تعیین هویت ارسال کننده با توجه به خطرات احتمالی و الزامات قانونی تعیین اقداماتی برای مستند نمودن روز و ساعت دریافت مدارک
مشخص نمودن منحصر بفرد بودن هر مدرک	تعیین یک روش برای مشخص نمودن منحصر بفرد بودن هر مدرک

حفظ قابلیت دسترسی، صحت و کامل بودن پرونده‌های الکترونیکی	
خروجی‌ها	**پیاده‌سازی و راه‌اندازی**
حفظ یکپارچگی پرونده‌های الکترونیکی در هنگام ایجاد یا ضبط آنها بگونه‌ای که آنها بصورت یک واحد قابل دسترسی، نمایش و مدیریت باشند.	تعیین خط‌مشی‌های مدیریت پرونده‌های الکترونیکی و مستندسازی خط‌مشی سازمان در مورد مدیریت و ذخیره‌سازی اطلاعات ایجاد سیستم‌های ذخیره‌سازی کنترل شده اطلاعات مطابق با الزامات قانونی توصیف الزامات نگهداری پرونده‌های الکترونیکی
نگهداری پرونده‌های الکترونیکی به نحوی که در حداقل مدت زمان قانونی نگهداری که توسط دولت اعلام می‌گردد قابل دسترسی باشند.	دریافت و استفاده از برنامه نگهداری و سازماندهی مدارک مطابق با قوانین دولتی یا محلی پذیرش و استفاده از استانداردهای فنی مورد ترجیح سازمان‌های دولتی نگهداری از پرونده‌های الکترونیکی بصورت رمزگذاری شده تنها به مدتی که مسائل امنیتی ایجاب می‌نمایند.
جستجو و بازیابی پرونده‌های الکترونیکی در روند طبیعی کسب و کار برای تمامی نیازهای کاری در حداقل زمان قانونی نگهداری از اطلاعات	ایجاد توانایی‌های کافی برای جستجو و بازیابی برای حصول اطمینان از اینکه پرونده‌های الکترونیکی برای تمامی مقاصد قانونی در تمام زمان نگهداری آنها قابل بازیابی هستند.
تهیه نسخه‌های صحیح از پرونده‌های الکترونیکی و ارائه آنها در یک قالب قابل استفاده، شامل نسخه‌های فیزیکی، برای اهداف کاری و تمامی نیازهای دسترسی عمومی	ایجاد یا بازنگری رویه‌های دسترسی و حفاظت از حریم شخصی افراد برای پرونده‌های الکترونیکی ایجاد روش‌هایی برای ایجاد دسترسی عمومی به پرونده‌های الکترونیکی و حفظ حریم شخصی افراد و محرمانه بودن اطلاعات ایجاد امکان دسترسی به پرونده‌های الکترونیکی به شکلی که کاربر ترجیح می‌دهد

ایجاد سیستم‌های پرونده‌های الکترونیکی ایمن، قابل اطمینان و قابل اعتماد	
خروجی‌ها	**پیاده‌سازی و راه‌اندازی**
حصول اطمینان از اینکه سیستم به شکلی دقیق، قابل اطمینان و پایدار در سیر طبیعی کسب و کار عمل می‌نماید.	تعریف و مستندسازی خط‌مشی‌ها و رویه‌های مدیریت سیستم تعیین نقش‌ها و مسئولیت‌های مدیریت سیستم و به اجرا گذاشتن اصل تفکیک وظایف پس از تهیه خط‌مشی‌های مکتوب تهیه و استفاده از رویه‌های رفع مشکلات، شامل گزارش‌دهی حوادث و فرآیندهای پاسخگویی به آنها سنجش کارایی سیستم، شامل قابلیت اطمینان نرم‌افزار و سخت‌افزار نگهداری نتایج ممیزی عملکردهای سیستم توسط یک سیستم یا فرآیندهای کاربردی یا کاربر ارائه آموزش و پشتیبانی کافی برای حصول اطمینان از اینکه کاربر فرآیندهای سیستم را به درستی پیاده‌سازی خواهد نمود
حفاظت از پرونده‌های الکترونیکی برای حفظ قابلیت بازیابی سریع و دقیق آنها در طول نگهداری	تهیه یک برنامه عملکرد در هنگام بحران، شامل تهیه نسخه پشتیبان، بازسازی پس از بحران و عملیات اضطراری ایجاد کنترل‌های لازم بر روی دقت و صحت ورود و خروج اطلاعات پیاده‌سازی سیستم‌های کنترل کننده رسانه (Media)
محدود نمودن دسترسی به سیستم برای افراد مجاز و برای مقاصد مجاز	ایجاد کنترل‌های امنیتی فیزیکی و محیطی ایجاد بستر مناسب برای تعیین و کنترل هویت ایجاد سیستم کنترل دسترسی ایجاد مکانیزم‌های کنترل دسترسی از بیرون

نتیجه‌گیری

با توجه به شرایط جهانی و پیشرفت سریع فن‌آوری، بکارگیری دولت الکترونیک اجتناب ناپذیر است و بکارگیری این مفهوم زمانی موفقیت آمیز خواهد بود که برنامه‌ای جامع جهت بکارگیری آن تدوین گردد و در این برنامه کلیه اهداف بلندمدت و کوتاه‌مدت استفاده از فن‌آوری اطلاعات در امور دولتی به شکل دولت الکترونیک، جزئیات آن و نحوه دستیابی به زیرساخت‌های لازم سیستم‌های اطلاعاتی معین و مشخص گردد.

استفاده از سیستم‌های مورد نیاز دولت الکترونیک از جمله مدیریت پرونده‌های الکترونیکی نیز نیازمند ایجاد سیستم‌های ایجاد کنترل امنیتی کارآمد و تعیین سطوح دسترسی مشخص و معین می‌باشد، زیرا فقط در این صورت است که کاربران دولت الکترونیک با اطمینان خطر از آن استفاده خواهند نمود و این اعتماد در موفقیت آن موثر است.

واژه‌نامه

Accessibility:

به ویژگی از پرونده‌های الکترونیکی یا اطلاعاتی که مربوط به در دسترس بودن آنها برای استفاده مناسب طی یک بازه زمانی معین می‌باشد، اتلاق می‌گردد. در مورد پرونده‌های الکترونیکی قابلیت دسترسی شامل وجود امکانات فنی مورد نیاز و Metadata (اطلاعاتی که مشخص کننده چگونگی، زمان، شخص ایجاد کننده پرونده‌های الکترونیکی و فرمت آن‌ها می‌باشند.) برای دستیابی، استفاده و درک محتویات آنها می‌باشد.

Alphanumeric:

به ترکیبی از تمامی حروف و اعداد از صفر تا ۹ اتلاق می‌شود. از آن برای ترکیب نمودن حروف و اعداد استفاده می‌شود چراکه تمامی برنامه‌ها بطور یکسان با آنها برخورد نموده و جدا از علائم مربوط به آئین نگارش در نظر گرفته می‌شوند. برای مثال بسیاری از سیستم‌های عامل به ما اجازه استفاده از حروف و اعداد در نام‌گذاری فایل را می‌دهند ولی نمی‌توان از علائم مربوط به نگارش در آنها استفاده نمود.

Asymmetric cryptography (crypto system):

یک سیستم رمزنگاری می‌باشد که در آن از دو ترکیب حرفی– عددی که بصورت محاساباتی به هم مرتبط هستند و معمولاً با نام یک زوج کلید (key pair) شناخته می‌شود، استفاده می‌گردد. از کلید خصوصی، که تنها در اختیار مالک آن قرار دارد،برای ایجاد یک امضای الکترونیکی یا رمزگشا، و کلید دیگر یا کلید عمومی که در اختیار سایر افراد تعیین شده نیز قرار دارد، برای تایید امضای الکترونیکی یا رمزگشا مورد استفاده قرار می‌گیرد.

Authenticity:

به روش‌های ارزیابی صحت پرونده‌های الکترونیکی گفته می‌شود. ارزیابی صحت با مساله یکپارچگی دارای ارتباط تنگاتنگی می‌باشد.

Biometrics:

در سیستم‌های امنیتی رایانه‌ای، biometric به تکنیک‌های ارزیابی صحت، که براساس ویژگی‌های فیزیکی قابل اندازه‌گیری که بطور اتوماتیک قابل کنترل هستند، اتلاق می‌شود. به عنوان نمونه می‌توان به تحلیل‌های رایانه‌ای اثر انگشت یا صدا گفته می‌شود.

Checksum:

یک برنامه ساده شناسایی خطا می‌باشد که در آن هر پیام ارسالی با یک مقدار عددی همراه می‌گردد که بر اساس بیت‌های پیام محاسبه می‌گردد. ایستگاه دریافت کننده، فرمول بکار رفته را مجدداً بر روی پیام دریافت شده اعمال می‌نماید تا اطمینان حاصل نماید که مقدار عددی همراه پیام تغییر نیافته باشد. در غیر اینصورت، دریافت کننده می‌تواند فرض کند که پیام تغییر یافته است.

Cryptographic:

به رمزنگاری‌هایی مربوط می‌باشد که (۱) علوم ریاضی مورد استفاده برای حفظ سری بودن و تعیین صحت اطلاعات بوسیله جایگزین نمودن شکل تغییر یافته اطلاعات بجای اصل آنها، بگونه‌ای که تنها توسط شخصی که دارای الگوریتم یا کلید رمزگشایی مناسبی باشد مجدداً به حالت اصلی قابل تبدیل می‌باشد. (۲) یک مجموعه از الزامات که تمامی اصول، ابزار و روش‌های ایجاد تغییر شکل اطلاعات برای پنهان ساختن محتویات اطلاعاتی آن، جلوگیری از ایجاد تغییرات ردیابی نشده و استفاده‌های غیرمجاز آن می‌باشد را در بر می‌گیرد.

Cryptographic keys:

به اطلاعات مورد استفاده برای رمزگذاری یا رمزگشایی یک پیام یا اطلاعات گفته می‌شود.

Electronic record:

به معنی هر مدرک ایجاد شده، ذخیره شده، ارسال و یا دریافت شده بصورت غیرفیزیکی که حاوی یا مرتبط با فن‌آوری‌های الکتریکی، دیجیتال، مغناطیسی، بی‌سیم، نوری، الکترومغناطیسی و سایر فن‌آوری‌هایی از این قبیل می‌باشند، گفته می‌شود.

Hashing:

به ایجاد مقادیر درهم ریخته برای دسترسی به اطلاعات یا برای امنیت گفته‌می‌شود. یک hash از خود متن کوچکتر بوده و توسط یک فرمول بگونه‌ای ایجاد می‌گردد که امکان اینکه از متن دیگری عددی مشابه ایجاد شود، بسیار کم است. hashها نقش مهمی را در سیستم‌های امنیتی ایفا می‌نمایند. آنها در این سیستم‌ها برای حصول اطمینان از اینکه پیام ارسال شده بدون ایجاد هیچگونه بازتابی دچار تغییر نشود، مورد استفاده قرار می‌گیرند. ارسال کننده اطلاعات یک hash برای پیام مورد نظر ایجاد می‌نماید، آنرا رمزگذاری کرده و به همراه پیام ارسال می‌نماید. دریافت کننده هم پیام و هم hash را رمزگشایی نموده و یک hash دیگر از پیام دریافت شده تهیه و آنرا با hash اولیه مقایسه می‌نماید. اگر آن دو یکی بودند، به احتمال قریب به یقین پیام ارسال شده دست نخورده باقی‌مانده است.

Integrity:

ویژگی است که نشان می‌دهد محتویات یک مدرک تغییر ننموده، حذف و یا جابجا نشده است. بعلاوه یکپارچگی دقت و صحت محتویات یک مدرک را نشان می‌دهد. سندیت و یکپارچگی هر دو از محدوده مسائل قانونی نشات می‌گیرند و نقش مهمی در پذیرش قانونی پرونده‌های الکترونیکی ایفا می‌نمایند.

Pretty Good Privacy (PGP):

یک تکنیک برای رمزگذاری نمودن پیام‌ها می‌باشد که توسط فیلیپ زیمرمن (Philip Zimmerman) ابداع گردید. PGP یکی از مرسوم‌ترین روش‌های محافظت از پیام‌ها بر روی اینترنت می‌باشد، به این دلیل که موثر بوده، استفاده از آن آسان می‌باشد و رایگان است. PGP بر اساس روش کلید عمومی تهیه شده است که در آن دو کلید که یکی از آنها یک کلید عمومی است که شما آنرا به اشخاصی که می‌خواهید از آنها پیامی را دریافت نمایید، اختصاص می‌دهید. کلید دیگر یک کلید اختصاصی می‌باشد که شما از آن برای رمزگشایی پیام‌های دریافتی استفاده می‌نمایید. برای رمزگذاری نمودن یک پیام با استفاده از PGP، یک بسته رمزگذاری PGP مورد نیاز می‌باشد که بصورت رایگان از منابع گوناگونی قابل دسترسی می‌باشد.

Plaintext:

در رمزنگاری متون ساده به پیام‌هایی اتلاق می‌شود که رمزگذاری نشده و بنابراین به راحتی قابل خواندن می‌باشد.

Private Key:

یک کلید رمزنگاری است که تنها در اختیار مالک آن قرار دارد. از کلیدهای اختصاصی مـی‌تـوان در ایجـاد امـضای الکترونیکی یا رمزگشایی پیام‌ها یا فایل‌ها استفاده نمود.

Public Key Infrastructure (PKI):

به معماری، سازمان‌دهی، تکنیک‌ها، اقدامات و رویه‌هایی که مجموعاً پیاده‌سازی و عملکرد یک سیستم غیرمتقـارن استاندارد را پشتیبانی می‌نمایند، اتلاق می‌شود. زیرساخت کلید عمومی متشکل از سیستم‌هایی است که در خصوص پیاده‌سازی امضای الکترونیکی، رمزنگاری و تعیین هویت همکاری می‌نمایند.

Security:

به حفاظت از دارایی‌های اطلاعاتی، شامل کنترل‌های فیزیکی و تکنیکـی بـر روی دسترسـی بـه اطلاعـات اتـلاق می‌شود. سیستم امنیتی دارای اجزاء تکنیکی، فیزیکی و فرآیندی می‌باشد.

Secure Sockets Layer (SSL):

پروتکلی است که توسط شرکت Netscape برای ارسال مدارک خصوصی از طریق اینترنت ایجاد گردیـد. SSL بـا استفاده از یک کلید اختصاصی برای رمزگذاری نمودن اطلاعاتی که با استفاده از ارتباط SSL ارسال می‌گردند، کـار می‌کند. هم Netscape Navigator و هـم Internet Explorer از SSL پـشتیبانی مـی‌نماینـد و بـسیاری از وب سایت‌ها از این پروتکل برای محرمانه نگهداشتن اطلاعات از قبیل شماره کارت اعتباری استفاده می‌نمایند. براسـاس قرارداد، آدرس صفحات وبی که نیازمند به یک ارتباط SSL هستند، بجای :http با :https آغاز می‌شوند.

Smart card:

یک کلید سخت‌افزاری است که دارای یک یا چند IC می‌باشد که توابع رمزنگاری توسط آنها بکارگرفته می‌شـوند و دارای مقاومت زیادی در برابر ایجاد تغییرات بدون مجوز دارند.

S/MIME:

خلاصه شده Secure/MIME می‌باشد که نسخه جدیدی از پروتکل MIME است که رمزگذاری بر روی پیام‌ها را پشتیبانی می‌نماید. S/MIME براساس فن‌آوری رمزنگاری کلید عمومی کشور آفریقای جنوبی ایجـاد شـده اسـت.

انتظار می‌رود که S/MIME بطور گسترده‌ای پیاده‌سازی گردد. در این حالت کاربران می‌توانند یک e-mail حفاظت شده را برای دیگری ارسال نمایند حتی در صورتیکه از برنامه‌های ارسال و دریافت e-mail، مختلفی استفاده نمایند.

Token:

یک ابزار سخت‌افزاری کوچک می‌باشد که از آن برای حفظ امنیت در ذخیره سازی اطلاعات مربوط بـه شناسـایی و تعیین هویت کاربران از قبیل کلید اختصاصی، استفاده می‌گردد.

Trustworthy system:

سخت‌افزار، نرم‌افزار و عملکردهای رایانه‌ای هستند که بطور قابل قبولی در مقابل سوء استفاده و نفوذ مصون هستند؛ قابلیت دسترسی، قابلیت اطمینان و عملکرد صحیح را تا حد قابل قبولی ایجاد می‌نمایند؛ تا حد زیادی بـرای اجـرای عملکردهای مورد نظر مناسب هستند و خط‌مشی‌های امنیتی قابل اعمال را تقویت می‌نماینـد. یـک سیـستم قابـل اعتماد، لزوماً یک سیستم قابل اطمینان نیست.

Virtual Private Network (VPN):

یک شبکه است که با ایجاد ارتباط بین nodeها بوسیله سیم معمولی ایجاد می‌شود. برای مثال سیستم‌های مختلفی وجود دارند که توانایی احداث شبکه‌ها را با استفاده از اینترنت به عنوان وسیله‌ای جهت انتقال اطلاعات، بـرای شـما ایجاد می‌نمایند. این سیستم‌ها از رمزنگاری و سایر مکانیزم‌های امنیتی برای حصول اطمینان از اینکه تنهـا کـاربران مجاز به شبکه دسترسی داشته و اطلاعات توسط افراد غیرمجاز قابل جابجایی نباشد، استفاده می‌نمایند.

منابع و مآخذ :

1- Electronic Records Management (Guidelines for State Government) - A National Electronic Commerce Coordinating Council E-Sign Policy Workgroup Paper (Exposure Draft)
2- E-government policy framework for electronic records management
3- www.GeorgiaArchives.org
4- National Archives the challenge of electronic records management by L. Nye Stevens