INSO

18959
1st.Edition
2015

جمهوری اسلامی ایران
Islamic Republic of Iran

سازمان ملی استاندارد ایران
Iranian National Standardization Organization

استاندارد ملی ایران
۱۸۹۵۹
چاپ اول
۱۳۹۳

مدیریت مدارک- اطلاعات ذخیره‌شدهٔ الکترونیکی- توصیه‌هایی برای قابلیت اعتماد و اعتبار

Document management- Information stored electronically- Recommendations for trustworthiness and reliability

ICS: 37.080

به نام خدا

آشنایی با سازمان ملی استاندارد ایران

مؤسسهٔ استاندارد و تحقیقات صنعتی ایران به موجب بند یک مادهٔ۳ قانون اصلاح قوانین و مقررات مؤسسهٔ استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱ تنها مرجع رسمی کشور است که وظیفه تعیین، تدوین و نشر استانداردهای ملی (رسمی) ایران را به عهده دارد.

نام مؤسسه استاندارد و تحقیقات صنعتی ایران به موجب یکصد و پنجاه و دومین جلسه شورای عالی اداری مورخ ۹۰/۶/۲۹ به سازمان ملی استاندارد ایران تغییر و طی نامه شماره ۲۰۶/۳۵۸۳۸ مورخ ۹۰/۷/۲۴ جهت اجرا ابلاغ شده است .

تدوین استاندارد در حوزه‌های مختلف در کمیسیون‌های فنی مرکب از کارشناسان سازمان، صاحب‌نظران مراکز و مؤسسات علمی، پژوهشی، تولیدی و اقتصادی آگاه و مرتبط انجام می‌شود وکوششی همگام با مصالح ملی و با توجه به شرایط تولیدی، فناوری و تجاری است که از مشارکت آگاهانه و منصفانهٔ صاحبان حق و نفع، شامل تولیدکنندگان، مصرف‌کنندگان، صادرکنندگان و واردکنندگان، مراکز علمی و تخصصی، نهادها، سازمان‌های دولتی و غیر دولتی حاصل می‌شود. پیش‌نویس استانداردهای ملی ایران برای نظرخواهی به مراجع ذی‌نفع و اعضای کمیسیون‌های فنی مربوط ارسال می‌شود و پس از دریافت نظرها و پیشنهادها در کمیتهٔ ملی مرتبط با آن رشته طرح و در صورت تصویب به عنوان استاندارد ملی (رسمی) ایران چاپ و منتشر می‌شود.

پیش‌نویس استانداردهایی که مؤسسات و سازمان‌های علاقه‌مند و ذی‌صلاح نیز با رعایت ضوابط تعیین‌شده تهیه می‌کنند درکمیتهٔ ملی طرح و بررسی و درصورت تصویب، به عنوان استاندارد ملی ایران چاپ و منتشر می‌شود. بدین ترتیب، استانداردهایی ملی تلقی می‌شوند که بر اساس مفاد نوشته شده در استاندارد ملی ایران شمارهٔ ۵ تدوین و در کمیتهٔ ملی استاندارد مربوط که سازمان ملی استاندارد ایران تشکیل می‌دهد به تصویب رسیده باشد.

سازمان ملی استاندارد ایران از اعضای اصلی سازمان بین‌المللی استاندارد (ISO)[1] ،کمیسیون بین‌المللی الکتروتکنیک (IEC)[2] و سازمان بین‌المللی اندازه‌شناسی قانونی (OIML)[3] است و به عنوان تنها رابط[4] کمیسیون کدکس غذایی (CAC)[5] در کشور فعالیت می‌کند. در تدوین استانداردهای ملی ایران ضمن توجه به شرایط کلی و نیازمندی‌های خاص کشور، از آخرین پیشرفت‌های علمی، فنی و صنعتی جهان و استانداردهای بین‌المللی بهره‌گیری می‌شود .

سازمان ملی استاندارد ایران می‌تواند با رعایت موازین پیش‌بینی‌شده در قانون، برای حمایت از مصرف‌کنندگان، حفظ سلامت و ایمنی فردی و عمومی، حصول اطمینان از کیفیت محصولات و ملاحظات زیست محیطی و اقتصادی، اجرای بعضی از استانداردهای ملی ایران را برای محصولات تولیدی داخل کشور و/ یا اقلام وارداتی، با تصویب شورای عالی استاندارد، اجباری نماید. سازمان می‌تواند به منظور حفظ بازارهای بین‌المللی برای محصولات کشور، اجرای استاندارد کالاهای صادراتی و درجه‌بندی آن را اجباری نماید. همچنین برای اطمینان بخشیدن به استفاده‌کنندگان از خدمات سازمان‌ها و مؤسسات فعال در زمینهٔ مشاوره، آموزش، بازرسی، ممیزی و صدور گواهی سیستم‌های مدیریت کیفیت و مدیریت زیست‌محیطی، آزمایشگاه‌ها و مراکز کالیبراسیون (واسنجی) وسایل سنجش، سازمان ملی استاندارد ایران این گونه سازمان‌ها و مؤسسات را بر اساس ضوابط سیستم تأیید صلاحیت ایران ارزیابی می‌کند و در صورت احراز شرایط لازم، گواهینامهٔ تأیید صلاحیت به آن‌ها اعطا و بر عملکرد آن‌ها نظارت می‌کند. ترویج دستگاه بین‌المللی یکاها، کالیبراسیون (واسنجی) وسایل سنجش، تعیین عیار فلزات گرانبها و انجام تحقیقات کاربردی برای ارتقای سطح استانداردهای ملی ایران از دیگر وظایف این سازمان است.

1- International Organization for Standardization
2 - International Electrotechnical Commission
3 - International Organization of Legal Metrology (Organisation Internationale de Metrologie Legale)
4 - Contact point
5 - Codex Alimentarius Commission

کمیسیون فنی تدوین استاندارد

«مدیریت مدارک- اطلاعات ذخیره‌شدهٔ الکترونیکی- توصیه‌هایی برای قابلیت اعتماد و اعتبار»

رئیس:	**سمت و/ یا نمایندگی**
سیفی، مهوش (فوق لیسانس مدیریت دولتی)	کارشناس استاندارد- بازنشسته سازمان ملی استاندارد ایران
دبیر:	
عزیزی، غلامرضا (فوق لیسانس فرهنگ و زبان‌های باستانی)	معاون اسناد ملی- سازمان اسناد و کتابخانه ملی ایران
اعضاء: (اسامی به ترتیب حروف الفبا)	
داوری- بیژن (لیسانس صنایع)	مدیر عامل و عضو هیئت مدیره- شرکت مهندسی و بهبود کیفیت شریف
زرین‌کلکی، بهناز (لیسانس حقوق قضایی)	مدیر کل اطلاع‌رسانی و ارتباطات- سازمان اسناد و کتابخانه ملی ایران
ضرغامی، زهرا (فوق لیسانس زبان انگلیسی)	کارشناس- سازمان اسناد و کتابخانه ملی ایران
کرمی، مینا (فوق لیسانس کتابداری و اطلاع‌رسانی)	رئیس گروه اسناد الکترونیکی- سازمان اسناد و کتابخانه ملی ایران
عرب، مهدی (لیسانس ریاضی کاربردی)	رئیس ادارهٔ ورود اطلاعات و بانک‌های اطلاعاتی- سازمان اسناد و کتابخانه ملی ایران
مروجی، سید سجاد (فوق‌لیسانس نرم‌افزار کامپیوتر)	مدیر عامل- شرکت سلامت الکترونیکی برکت
واقف‌زاده، محمد حسین (فوق‌لیسانس صنایع)	سرپرست ادارهٔ کل برنامه‌ریزی و توسعه- سازمان اسناد و کتابخانه ملی ایران

فهرست مندرجات

ادامه فهرست مندرجات

پیش‌گفتار

استاندارد «مدیریت مدارک- اطلاعات ذخیره‌شدهٔ الکترونیکی- توصیه‌هایی برای قابلیت اعتماد و اعتبار» که پیش‌نویس آن در کمیسیون‌های مربوط توسط سازمان ملی استاندارد ایران تهیه و تدوین شده و در یکصد و پنجاه و سومین اجلاسیه کمیته ملی اسناد و تجهیزات اداری و آموزشی مورخ ۱۳۹۳/۱۱/۲۷مورد تصویب قرار گرفته است، اینک به استناد بند یک مادهٔ ۳ قانون اصلاح قوانین و مقررات مؤسسه استاندارد و تحقیقات صنعتی ایران مصوب بهمن ماه ۱۳۷۱، به عنوان استاندارد ملی ایران منتشر می‌شود.

برای حفظ همگامی و هماهنگی با تحولات و پیشرفت‌های ملی و جهانی در زمینه صنایع، علوم و خدمات، استانداردهای ملی ایران در مواقع لزوم تجدیدنظر خواهد شد و هرگونه پیشنهادی که برای اصلاح و تکمیل این استاندارد ارائه شود، هنگام تجدیدنظر درکمیسیون فنی مربوط مورد توجه قرار خواهد گرفت. بنابراین باید همواره از آخرین تجدیدنظر استانداردهای ملی ایران استفاده کرد.

منبع و مأخذی که برای تهیه این استاندارد به‌کاررفته به شرح زیر است:

ISO/TR 15801: 2009, Document management- Information stored electronically- Recommendations for trustworthiness and reliability

مقدمه

این استاندارد، اقدامات توصیه‌شده برای ذخیره‌سازی الکترونیکی اطلاعات اداری یا اطلاعات دیگر در قالب الکترونیکی را تعریف می‌کند. حتی در مواقعی که اعتمادپذیری این اطلاعات به چالش کشیده می‌شود، پیروی کردن از این توصیه‌ها برای سازمان‌ها ارزشمند است.

اطلاعات در قالب اشیاء رقمی[1]، از منابع مختلفی به‌وجود می‌آیند. این استاندارد اشیاء رقمی در قالب‌های مختلف را در بر می‌گیرد از جمله: تصاویر پویش‌شدهٔ[2] سنتی، مدارکی که با نرم‌افزار word پردازش شده‌اند و صفحه گسترده‌ها[3]، تا قالب‌های جدیدتر که شامل نامه‌های الکترونیکی[4]، محتوای وب[5]، پیام‌های پیوسته[6]، پرونده‌های طراحی CAD [7]، وبلاگ‌ها[8]، ویکی‌ها[9] و غیره.

بهتر است، استفاده‌کنندگان از این استاندارد آگاه باشند که به‌کارگیری این توصیه‌ها به‌طور خودکار باعث اطمینان از مقبولیت شواهد موجود در اطلاعات نمی‌شود. توصیه می‌شود، زمانی که در مراجع قضایی به وجود اطلاعاتی که به صورت الکترونیکی ذخیره شده‌اند نیاز داریم، از این استاندارد برای جست‌وجوی شواهد قانونی استفاده شود تا موقعیت دقیق در محیط قانونی مرتبط با آنها، ثابت شود.

این استاندارد ابزارهایی را توصیف می‌کند که با استفاده از آن می‌توان در هر زمان نشان داد که محتوای یک شیء الکترونیکی خاص که در سیستم رایانه‌ای تولید و یا در آن وجود داشته، از زمان ایجاد در سیستم یا ورود به آن، تغییر نکرده است.

صرف‌نظر از قالب اصلی، می‌توان نشان داد اطلاعاتی که به شکل قابل اطمینان در سیستم ذخیره شده‌اند، به‌طور معتبر و به شکل پیوسته بازتولید و آنچه که در ابتدا و بدون اعمال اصلاحات ذخیره شده، به‌طور صحیح انعکاس می‌یابد.

نسخه‌های دیگر اطلاعات مثلاً چاپ اصلاح‌شدهٔ یک قرارداد، به‌طور قانونی ایجاد می‌شود. در چنین مواردی، این نسخه‌ها به عنوان اشیاء رقمی جدید در نظر گرفته می‌شود. وقتی که در مدارک موجود در محیط جاری، تغییر عمده‌ای به وجود آمده باشد، می‌توان از اصول مشابهی استفاده کرد.

همان‌طور که در استاندارد ملی ایران شماره ۱-۱۰۰۴۷ تعریف شده است، سیستم‌های مدیریت مدارک، سوابق و مدارک را در قالب الکترونیکی ذخیره می‌کنند. این استاندارد، ابزارهایی برای ذخیره‌سازی انواع مختلف اطلاعات الکترونیکی به شکل قابل اعتماد و معتبر را توصیف می‌کند. جایی که سوابق ذخیره می‌شوند، می‌توان الزامات این استاندارد را همراه با الزامات مشخص‌شده در استاندارد ملی ایران شماره ۱-۱۰۰۴۷ به‌کار برد تا اطمینان حاصل شود که خط‌مشی‌ها و روش‌های

---

1 - Digital objects
2 - Scanned
3 - Spreadsheets
4 - E-mail
5 - Web content
6 - Instant messages
7 - CAD drawing files
8 - Blogs
9 - Wikis

توصیف‌شده در این استاندارد در کنار الزامات مشخص‌شده در استاندارد ملی ایران شماره ۱-۱۰۰۴۷، قابل اجرا هستند.

به خوانندگان توصیه می‌شود این استاندارد را همراه با منابع ملی دیگر که تا حدی با الزامات دولتی و قانونی در کشور خود مرتبط هستند، به‌کار گیرند.

مدیریت مدارک- اطلاعات ذخیره‌شدهٔ الکترونیکی- توصیه‌هایی برای قابلیت اعتماد و اعتبار

۱ هدف و دامنهٔ کاربرد

هدف از تدوین این استاندارد، توصیف مراحل پیاده‌سازی و بهره‌برداری از سیستم‌های مدیریت مدارک است که اطلاعات الکترونیکی را به شکل قابل اعتماد و معتبر، ذخیره می‌کنند.
این استاندارد برای سازمان‌هایی کاربرد دارد که از سیستم مدیریت مدارک برای ذخیرهٔ اطلاعات الکترونیکی موثق، معتبر و قابل استفاده/ قابل خواندن در طول زمان استفاده می‌کنند. چنین سیستم‌هایی، خط‌مشی‌ها، روش‌ها، فناوری‌ها و الزامات حسابرسی را به‌کار می‌گیرند تا اطمینان حاصل شود که یکپارچگی اطلاعات الکترونیکی حین ذخیره‌سازی، حفظ شده است.
این استاندارد در مورد روش‌های استفاده‌شده برای ارزیابی اطمینان‌پذیری اطلاعات قبل از ورود به سیستم و ذخیره در آن، کاربرد ندارد. این استاندارد برای نمایاندن اینکه خروجی سیستم پس از ذخیره اطلاعات، بازتولید دقیق و صحیحی از اطلاعات اولیه است، کاربرد دارد.
در این استاندارد، کلمه «سیستم» معادل با سیستم مدیریت مدارک[1] در نظر گرفته می‌شود مگر اینکه نوع سیستم موردنظر مشخص شود.

۲ مراجع الزامی

مدارک الزامی زیر حاوی مقرراتی است که در متن این استاندارد ملی ایران به آنها ارجاع داده شده است. بدین ترتیب آن مقررات جزئی از این استاندارد ملی ایران محسوب می‌شود.
در صورتی که به مدرکی با ذکر تاریخ انتشار ارجاع داده شده باشد، اصلاحیه‌ها و تجدیدنظرهای بعدی آن موردنظر این استاندارد ملی ایران نیست. در مورد مدارکی که بدون ذکر تاریخ انتشار به آنها ارجاع داده شده است، همواره آخرین تجدیدنظر و اصلاحیه‌های بعدی آنها مورد نظر است.
استفاده از مراجع زیر برای این استاندارد الزامی است:

۲-۱ استاندارد ملی ایران شماره ۱-۱۰۰۴۷، اطلاعات و مستندسازی- مدیریت سوابق- قسمت اول: کلیات

۲-۲ استاندارد ملی ایران شماره ۹۰۰۰، سیستم‌های مدیریت کیفیت- مبانی و واژگان

1 - Document Management System

2-3 ISO 2859-1, Sampling procedures for inspection by attributes — Part 1: Sampling schemes indexed by acceptance quality limit (AQL) for lot-by-lot inspection

2-4 ISO/TR 12033, Document management — Guidance for the selection of document image compression methods

2-5 ISO/TR 12037, Electronic imaging — Recommendations for the expungement of information recorded on write-once optical media

2-6 ISO 12653-2, Electronic imaging — Test target for the black-and-white scanning of office documents — Part 2: Method of use

2-7 ISO/IEC 27001, Information technology — Security techniques — Information security management systems — Requirements

2-8 ISO/TR 18492, Long-term preservation of electronic document-based information

۳ اصطلاحات و تعاریف

در این استاندارد، اصطلاحات و تعاریف زیر به‌کار می‌رود:

۳-۱

نوع اطلاعات[1]

گروه‌هایی از مدارک مرتبط است.

یادآوری- در برخی کاربردهای خاص، گروه‌ها به معنای «مجموعه‌ها[2]»، «پرونده‌ها[3]» و «کلکسیون‌ها[4]» است.

مثال:

صورتحساب‌ها، مدارک مالی، صفحهٔ داده‌ها، مکاتبات.

۳-۲

سیستم قابل اعتماد[5]

سیستم مدیریت مدارک استفاده‌شده برای ذخیره الکترونیکی اطلاعات به شکل موثق، معتبر و قابل استفاده/ قابل خواندن که باعث اطمینان از یکپارچگی اطلاعات در طول زمان می‌شود.

1 - Information type
2 - Sets
3 - Files
4 - Collections
5 - Trusted system

۴ خط‌مشی مدیریت مدارک

۴-۱ کلیات

اطلاعات یکی از مهم‌ترین دارائی‌های هر سازمان است. هر کاری که سازمان انجام می‌دهد شامل استفاده از اطلاعات به روش‌های مختلف می‌باشد. حجم اطلاعات بسیار زیاد است و روش‌های متفاوتی برای نمایش و ذخیره آنها وجود دارد. ارزش اطلاعات استفاده‌شده و روش به‌کارگیری و جابه‌جایی آن بین سازمان‌ها، موفقیت یا شکست سازمان‌ها را مشخص می‌کند.

همانند دارائی‌های دیگر، اطلاعات به طبقه‌بندی، ساختاربندی، اعتبارسنجی، ارزش‌گذاری، ایمن‌سازی، نظارت، سنجش و مدیریت مؤثر و کارآمد نیاز دارد.

این استاندارد مستنداتی را توصیف می‌کند که خط‌مشی‌های سازمان‌ها برای مدیریت اطلاعات را به تصویر می‌کشد. همچنین این استاندارد، راهنمایی‌های لازم درباره سطح مستندات موردنیاز را به سازمان‌ها ارائه می‌دهد تا بتوانند به وضوح مشخص کنند چگونه اطلاعات موجود در سیستم قابل اعتماد مدیریت مدارک، معتبر، صحیح و قابل اعتماد است. با استفاده از این مستندات می‌توان نشان داد که مدیریت مدارک بخشی از روش‌های عادی اداری است.

هرگاه سیستم اطلاعاتی را ذخیره کند که بتوان از آنها در فرایندهای قانونی یا اداری استفاده کرد، بهتر است، با مشاور حقوقی مشورت شود (به بند ۵-۴ مراجعه شود) تا از تطابق با الزامات حقوقی یا قانونی اطمینان حاصل شود. به دلیل اینکه الزامات قانونی در کشورهای مختلف (و گاهی اوقات درون یک کشور) متفاوت هستند، بهتر است، توصیه‌های قانونی حوزه مورد نظر را تحت پوشش قرار دهند.

۴-۲ سند خط‌مشی مدیریت مدارک

۴-۲-۱ محتوا

توصیه می‌شود، سند خط‌مشی مدیریت مدارک (سند خط‌مشی[1]) تدوین شود و خط‌مشی سازمان درباره ذخیره‌سازی و مدیریت مدارک را که برای سیستم‌های قابل اعتماد مدیریت مدارک قابل اجرا هستند، مستند کند.

بهتر است، سند خط‌مشی شامل موارد زیر باشد:

الف- اطلاعات تحت پوشش را مشخص کند (به بند ۴-۲-۲ مراجعه شود)؛

ب- خط‌مشی‌های مرتبط با رسانه ذخیره‌سازی را بیان کند (به بند ۴-۲-۳ مراجعه شود)؛

پ- خط‌مشی‌های مرتبط با قالب پروندهٔ اشیاء الکترونیکی و نظارت نسخه را بیان کند (به بند ۴-۲-۴ مراجعه شود)؛

ت- خط‌مشی‌های مرتبط با استانداردهای مدیریت مدارک را بیان کند (به بند ۴-۲-۵ مراجعه شود)؛

ث- خط‌مشی‌های نگهداری و امحاء را تعریف کند (به بند ۴-۲-۶ مراجعه شود)؛

1 - Policy document

ج- مسئولیت‌های مدیران اسناد[1] را تعریف کند (به بند ۴-۲-۷ مراجعه شود)؛
چ- با این خط‌مشی، مسئولیت‌های نظارت بر تطابق را تعریف کند (به بند ۴-۲-۸ مراجعه شود).

توصیه می‌شود، مدیران ارشد سازمان این خط‌مشی را تأیید کرده و خط‌مشی در فواصل زمانی منظم، بازبینی شود.
موافقت با جدول زمانی نگهداری[2] از اطلاعات ذخیره‌شده و استفاده از آن برای این استاندارد ضروری است. در قسمت‌هایی از این استاندارد که به سند خط‌مشی اشاره می‌شود، این ارجاع، جدول زمانی نگهداری را نیز دربرمی‌گیرد.

۴-۲-۲ اطلاعات تحت پوشش

به‌منظور تعریف خط‌مشی مدیریت مدارک سازمان، بهتر است، اطلاعات در گروه‌های مختلف طبقه‌بندی شده و خط‌مشی مدون، برای تمام اطلاعات پایدار باشد. برای مثال: انواع اطلاعات را می‌توان با اشاره به کاربرد (مانند: طرح‌های مالی، صورت‌حساب‌ها، نشانی مشتریان)، با ارتباط دادن آنها به یک فرایند اداری خاص (مانند: برنامه‌ها، شکایات، نوسازی‌ها) یا با اشاره به گروه‌های عمومی (مانند: داده‌های حسابرسی، مدارک مشتریان و مدارک کارخانه سازنده)، طبقه‌بندی کرد.
ممکن است لازم باشد حین تدوین پیش‌نویس سند خط‌مشی، اطلاعات خاصی دوباره گروه‌بندی شوند تا از پایداری خط‌مشی در آن نوع اطلاعات، اطمینان حاصل شود.
توصیه می‌شود، سند خط‌مشی انواع اطلاعاتی لازم را فهرست کند. بهتر است، سند خط‌مشی شامل تمام مدارک ایجادشده در پیروی از این خط‌مشی باشد.

۴-۲-۳ رسانه ذخیره‌سازی

انواع مختلف رسانه‌های ذخیره‌سازی، ویژگی‌های مختلفی در زمینهٔ ذخیره‌سازی بلندمدت دارند. اکثر سازمان‌ها اطلاعات خود را روی انواع مختلفی از رسانه‌ها مانند کاغذ، ریزفرم[3]، قالب‌های الکترونیکی (فقط یکبار قابل نوشتن و قابل نوشتن مجدد/ قابل پاک کردن[4]) یا نوری (فقط یکبار قابل نوشتن و قابل نوشتن مجدد/ قابل پاک کردن)، ذخیره می‌کنند. در برخی برنامه‌های کاربردی، بخش‌های خاصی از اطلاعات را می‌توان در کل دوره نگهداری، روی انواع متفاوتی از رسانه‌ها در زمان‌های مختلف، ذخیره کرد.
توصیه می‌شود، سازمان‌ها با در نظر گرفتن انواع رسانه‌های ذخیره‌سازی برای الزامات مختلف ذخیره‌سازی اطلاعات (مانند: الزامات دسترسی، دوره‌های نگهداری و الزامات امنیتی)، خط‌مشی‌هایی داشته باشند. بهتر است، این موارد در سند خط‌مشی، شرح داده شود.

---

1 - Record managers
2- Retention schedule
3 - Microform
4 - Write-once and rewritable/ erasable

توصیه می‌شود، نوع رسانه‌ای که برای نگهداریِ هر نوع از اطلاعات استفاده می‌شود مشخص شود (به بند ۴-۲-۲ مراجعه شود).

جایی که رونوشت‌هایی از اشیاء الکترونیکی وجود دارد، می‌توان نشان داد که در هیچ کدام از رونوشت‌های موردنظر، تغییری ایجاد نشده است. در مورد آن‌دسته از اشیاء الکترونیکی که در نسخه‌های متفاوت وجود دارند، توصیه می‌شود، هر نسخه به عنوان منبع جدید یا شیء اصلی در نظر گرفته شود.

بهتر است، خط‌مشی مرتبط با مدیریت نسخه‌های اشیاء الکترونیکی را در سند خط‌مشی، شرح داد.

۴-۲-۴ قالب و فشرده‌سازی پرونده داده‌ها

توصیه می‌شود، سند خط‌مشی حاوی اطلاعات مشروح درباره قالب‌های داده‌ای مورد تأیید باشد که می‌توان برای هر نوع از اطلاعات به‌کار گرفت.

تمام اطلاعات ذخیره‌شده روی سیستم رایانه‌ای برای بازیابی و نمایش به نرم‌افزار نیاز دارند. این نرم‌افزار به دلیل به‌کارگیری نسخه‌های منتشرشدهٔ جدید یا بر اثر تغییرات ایجادشده در سیستم عامل / یا سخت‌افزارها، در معرض تغییر قرار دارند. با به‌کارگیری قالب‌های داده و فناوری‌های فشرده‌سازی مورد تأیید، گذار[1] ضروری داده‌ها یا روش‌های جایگزین را می‌توان به‌کارگرفت تا از بازیابی بلندمدت اطلاعات ذخیره‌شده اطمینان حاصل شود.

بهتر است، جایی که فناوری‌های فشرده‌سازی وجود دارند، خط‌مشیِ نحوهٔ استفاده از آنها مستند شود.

در صورت ذخیره‌سازی نسخه‌های مختلف از یک پرونده به یک خط‌مشی نیاز داریم که اطیمنان می‌دهد تمام نسخه‌های مرتبط ذخیره و ارتباط آنها حفظ شده است. توصیه می‌شود، سند خط‌مشی حاوی اطلاعات مشروح درباره خط‌مشی ذخیره‌سازی نسخه‌های مختلف مدارک باشد.

برای کسب اطلاعاتی بیشتر به بندهای ۶-۵-۲، ۶-۱۰، ۷-۱۰ و ۸-۲-۳ مراجعه شود.

۴-۲-۵ استانداردهای مرتبط با مدیریت مدارک

سازمان‌هایی که یک سیستم مدیریت کیفیت (مانند: مجموعه استانداردهای ملی ایران ایزو ۹۰۰۰) را اجرا می‌کنند و دامنهٔ آنها شامل بخش‌هایی از سیستم قابل اعتماد مدیریت مدارک یا کل آن است، توصیه می‌شود، تمام مستندات رویه‌ای مرتبط در سیستم کیفیت وجود داشته باشند.

توصیه می‌شود، هرگاه الزامات ملی یا بین‌المللی حقوقی اجباری، یا جایی که استانداردهای ملی یا بین‌المللی قابل اجرا هستند، از آنها پیروی شود.

۴-۲-۶ جداول زمانی نگهداری و امحاء

در مورد جداول زمانی نگهداری و امحاء، موارد زیر توصیه می‌شود:

---

1 - Migration

الف- برای هر نوع از اطلاعات یک جدول زمانی نگهداری تدوین شود.
ب- جداول زمانی نگهداری مورد موافقت تمام ادارات و کارکنان سازمان قرار گیرد.
پ- جداول زمانی نگهداری پس از کسب توصیه‌های لازم برای اطمینان از حل موضوعات قانونی، مقرراتی یا هر دوی آنها، مورد موافقت قرار گیرد.
ت- جداول زمانی نگهداری تمام سیستم‌ها و مستندات رویه‌ای مرتبط را که ایجاد شده‌اند، پوشش دهد.
ث- جدول زمانی نگهداری شامل خط‌مشی سازمان برای بررسی‌های دوره‌ای باشد.
ج- جدول زمانی نگهداری شامل خط‌مشی سازمان برای امحاء کنترل‌شدهٔ اطلاعات باشد.

۴-۲-۷ مسئولیت‌های مدیریت مدارک

توصیه می‌شود، مسئولیت‌های فردی یا اداری برای سند خط‌مشی در آن تعریف شود.
بهتر است، مسئولیت‌های فردی یا اداری برای انواع مختلف اطلاعات مشخص و در سند خط‌مشی ارائه شود.
توصیه می‌شود، مسئولیت‌های فردی یا اداری شامل نیاز به کسب توصیه‌های لازم در هنگام ایجاد یا به‌روزرسانی محتوای سند خط‌مشی باشد.

۴-۲-۸ تطابق با خط‌مشی

اگر لازم است تطابق با سند خط‌مشی اثبات شود، توصیه می‌شود، مسئولیت‌های فردی یا اداری برای فراهم‌آوری و نگهداری از این تطابق‌ها مشخص و تعریف شود.

۵ وظیفه مراقبت

۵-۱ کلیات

۵-۱-۱ سیستم قابل اعتماد

سیستم قابل اعتماد مدیریت مدارک سیستمی است که اطمینان می‌دهد صرف‌نظر از قالب اصلی، تمام اطلاعاتی که به صورت الکترونیکی ذخیره شده‌اند را می‌توان به عنوان رونوشت دقیق و درست از اطلاعات اصلی در نظر گرفت. لازم است سیستم قابل اعتماد مدیریت مدارک حداقل قابلیت‌های زیر را داشته باشد:
الف- ایجاد حداقل یک نسخه از اطلاعات ذخیره‌شده روی رسانه‌ای که از آنها در برابر اصلاح، افزایش‌های نامناسب یا حذف در طول چرخه حیات تأییدشده آن، محافظت می‌کند؛ لازم است این نسخه در یک مکان ایمن و مطمئن ذخیره و نگهداری شود که از محل نگهداری دیگر نسخه‌های موجود از اطلاعات ذخیره شده، متمایز باشد؛

ب- به‌کارگیری آن‌دسته از سخت‌افزارها و رسانه‌های ذخیره‌سازی کـه از اطلاعـات ذخیـره‌شـده در برابر اصلاح، افزایش‌های نامناسب یا حذف در طول چرخه حیات تأییدشده آن، محافظت می‌کند (به بند ۷-۳ مراجعه شود)؛

پ- صحه‌گذاری بر امکان اجرای اطلاعات اصلی ذخیره‌شده در طول چرخه حیات تأییدشدهٔ آنهـا از طریق فرایندهای ممیزی مستقل نرم‌افزار، سخت‌افـزار و/ یـا روش شناسـایی (هـای) ذخیـره‌سـازی رسانه‌ها.

سیستم قابل اعتماد مدیریت مدارک که ترکیبی از خط‌مشی‌ها، روش‌های عملیـاتی و فنـاوری‌هـای توصیف‌شده در این استاندارد که به خوبی نصب و مدیریت شده‌اند را به‌کار می‌برد، سـازمان را قـادر می‌سازد تا قابلیت اعتماد و اعتبار را نشان دهد.

۵-۱-۲ کنترل‌ها

ضروری است که سازمان‌ها از اهمیت طراحی و نگهـداری تمـام جنبـه‌هـای سیسـتم قابـل اعتمـاد مدیریت مدارک آگاهی داشته و مسئولیت‌های خود را مطابق با اصـول وظیفـه مراقبـت، بـه انجـام برسانند.

برای رسیدن به این هدف لازم است سازمان کارهای زیر را انجام دهد:

الف- ایجاد زنجیرهٔ پاسخگویی و تخصیص مسـئولیت‌هـا بـرای فعالیـت‌هـای دربردارنـدهٔ مـدیریت اطلاعات الکترونیکی در تمام سطوح؛

ب- آگاهی از نهادهای قانون‌گذار و قضایی مرتبط با کار سازمان؛

پ- حفظ توسعهٔ فنی، رویه‌ای، حقوقی و قانونی از طریق برقراری تماس بـا نهادهـا و سـازمان‌هـای مناسب؛

ت- به‌کارگیری خط‌مشی امنیت اطلاعات.

۵-۱-۳ جداسازی نقش‌ها

جداسازی نقش‌ها یکی از جنبه‌های اساسی در وظیفهٔ مراقبت است. این کار باعث ایجاد نظـارت بـر خطا و تحریف عمدی سوابق می‌شود (در این رابطه، جداسازی نقش‌ها مخصوصاً در سیستم‌هایی که در معرض خطر سوء استفاده یا اقدامات تبهکارانه قرار دارند، حائز اهمیت است).

وقتی که جداسازی نقش‌ها در نظر گرفته می‌شود، جنبه‌های مختلفی از مدیریت مـدارک بـه شـرح زیر وجود دارد:

الف- اصلاح داده‌های ورودی (به بند ۶-۴-۳ مراجعه شود)؛

ب- نظارت کیفی (به بند ۶-۴-۶ مراجعه شود)؛

پ- ورود داده‌ها (به بند ۶-۶ مراجعه شود)؛

ت- حذف اطلاعات (به بند ۶-۱۱ مراجعه شود)؛

ث- امنیت اطلاعات (به بند ۵-۲ مراجعه شود).

۵-۲ مدیریت امنیت اطلاعات

۵-۲-۱ خط‌مشی امنیت اطلاعات

صرف‌نظر از رسانه‌ای که اطلاعات روی آن ذخیره شده است، اطلاعات در برابر فقدان یا تغییر تصادفی یا عمدی، آسیب‌پذیر است. برای حفاظت از اطلاعاتی که به صورت الکترونیکی ذخیره شده‌اند، لازم است معیارهای امنیتی تدوین و برای کاهش ریسک[1] به چالش کشیدن اطمینان‌پذیری اطلاعات به‌کار گرفته شود. این معیارهای امنیتی باید با طبقه‌بندی اطلاعاتی که استفاده می‌شوند مطابقت داشته باشند.

امنیت اطلاعات به معنای قابلیت اعتماد برای اطمینان از عدم دسترس‌پذیری اطلاعات خارج از الزامات سازمان در نظر گرفته می‌شود. اگرچه این موضوع برای فعالیت‌های سازمان مهم (و در برخی موارد حیاتی) است، موضوع امنیتی به هیچ وجه مرتبط با این استاندارد نیست.

هدف کلیدیِ خط‌مشی امنیت اطلاعات، اطمینان از حفظ یکپارچگی اطلاعات ذخیره‌شده است. هنگام تدوین معیارهای امنیتی لازم است تا مسئلهٔ یکپارچگی را که با هزینه‌های به‌کارگیری چنین معیارهایی به خطر می‌افتد در نظر بگیریم. لازم است معیارهای امنیتی شامل نسخه پشتیبان و نسخه‌های دیگر از اطلاعات ذخیره‌شده باشند چرا که یکپارچگی آنها هنگامی که به‌عنوان جایگزین‌هایی برای داده‌های جاری به‌کار می‌روند، حائز اهمیت است.

دسترس‌پذیری نیز یکی از مسائل مهم است. در برخی موارد، لازم است بتوانیم نشان دهیم که تمام اطلاعات موجود درباره یک موضوع خاص برای بازبینی در هر زمان، در دسترس قرار دارند. در این طبقه‌بندی، موضوعاتی مانند دقت و صحت نمایه‌سازی و برنامه‌ریزی برای پیوستگی اداری از مفاهیم کلیدی هستند.

موضوع امنیت فقط درباره سیستم‌های رایانه‌ای مطرح نیست. امنیت و دسترس‌پذیری محیط عملیاتی (اعم از ساختمان‌ها، کنترل‌های دمایی، پیوندهای شبکه و غیره) و اجرای فرایندهای قابل ممیزی توسط کاربران به شکل قابل بررسی، دو عامل کلیدی هستند.

توصیه می‌شود، سازمان‌ها یک خط‌مشی امنیت اطلاعات تدوین کنند که تمام عوامل سیستم قابل اعتماد مدیریت مدارک را پوشش دهد.

توصیه می‌شود، وقتی که سازمان برای سیستم‌های دیگر، خط‌مشی امنیت اطلاعات دارد، استفاده از سیستم قابل اعتماد مدیریت مدارک در گسترهٔ این خط‌مشی قرار داشته باشد.

بهتر است، سند خط‌مشی مدیریت مدارک حداقل شامل موارد زیر باشد:

الف- دامنهٔ کاربرد خط‌مشی؛

ب- شرح اهداف مدیریتی با توجه به مسئله امنیت؛

پ- مشخص کردن خط‌مشی‌های خاص؛

ت- الزامات مورد نیاز برای رده‌بندی طبقه‌های مختلف اطلاعات؛

ث- تعریف و تخصیص مسئولیت‌های امنیت اطلاعات؛

---

1 - Risk

ج- خط‌مشی مرتبط با نقض امنیت؛
چ- خط‌مشی تطابق با استانداردهای مرتبط.

توصیه می‌شود، مدیران ارشد سازمان سند خط‌مشی امنیت اطلاعات را تأیید کنند. بهتر است، تأیید سند خط‌مشی مستند شود.
توصیه می‌شود، سازمان با سطوح مناسب امنیت برای مدیریت اطلاعات مطابق با سند خط‌مشی امنیت اطلاعات موافقت و آن را مستند کند.
بهتر است، موضوع تطابق با استاندارد ISO 27001 را در نظر گرفت. توصیه می‌شود، هنگام تدوین کنترل‌های مورد نیاز برای انطباق با استاندارد ISO 27001، با اشاره به سیستم مورد اعتماد مدیریت مدارک، الزامات این استاندارد را در نظر گرفت.

۵-۲-۲ ارزیابی ریسک

معیارهای امنیتی غالباً با استفاده از رهیافت موردی، واکنش در برابر رویدادهای امنیتی یا دسترس‌پذیری ابزارهای نرم‌افزار رایانه‌ای، تدوین می‌شوند. اکثر مواقع، چنین روش‌هایی باعث به جا ماندن خلأهای امنیتی می‌شود که بعداً رفع خواهند شد. یکی از رهیافت‌های ساختاریافته‌تر، بررسی دارایی‌های اطلاعاتی سازمان و تخصیص عوامل ریسک (بر اساس ارزش دارایی، آسیب‌پذیری سیستم و احتمال حمله) است. سپس می‌توان خط‌مشی امنیت اطلاعات را بر اساس معیارهای امنیتی قابل بررسی، ایجاد و ممیزی کرد.
توصیه می‌شود، سازمان، تحلیل ریسک امنیت اطلاعات را انجام داده و نتایج حاصل را مستند کند.
معیارهای امنیتی به‌کار گرفته شده برای نظارت بر رسانه ذخیره‌سازی اطلاعات، هم رسانه‌های جاری و هم رسانه‌های پشتیبان، از اهمیت خاصی برخوردار هستند. لازم است تحلیل ریسک، عوامل آسیب‌پذیری را مطابق با نوع رسانهٔ استفاده‌شده (برای مثال: WORM یا با قابلیت نوشتن مجدد) دربرداشته باشد.
توصیه می‌شود، هر کجا که از انواع مختلف رسانه‌های ذخیره‌سازی استفاده می‌شود، تأثیر آنها بر نتایج تحلیل ریسک مورد بررسی قرار گیرد.
وقتی تحلیل ریسک پایان یافت، لازم است این تحلیل به عنوان بخشی از معیارهای امنیتیِ به‌کار گرفته‌شده مورد بررسی قرار گیرد. ضروری است حین مرحله بررسی، عواملی مانند توازن بین هزینه اجرا ، امنیت به‌دست آمده و ارزیابی ریسک مورد توجه قرار گیرد.
توصیه می‌شود، بر اساس نتایج تحلیل ریسک، کارآمدیِ معیارهای امنیتی موجود مورد بررسی قرار گیرد.
بهتر است، وقتی که بررسی‌ها نشان می‌دهد که تغییرات اعمال‌شده در روش‌های امنیتی مناسب هستند، این تغییرات را به‌کار گرفت.

۵-۲-۳ چارچوب امنیت اطلاعات

بهتر است، برای آغاز و کنترل به‌کارگیری امنیت اطلاعات در سازمان چارچوب مدیریتی ایجاد شود. توصیه می‌شود، این چارچوب اهداف زیر را دربرداشته باشد:

الف- تأیید و بررسی خط‌مشی امنیت اطلاعات؛

ب- نظارت بر تهدیدهای امنیتی؛

پ- نظارت و بررسی خلأهای امنیتی؛

ت- تأیید ابتکارات عمده برای بالا بردن امنیت اطلاعات.

۵-۳ برنامه‌ریزی برای پیوستگی کسب و کار (اداری)

گهگاهی مشکلاتی در سیستم‌های قابل اعتماد مدیریت مدارک به وجود می‌آید که مستلزم به‌کارگیری روش‌های اضطراری برای رفع مشکل است. ممکن است این روش‌ها شامل استفاده موقتی از منابع بیشتر یا منابع شخص ثالث باشد. به منظور اطمینان از عدم به خطر افتادن یکپارچگی اطلاعات حین انجام این عملیات، می‌توان از طرح پیوستگی کسب و کار (اداری) موافقت و تأییدشده (که گاهی اوقات به عنوان طرح بازیابی حوادث و بلایا شناخته می‌شود)، استفاده کرد.

بهتر است، روش‌هایی را تدوین، آزمایش و نگهداری کرد که در مورد تجهیزات عمده، شکست محیطی یا شکست کارکنان به کار گرفته شوند. با این روش‌ها اطمینان حاصل می‌شود که یکپارچگی اطلاعات حین به‌کارگیری آنها، نادیده گرفته نشده‌اند.

۵-۴ رایزنی‌ها

استفاده از سیستم‌های قابل اعتماد مدیریت مدارک می‌تواند برای سازمان‌های زیر حائز اهمیت باشد:

الف- نهادهای قانونگذار؛

ب- نهادهای دولتی؛

پ- نهادهای بازرسی برون سازمانی؛

ت- مشاوران حقوقی (مانند: وکلای سازمان).

توصیه می‌شود، سازمان پیش از به‌کارگیری سند خط‌مشی مدیریت مدارک با نهادهایی که با موضوع اطمینان‌پذیری، اعتبار و یکپارچگی اطلاعات ذخیره‌شده در ارتباط هستند، مشورت کند.

این مؤسسات عبارتند از:

الف- حقوق ملی و بین‌المللی؛

ب- بخش صنعتی؛

پ- جامعه؛

ت- سازمان‌ها؛

ث- ادارات؛

ج- اشخاص حقیقی.

بهتر است، سازمان‌ها پیش از به‌کارگیری سند خط‌مشی مدیریت مدارک با سازمان‌های دیگر مشورت کند.

این رایزنی‌ها می‌تواند شامل موضوعات زیر باشد:

الف- موضوعات حقوقی؛

ب- مقررات دولتی؛

پ- مقررات مالی (مانند: پرداخت مالیات)؛

ت- مقررات خاص (که در بخش‌های ویژه‌ای قابل اجرا هستند).

توصیه می‌شود، در سند خط‌مشی به نتایج این رایزنی‌ها اعم از اقدامات توافق، برنامه‌ریزی یا اجرا شده، اشاره شود.

جایی که قوانین و/ یا مقررات مناسب وجود دارند از آنها پیروی شود.

سند خط‌مشی مشخص کند که لازم است از کدام استانداردهای ملی یا بین‌المللی یا بخش‌های آن پیروی شود.

بهتر است، هرگاه سازمان از استانداردهای مرتبط ملی یا بین‌المللی پیروی می‌کند، سیستم قابل اعتماد مدیریت مدارک را در بر داشته باشد.

۶ روش‌ها و فرایندها

۶-۱ کلیات

این بند با روش‌های مرتبط با عملیات سیستم قابل اعتماد مدیریت مدارک در ارتباط است.

۶-۲ شیوه‌نامه اجرایی[1]

۶-۲-۱ مستندسازی

توصیه می‌شود، سازمان برای هر سیستم قابل اعتماد مدیریت مدارک، شیوه‌نامه اجرایی را نگهداری کند.

در این بخش هر کجا که به مستندسازی نیاز است، در شیوه‌نامهٔ اجرایی ارائه شده یا در آن مورد اشاره قرار گرفته است. شیوه‌نامه اجرایی می‌تواند شامل ارجاع به مستندات دیگر باشد.

بهتر است، روش‌های موجود در شیوه‌نامهٔ اجرایی یا ارجاع داده شده در آن برای تمام کاربران مجاز سیستم در دسترس باشند.

1 - Procedure manual

۶-۲-۲ محتوا

توصیه می‌شود، شیوه‌نامهٔ اجرایی شامل روش‌های موردنیاز برای عملیات سیستم قابل اعتماد مدیریت مدارک بوده و یا به آنها اشاره داشته باشد و موارد زیر را دربر گیرد:

الف- دریافت[1] اطلاعات (به بند ۶-۳ مراجعه شود)؛

ب- دریافت تصویر مدرک (به بند ۶-۴ مراجعه شود)؛

پ- دریافت داده (به بند ۶-۵ مراجعه شود)؛

ت- نمایه‌سازی (به بند ۶-۶ مراجعه شود)؛

ث- روش مجاز ارائهٔ خروجی[2] (به بند ۶-۷ مراجعه شود)؛

ج- انتقال پرونده (به بند ۶-۸ مراجعه شود)؛

چ- بازیابی مدرک (به بند ۶-۹ مراجعه شود)؛

ح- حفاظت و نگهداری اطلاعات (به بند ۶-۱۰ مراجعه شود)؛

خ- امحاء اطلاعات (به بند ۶-۱۱ مراجعه شود)؛

د- نسخهٔ پشتیبان و بازیابی سیستم (به بند ۶-۱۲ مراجعه شود)؛

ذ- تعمیر و نگهداری سیستم (به بند ۶-۱۳ مراجعه شود)؛

ر- امنیت و حفاظت (به بند ۶-۱۴ مراجعه شود)؛

ز- استفاده از خدمات پیمانکاری (به بند ۶-۱۵ مراجعه شود)؛

ژ- گردش کاری (به بند ۶-۱۶ مراجعه شود)؛

س- نشانگرهای تاریخ و زمان (به بند ۶-۱۷ مراجعه شود)؛

ش- کنترل نسخه (به بند ۶-۱۸ مراجعه شود)؛

ع- نگهداری مستندات (به بند ۶-۱۹ مراجعه شود).

برای سهولت بیشتر، شیوه‌نامه اجرایی را می‌توان به عنوان تعدادی از مدارک فیزیکی مجزا که با حیطه‌های مختلف مدیریت مدارک مرتبط هستند، نگهداری کرد.

وقتی که سازمان‌ها دارای سیستم‌های قابل اعتماد مدیریت مدارک متعدد هستند، مستندسازی می‌تواند شامل یک یا چند شیوه‌نامه اجرایی باشد.

۶-۲-۳ انطباق با روش‌ها

به‌منظور انطباق با روش‌های معرفی‌شده در شیوه‌نامه اجرایی، لازم است کارکنان از این روش‌ها آگاه بوده و توانایی پیروی از آنها را داشته باشند. این موقعیت با آموزش رشته‌های خاص یا حین انجام کارهای روزانه، حاصل می‌شود.

در جایی‌که سازمان دارای سیستم‌های قابل اعتماد مدیریت مدارک متعدد می‌باشد، بهتر است، مستندسازی‌ها با یک شیوه‌نامهٔ اجرایی یا شیوه‌نامه‌های اجرائی متعدد، مطابقت داشته باشند.

---

1 - Capture

2 - Authenticated output procedure

۶-۲-۴ به‌روزرسانی و کنترل

اطمینان یافتن از این که روش‌های به‌کارگرفته‌شده در دوره ذخیره‌سازی هر بخش خاص از اطلاعات را می‌توان تعیین کرد، مهم است. این هدف با اطمینان از به‌روز نگاه داشتن شیوه‌نامهٔ اجرایی و اینکه تمام نسخه‌های قبلی مطابق با سند خط‌مشی نگهداری شده‌اند، حاصل می‌شود.

بهتر است، هرگونه تغییر در روش‌های عملیاتی مستند شود. توصیه می‌شود، این مستندسازی‌ها شامل جزئیات مربوط به روش‌های کنترلِ تغییر و اطمینان از به‌کارگیری روش‌های جدید باشد.

در جاهایی که تغییرات اعمال شده‌اند، توصیه می‌شود، این تغییرات کنترل شوند تا اطمینان حاصل شود که الزامات عملیاتی و الزامات سند خط‌مشی، نادیده گرفته نشده‌اند.

بهتر است، نسخه‌های جایگزین شیوه‌نامه اجرایی مطابق با سند خط‌مشی، نگهداری شود.

به منظور تأیید به‌روز بودن مستندات، انجام کنترل‌های منظم، ضروری است. همچنین این کنترل‌ها در هنگام اعمال تغییرات قانونی یا حقوقی لازم هستند.

بهتر است، این کنترل‌ها حداقل سالی یک بار انجام شوند تا اطمینان حاصل شود که هر نوع تغییر در روش‌ها یا فناوری‌ها در شیوه‌نامه اجرایی، منعکس شده است.

توصیه می‌شود، نتایج کنترل‌های دوره‌ای مستندشده و فرد مسئول در قبال عملیات‌های بخش مربوطه سیستم، آن را تأیید کند.

۶-۳ دریافت اطلاعات

۶-۳-۱ کلیات

توصیه می‌شود، هرگاه از سیستم قابل اعتماد مدیریت مدارک برای ذخیره‌سازی اشیاء الکترونیکی استفاده شود، روش‌های دخیل در دریافت این اشیاء مستند شوند.

این روش‌ها شامل موارد زیر هستند:

الف- دریافت شیء الکترونیکی؛

ب- آماده‌سازی مدرک؛

پ- دسته‌بندی مدرک؛

ت- رونوشت‌برداری؛

ث- پویش[1]؛

ج- کنترل کیفیت تصویر.

این مدارک شامل قالب کاغذی یا ریزفیلم[2] است.

زیربند ۶-۴ حاوی اطلاعات بیشتر درباره روش‌های مرتبط با پویش مدارک است.

---

1 - Scan
2 - Microfilm

۶-۳-۲ از دست رفتن اطلاعات

هرگاه اشیاء الکترونیکی در سیستم قابل اعتماد مدیریت مدارک ذخیره شوند، احتمال از دست رفتن برخی از اطلاعات وجود دارد. برای مثال: هنگام پویش مدارک کاغذی، ممکن است وضوح به شکلی باشد که نویسه‌های کوچک در تصویر رقمی، ناخوانا باشند؛ یا وقتی مدارک رقمی به قالب دیگری تبدیل می‌شوند، برخی از فراداده‌ها از دست می‌روند.

وقتی که رسانه ذخیره‌سازی تغییر می‌کند، شواهد فیزیکی (مانند: اثر انگشت روی مدارک کاغذی یا لوح‌های فشرده) در شیء الکترونیکی بازتولید نخواهند شد. در این موارد، سازمان باید هر نوع فقدان احتمالی اطلاعات را بررسی کرده و درباره پذیرش یا عدم پذیرش این فقدان در مراحل اداری، تصمیم‌گیری کند. اگر فقدان اطلاعات قابل قبول نیست، توصیه می‌شود، برای اطمینان از دریافت/ نگهداری اطلاعات اقداماتی صورت پذیرد.

۶-۳-۳ ایجاد و ورود اطلاعات

ممکن است اطلاعات الکترونیکی در سیستم قابل اعتماد مدیریت مدارک ایجاد یا وارد آن شده باشند. اطمینان‌پذیری مدارک در زمان ایجاد یا ورود به سیستم حائز اهمیت فراوان است و به همین دلیل سیستم قابل اعتماد مدیریت مدارک به‌طور پیوسته اطلاعات ذخیره شده را بازتولید می‌کند.

اطلاعات الکترونیکی را می‌توان در دو قالب تصویر یا داده، ذخیره کرد. می‌توان هر دو نوع این اطلاعات را در قالب‌های مختلف وارد سیستم قابل اعتماد مدیریت مدارک کرد.

قالب‌های تصویر عموماً از منابع زیر به‌دست می‌آیند:

الف- مدارک کاغذی (مدارک اصلی، رونوشت‌ها، نمابرها)؛

ب- مدخل پست تصویری خودکار[1] (از طریق کارساز نمابر[2])؛

پ- دریافت نماگرفت[3] ، وقتی که بخش‌های متعددی از اطلاعات به‌طور همزمان به نمایش در می‌آیند (که به‌عنوان مدارک ناپایدار مرکب[4] نیز شناخته می‌شود)؛

ت- میکروفیلم و ریزفیش[5].

قالب‌های تصویر عموماً الگوهای دودوئی[6] از مدرک غیررقمی[7] اصلی هستند. قالب‌های تصویر را می‌توان از مدارک رقمی نیز به‌دست آورد. جزئیات مربوط به روش‌های دریافت مدارک غیررقمی در قالب تصویری در بند ۶-۴ توضیح داده شده است.

قالب‌های داده، اطلاعات را در قالب «اصلی[8]» ذخیره کرده و ممکن است مستلزم استفاده از نرم‌افزار نرم‌افزار اصلی برای بازیابی اطلاعات موجود باشد. قالب‌های استانداردی وجود دارد که می‌توان آنها

---

1 - Automatic facsimile entry
2 - Fax server
3 - Screenshot
4 - Compound transient documents
5 - Microfiche
6 - Bit maps
7 - Analogue
8 - Native

را از بسته‌های نرم‌افزاری (برای مثال: پرونده‌های حاوی متن[1]، پرونده‌های مجزاشده توسط ویرگول[2] ویرگول[2]) بازیابی کرد. نمونه‌هایی از قالب داده‌ها به شرح زیر هستند:

الف- سیستم‌های اداری[3] مانند پردازش‌گرهای کلمه، صفحه گسترده‌ها و غیره؛

ب- نقشه‌های CAD؛

پ- پیام‌های الکترونیکی؛

ت- پرونده‌های تبادل داده‌های الکترونیکی (EDI)[4]؛

ث- پیام‌های پیوسته[5]؛

ج- پیام‌های زبان نشانه‌گذاری گسترش‌پذیر (ایکس‌ام‌ال)[6]؛

چ- نماگرفت‌ها (مثلاً، مدارک ناپایدار).

توصیه می‌شود، در تمام موارد، اطلاعات موجود در این داده‌ها با استفاده از برنامه‌های نرم‌افزاری مناسب قابل دسترسی باشد. جزئیات مربوط به روش‌های دریافت مدارک غیررقمی در قالب داده در بند ۶-۵ توضیح داده شده است.

یادآوری- امکان وجود مدارک رقمی در قالب‌های ترکیبی تصویر و داده (مثلاً یک حرف در قالب Word با امضای دودوئیِ جاسازی‌شده) هم وجود دارد.

زمانی که اطلاعات در سیستم قابل اعتماد مدیریت مدارک الکترونیکی ذخیره می‌شود که خارج از محدوده کنترل سازمان قرار دارد، ممکن است آگاهی یا کنترلی روی روش‌های دخیل در ایجاد یا اعطاء مجوز به آن اطلاعات وجود نداشته باشد. در این شرایط، لازم است سازمان به موارد زیر دقت داشته باشد: اطلاعات همان چیزی هستند که باید باشند، اطلاعات تغییر نکرده‌اند و هویت ایجادکننده اطلاعات مشخص است. سطح بررسی این معیارها به ماهیت اطلاعات خاص مورد نظر، بستگی دارد.

چنین موقعیت‌های محدودکننده‌ای در سازمان نیز وجود خواهند داشت. در این شرایط، بخشی از سازمان که دارای سیستم قابل اعتماد مدیریت مدارک است نمی‌تواند به این دلیل که اطلاعات از بخش دیگری از همین سازمان آمده‌اند، چنین فرض کند که تصویر یا پرونده داده، دقیقاً همان چیزی هستند که باید باشند.

1 - Text file
2 - Comma-separated delimited files
3 - Office systems
4 - Electronic Data Interchange
5 - Instant messages
6 - XML: Extensible Markup Language

۶-۳- ۴ فراداده‌ها

توصیه می‌شود، وقتی که مدارک رقمی و/ یا غیر رقمی ایجاد یا وارد می‌شوند با دقت اطمینان حاصل شود که فراداده‌های مرتبط نیز منتقل شده‌اند. بهتر است، اطمینان حاصل شود که فراداده‌های ضروری دریافت شده و مدارک رقمی / غیر رقمی تفسیر صحیحی دارند.

ممکن است لازم باشد کامل و مناسب بودن محتوای فراداده‌ها مورد بررسی قرار گیرد. دسترس‌پذیری کل مجموعهٔ فراداده‌ها با محتوای مناسب، ارزش شهودی اطلاعات موجود در آنها را افزایش می‌دهد. بهتر است، استفاده از طرح‌های فراداده‌ای نیز در نظر گرفته شود.

۶-۴ دریافت تصویر مدرک

۶-۴-۱ کلیات

این زیربند شامل توصیه‌های مرتبط با روش‌های ایجاد تصاویر رقمی از مدارک غیر رقمی است. توصیه‌های این بخش برای کاربرانی ارائه شده که سیستم قابل اعتماد مدیریت مدارک آنها شامل دریافت و ذخیره مدارک غیر رقمی در قالب رقمی با استفاده از پویشگرها[1] است. این توصیه‌ها، روش‌های زیر را پوشش می‌دهد:

الف- آماده‌سازی مدارک؛

ب- دسته‌بندی مدارک؛

پ- رونوشت‌برداری؛

ت- پویش؛

ث- پردازش تصویر.

۶-۴-۲ آماده‌سازی مدارک کاغذی

لازم است تمام مدارک کاغذی قبل از فرایند پردازش مورد بررسی قرار گیرند تا اطمینان حاصل شود که تصویر مناسبی به دست آمده است. خصوصیاتی مانند: اندازه کاغذ، وزن و شیرازه و رنگ نسخه چاپی، فرایند پویش فیزیکی را تحت تأثیر قرار می‌دهند.

لازم است مدارک کاغذی قبل از فرایند پردازش مورد کنترل قرار گیرند تا از مناسب بودن آنها برای پویش، اطمینان حاصل شود. توصیه می‌شود، روش‌های به‌کارگرفته‌شده برای این کنترل‌ها مستند شوند.

بهتر است، عواملی مانند شرایط فیزیکی (کاغذهای نازک، چروک، منگنه‌شده و غیره) و خصوصیات اطلاعات (سیاه و سفید، رنگی، محدوده توناژ و غیره) را در نظر گرفت.

اگر مدارک کاغذی کیفیت مطلوب نداشته باشند و احتمال پذیرش آنها در دستگاه پویشگر کم باشد، روش‌هایی وجود دارد که می‌توان از آنها استفاده کرد. به‌طور مثال: بهتر است، از مدرک اصلی رونوشت تهیه یا از پوشش‌های شفاف استفاد کرد.

---

1 - Scanners

بهتر است، روش‌های استفاده‌شده برای مدارک کاغذی که موجب بروز مشکل در پویش می‌شوند، مستند شود.
هنگام برداشتن منگنه‌ها، گیره‌ها یا شیرازه‌های دیگر، اطمینان حاصل کنید که هیچ آسیبی به مدرک اصلی وارد نمی‌شود که دریافت اطلاعات از مدرک را تحت تأثیر قرار دهد.
توصیه می‌شود، وقتی که مدرک کاغذی دارای ضمیمه‌های فیزیکی مانند کاغذهای یادداشت چسبی است، سیستم امکان تشخیص این ضمیمه‌ها از مدرک اصلی را داشته باشد.
این کار با دریافت تصویری مجزا از ضمیمه همراه با داده‌های مرتبط با صفحهٔ منبع، امکان‌پذیر است. اگر تصویر فقط در حالی گرفته می‌شود که ضمیمه به مدرک متصل است، بهتر است، داده‌ها بیانگر این حقیقت باشند که ضمیمه‌ای به مدرک متصل است. اگر این ریسک وجود دارد که ضمیمه باعث پوشاندن یا تار شدن اطلاعات روی مدرک کاغذی شود، بهتر است، اطمینان پیدا کنیم که تصویری از مدرک کاغذی بدون ضمیمه آن، دریافت شده است.
توصیه می‌شود، وقتی که مدرک کاغذی دارای اصلاحیه‌های فیزیکی مانند رنگ مات سفید است، اطمینان پیدا کنیم که وجود این اصلاح در سیستم ذکر شده است.
بهتر است، روش‌های به‌کارگرفته‌شده هنگام پویش مدارک کاغذی چند برگی که با منگنه یا گیره به هم متصل شده‌اند، مستند شود.
توصیه می‌شود، تمام صفحات مدارک کاغذی چند برگی قبل، بعد و حین پویش، کنار هم و به ترتیب نگهداری شوند.

۶-۴-۳ دسته‌بندی مدارک

در صورت امکان، بهتر است، مدارک کاغذی برای پویش دسته‌بندی شوند.
دسته‌بندی مدارک، کنترل مدارک کاغذی را آسانتر کرده و امکان انجام کنترل کیفیت و روش‌های دیگر بر اساس نمونه‌گیری را فراهم می‌آورد.
تعداد مدارک کاغذی موجود در هر دسته به ابزار استفاده‌شده، بستگی دارد. برای مثال: اگر مدارک در پوشش‌های پرونده قرار دارند، میانگین تعداد مدارک به ازای هر پوشش پرونده تقریباً زیاد، برای مثال: ۱۰۰ صفحه، خواهد بود؛ پس مدارک موجود در هر پوشش پرونده مستقل می‌توانند یک دسته را تشکیل دهند. اگر پوشش پرونده حاوی تعداد کمی از مدارک، برای مثال: ۱۰ صفحه است، هر دسته می‌تواند از بیش از یک پوشش پرونده تشکیل شود. اگر مدارک روی حلقه‌های ریزفیلم هستند، هر حلقه را می‌توان یک دسته در نظر گرفت.
اندازه دسته را طوری انتخاب کنید تا حجم آن بزرگتر از حدی نشود که مدیریت آن را دشوار کند و همچنین حجم آن کمتر از حدی نباشد که بررسی کیفیت با نمونه‌گیری از دسته، منجر به ناکارآمدی چشمگیر فرایندها شود. ممکن است لازم باشد تا اندازهٔ نمونه با استفاده از روش‌های نمونه‌گیری آماری تعیین شود.

برای برخی از کاربردها، نمی‌توان دسته را به‌راحتی تعریف کرد. در این موارد، دسته را می‌توان به‌عنوان داده‌های ورودی مدارک کاغذی در یک دوره زمانی خاص، تعریف کرد. به‌عنوان مثال: یک دسته می‌تواند تمام داده‌های مدرک در یک ساعت یا یک روز را شامل شود.
در مورد برخی از کاربردها (مخصوصاً جایی که گردش کاری اجرا می‌شود) که نمی‌توان دسته را به کار گرفت، بهتر است، برای اطمینان از اینکه تمام مدارک کاغذی پویش شده‌اند، روش‌های جایگزینی ایجاد کرد. این روش‌ها شامل نشانه‌گذاری مدارک پس از پویش یا کنترل بیشتر تصاویر در مقایسه با کاغذهای اصلی است.

۶-۴-۴ رونوشت‌برداری

برای برخی از مدارک کاغذی، رونوشت‌برداری از آنها قبل از پویش، کمک‌کننده خواهد بود. این مدارک عبارتند از:
الف- مدارکی که به‌طور معکوس تحت تأثیر فرایند پویش قرار می‌گیرند، مانند: مدارک آسیب‌دیده یا حساس؛
ب- مدارکی که در آن تغییرات اساسی کنتراست یا تراکم در محوطه اصلی وجود داشته و رونوشت‌برداری به‌طور آشکار باعث ارتقای کیفیت تصویر می‌شود؛
پ- مدارک حاوی کاغذ یا رنگ‌های جوهری که باعث ایجاد تصاویر پویش‌شده ناخوانا می‌شوند.

یادآوری ۱- ممکن است دستگاه‌های رونوشت‌برداری و پویش پاسخ‌های متفاوتی به رنگ‌های مختلف نشان دهند و فقط در برخی موارد استثنائی، روش‌های رونوشت‌برداری قبل از پویش باعث ایجاد نتایج رضایت‌بخش نمی‌شود.

ت- مدارک تا شده که اندازهٔ آنها بزرگتر از حدی است که به عنوان یک تصویر کامل، پویش شوند.

یادآوری ۲- هنگام پویش می‌توان از کاهش- تصویر استفاده کرده / می‌توان از مدارک اصلی یا از رونوشت‌های آن، تصاویر پویش‌شده متعدد دریافت کرد.

بهتر است، رونوشت‌ها کنترل شوند تا اطمنیان حاصل شود در این مرحله، فقدان اطلاعات رخ نداده است.
توصیه می‌شود، جایی که قبل از مرحله پویش از مدارک کاغذی رونوشت تهیه شده است، روش استفاده‌شده در شیوه‌نامه اجرایی مستند شود.
بهتر است، روش‌های بیشتر کنترل کیفیت ایجاد شوند تا اطمینان حاصل شود که حین پویش مدارک کاغذی رونوشت‌برداری‌شده، اطلاعات مهم از دست نرفته‌اند.
در صورت کاهش- تصویر، بهتر است، کنترل‌هایی انجام شود تا اطمینان پیدا کنیم که بر اثر وضوح مؤثر تصویر کوچک‌شده (در مقایسه با مدرک اصلی) تصاویر پویش‌شده در مقایسه با کاغذ اصلی دچار فقدان اطلاعات نشده‌اند.

در صورتی که تصاویر متعدد دریافت شده‌اند، این تصاویر باید روی‌هم قرار گیرند تا اطمینان حاصل شود که در لبهٔ بین تصاویر مجاور هم، فقدان اطلاعات رخ نداده است.
وقتی که از روی رونوشت تصویری ایجاد می‌شود، بهتر است، این موضوع برای کاربر روشن باشد. همچنین بهتر است، مشخص باشد که حین آماده‌سازی مدرک از روی مدرک کاغذی، رونوشت تهیه شده و اینکه مدرک کاغذی به عنوان یک رونوشت شناخته می‌شود. این کار انجام می‌شود تا اطمینان پیدا کنیم که حتی اگر به عنوان بخشی از مراحل آماده‌سازی، یک رونوشت میانجی تهیه شده، آن تصویر به درستی به عنوان رونوشت اصلیِ یک مدرک کاغذی مشخص می‌شود و این تصاویر از رونوشت‌هایی که در شرایط نامشخص تهیه شده‌اند، قابل تمایز هستند.
این کار حین مراحل آماده‌سازی، با مهر یا نشانه‌گذاری کردن مدرک به عنوان رونوشت یا رونوشت اصلی یا با نشانه‌گذاری الکترونیکی تصویر به عنوان تصویری که از رونوشت دریافت شده، انجام می‌شود و بین رونوشت‌های تهیه‌شده حین آماده‌سازی مدرک و مدارکی که به عنوان رونوشت شناخته می‌شوند، تمایز قائل می‌شود.
توصیه می‌شود، روش‌هایی که برای تعیین اصلی یا رونوشت بودن مدرک کاغذی به کار گرفته می‌شود، مستند شود.

۶-۴-۵ فرایندهای پویش

بهتر است، جزئیات مربوط به روش‌های استفاده‌شده در پویش مدارک غیر رقمی در شیوه‌نامه اجرایی ارائه شود.
توصیه می‌شود، هرگونه تغییر در روش‌های پویش به سبب نوع مدرک پویش‌شده در شیوه‌نامهٔ اجرایی شرح داده شود.
برای مثال ممکن است این تغییرات برای مدارک کاغذی یک رویه در مقابل مدارک کاغذی دو رویه یا تصاویر رنگی در مقابل تصاویر سیاه و سفید، به‌کار گرفته شود.
توصیه می‌شود، رویه‌ها باعث اطمینان یافتن از این موضوع شوند که تمام مدارک کاغذی در یک دسته، به‌طور کامل پویش شده و هیچ مدرک پویش‌نشده‌ای وجود ندارد.
توصیه می‌شود، به منظور کنترل اینکه تمام مدارک پویش شده‌اند، تعداد تصاویر دریافت‌شده با تعداد مدارک موجود در هر دسته، مقایسه شود. وقتی که از دسته‌بندی استفاده نمی‌شود، برای اطمینان یافتن از اینکه همه مدارک پویش شده‌اند، استفاده از روش‌های جایگزین، ضروری است.
توصیه می‌شود، وقتی که لازم است تمام صفحات در یک مدرکِ حاوی برگه‌های متعدد پویش شوند، برای اطمینان از پویش تمام صفحات، روش‌هایی به‌کار گرفته شود.
تعداد تصاویر دریافت‌شده به ازای هر مدرک باید با تعداد صفحات در هر مدرک مقایسه شده و فرایند حذف صفحات خالی را در نظر گرفت. هر چند، خطا در شمارش دستی مدارک کاغذی فیزیکی و تعداد صفحات موجود در آن، این فرایند را بی‌نتیجه می‌کند. به‌کارگیری این رویه‌ها در شرایطی رضایت‌بخش خواهد بود که ریسک عدم پویش مدارک به‌طور قابل قبولی، کم باشد. بهتر

است، میزان این ریسک ارزیابی شده و در صورت نیاز از روش‌هایی برای بررسی این ریسک استفاده شود.

بسیاری از پویشگرها دارای تغذیه‌کننده خودکار[1] مدارک کاغذی هستند که به طور مطمئن، عدم تغذیه مدارک را مشخص و بنابراین ریسک گذشتن یک مدرک از پویشگر بدون پویش آن را کاهش می‌دهد. اگر دستگاه فاقد چنین تجهیزات جانبی است، به روش‌هایی نیاز داریم تا اطمینان پیدا کنیم که فرد پویش‌کننده، تمام مدارک را به صورت دستی در دستگاه قرار داده است تا احتمال عدم پویش مدارک را کاهش دهد.

توصیه می‌شود، وقتی حصول اطمینان از پویش همه صفحات لازم است، کاربران به منظور دریافت صحیح تعداد صفحات به ازای هر مدرک یا به ازای هر دسته از مدارک، شمارش یا شاخص‌گذاری قبلی مدارک کاغذی را در نظر بگیرند.

استفاده از روش دو مدخلی می‌تواند تا حد زیادی درستی تعداد صفحات را افزایش دهد. بعداً می‌توان این داده‌ها را با تعداد صفحات پویش‌شده مقایسه کرد؛ هر گونه کسری در تعداد مشخص می‌کند که بیش از یک صفحه وارد دستگاه پویشگر شده یا صفحات بین شاخص‌گذاری قبلی و پویش، در مکان نادرستی قرار گرفته‌اند.

در صورت استفاده از پویشگر یک رویه[2] (یعنی پویشگرهایی که هر بار فقط یک سمت از مدرک کاغذی را پویش می‌کنند) برای پویش مدارک دو رویه[3]، باید دقت شود تا از پشت و رو شدن مدرک و پویش سمت مقابل آن، اطمینان حاصل شود.

اگر مدارک بزرگ به صورت بخش‌بخش پویش می‌شوند، تصاویر متعددی دریافت می‌شود؛ بهتر است، این بخش‌ها روی هم قرار گیرند تا از عدم فقدان اطلاعات بین لبه‌های تصاویر مجاور، اطمینان حاصل شود.

بهتر است، سیستم پویشگر قادر باشد هر مدرک رقمی را به صورت منحصر به فرد و به روشی شناسایی کند که به جز در مواردی که در بند ۷-۱۱ مجاز است، منحصر به فرد بودن مدرک رقمی تغییر نکرده یا حذف نشود.

این ویژگی منحصربه‌فرد می‌تواند اعداد متوالی باشد که سیستم ایجاد کرده و فقط برای کنترل داخلی به‌کار می‌رود.

۶-۴-۶ کنترل کیفیت

۶-۴-۶-۱ مجموعهٔ نمونه

به رویه‌هایی نیاز داریم تا ریسک پایین آمدن کیفیت تصاویر پویش‌شده را کاهش دهد. اگر بتوانیم نشان دهیم که تصاویر از کیفیت مناسبی برخوردار هستند و دستگاه پویشگر در زمان پویش مطابق با استانداردهای پذیرفته‌شده کار کرده است، اثبات اطمینان‌پذیری تصاویر آسان‌تر خواهد بود.

1- Automatic feeder
2 - Simplex scanners
3 - Double-sided documents

توصیه می‌شود، به منظور ارزیابی نتایج پویش درمقایسه با معیارهای پذیرفته‌شدهٔ کنترل کیفیت، یک مجموعهٔ نمونه از مدارک گردآوری شود. بهتر است، مدارک موجود مجموعهٔ نمونه نمایانگر کل مجموعه مدارکی باشد که پویش خواهند شد. توصیه می‌شود، مدارک موجود در مجموعهٔ نمونه دربردارندهٔ نمونه‌هایی از مدارک کاغذی باشند که کیفیت آنها در مقایسه با اکثر مدارک، کمتر است.
معیارهای کنترل کیفیت موارد زیر را پوشش می‌دهد:

الف- خوانایی کلی؛

ب- کوچک‌ترین جزئیاتی که به صورت خوانا دریافت شده‌اند (یعنی، کوچک‌ترین اندازه برای متن؛ وضوح نشانه‌های نقطه‌گذاری، شامل نقطه‌های اعشاری)؛

پ- کامل بودن جزئیات (یعنی مقبولیت نویسه‌های گسسته، بخش‌های از دست‌رفتهٔ خطوط)؛

ت- درستی ابعاد در مقایسه با مدرک اصلی؛

ث- لکه‌های ایجادشده توسط دستگاه پویشگر (یعنی لکه‌هایی که روی مدرک اصلی وجود ندارند)؛

ج- کامل بودن سطح کلی تصویر (یعنی اطلاعات از دست‌رفته در لبه‌های سطحی تصویر)؛

چ- تراکم سطح سیاه رنگ؛

ح- درستی رنگ‌ها.

بهتر است، با توجه به ماهیت منبع و خصوصیات ابزار پویش، معیارهای کنترل کیفیت برای کیفیت تصویر واقع‌گرایانه باشند.

توصیه می‌شود، معیارهای کنترل کیفیت برای کیفیت تصاویر پویش‌شده مستند شوند. بهتر است، این معیارها از سوی تمام گروه‌هایی که استفادهٔ آنها از تصاویر تحت تأثیر کیفیت تصویر قرار خواهد گرفت، مانند کاربران داخلی و بیرونی، مورد قبول قرار گیرد.

بهتر است، معیارهای کنترل کیفیت بر اساس مجموعهٔ نمونه از مدارک کاغذی باشد.

۶-۴-۶-۲ ارزیابی کیفیت تصویر

توصیه می‌شود، روش‌هایی که فرایندهای استفاده‌شده برای ارزیابی روزانهٔ کیفیت تصویر را مشخص می‌کنند، مستند شوند.

بهتر است، روش‌های ارزیابی کیفیت تصویر شرح کامل نتایج ارزیابی، شامل خصوصیات دستگاه بازیابی تصویر را دربرداشته باشد.

توصیه می‌شود، هنگام ارزیابی نتایج روش‌های کنترل کیفیت، دقت شود. ممکن است نتایج به‌دست‌آمده به دستگاه خاص خروجی (مانند نمایشگر یا چاپگر)، بستگی داشته باشد.

اگر برای روش‌های کنترل کیفیت از دستگاه چاپگر استفاده می‌شود، بهتر است، وضوح چاپگر برابر با وضوح تصاویر پویش‌شده یا بیشتر از آن باشد.

توصیه می‌شود، دستگاه چاپگر قادر به بازتولید صحیح طیف خاکستری یا رنگی در برنامه‌های کاربردی مرتبط باشد.

بهتر است، وقتی مسئله بازتولید طیف خاکستری یا رنگی مطرح است، درجهٔ دقت اجرای طیف خاکستری یا رنگی ارزیابی شود.

توصیه می‌شود، وقتی درجهٔ دقت ابعادی مهم است، روش‌های استفاده‌شده برای کنترل اطلاعات ابعادی که در رواداری موردنظر بازتولید شده‌اند، مستند شود. به‌طور نمونه این کار می‌تواند شامل کنترل درجهٔ دقت وضوح اسمی باشد به‌طوری‌که ابعاد در تصویر رقمی را بتوان با شمارش تعداد نقاط بین محل‌های مشخص در تصویر، تعیین کرد.

اگر متصدی پویش حین پویش، کیفیت تصاویر را کنترل می‌کند، کارکنانی غیر از افراد مسئول پویش باید دومین کنترل کیفیت را انجام دهند. ممکن است دومین کنترل کیفیت شامل روش‌های نمونه‌گیری آماری باشد.

توصیه می‌شود، روش‌های کنترل کیفیت با فرایند دسته‌بندی که در بند ۶-۴-۳ تعریف شد، مرتبط بوده و پذیرش یا عدم پذیرش هر دسته را به صورت مستقل از سایر دسته‌ها، امکان‌پذیر سازد.

بهتر است، نتایج کنترل کیفیت در دفتر کنترل کیفیت ذخیره شوند (که این دفتر را می‌توان به صورت دستی یا خودکار ایجاد کرد).

در محیط‌های گردش کاری که هر مدرک رقمی در فرایند گردش کاری در نظر گرفته شده و به‌طور آشکار اقداماتی برای کنترل کیفیت تصویر و عدم پذیرش تصاویر بی‌کیفیت صورت می‌پذیرد، بهتر است، این اقدامات را به عنوان یکی از فرایندهای کنترل کیفیت در نظر گرفت.

هرگاه روش‌های کنترل کیفیت شامل نمونه‌گیری از تصاویر پویش‌شده و داده‌های مرتبط (مانند یادداشت‌ها) باشد، نیازی به ثابت شدن بخش نمونه‌گیری‌شده نیست، اما امکان دارد در زمان‌های مختلف، بسته به تناوب مشکلات مواجه‌شده یا ماهیت منبع، متفاوت باشد. توصیه می‌شود، در صورت مناسب بودن، برای تعیین درصد تصاویر پویش‌شده که باید بررسی شوند از روش‌های نمونه‌گیری آماری استفاده کرد. برای کسب اطلاعات بیشتر درباره نمونه‌گیری به استاندارد ISO 2859-1 مراجعه شود.

معمولاً کنترل تمام منابع پردازش‌شده عملی نبوده و عموماً فقط بخشی از منابع پردازش‌شده مورد کنترل قرار خواهند گرفت. به‌عنوان مثال: در ابتدای پویش، نمونهٔ نسبتاً بزرگی از مدارک (مانند: ۲۰ درصد) انتخاب می‌شود؛ همان‌طور که مطابقت با استانداردهای کیفی مورد نیاز نشان می‌دهد می‌توان این نمونه را (برای مثال: تا ۱۰ یا حتی تا ۵ درصد) کاهش داد.

توصیه می‌شود، جایی که کنترل کیفیت شامل نمونه‌گیری از تصاویر پویش‌شده است، تناوب نمونه مستند شود.

۶-۴-۶-۳ بررسی عملکرد دستگاه پویشگر

برای نظارت بر سیستم و قرار داشتن آن در رواداری پذیرفته‌شده بهتر است، بررسی عملکرد دستگاه پویشگر به شکل دوره‌ای انجام شود.

نسخه‌های چاپ‌شده را می‌توان از تصاویر پویش‌شدهٔ نمونه‌های آزمایشی تهیه و برای تعیین تحقق معیارهای کیفی که در روش‌ها توصیف شده‌اند، با اهداف آزمون مقایسه کرد.
اهداف آزمون امکان ارزیابی و اندازه‌گیری عملکرد پویشگر را فراهم می‌آورد. استفاده مکرر نشان می‌دهد که آیا پویشگر به‌طور پیوسته و مطابق با مشخصه‌ها، عمل کرده است. برای این ارزیابی‌ها می‌توان از آزمون هدف ارائه‌شده در استاندارد ISO 12653-2 استفاده کرد.
بهتر است، تناوب کنترل‌های عملکرد دستگاه پویشگر به کاربرد سیستم وابسته بوده و با نقش موردانتظار در عملکرد سیستم، مرتبط باشد. ممکن است انجام این کار مستلزم به‌کارگیری توصیه‌های تأمین‌کننده و همچنین تجربهٔ استفاده از این سیستم باشد. در ابتدا ممکن است پویش یک هدف آزمون برای چند صد برگ اولیهٔ پویش‌شده، مناسب باشد.
در صورت استفاده از دستگاه‌های پویشگر دو رویه، ترجیحاً باید از اهداف آزمون دو رویه استفاده شود. فقط در صورت عدم دسترسی به اهداف آزمون دو رویه باید از اهداف آزمون یک رویه در دستگاه‌های پویشگر دو رویه استفاده شود.
اهداف آزمون نشانگر مدارک کاغذی پویش‌شده نبوده و بهتر است، به‌عنوان جایگزینی برای مجموعهٔ نمونه مدارک در نظر گرفته نشود.

۶-۴-۷ پویش مجدد

توصیه می‌شود، روش‌های استفاده‌شده برای پویش مجدد مدارک کاغذی مستند شود. اگر تصویر اصلی به دلیل کیفیت پایین یا عوامل دیگر مورد قبول قرار نگیرد، پویش مجدد انجام می‌شود.
بهتر است، روش‌هایی به‌کار گرفته شود تا از جایگزینی تصاویر اصلی به جای تصاویر حاصل از پویش مجدد و به خطر نیفتادن تعداد دسته‌ها و مراحل ممیزی، اطمینان حاصل شود.

۶-۴-۸ پردازش تصویر

توصیه می‌شود، روش‌های پردازش تصویر که برای ارتقای کیفیت به‌کارگرفته می‌شوند در شیوه‌نامه اجرایی شرح داده شود.
بهتر است، در صورت امکان استفاده از تجهیزاتی که توسط افراد کنترل می‌شوند، جزئیات مربوط به وسیله به‌کارگرفته‌شده برای یک مدرک رقمی خاص، مستند شود.

۶-۵ دریافت داده‌ها

۶-۵-۱ داده‌های جدید

داده‌ها را می‌توان از مدارک غیر رقمی / رقمی کنونی دریافت و به روش‌های مختلف از جمله روش دستی (یعنی وارد کردن مستقیم داده‌ها با صفحه کلید)، خودکار (رمزینه‌خوان[1]، نشان خوان نوری[2]،

1 - Bar code
2 - OMR: Optical Mark Reading

نویسه خوان هوشمند/ نویسه خوان نوری[1]) یا نیمه خودکار (جایی که داده‌ها به صورت خودکار برای مثال با «نویسه خوان نوری» دریافت شده و با ورود دستی، تأیید می‌شوند)، وارد رایانه شوند. موضوع همه این موارد ابراز اطمینان از دریافت داده‌های صحیح است. در عمل، اطمینان از صحت ۱۰۰ درصدی در دریافت داده، دشوار اما ممکن است و کاربر باید ریسک مرتبط با وجود خطا را ارزیابی کند.

توصیه می‌شود، وقتی که داده‌های بیرونی برای ثبت در سیستم دریافت می‌شوند، سطح کیفی موردنیاز مشخص شود. بهتر است، سطوح کیفی درستی و کامل بودن داده‌های دریافت‌شده را پوشش دهد.

با توجه به کاربرد و اهمیت هر کدام از داده‌ها، سطوح کیفی مشخص‌شده متفاوت است.

توصیه می‌شود، برای کنترل دست‌یابی به سطح درستی، روش‌هایی تعریف شود. بهتر است، این روش‌ها عموماً بر اساس نمونه‌گیری تصادفی یا نیمه تصادفی از دسته داده‌های دریافت‌شده، با مقایسه آنها با منبع باشد. به‌طورکلی، دسته‌هایی که درستی آنها تأیید نمی‌شود، دوباره پردازش شده و نتایج مجدداً کنترل شود تا از حصول سطح درستی موردنظر، اطمینان یابیم.

توصیه می‌شود، سوابق مربوط به نتایج کنترل درستی داده‌ها نگهداری شود.

بهتر است، وقتی که داده‌ها از یک مدرک الکترونیکی استخراج می‌شوند، مدرک اصلی ذخیره و با داده‌های استخراج‌شده، مرتبط شود.

۶-۵-۲ انتقال و گذار

وقتی که داده‌ها به عنوان بخشی از فرایند گذار سیستم ذخیره‌سازی، از سیستم دیگر (یا بخشی از سیستم) دریافت می‌شوند، لازم است برای این مرحله، روش‌ها و فرایندهایی ایجاد، اجرا و مستند شود.

توصیه می‌شود، وقتی که اطلاعات از قالب کنونی به قالب جدید منتقل می‌شود، هرگونه فقدان اطلاعاتِ (از جمله اطلاعاتِ مراحل ممیزی) ناشی از این فرایند مستند شود.

۶-۶ نمایه‌سازی

۶-۶-۱ کلیات

نمایه‌سازی یکی از بخش‌های مهم فرایند ذخیره‌سازی اطلاعات روی رسانه‌های الکترونیکی است به طوری‌که امکان دسترسی به اطلاعات مرتبط را امکان‌پذیر می‌سازد. وقتی نمایه‌های اطلاعات از بین می‌رود، ممکن است اطلاعات ذخیره‌شده هم از بین برود.

نمایه‌سازی می‌تواند به‌صورت خودکار (یعنی توسط سیستم و بدون دخالت متصدی) یا دستی، انجام شود. در صورتی که نمایه‌سازی به صورت دستی انجام شود، اطمینان از مطابقت با روش‌های مستند، ضروری است.

1 - OCR/ICR: Optical Character Recognition/ Intelligent Character Recognition

برخی سیستم‌ها پس از دریافت اطلاعات، امکان ذخیره‌سازی اطلاعات جزئی نمایه را امکان‌پذیر می‌سازد. ذخیره‌سازی اطلاعات جزئی می‌تواند با ثبت دستی نمایه‌ها در زمان دیگر، ترکیب شود.
توصیه می‌شود، روش‌ها و قوانین نمایه‌سازی اطلاعات ذخیره‌شده، مستند شود.

۶-۶-۲ نمایه‌سازی دستی

نمایه‌سازی دستی شامل بررسی بصری اطلاعات دریافت‌شده توسط سیستم، قبل از دریافت یا به‌عنوان بخشی از فرایندهای پس از دریافت است.
بهتر است، کارکنانی که نمایه‌سازی دستی را انجام می‌دهند از آموزش‌های تخصصی لازم بهره‌مند شوند تا دقت و درستی کار افزایش یابد. توصیه می‌شود، الزامات و روش‌های آموزشی نمایه‌سازی، مستند شود.

۶-۶-۳ نمایه‌سازی خودکار

ممکن است نمایه‌سازی خودکار تحت تأثیر رمزینه‌خوان‌ها یا استفاده از روش‌های نویسه‌خوان نوری/ نویسه‌خوان هوشمند، قرار گیرد.

۶-۶-۴ ذخیره‌سازی نمایه

توصیه می‌شود، داده نمایه حداقل تا زمانی که اطلاعات مرتبط با آن نگهداری می‌شود، حفظ شود.
در برخی از سیستم‌ها عموماً به منظور ارتقای عملکرد پایگاه داده‌ها، لازم است پایگاه داده‌های نمایه، به‌صورت دوره‌ای بازسازی شود.

۶-۶-۵ اصلاحات نمایه

ممکن است فرایندهای نمایه‌سازی شامل روش‌هایی برای آشکارسازی اطلاعات از دست‌رفته باشد.
نمایه‌سازی از اطلاعات نمایش‌داده‌شده باعث آشکار شدن اطلاعات از دست‌رفته نمی‌شود مگر اینکه اطلاعات نمایش‌داده‌شده در مقابل اطلاعات اصلی بررسی شده و یا یک توالی تعریف‌شده (برای مثال: با عددگذاری متوالی) از اطلاعات وجود داشته باشد.
توصیه می‌شود، روش‌های تصحیح داده‌های نمایه مستند شود. اگر مدخل نمایه اصلاح شده است، بهتر است، جزئیات مربوط به محتوای نمایه، قبل و بعد از تغییر، نگهداری شود.
بهتر است، وقتی یک مدخل نمایه با اطلاعات حذف‌شده در ارتباط است، این وضعیت ذخیره شود.
توصیه می‌شود، وقتی که به دلیل اصلاح مدخل‌های نمایه، لازم است حذف اطلاعات ذخیره‌شده با الزامات قانونی یا حقوقی مطابقت داشته باشد، روش‌های پیروی‌شده برای این کار، مستند شود.

۶-۶-۶ درستی نمایه

ممکن است داده نمایه برای تصاویر پویش‌شده، نادرست باشد. درحالی‌که نمایه‌سازی درست، بازیابی اطلاعات ذخیره‌شده را تسهیل می‌کند، اطمینان‌پذیری این اطلاعات در صورتی اثبات می‌شود که

بتوان ارتباط و کامل بودن آنها را از درستی داده نمایهٔ مرتبط، مشخص کـرد. بـالعکس، داده نمایـه نادرست می‌تواند منجر به عدم توانایی کاربر در بازیابی اطلاعات مرتبط یا بازیابی اطلاعات نـامرتبط شود.

معیارهای درستی داده نمایه بسته به کاربرد، متفاوت هستند. در برخـی مـوارد، درسـتی بـه‌عنـوان حداکثر تعداد قابل قبول از نویسه‌های خطا به ازای صد نویسهٔ دریافت‌شده (یا درصد مشابه بـا آن)، تعریف می‌شود. در موارد دیگر، درستی به‌عنوان حداکثر تعداد قابل قبول کلماتِ (یـا مجموعـه‌هـای مشابه از نویسه‌ها، برای مثال: شماره مشتری یا بخش) حاوی خطا (یـک یـا بـیش از یـک نویسـه)، تعریف می‌شود.

بهتر است، برای بررسی سطح درستی، معیارهای زیر واقع‌گرایانـه باشـد: روش اسـتفاده‌شـده بـرای دریافت داده نمایه، میزان معمول خطای تصادفی کـه کارمنـدان ثبـت داده، بـه دسـت آورده‌انـد و خوانایی منبع بسته به نوع اطلاعات نمایه‌شده، سطح درستی متفاوت است.

توصیه می‌شود، وقتی که از روش‌های نمایه‌سازی دستی یا خودکار استفاده می‌شود، سطح درسـتی پذیرفته و مستند شود. بهتر است، روش‌های به‌کاررفته برای کنترل درستی دادهٔ نمایه مستند شود.

۷-۶ روش‌های مجاز ارائهٔ خروجی

ممکن است ایجاد داده‌های خروجی از سیستم‌های ذخیره‌سازی الکترونیکی، چه در قالب نسخه‌های کاغذی و چه در قالب اشیاء رقمی موجود روی رسـانه‌هـای ذخیـره‌سـازی مناسـب، بـرای اسـتفاده به‌عنوان شواهد مستند، موردنیاز باشد. عموماً به منظور کاهش احتمال عدم پذیرش یا چالش، بهتـر است، این نسخه‌ها مطابق با الزامات محلی، به‌عنوان رونوشت‌های صحیح از نسخه‌های اصـلی تأییـد شوند.

توصیه می‌شود، روش‌های ایجاد نسخه‌هایی از اطلاعات ذخیره‌شده که ممکن است به‌عنوان شـواهد مستند مورد استفاده قرار گیرند، مستند شود. ممکن اسـت چنـین روش‌هـایی مسـتلزم اسـتفاده از خصوصیات استاندارد سیستم برای رونوشت‌برداری و تأیید کتبی از فـرد مجـاز باشـد کـه مشـخص می‌کند مرحله رونوشت‌برداری به درستی انجام شده است. روش‌ها مشخص می‌کنند که بعداً از ایـن نسخه‌ها چگونه استفاده خواهد شد. ممکن است این روش‌ها بـه عنـوان داده‌هـای مراحـل ممیـزی شناخته شوند چرا که مراحل انجام‌شده حین رونوشت‌برداری را تأیید می‌کنند.

توصیه می‌شود، وقتی که مدرک کاغذی به عنوان بخشی از داده خروجی ایجـاد مـی‌شـود، روش‌هـا شامل استفاده از امضای مجاز یا روش‌های دیگر برای تأیید درستی رونوشت مدرک باشد.

بهتر است، که ماهیت و گستره تغییرات ایجادشده توسط ابزارهای بازیابی شـناخته و ارتبـاط آنهـا، سنجیده شود. ممکن است آنچه که در کاربردهای عادی قابـل قبـول در نظـر گرفتـه مـی‌شـود، در شرایط دیگری که مستلزم وجود داده‌های خروجی برای استفاده به عنوان شاهد اسـت، قابـل قبـول نباشد. برای مثال:

الف- ممکن است تبدیل تصویر رنگی به تک رنگ در شرایطی قابل قبول باشد که مسئله رنگ نامرتبط است اما در شرایط دیگری که رنگ مهم است، وجود ابزار بازیابی متفاوت لازم است؛
ب- ممکن است دیدن تصویر با وضوح پایین‌تر از آنچه که در پویش کاغذ اصلی مورد استفاده قرار گرفته در بازیابی‌های عادی مورد قبول باشد اما جزئیات دقیقی که در این میان از بین می‌روند در موقعیت‌های دیگر مهم بوده و به‌طور مثال دارای اهمیت قانونی باشند؛
پ- وقتی بین وضوح تصویر پویش‌شده و ابزار بازیابی، تطابق کامل وجود ندارد، ممکن است درستی ابعاد در حالت بازتولید از بین برود؛
ت- وقتی که پرونده داده‌های ذخیره‌شده به‌طورعادی برای نمایش یا چاپ به قالب دیگری منتقل می‌شود، ممکن است بر اثر فقدان جزئیات یا تفاوت‌های موجود در صفحه‌آرایی، اطلاعات از بین رفته و یا به شکل دیگری ارائه شود. ممکن است این تفاوت‌ها هنگام آزادسازی اطلاعات غیرقابل قبول بوده و در این مورد ممکن است به تجهیزات بازیابی مختلفی نیاز باشد که در مرحله تبدیل مورد استفاده قرار نگرفته‌اند.
اگر تجهیزات استفاده‌شده برای بازیابی، نمایش / چاپ اطلاعات ذخیره‌شده، صفحه‌آرایی مدرک اصلی را حفظ نمی‌کند (شکل حروف، صفحه‌گذاری‌ها)، بهتر است، ویژگی‌های بازیابی اطلاعات مورد پذیرش قرار گرفته و مستند شود.

۶-۸ انتقال پرونده

۶-۸-۱ انتقال پرونده داده‌ها داخل سیستم

۶-۸-۱-۱ کلیات

انتقال پرونده داده‌ها داخل سیستم، آن‌دسته از انتقال‌ها هستند که طبق آنچه در بند ۷-۲ تعریف‌شده، در درون سیستم اتفاق می‌افتند. انتقال‌های پرونده درون سیستم عبارتند از:
الف- انتقال‌های شبکه محلی؛
ب- جابه‌جایی بین زیرسیستم‌های تحت کنترل سیستم مانند سیستم مدیریت ذخیره‌سازی سلسله مراتبی یا بین لوح‌های مخزن و لوح‌های مغناطیسی؛
پ- انتقال بین زیر سیستم‌های ذخیره‌سازیِ تحت کنترل متصدی.
در چنین انتقال‌هایی، روش‌های دستی و الکترونیکی، تحت کنترل سازمان قرار دارند.
بهتر است، روش‌ها و فرایندهایی به‌کارگرفته شود تا از عدم به خطر افتادن یکپارچگی پرونده‌های منتقل‌شده در سیستم، اطمینان حاصل شود.
توصیه می‌شود، انتقال پرونده از یک وسیله به وسیلهٔ دیگر با برنامهٔ نرم‌افزاری کنترل شود.
وقتی که به معیارهای امنیتی بیشتر نیاز است، بهتر است، استفاده از امضای رقمی را در نظر گرفت.

یادآوری- این زیربند برای الزامات گذار پرونده، جایی‌که نوع رسانه و/ یا قالب پرونده داده به دلیل فناوری‌های گذار تغییر کرده، قابل اجرا نیست. به بند ۷-۱۰ مراجعه شود.

۶-۸-۱-۲ انتقال شبکه محلی

در برخی برنامه‌ها، می‌توان پرونده‌هایی که با استفاده از شبکه محلی تعریف شده در بند ۷-۲، تحت کنترل متصدی قرار دارند را از یک وسیلهٔ ذخیره‌سازی به وسیلهٔ دیگر منتقل کرد. شبکه‌های محلی می‌تواند شامل اتصالات بین مکان‌های دور از هم با استفاده از خطوط ثابت باشد.

جایی که پرونده‌ها از طریق شبکه محلی منتقل می‌شوند، بهتر است، روش‌ها و فرایندهایی به‌کارگرفته شود تا اطمینان حاصل شود که یکپارچگی پرونده‌های منتقل‌شده نادیده گرفته نشده است.

توصیه می‌شود، جایی که پرونده‌ها از طریق خطوط ارتباطی ثابت (استیجاری) بین مکان‌های دور از هم منتقل می‌شوند، روش‌ها و فرایندهایی به‌کارگرفته شود تا اطمینان حاصل شود که یکپارچگی پرونده‌های منتقل‌شده نادیده گرفته نشده است.

۶-۸-۲ انتقال برون سازمانی پرونده‌ها

این زیربند با پرونده‌های منتقل‌شده بین یک سیستم و سیستم دیگر از طریق سیستم‌های ارتباطی برون سازمانی و گسترده، سروکار دارد. چنین سیستم‌هایی برای سیستم‌های توصیف‌شده در بند ۷، برون سازمانی محسوب می‌شوند. سیستم‌های ارسال و دریافت‌کننده از یکدیگر دور بوده و می‌توانند در یک سازمان یا در سازمان‌های مختلف قرار داشته باشند که در هر دو مورد، گروه دیگر، خدمات انتقال را ارائه می‌دهد.

ممکن است سیستم ارتباطی شامل انتقال بی‌درنگ یا با تأخیر (ذخیره و ارسال مجدد)، مانند آنچه در خدمات پست الکترونیکی اتفاق می‌افتد، باشد.

این استاندارد با یکپارچگی اشیاء الکترونیکی که به گروه دیگری منتقل شده و یکپارچگی اشیاء الکترونیکی که از گروه دیگری دریافت شده‌اند، در ارتباط است. این استاندارد مستقیماً با خدمات انتقال در ارتباط نیست. با پیروی از توصیه‌های ارائه‌شده در این استاندارد، کاربران می‌توانند نشان دهند که نسخه‌ای از شیء رقمی که پیش از این به گروه دیگر منتقل شده، از آن زمان به بعد تغییر نکرده و پرونده‌ای که پیش از این از طریق یک انتقال از گروه دیگر دریافت شده، از زمان دریافت به بعد، دچار تغییر نشده است.

بهتر است، انتقال پرونده از یک وسیله به وسیلهٔ دیگر با برنامه نرم‌افزاری کنترل شود.

توصیه می‌شود، جایی که یک پرونده از طریق انتقال برای گروه دیگر نسخه‌برداری می‌شود، پرونده اصلی در سیستم ذخیره شود.

بهتر است، تاریخ و زمان انتقال پرونده به‌عنوان بخشی از مراحل ممیزی ذخیره شود.

جایی که یک پرونده از طریق انتقال از گروه دیگر دریافت می‌شود، بهتر است، پرونده اصلی در سیستم ذخیره شود.

توصیه می‌شود، تاریخ و زمان دریافت پرونده به‌عنوان بخشی از مراحل ممیزی ذخیره شود. تفاوت‌های بین پرونده‌های دریافت و ارسال‌شده ممکن است بر اثر خطا در انتقال یا با تغییر عمدی

پرونده‌ها صورت پذیرد. اثبات اینکه پرونده دریافت‌شده و پرونده ارسال‌شده حاوی داده‌های یکسانی هستند با اثبات اینکه دو نسخه از مدارک با هم یکسان هستند، تفاوتی ندارد. لازم است نشان دهیم که کدام پرونده، پرونده منبع و کدام پرونده رونوشت است؛ یعنی اول کدام پرونده وجود داشته است. در برخی نمونه‌ها، این لازمه با مقایسه زمانی که پرونده‌ها ذخیره شده‌اند، محقق می‌شود. اگر ساعت سیستم درست باشد (با در نظر داشتن ساعت جهانی)، پرونده دریافت‌شده باید بعد از زمانی که پرونده منبع منتقل شده است، ذخیره شده باشد. بنابراین، موضوع ، اثبات اعتبار و درستی زمانبندی این دو رویداد است.

برای مثال، می‌توان از امضاهای رقمی برای تأیید این موضوع استفاده کرد که مدرکی که به صورت رقمی/ الکترونیکی امضا شده، دقیقاً همان پرونده‌ای است که ارسال شده و برای تأیید هویت ارسال‌کننده نیز به‌کار گرفته می‌شود. اگر گواهینامهٔ اولیه بیش از این اعتبار نداشته و توسط مرجع صادرکننده گواهی نگهداری می‌شود، ممکن است تأیید هویت به خطر بیافتد. اگر گواهی امضای رقمی/ الکترونیکی دیگر در دسترس نبوده یا تاریخ انقضای آن تمام شده باشد، امضای رقمی اطلاعات مرتبط با تغییر مدرک پس از امضای آن را ارائه می‌دهد.

به دلایل امنیتی یا موارد دیگری مثل جلوگیری از افشای غیرمجاز اطلاعات موجود در یک پرونده، می‌توان روش‌های بیشتری (خارج از دامنهٔ این استاندارد) تدوین کرد.

جایی که توانایی اثبات تحویل یک پرونده حائز اهمیت است، ممکن است تأیید دریافت پرونده از سوی دریافت‌کننده برای ارسال‌کننده، لازم باشد؛ بهتر است، این تأیید شامل شناسه انتقال و تاریخ و زمان دریافت باشد.

اگر از این روش‌ها پیروی شود، ریسک اصلاح پرونده یا ارسال آن از سوی شخصی غیر از ارسال‌کننده مشخص‌شده، کاهش پیدا می‌کند.

توصیه می‌شود، سطح ریسک امنیتی در نظر گرفته‌شده حین انتقال پرونده بیرونی ارزیابی شود تا از انطباق با الزامات خط‌مشی امنیت اطلاعات، اطمینان حاصل شود.

۹-۶ نگهداری مدارک

هر گاه مدارک کاغذی پویش شده و خط‌مشی مدیریت مدارک بر امحاء نوع خاصی از مدارک کاغذی تأکید دارد، ممکن است مواردی وجود داشته باشد که بهتر است، در آن برخی استثنائات به‌کارگرفته شده و مدارک کاغذی نگهداری شوند. لازم به ذکر است که وقتی مدرک کاغذی «اصلی» نگهداری می‌شود، دسترسی به مدرک جهت اثبات اطمینان‌پذیری «رونوشت» الکترونیکی، لازم است.

توصیه می‌شود، روش‌های نگهداری مدارک کاغذی خاص، مستند شود.

شرایطی که ممکن است مستلزم وجود این مستندات باشند عبارتند از:

الف- کیفیت مدرک کاغذی پایین است، بنابراین تصویر خوانایی از آن به‌دست نمی‌آید؛

ب- می‌توان مدرک کاغذی را نگهداری کرد تا امکان مطرح شدن این موضوع که تصویر عمداً ناخوانا شده را کاهش دهد؛ نگهداری از مدرک کاغذی باعث اجتناب از ریسک عدم پذیرش تصویر بر اساس احتمال رونوشت‌بودن آن، می‌شود.
پ- توصیه می‌شود، یادداشتی نگهداری شود که نشان می‌دهد کیفیت مدرک کاغذی، اصلی پایین بوده و شامل جزئیاتی دربارهٔ اطلاعات مشهود است که لازم است ذخیره شوند؛
ت- مدرک کاغذی حاوی اصلاحات فیزیکی یا یادداشت‌هایی که در تصویر پویش‌شده قابل تشخیص نیستند؛
ث- سند مجزایی که اصلاحات فیزیکی یا یادداشت‌های موجود روی مدرک کاغذی را به‌علاوه جزئیاتی مربوط به اصلاحات کافی هستند، ارائه می‌دهد؛
ج- سوءاستفاده‌ها مشخص شده یا دعوی قضایی در جریان بوده و یا مورد انتظار است؛
چ- مدرک کاغذی مانند مدارکی اصلی امضاءشده مرتبط با یک قرارداد بزرگ، از ارزش زیادی برخوردار هستند.

توصیه می‌شود، روش‌های تعیین اطلاعاتی که موارد سوءاستفاده از آنها مشخص‌شده یا دعوی قضایی در جریان بوده و یا مورد انتظار است، مستند شود. بهتر است، این روش‌ها شامل توقف امحاء مدرک کاغذی مرتبط با این اطلاعات باشد.

۶-۱۰ حفاظت و نگهداری اطلاعات

توصیه می‌شود، روش‌های حفاظت و نگهداری بلند مدت اطلاعات، مستند شود. بهتر است، این روش‌ها، جداول زمانی نگهداری لازم و عمر مورد انتظار سیستم‌های ذخیره‌سازی را در نظر بگیرند.
توصیه می‌شود، هرگاه دوره نگهداری بیشتر از عمر سیستم‌های ذخیره‌سازی است، طرح‌های گذار داده‌ها در سیستم‌های جدید، مستند شود (به بند ۷-۱۰ مراجعه شود). برای کسب اطلاعات بیشتر به استاندارد ISO/TR 18492 مراجعه شود.

۶-۱۱ امحاء اطلاعات

توصیه می‌شود، روش‌های تعیین‌تکلیف یا امحاء اطلاعات در انتهای دوره نگهداری، مستند شود.
بهتر است، این روش‌ها جنبه‌های امنیتی مناسب با حساسیت اطلاعاتی که امحاء می‌شوند را در نظر بگیرند.
توصیه می‌شود، تا زمانی که تصاویر ذخیره و روش‌های پشتیبانی مناسب کامل می‌شوند، هیچ‌کدام از مدارک کاغذی امحاء نشود.

۱۲-۶ نسخه پشتیبان و بازیابی

توصیه می‌شود، برای تهیه نسخه پشتیبان از پرونده‌ها، روش‌های مؤثری به‌کارگرفته شود تا حداقل دو نسخهٔ به‌روز از مدارک برای استفاده در صورت فقدان یا تحریف کل داه‌های جاری یا بخشی از آن وجود داشته باشد. ضروری است داده‌های پشتیبان شامل تمام اطلاعات مرتبط (مانند: پرونده‌های نمایه، مراحل ممیزی) باشد تا در صورت فقدان کلی سیستم اصلی بتوان یک سیستم جدید کامل را ایجاد کرد.

توصیه می‌شود، این روش‌ها شامل منبع ذخیره‌سازی، خارج از محل نسخه‌های پشتیبان باشد.

برای اثبات اینکه روش‌ها از جهت اعتبار آنها، کنترل و آزمایش شده‌اند، بهتر است، روش بازیابی سیستم نیز مستند شود.

امور مربوط به امنیت نسخه پشتیبان داده‌ها از اهمیت بسیاری برخوردار است زیرا امکان دارد امنیت نسخه پشتیبان به خطر افتاده و سازش صورت گرفته شده باشد. می‌توان گفت رسانهٔ پشتیبان به خطر افتاده و اجباراً اطلاعات از دست رفته، بازیابی شده و اطمینان‌پذیری اطلاعات ذخیره‌شده را تحت‌تأثیر قرار داده است. در برخی موارد، می‌توان داده‌های پشتیبان که در رسانه ذخیره‌سازی مطمئن نگهداری شده و فقط در مواردی که اطمینان‌پذیری داده‌های جاری به چالش کشیده شده مورد استفاده قرار می‌گیرند، برای اثبات اطمینان‌پذیری اطلاعات ذخیره‌شده، در دسترس قرار گیرند.

توصیه می‌شود، ابزارهای سیستم امکان تهیه نسخه پشتیبان و تأیید تمام پرونده‌ها و اطلاعات مرتبط اعم از مراحل ممیزی را در فواصل زمانی منظم، فراهم آورد.

توصیه می‌شود، اطلاعات مربوط به مراحل ممیزیِ تمام اقدامات تهیه نسخه پشتیبان در سیستم نگهداری شود که این اطلاعات بهتر است، شامل جزئیات مرتبط با مشکلات رویداده حین اجرای روش‌ها باشد.

توصیه می‌شود، در صورتی که ساختار پرونده‌های نگهداری‌شده روی نسخه پشتیبان با ساختار پرونده‌های اصلی متفاوت است، ساختار پرونده‌های اصلی در دستورالعمل توصیف سیستم‌ها، شرح داده شود.

بهتر است، مراحل ممیزی تمام اقدامات بازیابی پرونده را شرح داده و شامل توصیف مشکلات مواجه‌شده حین فرایند بازیابی باشد.

توصیه می‌شود، روش‌های بررسی عدم به خطر افتادن یکپارچگی پرونده‌ها پس از ذخیره‌سازی مجدد، مستند شود.

رسانه استفاده‌شده برای نسخه‌های پشتیبان لزوماً شرایط ذخیره‌سازی دائمی را ارائه نمی‌دهد. تأمین‌کنندگان رسانه معمولاً اطلاعات مرتبط با فراوانی آزمایش توصیه‌شده را ارائه می‌دهند. به‌صورت جایگزین، اگر چنین اطلاعات خاصی وجود ندارند، غالباً می‌توان توصیه‌های عمومی را در استانداردهای ملی و بین‌المللی پیدا کرد.

آزمایش کردن رسانه روی سخت‌افزار مشابه هیچ تضمینی نمی‌دهد که این رسانه روی تجهیزات دیگر، حتی تجهیزاتی که تأمین‌کنندهٔ مشابه ارائه کرده و تجهیزاتی با مدل یکسان، خوانده شوند. اگر فقط سخت‌افزاری که می‌تواند نسخه‌های پشتیبان را بخواند از بین برود، این نسخه‌ها بی ارزش می‌شوند.

توصیه می‌شود، رسانهٔ نسخه پشتیبان در فواصل زمانی منظم و با استفاده از سخت‌افزارهای مختلف برای خواندن رسانه، مورد آزمایش قرار گیرند.

۶-۱۳ تعمیر و نگهداری سیستم

۶-۱۳-۱ کلیات

توصیه می‌شود، سیستم قابل اعتماد مدیریت مدارک نگهداری شده و تعمیرات اساسی را توسط کارکنان دارای صلاحیت انجام دهند تا اطمینان حاصل گردد که عملکرد آن تا حدی دچار مشکل نشده است که یکپارچگی داده‌های دریافت، ایجاد یا ذخیره شده روی آن تحت تأثیر قرار گیرند.

برای مثال: نگهداری از سیستم پویش مدرک کاغذی مطابق با دفترچه مشخصات کارخانه سازنده به منظور حفظ کیفیت تصویر، از اهمیت خاصی برخوردار است.

توصیه می‌شود، نگهداری پیشگیرانه به‌طور منظم و مطابق با توصیه‌های فروشنده انجام شود.

بهتر است، روش‌های استفاده‌شده برای نگهداری پیشگیرانه، مستند شود.

ممکن است این روش‌ها توسط متصدی سیستم یا کارکنان متخصص خدمات انجام شود.

توصیه می‌شود، محلی برای نگهداری وقایع[1] ایجاد شود که نشان دهد روش‌های پیشگیرانه یا اصلاح‌کننده تکمیل شده است.

بهتر است، روش‌هایی که برای کنترل استفاده از سخت‌افزار / نرم‌افزار نگهداری سیستم که ممکن است کنترل‌های دسترسی سیستم را پست سر گذارند، مستند شود. بهتر است، دسترسی به این ابزارها و تجهیزات به شدت کنترل و نظارت شود.

توصیه می‌شود، اطلاعات راجع به مدت از کارافتادگی سیستم و جزئیات اقدامات انجام‌شده در دفتر نگهداری ذخیره شود.

۶-۱۳-۲ سیستم‌های پویشگر

توصیه می‌شود، جایی که پویش مدارک کاغذی به‌کار گرفته می‌شود، برای کنترل اینکه سیستم پویشگر پس از تکمیل روش‌های نگهداری، به ایجاد کیفیت خروجی موردنیاز سیستم ادامه می‌دهد از روش‌های توصیف‌شده در بخش کنترل کیفیت استفاده شود.

نتایج آزمایش‌ها برای تأیید این موضوع در زمان‌های آتی استفاده می‌شود که کیفیت پایین تصویر به علت عملکرد نادرست سیستم نبوده است. در صورت وجود هرگونه نقص در خروجی، نگهداری اصلاح‌کننده مناسب لازم است.

---

1 - Maintenance Log

۶-۱۴ امنیت و حفاظت

۶-۱۴-۱ روش‌های امنیتی

توصیه می‌شود، راهنماهای امنیتی قابل اجرا برای سازمان و کاربردهای مرتبط را به‌کار گرفت. برای نمونه، چنین راهنماهایی ممکن است همراه با خط‌مشی‌ها و اقدامات، راهنماهای منطقه‌ای خاص (مانند:راهنماهای مالی، پزشکی) و استانداردهای ملی و بین‌المللی یا به‌عنوان الزامات قانونی وجود داشته باشند.

در صورت عدم وجود راهنماهای داخلی، ممکن است اطلاعات منتشرشده، راهنمای جامع امنیتی را ارائه دهد که برای تحقق نیازهای سازمان طراحی شده‌اند. ممکن است این اطلاعات مبنای کافی برای ایجاد راهنماهایی که الزامات سازمان را برآورده می‌سازند، ارائه دهد. برخی از سازمان‌ها پذیرش طرح‌های امنیتی معتبر بیرونی را به عنوان تأیید بیشتر تطابق با خط‌مشی امنیتی، در نظر می‌گیرند.

توصیه می‌شود، روش‌های به‌کارگرفته‌شده که با خط‌مشی امنیت اطلاعات سازمان منطبق هستند، مستند شود.

بهتر است، برای کنترل دسترسی به سطوح مختلف سیستم (مانند: مدیریت، ورود داده و بازیابی)، سیستم ایمن کنترل دسترسی به‌کارگرفته شود.

توصیه می‌شود، محیط همسازی و عملیاتی برای سیستم‌های قابل اعتماد مدیریت مدارک و برای ذخیره‌سازی، برچسب‌گذاری، جابه‌جایی و نگهداری رسانه ذخیره‌سازی، مطابق با توصیه‌های تأمین‌کنندگان و یا استانداردهای مرتبط ملی یا بین‌المللی باشد.

بهتر است، بخش مرکزی سیستم (شامل کارسازهای پرونده، ذخیره‌سازی و غیره) در محل‌های ایمن (که در روش‌های امنیتی سازمان تعریف شده‌اند) و با دسترسی محدود هستند، نصب شوند.

۶-۱۴-۲ کلیدهای کدگذاری

برای ارتقای امنیت و یکپارچگی داده‌های ذخیره‌شده، می‌توان از روش‌های کدگذاری استفاده کرد. ممکن است یک پرونده کامل الکترونیکی کدگذاری شود تا اطلاعات موجود در آن بدون استفاده از کلید کدگذاری قابل بازیابی نباشد. کدگذاری موضوعی پیچیده و در حال تغییر است.

استفاده از کدگذاری برای ذخیره‌سازی بلندمدت مشکل‌آفرین خواهد بود چرا که کلیدها / گواهینامه‌ها به هر دلیل از دسترس خارج می‌شوند.

بهتر است، جایی که از کدگذاری استفاده می‌شود، کلیدها به‌طور مطمئن نگهداری شده و فقط در دسترس افرادی قرار داشته باشند که به‌صورت مجاز، مسئول انجام اقداماتی هستند که مستلزم دسترسی به کلیدها می‌باشد.

توصیه می‌شود، برای تخصیص و مدیریت کلید کدگذاری و مدیریت گواهینامه‌ها، روش‌هایی به‌کارگرفته شود.

توصیه می‌شود، جایی که از کدگذاری استفاده می‌شود و از بازیابی/ مدیریت کلید شخص ثالث و کلید حق استفاده منافعی به‌دست می‌آید، استفاده از آنها را مورد نظر قرار داد.
ممکن است فردی که در ابتدا مسئول مدیریت مطمئن کلیدها و گواهینامه‌ها در سازمان بوده، دیگر مشغول به‌کار نباشد؛ بنابراین بهتر است، برای اطمینان از دسترس‌پذیری پیوسته کلیدها و گواهینامه‌ها روش‌هایی به‌کار گرفته شود.

۶-۱۵ استفاده از خدمات پیمانکاری

۶-۱۵-۱ کلیات

غالباً برای پویش، نمایه‌سازی، تبدیل داده‌ها، ذخیره‌سازی و خدمات دیگر از ارائه‌دهندگان خدمات تخصصی استفاده می‌شود.
الف- توصیه می‌شود، با ارائه‌دهنده خدمات قراردادی امضا شود که خدمات مورد استفاده در آن شرح داده شده است.
ب- اگر قرارداد موردنظر مستلزم پذیرش تمام توصیه‌های مرتبط در این استاندارد از سوی پیمانکار نمی‌باشد، توصیه می‌شود، روش‌های کنترل کاربر در زمینه خدمات ارائه‌شده به نحوی باشد که هیچ سوءبرداشتی نسبت به تمامیت، کیفیت و درستی خدمات به‌وجود نیاید.

روش‌ها و توصیه‌های این زیربند انواع خدمات، اعم از خدماتی که بر مبنای مدیریت ابزارها ارائه شده یا برای اطمینان یافتن از موارد زیر به‌کار می‌روند را پوشش می‌دهد:
الف- جایی که ارائه‌دهنده خدمات، کار را انجام می‌دهد، بهتر است، روش‌های اثبات اطمینان‌پذیری نتایج حاصل با روش‌های به‌کارگرفته‌شده در مواردی که کل کار در سازمان مشتری انجام می‌شود، یکسان باشد؛
ب- حتی اگر ارائه‌دهنده خدمات از کار خود دست بکشد، سازمان مشتری سال‌ها پس از یک رویداد قادر است تطابق با آن را اثبات کند.

توصیه می‌شود، وقتی که کار در محلی خارج از سازمان انجام می‌شود، جزئیات مربوط به روش‌های استفاده‌شده در انتقال اطلاعات و/ یا رسانه از سازمان مشتری به ارائه‌دهنده خدمات و از ارائه‌دهنده خدمات به سازمان، مستند شود.
اگر ارائه‌دهنده خدمات از روش‌هایی استفاده می‌کند که با سند خط‌مشی تطابق دارند، بهتر است، سازمان مشتری رونوشتی از مستندات تطابق ارائه‌دهنده خدمات را نگهداری یا در صورت لزوم به آن دسترسی داشته باشد.

۶-۱۵-۲ ملاحظات رویه‌ای

در شرایط ایده‌آل، جایی که ارائه‌دهنده خدمات قادر به اثبات تطابق روش‌های به‌کارگرفته‌شده با سند خط‌مشی مدیریت مدارک می‌باشد، فقط لازم است که قرارداد این موضوع را تأیید کرده و حاوی روش‌های توافق‌شده برای بررسی تطابق باشد.

هرگاه ارائه‌دهنده خدمات با روش‌های توافق‌شده تطابق دارد، بهتر است، این قرارداد شامل جملاتی باشد که روش‌های به‌کارگرفته و ممیزی شده را شرح می‌دهد.

فهرست زیر روش‌ها و فرایندهایی که لازم است کنترل شده و در قرارداد وارد شوند را مشخص می‌کند:

توصیه می‌شود، سازمان مشتری موارد زیر را کنترل کند:

الف- ارائه‌دهنده خدمات می‌تواند خروجی را بر اساس استانداردهای کیفی قابل قبول و پذیرفته‌شده، ایجاد کند؛

ب- ارائه‌دهنده خدمات می‌تواند نمونه‌ای از منبع ورودی را برای ایجاد خروجی روی رسانه پیشنهادی و در قالب پیشنهادی پردازش کند که به‌طور موفقیت‌آمیز روی سیستم موردنظر سازمان مشتری، بارگذاری می‌شود. بهتر است، از این نمونه نگهداری شود؛

پ- ارائه‌دهنده خدمات می‌تواند نسخه‌ای از مراحل ممیزی پردازش‌های انجام‌شده را به شکل خوانا ارائه دهد؛

ت- هنگامی که خدمات نمایه‌سازی ارائه می‌شود، الزامات پیشنهادی درباره درستی داده‌های نمایه‌سازی قابل قبول بوده و مستند شده‌اند؛

ث- مکان پیشنهادی انجام کار قابل قبول بوده و معیارهای امنیتی مناسب با نیازهای سازمان مشتری را محقق می‌سازد؛

ج- روش‌ها و فرایندهای پیشنهادی نسبت به فرایندهای سازمان مشتری، خطر آسیب بیشتر به منابع سازمان را در پی ندارد؛

چ- وقتی که منابع پردازش‌شده منحصربه‌فرد یا دارای ارزش خاصی هستند، سیستم‌های کاشف و مانع از آتش‌سوزی در مکان پیشنهادی به‌کارگرفته شده‌اند؛

ح- هرگاه امنیت مواد پردازش‌شده حائز اهمیت است، ارائه‌دهنده خدمات، معتمد بودن کارکنان عملیاتی موردنظر را تضمین می‌کند. بهتر است، همه کارکنان سازمان به عنوان بخشی از شرایط کاری، توافقنامه محرمانگی را امضا کنند؛

خ- اگر مدارک کاغذی برای پویش ارسال شوند، ارائه‌دهنده خدمات و سازمان مشتری درباره دسترسی سازمان به مدارک در زمانی که خارج از سازمان هستند، توافق می‌کنند.

۶-۱۵-۳ حمل‌ونقل مدارک کاغذی

وقتی مدارک کاغذی به صورت فیزیکی از سازمان مشتری به محل ارائه‌دهندهٔ خدمات منتقل می‌شوند، امکان فقدان مدارک یا آسیب به آنها وجود دارد. لازم است درباره روش‌هایی توافق شود تا

از قابل قبول بودن این میزان ریسک، اطمینان حاصل شود. توصیه می‌شود، هر محموله از منابع که برای سازمان مشتری ارسال یا از آن دریافت می‌شود همراه با یک سابقهٔ کنترل باشد که خصوصیات و تعداد فقره‌های موجود در محموله را مشخص می‌کند.
بهتر است، تمام مواد فرستاده‌شده به‌خوبی بسته‌بندی شوند تا از خطر آسیب به منابع حین حمل و نقل، جلوگیری شود.
توصیه می‌شود، دریافت‌کننده بلافاصله منابع را بر اساس سابقهٔ ارسال‌شده کنترل کرده و هر چه سریعتر وجود اختلاف‌ها را به اطلاع ارسال‌کننده برساند.
سازمان کاربر، شخص ثالث یا پیک مستقل می‌تواند خدمات حمل‌ونقل را ارائه دهد.
بهتر است، شخص ثالثی که خدمات حمل‌ونقل را ارائه می‌دهد سازمان‌هایی باشند که معیارهای کیفی و اعتباری سازمان مشتری را برآورده می‌سازد.
توصیه می‌شود، تاریخ و زمان تحویل منابع به شرکت خدمات حمل‌ونقل و تاریخ و زمان دریافت منابع توسط ارائه‌دهنده خدمات یادداشت و فرد تحویل‌دهنده و دریافت‌کننده آن را امضا کنند. بهتر است، هنگام دریافت منابع بازگردانده شده، فرایند مشابهی را به‌کار گرفت.

۶-۱۵-۴ استفاده از شخص ثالث قابل اعتماد

یکی از ابزارهای مطمئن برای پیدا کردن هر نوع تحریف در پرونده داده‌ها یا تشخیص محتوای پرونده، ذخیرهٔ یک نسخه از پرونده توسط شخص ثالث قابل اعتماد، است.
در صورت استفاده از این رهیافت، بهتر است، یک نسخه معتبر از پرونده الکترونیکی ایجاد و به صورت فیزیکی یا الکترونیکی و با استفاده از ابزارهای مطمئن به شخص ثالث تحویل داده شود.
توصیه می‌شود، شخص ثالث قابل اعتماد از روش‌های مرتبط برای ذخیره‌سازی اطلاعات که در این استاندارد توصیه‌شده استفاده کرده و همانند صاحب مدارک قادر به نشان دادن کارآمدی و امنیت خدمات باشد.

یادآوری- الزامات امنیتی برای شخص ثالث قابل اعتماد غالباً دقیق‌تر از الزامات سازمانی است که اطلاعات آن ذخیره می‌شود.

وقتی که برای تأیید اطمینان‌پذیری از امضای رقمی استفاده می‌شود، سازمان به جای ذخیره امضای رقمی در سیستم خود می‌تواند امضای رقمی پرونده را به شخص ثالث منتقل کند. شخص ثالث امضای رقمی را در شرایط مطمئنی ذخیره می‌کند که بعداً بتواند آن را بازیابی کند.

۶-۱۶ گردش کاری

برخی از سیستم‌های مدیریت مدارک از قابلیت گردش کاری استفاده می‌کنند. این سیستم‌ها امکان خودکارسازی رویه‌ایِ فرایندهای اداری را با مدیریت توالی اقدامات کاری و به‌کارگیری منابع انسانی و سیستم‌های مرتبط با هر مرحله از اقدامات، فراهم می‌آورد.

توصیه می‌شود، هنگامی که سیستم‌های گردش کاری به‌کار گرفته می‌شوند، جزئیات عملیاتی (مانند: نمودار جریان کار)، طبقه‌بندی‌های تعریف فرایند و تعریف فرایند، مستند شود.
چرخه حیات تعریف فرایند شامل موارد زیر است:

الف- تعریف؛

ب- تدوین؛

پ- اجرا؛

ت- استرداد؛

ث- اصلاح.

بهتر است، تمام داده‌ها (پایگاه داده‌ها، مراحل ممیزی و غیره) که روی سیستم گردش کاری نگهداری می‌شوند برای الزامات بازیابی و در صورت اجرایی بودن، برای ذخیره‌سازی مطابق با سند خط‌مشی مدیریت مدارک، بازبینی شود.
توصیه می‌شود، وقتی که تغییراتی در سیستم گردش کاری اعمال می‌شود، برای اطمینان از اینکه اطلاعات ذخیره‌شده حین انجام روش‌ها از بین نرفته‌اند، روش‌های کنترل تغییر به‌کار گرفته شود.
جایی که یک گردش کاری مطالعاتی ویژه (یعنی آن نوع از گردش کاری که در آن می‌توان حین عملیات پردازش، قوانین را تغییر داده یا قوانین جدید ایجاد کرد) به‌کار گرفته می‌شود، بهتر است، یک مرحله ممیزی کامل از این فرایند همراه با مشخصاتِ فردی که تغییرات را در روش‌های استاندارد گردش کاری اعمال کرده، نگهداری شود.

۶-۱۷ نشانگرهای تاریخ و زمان

توصیه می‌شود، روش‌های کنترل منظم ساعت سیستم برای درستی تاریخ و زمان، مستند شود.
بهتر است، خطاها اصلاح شده و اقدامات انجام‌شده، مستند شود.
اگر ساعت بر مبنای فصل، برای مثال: شش ماههٔ اول و دوم سال، تغییر می‌کند، بهتر است، روش‌های استفاده‌شده مستند شود.
توصیه می‌شود، فقط کارکنان مجاز، امکان تغییر ساعت را داشته باشند.
هنگامی که لازم است درستی نشانگرهای تاریخ و زمان اثبات شود، بهتر است، استفاده از خدمات شخص ثالث قابل اعتماد را در نظر گرفت. توصیه می‌شود، جایی که از زمان مورد اعتماد استفاد می‌شود، روش‌های اثبات یکپارچگی و اطمینان‌پذیری نشانگر زمان و ارتباط آن با بخش خاصی از اطلاعات، مستند شود.

۶-۱۸ کنترل نسخه

۶-۱۸-۱ اطلاعات

در برخی برنامه‌های کاربردی، ممکن است مدارک رقمی در معرض تغییر قرار داشته باشند. نوع معمول این برنامه‌ها آنهایی هستند که برای نقشه‌های فنی کنترل‌کننده در دفاتر نقشه‌کشی به‌کار

می‌روند. ممکن است در طول یک دورهٔ زمانی، نسخه‌های مختلفی از یک مدرک رقمی ایجاد شود که به هر کدام از آنها یک شمارهٔ نسخه اختصاص داده می‌شود. نکتهٔ مهم در این برنامه‌ها، نگهداری هر نسخه به‌عنوان یک مدرک رقمی مجزا و همچنین حفظ پیوند بین نسخه‌ها است.
توصیه می‌شود، هرگاه ایجاد تغییر در اشیاء رقمی ذخیره‌شده مجاز است، روش‌های اعطاء مجوز و به‌کارگیری تغییرات، مستند شود.
بهتر است، مستندات مرتبط با الزامات موردنیاز برای نگهداری نسخه‌های مختلف این پرونده‌ها، در دسترس باشد.

۶-۱۸-۲ مستندسازی

برای اطمینان از اینکه می‌توان تمام نسخه‌های مرتبط با مدرک را در چرخه حیات اطلاعات ذخیره‌شده مشخص کرد، از سیستم کنترل نسخه استفاده می‌شود. توصیه می‌شود، برای تمام مستندات، روش کنترل نسخه ایجاد شود.
بهتر است، نسخه‌های قبلی حداقل تا زمانی که اطلاعات مرتبط نگهداری می‌شوند، حفظ شود.
سوابق این نگهداری مورد نیاز هستند بنابراین خط‌مشی‌ها و روش‌های اجرایی در زمان دریافت مدارک و پس از آن را می‌توان توصیف و تأیید کرد. در صورت عدم انجام این کار، یکپارچگی اطلاعات به خطر می‌افتد. برای مثال: اگر امکان اطمینان از عمر روش‌های پویش استفاده‌شده برای دریافت تصویر یک مدرک کاغذی و روش‌های پیروی‌شده پس از دریافت آن وجود ندارد، ممکن است اثبات اطمینان‌پذیری و یکپارچگی اطلاعات، دشوار یا غیرممکن باشد.

۶-۱۸-۳ روش‌ها و فرایندها

توصیه می‌شود، تمام تغییرات اعمال‌شده در روش‌ها / فرایندها مطابق با روش کنترل تغییر به‌کار گرفته شود.

۶-۱۹ نگهداری از مستندات

تطابق با سند خط‌مشی مدیریت مدارک مستلزم دسترس‌پذیری و استفاده از مستندات مشخص است. بهتر است، روش‌های نگهداری از این مستندات در شیوه‌نامه اجرایی وجود داشته باشد. توصیه می‌شود، روش‌های نگهداری در حفظ سوابق نگهداری به‌کار گرفته شود.
نگهداری لازم است چرا که با گذشت زمان، الزامات جدید منتشر شده و فناوری‌ها و قوانین تغییر خواهند کرد. در برخی موارد، کافی است که نگهداری بر اساس مطالعات ویژه، تغییر کند. علاوه‌براین، عموماً برای اطلاعات مهم، بررسی منظم و جاری، مناسب خواهد بود.
بهتر است، روش‌هایِ اطمینان از روزآمدی مستندات، مستند شود.
توصیه می‌شود، این مستندات مطابق با مقررات مدیریت سوابق باشند که متناسب با مقررات به‌کارگرفته‌شده برای دیگر سوابق اداری ضروری سازمان هستند.

مخصوصاً وقتی یک فقره از مستندات بازبینی می‌شود، بهتر است، رونوشتی از آن فقره پیش از تغییر حداقل تا زمانی که اطلاعات مرتبط با آن نگهداری می‌شود، حفظ گردد.
توصیه می‌شود، ذخیره این مستندات امکان شناسایی و بازیابی تمام مستندات در زمان‌های مقتضی را برای گروه‌های مجاز (برای مثال: ویراستاران) فراهم آورد.
ممکن است همان‌طور که کاغذ یا ریزفیلم یا ترکیب هر دو روش، در مکان‌های مطمئن نگهداری می‌شوند، مستندات به صورت الکترونیکی در سیستم قابل اعتماد مدیریت مدارک الکترونیکی ذخیره شوند که در معرض کنترل‌های مشابه با موارد مطرح‌شده در این استاندارد قرار دارد.
بهتر است، خط‌مشی اتخاذشده برای ذخیره مستندات، در سند خط‌مشی مستند شود.
در اکثر موارد، روش مطلوب این است که تغییرات به شکلی مستند شود که امکان پیگیری تغییرات رویداد بین نسخه‌ها را برای گروه‌های علاقه‌مند، فراهم آورد. ممکن است این کار با ثبت پیشینهٔ تغییرات برای هر بخش از مستندات صورت گیرد.

۷ فناوری‌های توانمندسازی

۷-۱ کلیات

این بند با موضوع فناوری‌های مرتبط با استاندارد حاضر به شرح زیر در ارتباط است:
الف- دستورالعمل توصیف سیستم (به بند ۷-۲ مراجعه شود)؛
ب- ملاحظات رسانهٔ ذخیره و زیر سیستم‌ها (به بند ۷-۳ مراجعه شود)؛
پ- سطوح دسترسی (به بند ۷-۴ مراجعه شود)؛
ت- بررسی یکپارچگی سیستم (به بند ۷-۵ مراجعه شود)؛
ث- پردازش تصویر (به بند ۷-۶ مراجعه شود)؛
ج- فناوری‌های فشرده‌سازی (به بند ۷-۷ مراجعه شود)؛
چ- جایگذاشت و حذف فرم (به بند ۷-۸ مراجعه شود)؛
ح- ملاحظات محیطی (به بند ۷-۹ مراجعه شود)؛
خ- گذار (به بند ۷-۱۰ مراجعه شود)؛
د- امحاء / حذف اطلاعات (به بند ۷-۱۱ مراجعه شود).

۷-۲ دستورالعمل توصیف سیستم

بهتر است، توصیف اجزاء سخت‌افزاری، نرم‌افزاری و شبکه تشکیل‌دهنده سیستم و نحوهٔ تعامل آنها در دستورالعمل توصیف سیستم وجود داشته باشد.
توصیه می‌شود، جزئیات مربوط به پیکربندی سیستم، مستند شود.
بهتر است، جزئیات مربوط به تمام تغییرات سیستم، مستند شود. این مستندات باید شامل جزئیات مربوط به فرایندهای به‌کارگرفته‌شده برای تحت تأثیر قرار دادن تغییرات باشد.

بهتر است، دستورالعمل توصیف سیستم ساختاریافته باشد تا جزئیات مربوط به سیستم در هر مقطع زمانی حین دورهٔ استفاده از آن، به‌راحتی قابل دسترسی باشد. این هدف با ایجاد نسخهٔ جدیدی از دستورالعمل به ازای هر بار تغییر حاصل می‌شود تا حدی که امکان دسترسی به توصیف دقیق از سیستم در هر مقطع زمانی در گذشته، وجود خواهد داشت.
توصیه می‌شود، کاربران مطابقت اجزاء سیستم با الزامات استانداردهای مرتبط ملی / بین‌المللی را ارزیابی کنند. این کار ویراستاران سیستم را قادر می‌سازد تا عملکرد و اعتبار سیستم را در مقابل این استانداردها، بررسی کنند.

۳-۷ ملاحظات رسانهٔ ذخیره و زیر سیستم

بسته به نوع رسانه و زیرسیستم‌های ذخیره‌سازی، میزان خطر اصلاح سهوی یا عمدی اشیاء رقمی ذخیره‌شده، متفاوت است. توانایی تشخیص این تغییرات نیز متفاوت است. به طور مثال: وقتی از رسانه‌هایی با قابلیت یکبار نوشتن استفاده می‌شود، به‌طور طبیعی امکان تغییر پرونده‌های الکترونیکی پس از ذخیرهٔ آنها وجود ندارد، چرا که این تغییرات برخی از اطلاعات را از بین برده و حتی اگر باعث آسیب‌های جبران‌ناپذیر نشوند، منجر به آسیب دیدن پرونده‌ها می‌شود. بالعکس، در مورد سیستم‌هایی که از ذخیره‌سازی برخط[1] استفاده می‌کنند، عدم اصلاح غیرمجاز که غالباً با کنترل دسترسی مدیریت می‌شود را هرگز نمی‌توان تضمین کرد.
امکان اصلاح اشیاء رقمی که روی لوح‌های مغناطیسی و دیگر رسانه‌های قابل بازنویسی با دسترسی اتفاقی ذخیره می‌شوند، وجود دارد. خطر تغییر در این نوع از رسانه‌ها نسبت به کنترل‌هایی که با زیرسیستم‌های ذخیره و با نرم‌افزار دسترسی به‌کار گرفته می‌شود، کمتر است. توانایی تغییر پرونده‌ها مستلزم دسترسی خواندن- نوشتن[2] است و سیستم‌هایی که به خوبی طراحی شده‌اند دارای کنترل‌هایی برای جلوگیری از دسترسی غیرمجاز خواندن- نوشتن هستند. کاربران با دسترسی فقط- خواندن، قادر به اصلاح پرونده‌ها نیستند. این قابلیت به خودی خود رضایت‌بخش نیست مگر اینکه سیستم، سابقهٔ مطمئنی از تمام دسترسی‌های خواندن- نوشتن را نگهداری کند. در سیستمی که اصلاحات زیادی روی پرونده صورت می‌گیرد، ممکن است ضرورت زیادی برای ثبت این اصلاحات وجود داشته باشد اما اگر سابقه نگهداری نشود، تشخیص تغییرات غیرمجاز توسط هکرهای ماهر یا افرادی با امتیاز مخصوص دسترسی، غیرممکن خواهد بود.
در مورد رسانه‌ها با قابلیت بازنویسی پیاپی مانند نوارهای مغناطیسی، تشخیص تغییرات غیرمجاز بسیار دشوارتر از رسانه‌هایی با دسترسی تصادفی است؛ چرا که اگر پرونده اصلاح‌شده، آخرین پرونده ذخیره‌شده روی رسانه نباشد، تمام پرونده‌های بعدی باید رونوشت‌برداری و بازنویسی شوند. موضوع امنیت فیزیکی رسانه برون خط[3] و دسترسی کنترل در حالیکه برخط است، حائز اهمیت می‌باشد.

---

1 - Online storage
2 - Read-write access
3 - Offline

توصیه می‌شود، نقطه‌ای در پردازش‌های کاربردی که در آن پرونده‌های الکترونیکی از سوی نرم‌افزار برای نوشتن جهت ذخیره‌سازی مورد درخواست قرار می‌گیرند، مستند شود.
بهتر است، رسانه ذخیره‌سازی و زیر سیستم‌های مرتبط به نحوی انتخاب شوند که از حذف و اضافه / جایگزینی‌ها، بدون آشکار کردن آنها، جلوگیری شود. توصیه می‌شود، روش آشکارسازی شامل استفاده از امضاهای رقمی/ الکترونیکی و/ یا نسخه‌های ذخیره‌شده در مکان‌های مختلف و احتمالاً شامل شخص ثالث قابل اعتماد باشد.
در سیستم‌های فاقد ابزارهایی که حین عملیات عادی، به‌طور خودکار تغییر غیرمجاز یا حذف پرونده‌ها را آشکار می‌کنند، بهتر است، کاربران برای تأیید اینکه پرونده‌های ثابت، تغییر نکرده یا حذف نشده‌اند، از بررسی‌های تصادفی استفاده کنند.
توصیه می‌شود، هرگاه از رسانه‌هایی استفاده می‌شود که قابلیت فقط یکبار نوشتن را دارند، دورهٔ نگهداری اطلاعات ذخیره‌شده به طور خاص مورد توجه قرار گیرد. بهتر است، در صورت امکان، اطلاعاتی که دارای دوره‌های نگهداری متفاوت هستند، روی یک رسانه ذخیره نشوند.

۷-۴ سطوح دسترسی

توصیه می‌شود، جزئیات مربوط به سطوح دسترسی موجود در سیستم و روش‌های استفاده از آن، مستند شود. سطوح دسترسی غالباً به شرح زیر می‌باشند:

الف- مدیر سیستم؛

ب- مجری سیستم؛

پ- مسئول نگهداری و تعمیر سیستم؛

ت- مسئول نویسندگان و تولیدکنندگان؛

ث- مسئول ذخیره‌سازی اطلاعات و نمایه‌سازی؛

ج- مسئول بازیابی اطلاعات.

توصیه می‌شود، فقط کارکنان دارای حقوق دسترسی مرتبط، مجاز به ورود یا اصلاح اطلاعات ذخیره‌شده باشند.
بهتر است، حقوق دسترسی سیستم فقط به کارکنانی اعطاء شود که صلاحیت خود را اثبات کرده‌اند.

۷-۵ بررسی یکپارچگی سیستم

۷-۵-۱ کلیات

توصیه می‌شود، سیستم، مجهز به ابزارهایی باشد که باعث اطمینان از حفظ یکپارچگی اطلاعات ذخیره‌شده در آن، از جمله حفظ اطلاعات حین انتقال به رسانه ذخیره‌سازی و انتقال از آن، شود.

یکی از رهیافت‌های مناسب، استفاده از کنترل مجموعه[1] است که بلافاصله بعد از دریافت اطلاعات محاسبه می‌شود. این روش اطمینان می‌دهد که هر نوع خطا در انتقال پرونده بین زیرسیستم‌ها به‌طور خودکار و با قطعیت، آشکار می‌شود. این روش به خودی خود امکان دستکاری اطلاعات در دوره زمانی بین دریافت و تحویل اطلاعات به رسانه ذخیره‌سازی را پوشش نمی‌دهد. اگر الگوریتمِ کنترل مجموعه شناخته شده باشد، ممکن است این دستکاری‌ها با محاسبه یک کنترل مجموعه جدید همراه شوند. برای رفع این احتمالات به روش‌های دیگری نیاز است. یک روش ساده برای انجام این کار، نوشتن کنترل مجموعه در مراحل ممیزی بعد از انجام محاسبات است.

توصیه می‌شود، برای حفاظت از اطلاعات ذخیره‌شده در برابر نرم‌افزارهای مخرب، نرم‌افزار حفاظتی مناسب نصب و به‌روزرسانی شود.

در صورت نیاز ، برای حفاظت از سیستم در برابر مشکلات برق، بهتر است، سخت‌افزارهای لازم نصب شود.

۷-۵-۲ امضاهای رقمی و الکترونیکی (از جمله امضاهای زیست‌شناختی[2])

امضاهای رقمی و الکترونیکی امکان اثبات اینکه اطلاعات بازیابی‌شده دقیقاً همان اطلاعات ذخیره‌شده هستند را فراهم می‌آورد. به‌کارگیری سیستم‌های امضا معمولاً مستلزم همکاری هر دو گروه است. امضاها یا به‌وسیلهٔ ابزارهای رقمی‌سازی (الکترونیکی) یا با استفاده از یک کلید (رقمی) ایجاد شده و با پرونده الکترونیکی مرتبط می‌شوند. در برخی موارد، فرد بازیابی‌کننده با استفاده از امضا، هویت امضاکننده اصلی و با استفاده از برخی سیستم‌های امضا، یکپارچگی پرونده را تأیید می‌کند. این روش هنگام ذخیره‌سازی، گردش‌کاری یا انتقالِ فوری یا ذخیره و ارسال مجدد در سیستم‌های انتقال، کاربرد دارد. جایی که توانایی تأیید یکپارچگی پرونده دریافت‌شده و احتمالاً هویت ارسال‌کننده پرونده حائز اهمیت می‌باشد، بهتر است، در برنامه‌های کاربردی از امضاها استفاده شود. توصیه می‌شود، امضاها به‌صورت مطمئن و ایمن ذخیره شده و دسترسی به پرونده‌های امضا، کلیدها و الگوریتم‌ها فقط برای کارکنان مجاز امکان‌پذیر باشد.

بهتر است، امضاهای رقمی و الکترونیکی استفاده‌شده برای اثبات عدم تغییر اطلاعات الکترونیکی شامل کنترل مجموعه یا تابع هاش[3] تعبیه‌شده در پرونده / ذخیره‌شده در سیستم ایمنِ محدود به اطلاعات رقمی باشد.

توصیه می‌شود، فرایندهای استفاده‌شده برای نگهداری / ایجاد امضاهای رقمی و الکترونیکی، مستند شود. بهتر است، این فرایندها، روش‌های تأیید هویت اصلی فرد پیش از ثبت او به‌شکل امضاکننده را شامل شود.

در صورت مبهم بودن اطمینان‌پذیری یک پرونده الکترونیکی، می‌توان از امضاها برای اثبات این موضوع استفاده کرد که پرونده ذخیره یا دریافت‌شده در اثر انتقال، حاوی اطلاعات مشابه با پرونده

---

1 - Checksum
2 - Biometric
3 - Hash value

اصلی است. توصیه می‌شود، برای بالا بردن اطمینان‌پذیری پروندهٔ حاوی امضای دیجیتالی، فرایندهای به‌کارگرفته شده، مستند شود.

۷-۶ پردازش تصویر

توصیه می‌شود، برای ارائه تصویر خروجی بهینه یا ارتقای میزان تشخیص برای فرایند دریافت خودکار داده‌ها، پردازش‌های پس از پویش را انجام داد. جایی که پردازش‌های پس از پویش انجام می‌شوند، بهتر است، تأثیر هر یک از فرایندها روی تصویر به صورت مجزا مستند شود.

عبارت «پردازش‌های پس از پویش» به توصیف روش‌های مختلف افزایش کیفیت تصویر اطلاق می‌شود که از سخت‌افزارها و/ یا نرم‌افزارهایی استفاده می‌کنند که به تنهایی یا به صورت مستقل روی خروجی تصویر ارائه‌شده و اندازه پرونده ذخیره‌شده، تأثیرگذار هستند. این سخت‌افزارها یا نرم‌افزارها را می‌توان در محل پویش یا روی کارساز شبکه نصب کرد.

رایج‌ترین روش‌های پردازش تصویر عبارتند از:

الف- اریب‌زدایی[1] کردن؛

ب- لکه‌زدایی / پاک کردن پس زمینه؛

پ- حذف حاشیه سیاه؛

ت- حذف فرم (به بند ۷-۸ مراجعه شود).

توصیه می‌شود، از ابزارهای پردازش تصویر با دقت استفاده شود. برای مثال: ممکن است فرایند لکه‌زدایی منجر به حذف نقطه‌های اعشاری و بنابراین تغییر ارزش اعداد شود.

بهتر است، هر نوع پردازش انجام‌شده روی تصویرهای رقمی‌شده، یکپارچگی تصویر به‌عنوان یک رونوشت عینی از تصویر اصلی را تحت تأثیر قرار ندهد. برای کنترل عدم تأثیر پردازش تصویر روی یکپارچگی تصاویر پویش‌شده، بهتر است، مجموعه نمونه‌ای از مدارک کاغذی در حالت فعال پردازش تصویر، پویش شده و نسخه‌های چاپ‌شده از این تصاویر با تصاویر اصلی مقایسه شود.

توصیه می‌شود، هرگاه از روش‌های پردازش تصویر استفاده می‌شود، تصاویر ذخیره‌شدهٔ مجموعه نمونه از مدارک کاغذی با پردازش تصویر و بدون پردازش تصویر در نظر گرفته شوند.

بهتر است، تأثیر پردازش‌های صورت گرفته روی تصویر طیف خاکستری قبل از تبدیل به تصویر سیاه و سفید، از نظر مقبولیت مورد بررسی قرار گیرد.

توصیه می‌شود، حذف لکه‌ها فقط با دقت زیاد صورت گرفته و استفاده از آن، مستند شود. حذف لکه‌ها باعث از بین رفتن نقاط مجزا یا گروه کوچکی از نقاط از تصویر رقمی شده و منجر به ایجاد تصویر شفاف‌تری می‌شود اما نمی‌توان برای حذف آسیب واردشده از دستگاه به تصویر، فقط به این روش کفایت کرد. در مورد برخی از مدارک کاغذی، خطر حذف اطلاعات، مانند بخشی از

1 - De-Skew

نویسه‌هایی که قبلاً قطع شده‌اند، نشانه‌های نقطه‌گذاری یا بخش‌هایی از جزئیات ریـز در نقشـه‌هـا، بسیار زیاد است.

اگر لکه‌زدایی تصاویر به صورت روزمره مورد استفاده قرار گرفته و اطلاعات واضحی دربـارهٔ تصـاویر وجود ندارد، می‌توان تلقی کرد که فرایند لکه‌زدایی برای تمام تصاویر به‌کار رفتـه اسـت. در صـورت مبهم بودن تمامیت تصاویر، این کار توانایی اثبات اطمینان‌پذیری آنها را تحت تأثیر قرار می‌دهد.

استفاده از روش لکه‌زدایی را می‌توان در دفتر گزارش روزانه متصدی، در مراحل ممیزی یا با استفاده از اطلاعات بیشتر مرتبط با تصویر، مستند کرد.

هرگاه جز اطلاعاتی که بر اثر وضـوح پـویش از بـین مـی‌رونـد، وجـود اطلاعـات کـافی در تصـاویر پویش‌شده، از اهمیت به‌سزائی برخوردار است، بهتر است، پس از ایجاد اولیه پرونده تصویر، پردازش بیشتری روی تصویر انجام نشود.

توصیه می‌شود، هنگامی که روش‌های پردازش ممکن است یکپارچگی تصویر ذخیره‌شده را به خطر اندازد، به ذخیره‌سازی تصویر اولیه (یعنی تصویر پردازش‌نشده) توجه ویژه‌ای شود.

۷-۷ روش‌های فشرده‌سازی

بهتر است، استفاده از روش‌های فشرده‌سازی مطابق با سند خط‌مشی مدیریت مدارک باشد. توصـیه می‌شود، این روش‌ها قبل یا حین ذخیره‌سازی برای پرونده‌های الکترونیکی به‌کـار گرفتـه شـوند تـا اندازه پرونده را کاهش داده و عملکرد سیستم را ارتقا دهند.

اگرچه برخی سیستم‌ها دارای برنامهٔ فشرده‌سازی داخلی هستند که کاربر راهی به جز استفاده از آن ندارد، اما نوع فشرده‌سازی استفاده‌شده معمولاً به برنامه کاربردی وابسته است. برای کسب اطلاعات بیشتر دربارهٔ روش‌های فشرده‌سازی به استاندارد ISO/TR 12033 مراجعه شود.

ممکن است فشرده‌سازی از رهیافت‌های ریاضی مختلفـی اسـتفاده کنـد امـا تمـام ایـن روش‌هـا را می‌توان در دو گروه به نام‌های فشرده‌سازی با اتلاف[1] و فشرده‌سازی بدون اتلاف[2]، طبقه‌بندی کرد.

توصیه می‌شود، روش فشرده‌سازی استفاده‌شده و ویژگی با اتلاف یا بدون اتـلاف بـودن آن، مسـتند شود. بهتر است، مستندات کمّی بوده و شامل الگوریتم به‌کاررفته برای محاسبهٔ میزان اتلاف باشد.

توصیه می‌شود، این اطلاعات به‌عنـوان بخشـی از پرونـده یـا داده‌هـای مـرتبط بـا آن یـا از طریـق گزارش‌های جداگانه، ذخیره شود.

یادآوری- برای مثال، در مورد پرونده‌های تصویری ذخیره‌شده در قالب TIFF[3] (و برخـی دیگـر از قالـب‌هـا)، روش فشرده‌سازی به‌طور خودکار در پرونده تصویر، ذخیره می‌شود.

1- Lossy
2- Lossless
3 - Tagged Image File Format

بهتر است، روش‌های فشرده‌سازی با اتلاف را با دقت مورد استفاده قرار داد. بر اساس تعریف، حتی در برخی نمونه‌ها که میزان اتلاف از نظر بصری قابل رؤیت نیست، روش‌های با اتلاف منجر به اتلاف غیر قابل برگشت داده‌ها می‌شوند. بنابراین، یک پرونده الکترونیکی بازشده[1] با پرونده اصلی یکسان نیست. این مسئله، اثبات یکپارچگی چنین پرونده‌هایی را دشوارتر می‌کند. برای مثال: ممکن است بخش‌هایی از متن یا نقشه‌ها از روی پرونده تصویری حذف شده و با داده‌هایی که به‌طور مصنوعی ایجاد شده‌اند، جایگزین شوند. بنابراین، ممکن است استفاده از روش فشرده‌سازی با اتلاف روی پرونده‌هایی که اساساً حاوی متن (از جمله دست‌نوشته‌ها) یا خطوط نقشه هستند، خطراتی را در پی داشته باشد.

هرگاه بتوان نشان داد که اتلاف قابل توجه اطلاعات در تصویر پویش‌شده وجود ندارد، فشرده‌سازی با اتلاف برای عکس‌ها یا مواد با تونالژ پیوسته، مدارک طیف خاکستری یا رنگی مناسب است.

در صورت استفاده از روش فشرده‌سازی با اتلاف، بهتر است، یک مجموعهٔ نمونه از پرونده‌های خارج‌شده از حالت فشرده با پرونده‌های اصلی مقایسه شوند تا عدم اتلاف اطلاعات مهم بررسی شود. توصیه می‌شود، در صورت استفاده از فشرده‌سازی با اتلاف، نسبت فشرده‌سازی به‌دست‌آمده مستند شود.

در صورت امکان بهتر است، نسبت فشرده‌سازی را انتخاب کرد تا تمام اطلاعات موردنیاز در دامنهٔ کاربری، در پرونده با برداشت فشار، ارائه شود.

حداکثر نسبت فشرده‌سازی قابل قبول را می‌توان از طریق مجموعهٔ نمونه از پرونده‌های اصلی تعیین کرده و ممکن است بین مدارک موجود در مجموعهٔ نمونه متفاوت باشد. ممکن است تصمیم‌گیری راجع به استفاده از نسبت‌های مختلف فشرده‌سازی برای مدارک مختلف یا استفاده از یک نسبیت منفرد برای همه مدارک، لازم باشد. در صورت استفاده از رهیافت دوم، میانگین اندازه پرونده تصویری بالاتر بوده اما سرعت پردازش هم به علت مداخله کمتر متصدی، بالاتر خواهد بود.

هرگاه عدم اتلاف اطلاعات در تصویر پویش‌شده، به جز اطلاعاتی که بر اثر وضوح پویش از بین می‌روند، حائز اهمیت است، بهتر است، از فشرده‌سازی با اتلاف استفاده نشود. نمونه‌هایی از مدارک رقمی که استفاده از فشرده‌سازی با اتلاف برای آنها توصیه نمی‌شود، تصاویر پرتونگاری‌شده[2] (تصاویر اشعهٔ ایکس پزشکی یا مهندسی) هستند.

هنگامی که از فشرده‌سازی استفاده می‌شود، بهتر است، سیستم ابزارهای کافی را ترجیحاً از طریق تجهیزات خودکار ارائه دهد تا اطمینان حاصل شود که الزامات کنترل کیفیت (مانند بررسی کیفیت تصویر پس از پویش با امکان پویش مجدد در صورت نیاز، اعمال کنترل روی درستی داده‌های مرتبط، اعمال کنترل روی یکپارچگی داده‌ها) در پرونده فشرده‌شده، رعایت شده‌اند.

1 - Decompressed
2 - Radiographs

۸-۷ جایگذاشت فرم[1] و حذف فرم

هنگامی که مدرک اصلی از یک فرم با اطلاعات موجود در جایگذاشت تشکیل شده است، بهتر است، فرم را پیش از ذخیره‌سازی، به‌صورت الکترونیکی از تصویر پویش‌شده حذف کرد (حذف فرم).

وقتی فرمی که به صورت الکترونیکی حذف شده، به‌صورت مجزا از تصویر پویش‌شدهٔ مرتبط با آن نگهداری می‌شود، بهتر است، به‌عنوان بخشی از تصویر پویش‌شده، تحت کنترل قرار گیرد.

توصیه می‌شود، سابقه‌ای نگهداری شود که تصویر حاصل از آن (بدون فرم) در معرض حذف فرم قرار گرفته و شناسه هر نمونه که برای حذف، مورد استفاده قرار گرفته نیز نگهداری شود. بهتر است، این اطلاعات همراه با تصویر حاصل، ذخیره شود. توصیه می‌شود، یک نسخه از هر نمونهٔ استفاده‌شده نیز ذخیره شود.

بهتر است، رونوشت ایجادشده در اثر ادغام نمونه با فرم علامت‌گذاری‌شده، به‌عنوان رونوشت عینی از مدرک اصلی در نظر گرفته نشود، اگرچه این رونوشت صحت کافی برای استفاده را دارا می‌باشد.

اثبات اطمینان‌پذیری تصاویر ادغام‌شده، مخصوصاً جایی که اختلاف فرم و اطلاعات جایگذاشت‌شده در تصویر ادغام‌شده مشهود است، بسیار دشوار خواهد بود.

نگهداری از رونوشت عینی فرم‌های اصلی با نگهداری از خود فرم‌های اصلی و ایجاد نسخه ریزفیلم یا نگهداری کل تصویر فرم، مناسب خواهد بود.

۹-۷ ملاحظات محیطی

توصیه می‌شود، شرح توصیه‌های کارخانه سازنده سخت‌افزارها برای محیط عملیاتی تمام اجزای سیستم و رسانه ذخیره‌سازی، مستند شود.

بهتر است، روش‌های جابه‌جایی و ذخیره‌سازی، مستند شود.

عمر انواع مختلف رسانه‌های ذخیره‌سازی، متفاوت است. برای اطمینان از اینکه اطلاعات ذخیره‌شده قابل بازیابی هستند، بررسی منظم رسانه مطابق با توصیه‌های سازندهٔ آن، ضروری است. توصیه می‌شود، روش‌های بررسی شرایط رسانه، مستند شود. بهتر است، رسانه به‌طور منظم مطابق با توصیه‌های سازنده رسانه، کنترل شود.

۱۰-۷ گذار

می‌توان اطلاعات را برای مدت زمان بسیار زیادی ذخیره کرد که این بازهٔ زمانی از عمر فناوری‌های موجود بیشتر است. پس برای اطمینان از یکپارچگی اطلاعات ذخیره‌شده، لازم است از ابتدا برنامه‌ای برای فرایند گذار داده‌ها در نظر گرفته شود. ممکن است این فرایندها شامل تغییر رسانه/ تغییر نرم‌افزار / سخت‌افزار رایانه‌ای باشند.

---

1 - Form Overlays

یکی از فناوری‌های مطمئن برای حل این مشکل بالقوه، اطمینان از ذخیره پرونده‌های الکترونیکی در قالب استاندارد صنعتی یا نگهداری از برنامه نمایش پرونده برای هر کدام از قالب‌های ذخیره‌شده است.

توصیه می‌شود، برای گذار پرونده‌های الکترونیکی شامل فراداده‌ها، داده‌های نمایه و مراحل ممیزی، به فناوری جدید بدون اتلاف اطلاعات و با مستندات کافی درباره فرایند گذار که امکان اثبات اطمینان‌پذیری اطلاعات ذخیره‌شده در آینده را فراهم می‌آورد، شرایطی در نظر گرفته شود.

۷-۱۱ امحاء / حذف اطلاعات

ممکن است به طور مثال برای تطابق با الزامات قانونی یا حقوقی، حذف/ امحاء اطلاعات خاص از سیستم قابل اعتماد مدیریت مدارک، لازم باشد.

گاهی‌اوقات، ممکن است شرایطی به‌وجود آید که مستلزم عدم امحاء اطلاعاتی باشد که طبق جداول زمانی نگهداری عادی، زمان امحاء آنها فرا رسیده است. توصیه می‌شود، فرایندهایی وجود داشته باشد که باعث اطمینان از بررسی اطلاعات پیش از امحاء آنها شده و بنابراین بتوان با نمونه‌های خاص تطابق پیدا کرد.

هنگامی که اطلاعات روی رسانه WORM ذخیره شده‌اند، امحاء اطلاعات خاص ممکن نخواهد بود (مگر اینکه فرایند کنترل‌شدهٔ رونوشت‌برداری منتخب روی رسانهٔ جدید به‌کارگرفته شده باشد). در برخی برنامه‌ها، معادل دانستن حذف تمام ارجاعات نمایه به اطلاعات حذف‌شده با حذف خود اطلاعات، مورد قبول است. در برخی دیگر از برنامه‌ها، نشانه‌گذاری اطلاعات به عنوان موارد حذف‌شده، قابل قبول است. در صورت لزوم، سازمان‌ها باید مقبولیت روش‌های به‌کارگرفته‌شده برای مراجع ذی‌صلاح را مورد بررسی قرار دهند. بهتر است، این روش‌ها با دقت کافی مورد استفاده قرار گیرند چرا که در برخی شرایط، ممکن است بازیابی اطلاعات حذف‌شده، لازم باشد.

وقتی که حذف فیزیکی[1] اطلاعات از سیستم لازم است، تعیین و حذف تمام نسخه‌های اطلاعات (از جمله رسانه پشتیبان)، باعث اطمینان از انجام اقدامات لازم می‌شود.

توصیه می‌شود، سیستم قابل اعتماد مدیریت مدارک، ابزارهایی برای حذف یا امحاء اطلاعات با استفاده از فرایندهای قابل پیگیری، داشته باشند.

بهتر است، وقتی عمل امحاء / حذف انجام می‌شود، پیش از اقدام به کار مجوزهای لازم را اخذ کرد.

توصیه می‌شود، سیستم قابل اعتماد مدیریت مدارک ابزارهایی برای اصلاح اطلاعات غلط یا حذف اطلاعات ناخواسته داشته باشد.

بهتر است، وقتی که اصلاح یا حذف مطابق با مقررات انجام می‌شود، سوابق مناسب نگهداری شود تا امکان اثبات تطابق با مقررات وجود داشته باشد.

برای کسب اطلاعات درباره حذف از سیستم‌های با قابلیت یکبار نوشتن، به استاندارد ISO/TR 12307 مراجعه شود.

---

1 - Positive removal

۸ مراحل ممیزی

۸-۱ کلیات

۸-۱-۱ داده‌های مراحل ممیزی

هنگام آماده‌سازی اطلاعات برای استفاده به‌عنوان گواهِ یک تراکنش یا رویداد، غالباً ارائه اطلاعات پشتیبان بیشتر، لازم است. این اطلاعات شامل جزئیاتی مانند تاریخ ذخیره‌سازی اطلاعات، جزئیات مربوط به انتقال اطلاعات از یک رسانه به رسانهٔ دیگر و گواهِ عملیات کنترل‌شدهٔ سیستم می‌باشد. این جزئیات به‌عنوان اطلاعات مراحل ممیزی شناخته می‌شود. مراحل ممیزی که در این استاندارد توصیف شده، شامل مجموعه‌ای از اطلاعات ضروری برای ارائه سابقهٔ تاریخی تمام رویدادهای مرتبط با اطلاعات ذخیره‌شده و سیستم قابل اعتماد مدیریت مدارک است. این اطلاعات را می‌توان به دو گروه زیر تقسیم کرد:

الف- سیستم؛

ب- اطلاعات ذخیره‌شده.

توصیه می‌شود، سوابق اقدامات یا رویدادهای تاریخی سیستم قابل اعتماد مدیریت مدارک که ممکن است در آینده و برای پشتیبانی از اطلاعات ذخیره‌شده، دوباره بازسازی شوند، نگهداری شود.

بهتر است، مراحل ممیزی شامل اطلاعات لازم و کافی برای امکان‌پذیر ساختن اثبات اطمینان‌پذیری اطلاعات ذخیره‌شده باشد.

غالباً برخی از ادارت (یا افراد) هر سازمان (یا خارج از سازمان) ممکن است به اطلاعات مراحل ممیزی، از جمله اطلاعات نشان‌دهندهٔ کاربر و وظایف حسابرسی و قانونی، نیاز داشته باشند.

توصیه می‌شود، محتوای مراحل ممیزی مورد موافقت تمام ادارات مرتبط سازمان قرار گیرد.

در اکثر سازمان‌ها، مراحل ممیزی شامل مجموعه‌ای از گزارش‌های روزانه سیستم و متصدی است.

بهتر است، مراحل ممیزی شامل داده‌هایی درباره تغییرات صورت‌گرفته روی اطلاعات ذخیره‌شده در سیستم باشد.

۸-۱-۲ ایجاد

توصیه می‌شود، داده‌های مراحل ممیزی تا حد امکان به‌صورت خودکار توسط سیستم ایجاد شده و دستورالعمل توصیف سیستم، فرایندها را شرح دهد.

در مورد داده‌های مراحل ممیزی که به‌صورت خودکار توسط سیستم ایجاد نشده‌اند، بهتر است، روش‌های ایجاد این داده‌ها در شیوه‌نامه اجرایی، مستند شود. بهتر است، به دامنهٔ هر مرحلهٔ ممیزی، توجه شود. برای مثال: جایی که بخش خاصی از اطلاعات در فرم پیش‌نویس ایجاد شده و با ایجاد چند پیش‌نویس دیگر دنبال شده است، آیا هر کدام از پیش‌نویس‌ها به یک مرحله ممیزی کامل احتیاج دارند یا فقط مدرک نهایی مستلزم وجود مراحل ممیزی است؟

مراحل ممیزی خودکار دارای ارجحیت هستند چرا که مدیریت و اطمینان‌پذیری آنها آسانتر است. توصیه می‌شود، هرگاه مراحل ممیزی خودکار در دسترس نیست، منابعی که لازم است فرایند خودکار را ایجاد کنند، به دقت مورد بررسی قرار گیرند.
توصیه می‌شود، روش‌هایی که هنگام تکمیل پرونده داده‌های مراحل ممیزی از آنها پیروی می‌شود (شناسایی این موقعیت)، در شیوه‌نامه اجرایی مستند شود.

۸-۱-۳ تاریخ و زمان

بهتر است، هر سابقهٔ دادهٔ مراحل ممیزی دارای تاریخ و زمان مرتبط باشد که با تاریخ و زمان رویداد ذخیره‌شده در ارتباط است.
توصیه می‌شود، تاریخ و زمان رویدادی که ذخیره شده به اندازه‌ای دقیق باشد که کنترل‌های بعدی، زنجیرهٔ رویدادها را مشخص کند.
در مورد آن‌دسته از داده‌های مراحل ممیزی که توسط سیستم ایجاد می‌شوند، بهتر است، داده‌ها بلافاصله پس از رویدادی که مستندشده، ایجاد شوند.
به‌طور عادی منظور از تاریخ و زمان، تاریخ و زمان ایجاد داده‌های مراحل ممیزی است اما اگر ایجاد داده‌ها در اصل همزمان با رویداد مستندشده انجام می‌شود، بهتر است، زمان تمام معانی و اهداف رویداد را دربرداشته باشد.
در مورد آن‌دسته از داده‌های مراحل ممیزی که به‌صورت دستی ایجاد می‌شوند، بهتر است، داده‌ها به سرعت پس از رویداد مستندشده، ایجاد شوند. برای مثال: اگر سابقه مربوط به زمان شروع به کار متصدی است، حقایق مربوط به آن زمان مستند می‌شود. اگر سابقه مربوط به زمان شروع آماده‌سازی دستهٔ خاصی از مدارک کاغذی است، حقایق قبل از آماده‌سازی آن دسته، مستند می‌شود.
توصیه می‌شود، جایی که زمان حقیقیِ وقوع رویداد حائز اهمیت است، استفاده از زمان قابل اعتماد را در نظر گرفت.

۸-۱-۴ ذخیره‌سازی

ذخیره‌سازی داده‌های مراحل ممیزی موضوعی است که غالباً در خط‌مشی‌های مدیریت مدارک سازمان در نظر گرفته نمی‌شود. از آنجا که این داده‌ها غالباً به‌صورت خودکار ایجاد و به ندرت در دسترس قرار می‌گیرند، به فراموشی سپرده شده و بنابراین در معرض کنترل‌های کافی قرار ندارند.
برخی از سیستم‌ها، اندازهٔ پرونده‌های دادهٔ مراحل ممیزی را با استفاده از مسیرهای بسته کنترل می‌کنند که حداکثر اندازه پرونده داده‌ها را تعیین کرده و وقتی به پرونده به این اندازه می‌رسد، داده‌های جدید روی داده‌های قدیمی موجود در پرونده، بازنویسی می‌شود. بنابراین، مراحل ممیزی‌های قدیمی از بین می‌روند.
توصیه می‌شود، داده‌های مراحل ممیزی به‌عنوان نوع خاصی از مدارک در سند خط‌مشی وارد شوند.

بهتر است، داده‌های مراحل ممیزی حداقل معادل با زمانی که اطلاعات مرتبط با آن نگهداری می‌شوند، ذخیره شوند.

۸-۱-۵ دسترسی

لازم است افراد مختلف در زمان‌های متفاوت به اطلاعات مراحل ممیزی دسترسی داشته باشند. در برخی برنامه‌ها، دسترسی فقط در مبنای خاص مورد نیاز بوده و بنابراین مستندسازی روش‌های دسترسی و تفسیر، حائز اهمیت است.

توصیه می‌شود، شیوه‌نامه اجرایی، چگونگی دسترسی به مراحل ممیزی و تفسیر آن را شرح دهد.

بهتر است، کارکنان مجاز برون سازمانی که آشنایی کمی با سیستم داشته یا با آن آشنا نیستند، به داده‌های مراحل ممیزی دسترسی داشته باشند.

۸-۱-۶ امنیت و حفاظت

اگر اطمینان‌پذیری اطلاعات ذخیره‌شده مبهم باشد، یکپارچگی مراحل ممیزی در ایجاد اطمینان‌پذیری اطلاعات ذخیره‌شده، نقش اساسی دارد. توصیه می‌شود، برای جلوگیری از اعمال تغییرات در داده‌های موجود، مراحل ممیزی در سطح امنیتی مناسب ، نگهداری شود.

بهتر است، داده‌های مراحل ممیزی به‌صورت مطمئن مطابق با خط‌مشی امنیت اطلاعات ذخیره شوند. توصیه می‌شود، مراحل ممیزی منوط به روش‌های داخلی مدیریت مدارک باشند که متناسب با دیگر سوابق حیاتی سازمان هستند.

بهتر است، نسخه‌های پشتیبان مطمئن از مراحل ممیزی نگهداری شوند. این کار برای داده‌های رد ممیزی روی رسانه‌های الکترونیکی و روی کاغذ/ ریزفیلم کاربرد دارد.

توصیه می‌شود، اطلاعات مراحل ممیزی که در سیستم قابل اعتماد مدیریت مدارک نگهداری می‌شوند، قابل اصلاح نباشند. جایی که از روش‌های بازیابی پرونده استفاده می‌شود، بهتر است، داده‌های مراحل ممیزی کافی ذخیره شود تا بتوان اثبات کرد که بازیابی پرونده، اطمینان‌پذیری اطلاعات را تحت تأثیر قرار نداده است.

برای کاهش ریسک، داده‌های مراحل ممیزی را روی رسانه WORM ذخیره کنید. در صورت استفاده از رسانه‌های با قابلیت نوشتن مجدد، لازم است برای جلوگیری از انجام تغییرات، روش‌های بیشتری به‌کار گرفته شود. استفاده از نوارهای مغناطیسی اصلاح داده‌ها را نسبتاً دشوار می‌کند چرا که نوارهای مغناطیسی معمولاً رسانه‌هایی هستند که به صورت متوالی نوشته می‌شوند.

اگر امکان اصلاح داده‌های مراحل ممیزی وجود دارد، اثبات اطمینان‌پذیری اطلاعاتی که این ممیزی‌ها برای آنها به‌کار گرفته می‌شود، دشوار است.

توصیه می‌شود، مدارک کاغذی استفاده‌شده برای داده‌های مراحل ممیزی، بارها از محل استفاده و ذخیره‌سازی مطمئن آنها، جابه‌جا شوند. هر چه مدت زمان نگهداری مدرک مورد استفاده برای داده‌های مراحل ممیزی (مانند: گزارش روزانه متصدی) در مکان نامطمئن بیشتر باشد، خطر

تحریف آن بیشتر خواهد بود. لازم است کاربران هنگام استفاده از مدارک کاغذی برای سوابق مراحل ممیزی، این ریسک را ارزیابی کنند. جایی که از مدارک کاغذی استفاده می‌شود، ذخیره‌سازی نسخه‌های آن روی سیستم قابل اعتماد مدیریت مدارک الکترونیکی، توصیه می‌شود.
برای حفاظت در دوره‌های زمانی طولانی با استفاده از گذار یا روش‌های دیگر، به بند ۸-۲-۳ مراجعه شود.

۸-۲ سیستم

۸-۲-۱ کلیات

این سوابق شامل جزئیاتی درباره موضوعات زیر است:

الف- اطلاعات مراحل ممیزی؛

ب- گذار و تبدیل.

۸-۲-۲ اطلاعات مراحل ممیزی

توصیه می‌شود، برای همهٔ داده‌های مراحل ممیزی سیستم، تعیین فرایندهای دخیل و تاریخ و زمان رویداد امکان‌پذیر باشد.
با توجه به اهمیت آن، اطلاعات تاریخ و زمان را می‌توان روی یک دسته یا بر مبنای رویداد منفرد، ذخیره کرد. هرگاه داده‌های مراحل ممیزی به‌صورت دستی توسط متصدی ذخیره می‌شوند، ممکن است ایجاد مراحل ممیزی به ازای هر مدرک، غیرعملی و غیرضروری باشد. برای مثال: هنگام آماده‌سازی مدارک کاغذی برای پویش، ممکن است مستند کردن زمان شروع و پایان آماده‌سازی یک دسته کافی باشد؛ مشروط به امکان‌پذیر بودن تعیین مدارکی که متصدی آماده کرده، ممکن است مستند کردن زمان شروع و پایان کار متصدی، کافی باشد.

۸-۲-۳ گذار و تبدیل

توصیه می‌شود، هنگامی که اطلاعات به‌عنوان بخشی از فرایند گذار، از یک وسیله ذخیره‌سازی به وسیله دیگر منتقل می‌شود، جزئیات مربوط به این انتقال در مراحل ممیزی ذخیره شود.
بهتر است، روش‌های گذار یا تبدیل شامل روش‌هایی برای اثبات این موضوع باشد که همه داده‌های مرتبط (مانند: فراداده‌ها) نیز منتقل شده‌اند.
در مورد سیستم‌های مدیریت ذخیره‌سازی سلسله مراتبی[1]، جایی که داده‌ها به شکل روزمره و خودکار بین تجهیزات ذخیره‌سازی و بدون مداخله کاربر منتقل می‌شوند، ایجاد داده‌های مراحل ممیزی درباره انتقال اطلاعات، لازم نیست. البته ممکن است اثبات عملکرد عادی سیستم مدیریت ذخیره‌سازی سلسله مراتبی هنگام انتقال اطلاعات، لازم باشد.

1 - Hierarchical Storage Management Systems

توصیه می‌شود، جایی که اطلاعات از یک قالب پرونده به قالب پرونده دیگر منتقل می‌شود، جزئیات این انتقال در مراحل ممیزی ذخیره شود. برای مثال مدرک رقمی ایجادشده با برنامه پردازشگر کلمه می‌تواند بدون تغییر متن مدرک به قالب تصویری منتقل شود. از یک منظر، این کار با رونوشت‌برداری از پرونده تفاوتی ندارد اما اگر قالب‌بندی با محتوای اطلاعات در ارتباط است، این امکان وجود دارد که محتوای اطلاعاتی پرونده تبدیل‌شده، دچار تغییر شود.

۸-۳ اطلاعات ذخیره‌شده

۸-۳-۱ کلیات

این سوابق شامل اطلاعاتی درباره موضوعات زیر هستند:

الف- دریافت اطلاعات؛

ب- دسته‌بندی اطلاعات؛

پ- نمایه‌سازی؛

ت- کنترل تغییر؛

ث- استفاده از امضاهای رقمی؛

ج- امحاء اطلاعات؛

چ- گردش کاری.

۸-۳-۲ دریافت اطلاعات

۸-۳-۲-۱ کلیات

داده‌های مراحل ممیزی درباره فرایند دریافت، برای کمک به اطمینان‌پذیری اطلاعات ذخیره‌شده، اطلاعات ارزشمندی را ارائه می‌دهد. وقتی اطمینان‌پذیری مدرک به چالش کشیده می‌شود، وجود جزئیاتی مانند زمان دریافت، فرد دریافت‌کننده، وسیله دریافت و نوع مدرک اصلی، ضروری است.

توصیه می‌شود، در مراحل ممیزی اطلاعات کلیدی، کلیهٔ اطلاعات بر اساس اطلاعات دریافت یا واردشده به سیستم، نگهداری شود. بهتر است، اطلاعات کافی مرتبط با هر یک از روش‌های پردازش، ذخیره شود.

اطلاعاتی که عموماً در مراحل ممیزی ذخیره می‌شوند شامل موارد زیر است:

الف- شناسگرهای مدرک یا پرونده؛

ب- نشانگرهای تاریخ و زمان پردازش؛

پ- مرجع دسته‌بندی (برای داده‌های ورودی دسته‌بندی)؛

ت- تعداد صفحات (برای پویش مدارک) یا سوابق داده‌ها (دریافت داده)؛

ث- تأیید بررسی کنترل کیفیت؛

ج- شناسه‌ای برای هر کدام از مدارک یا پرونده‌های نمایه‌سازی‌شده؛

چ- شناسه فرد یا ایستگاه کاری؛

ح- یادداشت نهایی برای ذخیره‌سازی.

انتخاب داده‌های حقیقی که در مراحل ممیزی ذخیره می‌شوند، به برنامه کاربردی و سیستم بستگی دارد.

۸-۳-۲-۲ اطلاعات پرونده

سیستم می‌تواند اطلاعات را بر اساس روش پرونده به پرونده دریافت کند. این موضوع مخصوصاً در مواردی صحیح است که پرونده‌های الکترونیکی وارد سیستم می‌شوند. توصیه می‌شود، جایی که اطلاعات بر اساس روش پرونده به پرونده دریافت می‌شود، اطلاعات مراحل ممیزی زیر ذخیره شود:

۱- شناسه منحصر به فرد پرونده؛

۲- تعداد مدارک/ صفحات موجود در پرونده؛

۳- حجم پرونده (برای مثال بر حسب کیلوبایت)؛

۴- قالب پرونده؛

۵- کد پرونده (برای مثال مقادیر EDI [1]، DTD [2] و غیره).

۸-۳-۲-۳ اطلاعات مدرک پویش‌شده

می‌توان اطلاعات را با پویش کردن مدارک اصلی در سیستم وارد کرد.

جایی که مدارک پویش می‌شوند، بهتر است، اطلاعات مراحل ممیزی زیر ذخیره شود:

۱- شناسه منحصر به فرد داخلی مدرک؛

۲- تعداد صفحات تصاویر پویش‌شده؛

۳- تعداد صفحات ارسال‌شده به وسیله ذخیره‌سازی.

۸-۳-۳ اطلاعات دسته‌بندی‌شده

الف- هنگامی که داده‌ها بر اساس دسته‌بندی ذخیره می‌شوند، مخصوصاً در برنامه‌های پویش مدارک، بهتر است، اطلاعات مراحل ممیزی زیر ذخیره شود:

۱- شناسه منحصر به فرد دسته؛

۲- شناسه فرد؛

۳- نوع مواد پویش‌شده، مانند مدارک کاغذی، حلقه‌های ریزفیلم، کارت‌های سوراخ‌دار؛

۴- مقدار مواد در هر دسته، مانند تعداد مدارک، تعداد صفحات (یک رو یا دو رو بودن)، تعداد فریم‌های ریزفیلم؛

۵- جزئیات مرتبط با پردازش‌های انجام‌شده حین فرایند پویش، جایی که این پردازش‌ها با پردازش‌های پیش‌فرض تصویر که در دستورالعمل توصیف سیستم شرح داده شده‌اند، تفاوت دارند.

1- Electronic Data Interchange
2 - Document Type Definition

ب- توصیه می‌شود، داده‌های مراحل ممیزی ذخیره شوند تا کنترل موارد زیر را تسهیل کنند:
۱- تمام اقدامات لازم برای دسته‌بندی انجام شده است؛
۲- جزئیات مربوط به موارد غیرعادی یا اشتباهی که رخ داده است؛

مثال:
تعداد صفحات ارسال‌شده برای ذخیره‌سازی با تعداد صفحات پویش‌شده همخوانی ندارد.

۴- پردازش‌های خاص مورد نیاز انجام شده‌اند.

۸-۳-۴ نمایه‌سازی

اطلاعات نمایه‌سازی برای مرحله بازیابی اطلاعات ضروری بوده و بنابراین درستی این اطلاعات، کلید ایجاد اطمینان‌پذیری اطلاعات ذخیره‌شده است. می‌توان از اطلاعات مراحل ممیزی که ایجاد و اصلاح نمایه‌ها را شرح می‌دهند برای اثبات به‌کارگیری صحیح روش‌های نمایه‌سازی، استفاده کرد.
توصیه می‌شود، اطلاعاتی در مراحل ممیزی نگهداری شود که تاریخ و زمان ایجاد، اصلاح و امحاء هر کدام از پرونده‌های نمایه‌شده را شرح می‌دهد. بهتر است، داده‌های مراحل ممیزی شامل شناسه هر مدرک یا پرونده نمایه‌شده باشد.
توصیه می‌شود، هرگاه امکان اصلاح یا امحاء داده‌های نمایه‌شده وجود دارد، داده‌های مراحل ممیزی ایجاد شود. اگر نمایه اصلاح شده باشد، بهتر است، جزئیات مربوط به اصلاح آن ذخیره شود.
هنگامی که مورد نمایه‌شده با اطلاعات امحاء یا حذف شده در ارتباط است، بهتر است، این موضوع نیز مستند شود.

۸-۳-۵ کنترل تغییر

توصیه می‌شود، هرگاه در اطلاعات ذخیره‌شده تغییری ایجاد می‌شود، داده‌های مراحل ممیزی ایجاد و ذخیره شوند که ماهیت تغییر و فرد یا برنامه (جایی که تغییر به صورت خودکار توسط سیستم رخ می‌دهد) آغازکننده تغییر را مشخص می‌کند.
در صورت نیاز، بهتر است، در داده‌های مراحل ممیزی به نسخه‌های قبلی اطلاعات اشاره شود تا ماهیت تغییر مشخص گردد.

۸-۳-۶ امضاهای رقمی

توصیه می‌شود، هرگاه از امضاهای رقمی (یا دیگر روش‌های امضای الکترونیکی) استفاده می‌شود، داده‌های مراحل ممیزی به شرح زیر نگهداری شود:
۱- شناسایی پرونده؛

۲- گواهی شناسایی پرونده؛
۳- تأیید هویت مرجع ذی‌صلاح؛
۴- تاریخ و زمان امضا؛
۵- گزارش تأیید یا دریافت؛
۶- سند اعتبارسنجی.

۸-۳-۷ امحاء اطلاعات

توصیه می‌شود، داده‌های مراحل ممیزی درباره امحاء مدارک کاغذی پس از پویش مدرک، نگهداری شود. بهتر است، داده‌های مراحل ممیزی درباره امحاء اطلاعات در انتهای دورهٔ نگهداری، حفظ شود. توصیه می‌شود، داده‌های مراحل ممیزی درباره اعطا مجوز امحاء، نگهداری شود.

۸-۳-۸ گردش کاری

توصیه می‌شود، هر بار که روش اداری جدیدی تعریف شده یا تعاریف موجود تغییر کرده‌اند، سابقه‌ای از مفهوم مراحل ممیزی وجود داشته باشد.

هرگاه از سیستم‌های گردش کاری استفاده می‌شود، بهتر است، نقاط اصلی تعریف شود که داده‌های مراحل ممیزی در این نقاط اصلی ایجاد گردد.

در اکثر سیستم‌های گردش کاری، یک نقطهٔ اصلی مراحل ممیزی در هر مرحله از گردش کاری وجود دارد. برای تطابق با سند خط‌مشی، ممکن است لازم نباشد برای هر نقطهٔ اصلی مراحل ممیزی، اطلاعات را نگهداری کرد. توصیه می‌شود، کاربر تصمیم بگیرد که با توجه به اهمیت شهودی احتمالی داده‌ها در گردش کاری، کدام نقاط اصلی مراحل ممیزی مرتبط هستند. بهتر است، برای ایجاد داده‌های مراحل ممیزی، این نقاط اصلی انتخاب شوند.

با تغییر روش‌های گردش کاری، نقاط اصلی مراحل ممیزی انتخاب‌شده نیز می‌توانند تغییر کنند.

توصیه می‌شود، سیستم به کاربر مجاز اجازه دهد تا نقاط اصلی که داده‌های مراحل ممیزی برای آن ایجاد شده‌اند را انتخاب کند.