استاندارد ملی ایران
۱۹۳۲۵-۱
چاپ اول
۱۳۹۴

جمهوری اسلامی ایران

Islamic Republic of Iran

سازمان ملی استاندارد ایران

Iranian Natioal Standardization Organizaion

INSO
19325-1
1st. Edition
2015

بایگانی الکترونیکی- قسمت ۱:
مشخصات مرتبط با طراحی و عملیات یک سامانه اطلاعاتی برای نگهداری اطلاعات الکترونیکی

Electronic archiving- Part 1:
Specifications concerning the design and the operation of an information system for electronic information preservation

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 موسسه 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 حوزه های مختلف در کمیسیون های فنی مرکب از کارشناسان سازمان ، صاحب نظران مراکز و مؤسسات علمی، پژوهشی، تولیدی و اقتصادی آگاه و مرتبط انجام می شود 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 وارد کنندگان، مراکز علمی و تخصصی، نهادها، سازمان های دولتی و غیر دولتی حاصل می شود .پیش نویس استانداردهای ملی ایران برای نظرخواهی به مراجع ذی نفع و اعضای کمیسیون های 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 می شود.

پیش نویس استانداردهایی که مؤسسات و سازمان های علاقه مند و ذی صلاح نیز با رعایت ضوابط تعیین شده تهیه می کنند درکمیتهٔ ملی طرح و بررسی و درصورت تصویب، به عنوان استاندارد ملی ایران چاپ و منتشر می شود .بدین ترتیب، استانداردهایی ملی تلقی می شوند 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 بین المللی استاندارد (ISO)[1] ،کمیسیون بین المللی الکتروتکنیک (IEC)[2] و سازمان بین المللی اندازه شناسی قانونی (OIML)[3] است و به عنوان تنها رابط[4] کمیسیون کدکس غذایی (CAC)[5] در کشور فعالیت می کند. در تدوین استانداردهای ملی ایران ضمن توجه به شرایط کلی و نیازمندی های خاص کشور ، از آخرین پیشرفت های علمی، فنی و صنعتی جهان و استانداردهای بین‌المللی بهره‌گیری می‌شود .

سازمان ملی استاندارد ایران می تواند با رعایت موازین پیش بینی شده در قانون، برای حمایت از مصرف کنندگان، 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 می تواند به منظور حفظ بازارهای بین المللی برای محصولات کشور، اجرای استاندارد کالاهای صادراتی و درجه‌بندی آن را اجباری نماید. همچنین برای اطمینان بخشیدن به استفاده کنندگان از خدمات سازمان ها و مؤسسات فعال در زمینهٔ مشاوره، آموزش، بازرسی، ممیزی و صدورگواهی سیستم های مدیریت کیفیت و مدیریت زیست‌محیطی، آزمایشگاه ها و مراکز کالیبراسیون (واسنجی) وسایل سنجش، سازمان ملی استاندارد ایران این گونه سازمان ها و مؤسسات را بر اساس ضوابط نظام تأیید صلاحیت ایران ارزیابی می کند و در صورت احراز شرایط لازم، گواهینامهٔ تأیید صلاحیت به آن ها اعطا و بر عملکرد آن ها نظارت می کند. ترویج دستگاه بین المللی 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

« بایگانی الکترونیکی- قسمت ۱: مشخصات مرتبط با طراحی و عملیات یک سامانه اطلاعاتی برای نگهداری اطلاعات الکترونیکی»

رئیس:	**سمت و/ یا نمایندگی**
ارسلان، علیرضا (فوق لیسانس مدیریت اجرایی)	رئیس انجمن کارشناسان استاندارد استان یزد
دبیر:	
جعفری ندوشن، زهرا (فوق لیسانس مدیریت صنعتی)	کارشناس اداره کل استاندارد یزد
اعضاء: (اسامی به ترتیب حروف الفبا)	
احمدی ندوشن، علیرضا (دانشجوی دکترای مدیریت)	شرکت گاز استان یزد
افضل‌آبادی، محمدرضا (دکترای مدیریت صنعتی)	سازمان صنعت، معدن و تجارت استان یزد
بهاری فرد، ناهید لیسانس مهندسی صنایع	شرکت تولیدی صنایع لاستیک استان یزد
تقوی، محمدمسعود (فوق لیسانس کامپیوتر)	کارشناس اداره کل استاندارد یزد
سجادی، نرگس‌السادات (لیسانس کتابداری)	شرکت پارس معیار سنجش ایساتیس
قنبریان، علی (لیسانس مهندسی صنایع)	شرکت بازرسی، نمونه‌برداری کیفیت‌آوران باستان یزد
ماندگاری، مریم (فوق لیسانس مدیریت سیستم و بهره‌وری)	رئیس اداره فناوری اطلاعات اداره کل استاندارد یزد
موسوی، سیدمحمودرضا (لیسانس مهندسی صنایع)	شرکت رهپویان کیفیت

فهرست مندرجات

عنوان		صفحه
آشنایی با سازمان ملی استاندارد ایران		ب
کمیسیون فنی تدوین استاندارد		ج
پیش گفتار		ه
۱	هدف و دامنه کاربرد	۱
۲	مراجع الزامی	۲
۳	اصطلاحات و تعاریف	۳
۴	مشخصه‌های کلی و سطوح الزامات	۹
۵	مشخصه‌های کلی	۱۳
۶	ملاحظات رسانه ذخیره‌سازی	۲۳
۷	سامانه‌های استفاده‌کننده از رسانه قابل حمل	۲۴
۸	سامانه‌های استفاده‌کننده از رسانه با قابلیت یکبار نوشتن چند بار خواندن منطقی	۲۵
۹	سامانه‌های استفاده‌کننده از رسانه با قابلیت بازنویسی مجدد	۲۵
۱۰	ضبط بایگانی	۲۷
۱۱	عملیات بایگانی	۳۹
۱۲	ارزیابی سامانه اطلاعات	۴۱
۱۳	بایگانی شخص ثالث معتمد	۴۳
۱۴	ارائه‌دهندگان خدمت	۴۷
پیوست الف (اطلاعاتی) خط مشی بایگانی		۴۸
پیوست ب (اطلاعاتی) اعلانیه بایگانی		۵۰
پیوست پ (اطلاعاتی) شرایط کلی خدمت		۵۱

پیش‌گفتار

استاندارد « بایگانی الکترونیکی- قسمت ۱: مشخصات مرتبط با طراحی و عملیات یک سامانه اطلاعاتی برای نگهداری اطلاعات الکترونیکی» که پیش‌نویس آن در کمیسیون‌های مربوط توسط سازمان ملی استاندارد ایران تهیه و تدوین شده و در یکصد و شصت و یکمین اجلاس کمیتهٔ ملی اسناد و تجهیزات اداری و آموزشی مورخ ۱۳۹۴/۰۱/۲۹ مورد تصویب قرارگرفته است، اینک به استناد بندیک مادهٔ ۳ قانون اصلاح قوانین و مقررات مؤسسهٔ استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه۱۳۷۱، به عنوان استاندارد ملی ایران منتشر می‌شود.

برای حفظ همگامی و هماهنگی با تحولات و پیشرفت‌های ملی و جهانی در زمینهٔ صنایع، علوم و خدمات، استانداردهای ملی ایران در مواقع لزوم تجدیدنظرخواهد شد و هرپیشنهادی که برای اصلاح وتکمیل این استانداردها ارائه شود، هنگام تجدیدنظردرکمیسیون فنی مربوط مورد توجه قرارخواهدگرفت.بنابراین، باید همواره از آخرین تجدیدنظر استانداردهای ملی استفاده کرد.

منبع و مأخذی که برای تهیهٔ این استاندارد مورد استفاده قرارگرفته به شرح زیراست:

1- ISO 14641-1:2012, Electronic archiving- Part1: Specification concering the desighn and the operation of an information system for electronic information preservation

بایگانی الکترونیکی- قسمت ۱: مشخصات مرتبط با طراحی و عملیات یک سامانه اطلاعاتی برای نگهداری اطلاعات الکترونیکی

۱ هدف و دامنه کاربرد

هدف از تدوین این استاندارد، فراهم کردن مجموعه‌ای از مشخصات فنی و خط مشی‌های سازمانی است که برای ضبط[1]، ذخیره‌سازی و دسترسی به اسناد الکترونیکی باید اجرا شود. این استاندارد درخصوص خوانایی، تمامیت و قابلیت ردیابی اسناد در دوره نگهداری آن‌ها اطمینان ایجاد می‌کند.

این استاندارد برای اسناد الکترونیکی به دست آمده از موارد زیر کاربرد دارد:

- روبش‌کردن[2] اسناد کاغذی یا اسناد ریزفرم (مانند میکروفیلم و میکروفیش)؛
- تبدیل محتوای تصویر یا صوت غیر رقمی (آنالوگ) (مانند تبدیل انواع نوار و ریل)؛
- ایجاد " نسخه اصیل[3]" توسط یک برنامه کاربردی سامانه اطلاعاتی، یا
- سایر منابعی که محتوای رقمی (دیجیتالی) مانند نقشه‌های دو یا سه بعدی، ترسیمات یا طراحی‌ها، صدا یا تصویر رقمی و تصویرهای رقمی پزشکی ایجاد می‌کنند.

این استاندارد برای سامانه‌های اطلاعاتی که کاربران آن می‌توانند اسناد را جایگزین کنند یا آنها را بعد از ضبط تغییر دهند، کاربرد ندارد.

این استاندارد برای کاربران زیر در نظر گرفته شده است:

الف- سازمان‌های اجرا کننده سامانه‌های اطلاعات در مواردی که:

الف-۱ اسناد الکترونیکی ایجاد شده از ضبط‌های روبش در محیطی نگهداری می‌شوند که از ثبات آنها با توجه به نسخه اصلی و نگهداری طولانی مدت، اطمینان حاصل می‌شود.

الف-۲ اسنادی که از ابتدا به طور رقمی ایجاد شده، در محیطی نگهداری می‌شوند که از تمامیت محتوای اطلاعات و خوانایی اسناد، اطمینان حاصل می‌شود.

الف-۳ از قابلیت ردیابی برای همه کابردهای مربوط به اسناد الکترونیکی، اطمینان حاصل می‌شود.

ب- سازمان‌های ارائه دهنده خدمات فناوری اطلاعات و ناشران نرم‌افزار، به دنبال توسعه سامانه‌های اطلاعاتی هستند که در خصوص ثبات و درستی اسناد الکترونیکی اطمینان ایجاد می‌کند.

---

1 - Capture
2- Scanning
3 - Native

پ- سازمان‌های ارائه دهنده خدمات بایگانی اسناد شخص ثالث.

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 وتجدیدنظرهای بعدی آن مورد نظر این استاندارد ملی ایران نیست. در مورد مدارکی که بدون تاریخ انتشار به آن‌ها ارجاع داده شده است، همواره آخرین تجدید نظر و اصلاحیه های بعدی آن‌ها مورد نظر است.

استفاده از مراجع زیر برای این استاندارد الزامی است:

۲-۱ استاندارد ملی ایران ایزو به شماره ۲-۱۲۶۵۳، سال ۱۳۹۳، تصویربرداری الکترونیکی- هدف آزمون برای روبش سیاه و سفید اسناد اداری، قسمت ۲: روش استفاده

2-2 ISO 2859, Sampling procedures for inspection by attributes[1]

2-3 ISO8601, Data elements and interchange formats- Information interchange- Representation of dates and times

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

2-5 ISO12653-1, Electronic imaging- Test target for the black and white scanning of office documents- part 1: Characteristics.

۱- مجموعه استاندارد ملی ایران به شماره ۶۶۶۵ متناظر با مجموعه استاندارد بین‌المللی ISO 2859 است و در حال حاضر قسمت‌های ۳، ۴، ۵ و ۱۰ تدوین شده و در خصوص سایر قسمت‌ها به استاندارد بین المللی ISO 2859 مراجعه شود.

۳ اصطلاحات و تعاریف

در این استاندارد، علاوه بر اصطلاحات و تعاریف تعیین شده در استاندارد ISO 12653-1 و استاندارد ملی ایران به شماره ۲-۱۲۶۵۳ و اصطلاحات و تعاریف زیر نیز به کار می‌رود.

۱-۳

دسترسی[1]

فرایندهای بازیابی و نمایش اسناد الکترونیکی که با اهداف کاربرد[2] ، استناد[3] یا سابقه سند[4] انجام می‌شود.

۲-۳

بایگانی(ها)

مجموعه‌ای از اسناد که توسط هر فرد، سازمان، خدمت عمومی یا خصوصی، در دوره فعالیت‌شان، بدون درنظرگرفتن تاریخ، قالب یا رسانه ذخیره‌سازی، ایجاد یا دریافت می‌شوند.

۳-۳

خط مشی بایگانی[5]

الزامات قانونی، کارکردی، کاربردی، فنی و امنیتی یک سامانه اطلاعاتی بیرونی یا درونی است.

یادآوری- اصول یک خط مشی و یک اعلانیه بایگانی از شیوه‌های بایگانی در پیوست های الف و ب آمده است.

۴-۳

گزارش چرخه حیات بایگانی[6]

گزارشی که با ثبت داده‌های خط سیر[7] ممیزی مرتبط با چرخه حیات بایگانی ایجاد می‌شود.

یادآوری- چرخه حیات یک پروژه (مثلاً یک بایگانی) عبارتست از دوره ایجاد وتکمیل آن پروژه(بایگانی).

۵-۳

بازگردانی بایگانی[8]

بازگرداندن و انتقال اسناد بایگانی به موسس[9] آن، یا به شخص یا سازمان مسئول.

---

1 - Access
2 - Operational
3- Evidential
4- Historical
5- Archival policy
6- Archive lifecycle log
7 - Audit trail
8- Archive restitution
9 -Originator

۶-۳

نمایه سامانه بایگانی[1]

مجموعه‌ای از خصوصیات که برای آن دسته از بایگانی‌هایی به کار می‌رود که در مشخصه‌های مرتبط با درجه محرمانگی[2]، برنامه زمانی فعالیت‌های نگهداری[3] و وارهایی[4]، و حقوق دسترسی (به طور مثال ایجاد، خواندن، خواندن، اصلاح، حذف) مشترک هستند.

۷-۳

واحد تأیید انطباق

ACU[5]

افزاره‌های سخت‌افزاری و/یا نرم‌افزاری برای تأیید انطباق‌های الکترونیکی.

یادآوری- تأیید انطباق‌ها ، شامل شناسه‌دستگاه[6] و یک شناسه‌خدمت[7] مرتبط با بایگانی است.

۸-۳

فن صوتی تصویری[8]

فنون ترکیب کردن صدا و تصویر در ارتباطات است.

۹-۳

خط سیر ممیزی

مجموعه‌ای از اطلاعات ضروری برای تهیه تاریخچه همه رویدادها[9]ی مهم مرتبط با سامانه اطلاعات و اطلاعات ذخیره شده است.

۱۰-۳

داده

شکل رقمی از اطلاعات که می‌تواند دستیابی، خوانده و/یا پردازش شود.

۱۱-۳

مهر زمان و تاریخ

توالی از نویسه‌هایی که نشانگر تاریخ و یا زمان وقوع یک رویداد خاص هستند.

---

1 -Archival system profile
2 - Confidentiality
3- Retention
4- Disposal
5- Attestation Creation Unit
6 - Unit identifier
8- Service identifier
8-Audiovisual
9 -Events

۱۲-۳

اسناد هم نمایه[1]

مجموعه‌ای از اسناد که در نمایه سامانه بایگانی یکسان، مشترک هستند.

۱۳-۳

بایگانی رقمی

مجموعه‌ای از اقدامات که با هدف شناسایی، ضبط، طبقه‌بندی، نگهداری، بازیابی، نمایش و فراهم‌کردن دسترسی به اسناد برای اهداف اطلاعاتی یا تاریخی، یا برای دوره‌ی مورد نیاز برای برآورده کردن تعهدات[2] قانونی، انجام می شود.

۱۴-۳

سند رقمی

نماینده رقمی از محتویاتی که به صورت الکترونیکی ذخیره و مدیریت می شود.

یادآوری- مجموعه‌ای از محتوا، ساختار منطقی و صفات نمایشی، که توسط افزاره‌ای که توانایی تبدیل و تحول[3]شیء[4] قابل خواندن توسط انسان (یا قابل‌خواندن توسط ماشین) را دارد، قابل بازیابی است. یک سند می‌تواند به صورت رقمی بوجود آید یا از تبدیل یک سند غیر رقمی(آنالوگ) ایجاد شود.

۱۵-۳

اثرانگشت رقمی

توالی بیتی ایجاد شده از یک سند رقمی با استفاده از روش محاسباتی ویژه که منحصراً سند اصلی را تعیین هویت می‌کند.

یادآوری- هرگونه اصلاح سند رقمی، اثرانگشت متفاوتی ایجاد خواهد کرد.

۱۶-۳

مهر و موم رقمی[5]

روشی برای اطمینان از تمامیت سند شامل توابع هش (درهم‌ساز)[6]، امضاهای رقمی و، به طورانتخابی، یک مهر تاریخ و زمان است.

1-Deposit
2 -Obligation
3- Rendering
4- Object
5- Digital seal
6 - Hash

۱۷-۳

امضای رقمی

داده‌هایی که، هرگاه به یک سند رقمی الحاق شوند، کاربر سند را قادر می‌سازد تا اصل بودن و تمامیت سند، را رسمیت بخشد.

۱۸-۳

رقمی‌سازی [1]

تبدیل یک سند غیر رقمی (کاغذ، ریزفرم، فیلم، نوارهای صوتی تصویری[2] یا صوتی غیررقمی) به شکل رقمی با هدف نگهداری یا پردازش است.

۱۹-۳

سند رقمی شده

نتیجه رقمی‌کردن اطلاعات که در ابتدا بر روی رسانه فیزیکی (کاغذ، ریزفرم و فیلم، نوارهای صوتی تصویری یا صوتی غیررقمی) ذخیره شده است.

۲۰-۳

ثبات سند [3]

خصوصیتی از یک سند بایگانی شده که همه اطلاعات دربرگرفته شده در سند منبع اصلی را منتقل می‌کند.

یادآوری- این مفهوم برای هرنوع تغییر شکل، شامل رقمی‌سازی یا تبدیل قالب، کاربرد دارد.

۲۱-۳

دوام [4]

صفتی از یک سند که قابلیت خواندن آن در کل چرخه استفاده از سند را حفظ می‌کند.

۲۲-۳

سامانه اطلاعات الکترونیکی

سامانه‌ای که برای دریافت، نگهداری، دسترسی و انتقال بایگانی‌ها در یک شکل الکترونیکی، طراحی می‌شود.

1- Digitization
3 - Audiovisual
3 - Fidelity
4- Durability

۲۳-۳

تأیید انطباق الکترونیکی[1]

اطلاعات تولید شده برای تهیه شواهد انجام یک عمل یا یک تراکنش الکترونیکی است.

۲۴-۳

گزارش رویدادها[2]

ثبت گزارش داده‌های خط سیر ممیزی مربوط به کلیه فعالیت‌های سامانه است.

۲۵-۳

تبدیل قالب

عملیات تبدیل یک سند رقمی از یک قالب به قالب الکترونیکی دیگر است.

یادآوری- این عمل، ثبات سند را حفظ می کند.

۲۶-۳

تابع درهم‌ساز

راه و روش ریاضی مورد استفاده برای تبدیل برخی انواع داده به اجزاء نسبتاً کوچک است.

۲۷-۳

تمامیت[3]

صفتی از یک سند که دلالت بر محتویات کامل و بدون تغییر دارد.

۲۸-۳

خوانایی[4]

صفتی از یک سند بایگانی شده که دسترسی به همه اطلاعات دربرگرفته شده آن را امکان‌پذیر می‌سازد.

یادآوری- این صفت می‌تواند از طریق برخی فراداده‌های همراه شده با سند تسهیل شود.

۲۹-۳

فشرده کردن با اتلاف[5]

1- Electronic Attestation
2 -Events log
3- Integrity
4-Legibility
5-Lossy compression

روش فشرده‌کردن که برخی اطلاعات فایل اصلی در طی فشرده‌کردن را از دست می‌دهد.

یادآوری- نتیجه نا فشرده‌کردن، فقط تقریبی از شیء اصلی است.

۳-۳۰

جابجایی رسانه‌ها[1]

فعالیت انتقال سند از یک رسانه به رسانه دیگر، به ویژه با رعایت مدیریت رسانه از رده خارج است.

۳-۳۱

فراداده

داده‌های توصیف کننده مفهوم، محتوا و ساختار یک سند و مدیریت آن‌ها در طول زمان است.

۳-۳۲

تکرار[2]

فرایندی که شامل کپی کردن اطلاعات در منابع اضافی، عمدتاً بوسیله نرم‌افزار یا سخت‌افزار است، تا قابلیت اعتماد، رواداری خطا یا قابلیت دسترسی، را بهبود دهد.

۳-۳۳

منبع زمان

اجزای داخلی یا خارجی یک سامانه اطلاعاتی که فراهم کننده یک مرجع زمانی قابل‌اعتماد و عینی، مناسب با الزامات است.

۳-۳۴

نشان مهر- زمان[3]

شئ داده‌ای که نمایش داده را با زمان دقیق (زمان برمبنای مختصات جهانی[4]) مقید می‌کند[5]، که در نتیجه ارائه دهنده شواهدی است دال بر این که داده در آن زمان وجود داشته است.

۳-۳۵

انتقال پذیری[6]

توانایی دوباره‌به‌دست‌آوردن یک بایگانی رقمی معتبر (اطلاعات، داده، اشیاء و همه فراداده‌های مرتبط از یک سامانه اطلاعاتی) به منظور انتقال آن به سامانه اطلاعاتی دیگر، بوسیله یک رویه از پیش‌تعیین شده است.

1- Media migration
2- Replication
3-Time- stamp token
4 - Coordinated Universal Time
5 - Binds
6-Transferability

یادآوری- این موضوع، هنگامی که اطلاعات توسط ارائه دهنده خدمت بایگانی شخص ثالث انجام شود، از اهمیت ویژه‌ای برخوردار است.

۳۶-۳

ارائه دهنده خدمات بایگانی شخص ثالث معتمد[1]

فرد یا سازمان شخص ثالث که متصدی نگهداری بایگانی‌هاست.

۴ مشخصه‌های کلی و سطوح الزامات

۴-۱ مشخصه‌ها

از آنجایی‌که یک سازمان ممکن است چارچوب مشخصات معلومی را برای ذخیره‌سازی، استفاده، بایگانی-کردن، بازیابی و نمایش اسناد الکترونیکی به کار گیرد، نیاز است هردو معیار سازمانی و فنی برای اطمینان از تمامیت و نگهداری طولانی مدت سند، مد نظر قرار گیرد. در این زمینه، یک سامانه اطلاعاتی الکترونیک، باید یک خط مشی بایگانی از پیش تعیین شده‌ای را به کار گیرد. یک توصیف از اصول عمومی، نظیر خط مشی، در پیوست الف بیان شده است.

تشخیص این‌که سامانه‌های اطلاعاتی، اسناد الکترونیکی را ضبط می‌کنند که برای ذخیره‌سازی و استفاده بلندمدت تأیید می‌شود، اهمیت دارد. اصطلاح "ضبط" در این مفهوم، دریافت و پردازش اطلاعاتی که توسط سامانه اطلاعاتی مدیریت می شود را منعکس می‌کند. از آن‌جایی‌که نیاز است نسخه چاپی اسناد در شکل الکترونیکی ذخیره و مدیریت شوند، این اسناد باید قبل از ضبط در سامانه اطلاعاتی، روبش و فهرست‌گذاری شوند.

این استاندارد فقط برای اسناد ضبط‌شده غیر قابل تغییر کاربرد دارد. داده‌های مرجع سند مربوطه در سامانه پرونده یا پایگاه داده نباید قابل پاک‌کردن یا قابل تغییر باشد یا بتواند توسط داده‌های جدید جایگزین شود.

رویه‌ها و الزامات امنیتی باید به منظورهای زیر اجرا شود:

الف- کنترل فرایند بایگانی کردن؛

ب- پیشگیری و یا آشکارکردن اصلاحاتی که در اسناد و یا داده‌های ضروری برای بازیابی و نمایش آن‌ها ایجاد شده است؛

پ- اطمینان از تمامیت داده‌های خط سیر ممیزی (شامل گزارش رویدادهای سامانه)

یک سامانه اطلاعاتی الکترونیک باید مشخصه‌های زیر را داشته باشد:

۱- مناسب بودن برای نگهداری طولانی مدت؛

۲- تمامیت؛

1-Trusted

۳- امنیت؛

۴- قابلیت ردیابی.

این استاندارد، موارد زیر را طرح می‌کند:

- مشخصات برای رویه‌های مرتبط با پردازش، نگهداری، دسترسی و بازگردانی اطلاعات روبش‌شده یا اطلاعاتی که به طور رقمی ایجاد شده، و الزامات برای ایمنی سامانه اطلاعاتی؛
- رویه‌های مرتبط با رقمی‌سازی اسناد غیررقمی؛
- رویه‌های مرتبط با ضبط اسناد، نگهداری، دسترسی و بازگردانی آن‌ها؛
- رویه‌های مرتبط با تعیین تکلیف بالقوه اسناد؛
- قواعد مرتبط با رویه‌های کاربردی مربوط به کاربر؛
- توصیف نتایج تأیید انطباق‌های این عملیات؛
- مشخصات مرتبط با موضوعات، تجهیزات و به کارگیری نرم‌افزارها؛
- شرایط ممیزی‌های سامانه و روش های اجرایی مربوطه؛
- مشخصه‌های کاربردی برای استفاده از اشخاص ثالث معتمد؛
- مشخصه های کاربردی برای استفاده از پیمانکاران فرعی.

دستورالعمل توصیف فنی، تأیید انطباق‌های انجام شده و گزارش جزئیات چرخه عمر بایگانی‌ها یا رویدادهای سامانه باید در شرایط یکسان با خود بایگانی‌ها نگهداری شود.

۲-۴ سطوح الزامات

سازمان‌های متفاوت ممکن است رویکردهای متمایز و منحصربفردی به خطرات و الزامات برای سامانه‌های اطلاعاتی مورد استفاده برای نگهداری اسناد الکترونیکی داشته باشند. جدول ۱ درجه سطوح این الزامات را طرح می کند. این جدول، مشخصه‌های عمومی و روش‌های عملی برای اجرا در سطح الزامات ترجیحی توسط سازمان، درخصوص ماهیت اسنادی که نگهداری می‌شوند و خطرات بالقوه‌ای که روی می‌دهند را به طور مختصر بیان می‌کند.

الزامات اضافه‌تر ممکن است برمبنای نیازهای مشخص و سطوح قابل پذیرش ریسک انتخاب شوند. انطباق یک سامانه اطلاعات با این استاندارد، باید در ارتباط با سطح الزامات انتخاب شده توسط سازمان، ارزیابی شود.

جدول ۱- الزامات سامانه های اطلاعاتی

مشخصه	حداقل الزامات	الزامات اضافه تر
مناسب بودن برای نگهداری طولانی مدت	استفاده از قالب‌های پرونده استاندارد شده یا دارای استاندارد صنعتی و عموماً دردسترس	تبدیل قالب روبش سند
	توصیف فراداده سند	قالب فراداده استاندارد
	انتقال رسانه	
	تبدیل قالب	کنترل و تبدیل قالب‌ها در زمان ضبط اعلام از رده خارج شدگی قالب تبدیل قالب با قابلیت ردیابی و طرح‌ریزی شده
	مدیریت تغییر سامانه	
تمامیت	ضمانت‌شده توسط ذخیره‌سازی بر روی رسانه: – WORM[1] فیزیکی – WORM منطقی بر روی رسانه ثابت به همراه: – گزارشات – فنون و رویه‌های برای تشخیص و پیشگیری از جایگزین‌های ورودی – WORM منطقی برای رسانه قابل حذف (رسانه قابل پاک کردن/ قابل بازنویسی را ببینید) – رسانه قابل پاک‌کردن/ قابل بازنویسی (سطح امنیت معمولی)	سطح امنیت قوی سطح امنیت پیشرفته سطح امنیت قوی سطح امنیت پیشرفته
	فرایند ضبط بایگانی‌ها	
	اعلام آمادگی قبل از انهدام بایگانی‌ها	
	توصیف فرایند انهدام بایگانی‌ها	تعریف تغییر رویه‌ها برای دوره‌های نگهداری نگهداری پس از انهدام از فراداده و خط‌سیر ممیزی
امنیت	شناسایی اشخاص و فرایندهای دسترسی به بایگانی‌ها	سندیت محکم
	نسخه‌های پشتیبان از بایگانی‌ها	استفاده از انواع و شکل‌های متفاوت رسانه محافظت در برابرخطرات سیل، آتش‌سوزی و ...
	عملیات بایگانی کنترل شده (شناسایی و قابلیت ردیابی)	تصدیق سخت بازیابی در قالب‌هایی غیر از قالب‌های ورودی
	تداوم دسترسی به بایگانی‌ها	
قابلیت ردیابی	مهرتاریخ و زمان	مهر تاریخ و زمان از شخص ثالث معتمد
	نگهداری یک پرونده فنی (خط مشی بایگانی، شرایط عمومی خدمات، رویه‌های عملیات، چرخه عمر سند)	تطبیق با فرایندهای سازمانی مشتری و تأیید انطباق‌های مربوطه
	نگهداری از خط سیر ممیزی چرخه عمر بایگانی‌ها و گزارش رویدادها	امضای رقمی و مهر تاریخ و زمان تأیید انطباق‌های‌عملیات و رویدادها، در واحدها یا دسته‌ها تعریف جزئیات برای دسته‌های رویدادها در مواردی که امضای رقمی به کار می‌رود تکرار بایگانی گزارشات و خط‌سیرهای ممیزی

1- Write- Once-Read-Many optical disks

۵ مشخصات کلی

۵-۱ کلیات

طراحی و عملیات سامانه اطلاعات باید به گونه‌ای باشد که اجرای رویه‌های تضمین‌کننده الزامات منتخب از بند ۴-۲ را مجاز کند.

۵-۲ دستورالعمل توصیف فنی

یک دستورالعمل توصیف فنی سامانه اطلاعات، باید ایجاد و نگهداری شود. این دستورالعمل باید حداقل شامل موارد زیر باشد

الف) فهرستی از اجزای سخت‌افزاری سامانه اطلاعات همراه با همه شماره سریال‌های پیوست شده توسط سازندگان، ویژگی‌های کلیدی این اجزا، تاریخ تولید، انطباق با استانداردهای ایمنی مربوطه؛

ب) برای یک سامانه شبکه، نوع[1] شبکه و نقشه[2] آن، همچنین توصیفی از اتصالات و تجهیزات امنیتی؛

پ) یک مدل معماری داده از اشیاء اطلاعاتی و ارتباطات آن‌ها، در خصوص استفاده آن‌ها در پشتیبانی از اهداف عمومی سامانه اطلاعات؛

ت)فهرستی از محصولات نرم‌افزاری و مستندات مربوطه، شناسایی نسخه‌های نصب شده و تاریخ نصب این نسخه‌ها؛

ث)فهرستی از نرم افزارهای کاربردی سفارشی[3] همراه با پرونده معماری/ طراحی، کد اصلی نرم‌افزارها یا با اثبات ذخیره سازی آن‌ها در محل محافظت شده؛

ج) توصیفی از تعاملات بین اجزای گوناگون سامانه اطلاعاتی؛

چ) توصیفی از محیط فیزیکی (دما، حداقل و حداکثر رطوبت و ...) در رابطه با مشخصات ارائه شده توسط سازندگان تجهیزات برای کارکرد مناسب و نگهداری از رسانه اطلاعاتی؛

ح) توصیفی از محیط فیزیکی و فنی برای عملکرد رضایت‌بخش سامانه‌های اطلاعاتی (به طور مثال نوع منبع تغذیه، مولدبرق ، سامانه آشکارساز آتش، ایجاد نسخه‌های احتیاطی[4])؛

خ) توصیفی از اقدامات حفاظت فیزیکی برای ایمنی و امنیت (محافظت، آشکارسازی از راه دور، محفظه‌ها، قفل‌ها، حفاظت الکترومغناطیسی و ...)؛

د) توصیفی از الزامات عملیات نگهداری برای سامانه اطلاعاتی.

---

1 - Typology
2 - Topography
3 - Customized
4 - redundancy implementation

۵-۳ نمایه‌های سامانه بایگانی

یک نمایه سامانه بایگانی، مجموعه قواعد قابل کاربرد برای اسنادی است که در اقدامات محرمانگی، مدت نگهداری، انهدام و حقوق دسترسی برای ضبط، بازیابی یا وارهایی ، مشترک هستند. این قواعد همچنین فراداده‌ای را تعیین می‌کند که نیاز است با اسناد مدیریت شده در نمایه همراه باشد. هرگونه ایجاد، اصلاح یا حذف یک نمایه سامانه بایگانی که در بایگانی گزارش چرخه عمر بایگانی، که تحت مسئولیت خدمات بایگانی سازمان یا توسط شخص ثالث معتمد نگه داشته شده، باید بایگانی شود. یک نمایه سامانه بایگانی می‌تواند برای اسناد الکترونیکی منفرد تعریف شود. با این‌حال برای بایگانی انبوه، می‌تواند خیلی زمانبر باشد . متعاقباً در این مورد ترجیح دارد از مجموعه قواعد از پیش تعیین شده‌ای که با همدیگر در یک نمایه سامانه بایگانی عمومی‌تر، گروه‌بندی شده‌اند، استفاده کنیم. یک نمایه سامانه بایگانی باید به ویژه حقوق اشخاص و/یا برنامه-های کاربردی مجاز در زمینه‌های زیر را تعیین کند:

الف) اصلاح یک نمایه سامانه بایگانی؛

ب) ایجاد اسناد هم نمایه؛

پ) دسترسی (دیدن یا نمایش) به اسناد هم نمایه؛

ت) طولانی‌کردن یا کاهش مدت اسناد هم نمایه؛

ث) حذف یا از بین بردن اسناد هم نمایه به صورت پیش از موقع یا برنامه‌ریزی شده.

۵-۴ رویه‌های عملیاتی

۵-۴-۱ کلیات

سازمان باید رویه‌هایی را برای ضبط، ذخیره سازی، دسترسی و بازیابی[1] اسناد برقرارکند. این رویه‌ها باید در دستورالعمل توصیف فنی، به‌تفصیل بیان شود و باید شامل حداقل اطلاعات زیر باشد:

- فنون و رویه مورد استفاده برای تحقیق و چاپ؛
- فنون و رویه‌ها برای ایجاد تمام انواع تأیید انطباق؛
- فنون و رویه‌ها برای ذخیره سازی و نگهداری از رسانه و ساختارهای ذخیره‌سازی؛
- قالب‌های پرونده استفاده شده؛
- فنون و رویه‌های برای نسخه‌برداری و تکرار اسناد و پشتیبان‌ها؛
- فنون و رویه‌های مورد استفاده برای رمزدارکردن رقمی و تمامیت داده‌ها.

1 - Restitution

۵-۴-۲ اسناد روبش شده

جایی‌که روبش‌کردن اسناد انجام شود، دستورالعمل توصیف فنی باید علاوه بر رویه‌های تعیین‌شده در بند ۵-۴-۱، شامل رویه‌های زیر نیز باشد.

- فنون و رویه‌های مورد استفاده برای رقمی‌سازی (توصیف سندی که روبش می‌شود و هرگونه ویژگی متمایز ویژه، عملیات مقدماتی مورد نیاز، از قبیل انتخاب قالب‌های خروجی، تفکیک‌پذیری تصویرسازی ، فن فشرده‌کردن در صورت استفاده، تجدید آمادگی سند بعد از رقمی‌سازی اگر قابل کاربرد باشد و ...)؛
- فنون و رویه‌های مورد استفاده برای شاخص‌گذاری (موقعیت سند، شناسایی مراجع سند بر روی تجهیزات یا بر روی اسناد ضمیمه، شناسایی مراجع پیام‌های الکترونیکی)؛
- فنون و رویه‌های مورد استفاده برای فراداده‌های مرتبط و هرگونه غنی‌سازی مرتبط با آن فراداده ها؛
- فنون و رویه‌های مورد استفاده برای کنترل کیفیت (استفاده از صفحه مرجع آزمون برای رقمی‌سازی، شمارش صفحه بسته[1]های روبش شده، کنترل صافی پیام‌های الکترونیکی، کنترل‌های کد با توجه به جداول مرجع اگر دارای کد باشد و ...) ؛
- فنون و رویه‌های مورد استفاده برای انهدام سند اصلی اگر کاربرد داشته باشد.

۵-۴-۳ اسناد ایجاد شده به صورت رقمی

علاوه بر رویه‌های تعیین شده در بند ۵-۴-۱، جایی که اسناد ایجاد شده به صورت رقمی مورد بحث باشند، دستورالعمل توصیف فنی باید رویه‌های زیر را نیز در برگیرد:

- فنون و رویه‌های مورد استفاده برای انتقال، دریافت و کنترل اسنادی که بایگانی می‌شود؛
- فنون و رویه‌هایی برای فراداده‌های مرتبط و هرگونه بهبود ممکن فراداده‌های مرتبط؛
- فنون و رویه‌هایی در ارتباط با تبدیل قالب‌های سند رقمی در طی مدت ضبط سامانه اطلاعاتی، یا بعد از آن، اگر قالب‌ها از رده خارج شوند.

۵-۵ امنیت

۵-۵-۱ مدیریت و سازماندهی امنیت

همه سازمان‌ها باید، یک رویه مدیریتی جاری داشته باشند تا از امنیت سامانه اطلاعاتی خود اطمینان حاصل کنند. سامانه مدیریت برای امنیت باید مجزا و متمایز از اداره عملیات سامانه اطلاعاتی یا سامانه‌های مخابراتی باشد. ساختار و اداره آن باید به طور شفاف تعریف شده و با همه کارکنان سازمان مرتبط شود. اداره و سازماندهی امنیت سامانه اطلاعاتی، باید اصول برگرفته از راهبرد کلی یا خط مشی سازمان و قواعد جاری را اعمال و به طور اخص موارد زیر را در برگیرد.

---

1 - Batch

- مدیریت کلیدی خصوصیات؛
- سامانه‌های امنیت برای کشف، نفوذ و اعلان خطر؛
- مطابقت سخت‌افزاری با مقررات مربوط به ایمنی انسان (به استاندارد ملی ایران به شماره ۴-۷۲۶۰ رجوع شود)؛
- عملکرد محصولات نرم‌افزاری، منابع شناخته شده و در دسترس؛
- توسعه نرم‌افزارهای سفارشی که به طور کافی مستند و آزمون شده‌اند؛
- مدیریت نمایه‌های دسترسی به سامانه اطلاعاتی (راهنما)؛
- استفاده از شبکه‌های انتقال با ویژگی‌هایی برای کاربران امنیتی، امنیت وکنترل تمامیت؛
- بکارگیری ارائه دهندگان شخص ثالث (امنیتی، حفاظتی، تمیزکاری، عملیات نگهداری).

یادآوری- برای الزامات امنیتی، باید به استاندارد ملی ایران به شماره ۲۷۰۰۱ و استانداردهای مربوطه رجوع شود.

۵-۵-۲ ارزیابی خطر

اقدامات امنیتی، اغلب در واکنش به رخدادهای امنیتی یا دردسترس بودن ابزارهای نرم‌افزاری رایانه‌ای با استفاده از یک نگرش یکسویه ایجاد می‌شود. چنین رویه‌هایی، به طور متناوب، شکاف‌هایی در امنیت به جا می گذارد که این شکاف‌ها در تاریخ‌های بعدی پر می‌شوند. یک رویکرد ساختار یافته‌تر اینست که داشته‌های اطلاعاتی سازمان را بازبینی کنیم و عوامل خطر را تعیین کنیم (بر مبنای ارزش داشته‌ها، آسیب‌پذیری و احتمال حمله). سپس یک خط‌مشی امنیت اطلاعات می‌تواند ایجاد و تصویب شود، به طوری‌که اقدامات امنیتی بتوانند با درنظرگرفتن آن ممیزی شوند. سازمان باید متعهد به تجزیه و تحلیل خطر امنیت اطلاعات شده و نتایج به دست آمده را مستند کند.

اقدامات امنیتی به کارگرفته شده برای کنترل رسانه ذخیره‌سازی اطلاعات، اعم از رسانه موجود و رسانه پشتیبان، از اهمیت ویژه‌ای برخوردارند. تجزیه و تحلیل خطر باید شامل آسیب‌پذیری عوامل خطر سازگار با نوع رسانه‌ای باشد که استفاده می‌شود (به طور مثال رسانه با قابلیت یکبار نوشتن چندبار خواندن و یا قابلیت بازنویسی). در جایی‌که انواع متفاوتی از رسانه ذخیره‌سازی استفاده می شود، تأثیر آن‌ها بر نتایج تجزیه و تحلیل خطر باید بازنگری شود. زمانی که تجزیه و تحلیل خطر کامل شود، باید به عنوان بخشی از بازنگری اقدامات امنیتی به کار گرفته شده، عمل شود.

عواملی نظیر تعادل بین هزینه‌های اجرا، امنیت به دست آمده و ارزیابی خطر باید در طی فرایند بازنگری مد نظر قرار گیرد. برمبنای نتایج تجزیه و تحلیل خطر، معیارهای امنیت موجود باید به منظور اثربخشی، بازنگری شوند. هرکجا بازنگری نشان دهد که اعمال تغییرات در رویه‌های امنیت مناسب است، تغییرات شناسایی شده باید اجرا شود.

۵-۵-۳ امنیت فیزیکی

معیارهایی باید برای امنیت فیزیکی، شامل پیشگیری از دسترسی غیرمجاز به سخت‌افزار، به سامانه‌های مخابراتی، به رسانه نگهدارنده اطلاعات و به اطلاعات اطمینان‌دهنده بازیابی و نمایش آن‌ها، خط‌سیرهای ممیزی، گزارشات و پشتیبان‌ها در نظر گرفته شود. اگر نیاز به مداومت در دسترسی باشد، توصیه می‌شود برای کسب کمترین احتمال خطر از خصوصیات امنیتی متفاوت استفاده شود و نیز از رسانه‌های متفاوت و/یا سامانه‌هایی که شامل پشتیبان (کپی) از اطلاعات و فنون عملیاتی نمودن آن‌هاست، استفاده کنیم .

رسانه قابل حمل باید به طور پیوسته، در طی مدت جابجایی یا انتقال از یک موقعیت حفاظت شده به موقعیت دیگر، پایش شود. باید امکان شناسایی همه نگهدارنده‌های هر نوع رسانه‌ای در هر زمان وجود داشته باشد. هرگاه رسانه قابل حمل عملاً استفاده نشود، آن رسانه باید در موقعیت‌های حفاظت شده معینی ذخیره شود.

اگر با انهدام فیزیکی اسناد روبرو باشیم، روش‌های معینی باید برای امنیت این عملیات، هم برای اسناد غیررقمی بر مبنای کاغذ و هم برای اسنادی که به صورت رقمی ایجاد شده‌اند، اجرا شود. اگر رسانه شامل اسنادی دورانداختنی باشد، معیارهای مناسبی باید در نظرگرفته شود تا بازسازی مجدد اطلاعاتی که از ابتدا بر روی آن رسانه موجود بود را غیر ممکن سازد.

۵-۵-۴ امنیت سخت افزار

معیارهای امنیتی در برگیرنده سخت‌افزار و نرم‌افزار، به طور مجزا یا مرتبط، برای امنیت سامانه های اطلاعاتی از طریق مجاز نمودن موارد زیر، مشارکت دارند:

الف) شناسایی پیکربندی سخت‌افزار، شامل دستگاه‌های جانبی؛

ب) کنترل‌هایی که عدم وجود هرگونه اصلاحات در پیکربندی سخت‌افزار، اعم از تصادفی یا بدخواهانه را ضمانت کند؛

پ) کنترل‌هایی که فقط کاربران مجاز را قادر به دسترسی به سخت‌افزار می سازد، را ضمانت کند.

بنابراین، توصیه‌های امنیتی باید هنگام انتخاب تجهیزات و در طی نصب و به کارگیری آن‌ها در نظرگرفته شوند. برای محدود کردن خطرات برداشت[1] غیرمجاز اطلاعات توسط عامل خارجی به سبب انتقال تابش‌های الکترومغناطیسی غیرعمدی، توصیه می‌شود سخت‌افزار را درانطباق با استاندارد ملی ایران به شماره۴-۷۲۶۰، آزمون کنید.

۵-۵-۵ امنیت نرم افزار سفارشی و محصولات نرم افزاری

1- Interception

نرم افزارسفارشی و محصولات نرم‌افزاری، جزء جدایی‌ناپذیر از پیکربندی سامانه هستند، از اینرو، آن‌ها باید با همان شرایط ایمنی سخت‌افزار، موضوعیت یابند.

سامانه‌های عامل و محصولات نرم افزاری که انتخاب شده‌اند باید موارد زیر را فراهم کنند:

- ابزارهای کنترل دسترسی برای حفاظت پیشرفته؛
- حفاظت در مقابل نرم‌افزارنفوذی و بدافزار؛
- کنترل‌های اطمینان‌دهنده از عدم وجود تغییرات عمدی یا تصادفی علیه پیکربندی نرم‌افزار؛

از امنیت نرم افزار باید با استفاده از موارد زیر اطمینان حاصل شود:

- کنترل‌های دسترسی، ضمانت‌کننده این‌که فقط کاربران مجاز می‌توانند از نرم افزار و اطلاعاتی که برای دسترسی عنوان کرده‌اند، استفاده کنند.
- آشکارسازی و دیده‌بانی سامانه‌ها به‌طوری که هرگونه تلاش برای دسترسی غیرمجاز بتواند کشف و گزارش شود.

توصیه می شود از نرم افزاری استفاده کنید که در حیطه عمومی قرار دارد، یا تا جایی که ممکن است، کدهای اصلی برنامه را از تأمین‌کننده بگیرد. روش‌های سخت‌گیرانه‌ای باید برای توسعه نرم افزار به کار رود؛ انتخاب بهترین روش‌ها و بررسی‌ها باید مسئولیت متصدی برنامه کاربردی باشد.

نرم‌افزار و محصولات نرم‌افزاری قبل از در خدمت قرارگرفتن، باید به قدر کافی بر روی دستگاهی غیر از دستگاه اصلی، یا بر روی یک دستگاه اصلی در زمانی که درحال کار نیست و قبلاً از اطلاعات و نمایه‌های آن، نسخه پشتیبان تهیه شده و همه رسانه‌های سامانه اطلاعاتی قابل حمل، از آن دستگاه جدا شده‌اند، به طور کامل مورد آزمایش قرار گیرد.

امنیت دسترسی و اعطای حقوق دسترسی به سامانه اطلاعاتی باید به طور دقیق از زمان آغاز طراحی سامانه، مطالعه، طراحی و اجرا شود. نرم‌افزار و محصولات نرم‌افزاری باید به خصوص حفاظت شوند، و حقوق دسترسی توانایی تغییر یا اصلاح آن‌ها فقط باید به افراد مجاز، اعطا شود. در موارد بدکارکردن، فوراً باید به مقام مسئول امنیت گزارش داده شود و بخشی از سامانه اطلاعات که خوب کار نمی‌کند باید به سرعت ممکن، مجزا شود.

۵-۵-۶ عملیات نگهداری سامانه اطلاعاتی

اطلاعات توصیف کننده هرگونه فعالیت عملیات‌نگهداری، باید در اسناد فنی سامانه اطلاعات ثبت شود. این اطلاعات باید شامل شناسایی فعالیت عملیات‌نگهداری، اعم از پیشگیرانه یا اصلاحی شود، که سازمان یا تأمین‌کنندگان شخص ثالث خصوصی، عهده دار آن هستند.

رسانه قابل حمل شامل اسناد الکترونیکی و فراداده‌های مرتبط با آن، هرگز نباید در طی عملیات نگهداری، در رانه‌ها[1]، رها شوند. اگر رسانه، قابل حمل نباشد، یک نسخه پشتیبان معتبر باید قبل از هرگونه فعالیت عملیات‌نگهداری ایجاد شود (به بند۵-۵-۸ رجوع شود). همه آزمون‌ها باید با رسانه قابل حمل که به طور

1 - Drives

ویژه به این وظیفه تخصیص داده شده، انجام شوند. اگر رسانه، قابل حمل نباشد، امکان این که آزمون‌ها، اطلاعات ثبت شده را تغییر داده یا معدوم نمایند، نباید وجود داشته باشد.
عملیات‌نگهداری پیشگیرانه باید به منظور اطمینان از عملکرد مناسب سامانه اطلاعاتی، انجام شود. به ویژه، کنترل‌های منظم رانه‌های لوح فشرده قابل حمل یا رسانه ثابت باید انجام شود تا بررسی کنیم که آیا این‌ها دارای نظم کاری مناسب، براساس توصیه‌های سازنده هستند یا خیر.

۵-۵-۷ تغییر مدیریت سامانه و انتقال رسانه

عملیات ارتقای دوره‌ای و اصلاح یا جایگزینی سخت‌افزار یا نرم‌افزار باید قبل از اجرا، طرح‌ریزی شود. همه این عملیات باید به تفصیل در دستورالعمل توصیف فنی سامانه اطلاعات بیان شود و در گزارش، ثبت شود.

از نگهداری طولانی مدت و تمامیت اسناد و فراداده‌های مرتبط با آن، باید هنگام انجام عملیات ارتقای دوره-ای، اطمینان حاصل شود.

دو موقعیت زیر ممکن است کاربرد داشته باشد:

الف- رسانه ذخیره‌سازی جدید، قابلیت خوانده شدن توسط سامانه اطلاعات قبلی را داشته باشد؛ قبل از این‌که رسانه ذخیره‌سازی قبلی کنار گذاشته شود، همه رسانه‌ها باید از نظر امکان خواندن سخت‌افزاری رسانه ذخیره‌سازی جدید، کنترل شوند.

ب- رسانه ذخیره سازی جدید، نمی‌تواند رسانه‌ای که توسط سامانه اطلاعات قبلی استفاده شده را بخواند؛ همه اسناد موجود بر روی رسانه قبلی، باید در رسانه جدید برروی سامانه سخت‌افزاری که موقتاً از هر دو نوع رسانه ذخیره‌سازی استفاده می‌کند، کپی شود.

۵-۵-۸ پشتیبان‌های امنیتی

سامانه اطلاعات در عمل باید حداقل دو نسخه از اطلاعات مشابه که در دو موقعیت دور جغرافیایی، نگهداری می‌شود را در همه زمانها نگهداری کند. حداقل یکی از این نسخه‌ها باید در رسانه غیرقابل تغییر نوشته شود.

رسانه مورد استفاده برای پشتیبان‌های امنیتی ممکن است از نوع و جنس متفاوتی نسبت به رسانه اولیه باشد.

هنگامی که رسانه از نوع غیرقابل حمل است، دو سامانه اطلاعاتی در موقعیت‌های دور جغرافیایی باید تکمیل شود.

هنگامی که رسانه از نوع قابل حمل باشد، ثبت اسناد بر روی رسانه پشتیبان باید با فوریت ممکن انجام شود تا اجازه ذخیره سازی در موقعیتی مجزا از موقعیت اولیه را بدهد.

هرزمان که یک پشتیبان امنیتی ایجاد شود، جزئیات فرایند و نام و مشخصه‌های فایل‌های پشتیبان باید در گزارش رویدادها ذخیره شود.

۵-۵-۹ تداوم دسترسی به بایگانی‌ها

همراه با هر سامانه اطلاعاتی، یک رویه بازیابی فاجعه (همچنین با عنوان طرح تداوم کسب وکار نیز شناخته می‌شود) باید دردسترس بوده و مستند شود.

این رویه باید اجازه استقرارمجدد[1] سامانه بدون هیچگونه اتلاف داده، فراداده، گزارش یا هرمجموعه دیگری از داده‌ها (فهرست کاربران، نمایه‌های سامانه بایگانی و...) را بدهد.

نرم‌افزار و روش‌های استقرار مجدد داده‌های سامانه باید در دستورالعمل توصیف فنی، شرح داده شوند.

سامانه اطلاعات در عمل باید اطمینان ایجاد کند که آخرین سند معتبر نمی‌تواند در هرنقطه از زمان از دست برود.

سامانه اطلاعات باید به طور خودکار، یک سابقه از همه فرایندهای استقرار مجدد ایجاد کند.

۵-۶ مهرزدن تاریخ و زمان

در چارچوب این استاندارد بسته به شیوه تحویل، دو نوع ممکن (داخلی یا شخص ثالث معتمد)، از مهر تاریخ و زمان وجود دارد که باید شامل حداقل مشخصه‌های زیر باشد:

الف) ایجاد یک مهر زمان مطابق با استانداردهای قابل کاربرد؛

ب) نگهداری از نشان مهر تاریخ و زمان برای دوره‌های مورد نیاز؛

پ) منبع زمان مرجع؛

ت) خط مشی عملیات قابل تصدیق برای مهر تاریخ و زمان؛

برای عملیات مربوطه، شکل منتخب مهر تاریخ و زمان باید در دستورالعمل توصیف فنی، تشریح شود. قالب های تاریخ و زمان باید مطابق با استاندارد ایزو ۸۶۰۱ باشد. مهر تاریخ و زمان باید یک تاریخ کامل همراه با ساعت، دقیقه، ثانیه و کسر ثانیه ارائه دهد که بر اساس قالب زیر نشان داده می شود:

YYYY-MM-DDThh:mm:ss.sTZD

به طوری که:

YYYY سال را با استفاده از چهار کاراکتر نشان می‌دهد؛

MM ماه را با استفاده از دو کاراکتر نشان می دهد(به طور مثال ۰۱ یعنی فروردین)؛

DD روز را با استفاده از دو کاراکتر نشان می‌دهد (۰۱ تا ۳۱)؛

hh ساعت را با استفاده از دو کاراکتر نشان می‌دهد (۰۰ تا ۲۴)؛

mm دقیقه را با استفاده از دو کاراکتر نشان می دهد (۰۰ تا ۵۹)؛

---

[1] - Restoration

ss ثانیه را با استفاده از دو کاراکتر نشان می دهد (۰۰ تا ۵۹)؛

s یک یا چند کاراکتر که نشان دهنده کسر دهم ثانیه است؛

TZD قلمرو زمانی را نشان می‌دهد (Z برای UTC (زمان هماهنگ جهانی) یا hh:mm+ یا hh:mm–).

به طور مثال:۰۰:۰۲+ ۰۹:۳۶.۴۵ T ۲۹-۰۸-۱۳۹۳

مهم است که درجه دقت اندازه‌گیری زمان را انتخاب کنیم برای این که تعیین کنیم بالاترین نرخ وقوع رویدادها در سامانه اطلاعاتی کدام است و سپس واحد زمانی به اندازه کافی کوچک انتخاب کنیم تا مطمئن شویم که دو رویداد از این نوع در تاریخ و زمان یکسان اتفاق نخواهد افتاد. برای اطلاعات تاریخ‌دار، باید از زمان جهانی مختصاتی (UTC) استفاده شود. دستورالعمل توصیف فنی باید منابع زمانی و روش‌ها و کنترل های بروز کردن، همچنین فرایندهای همزمان‌سازی ساعت های گوناگون سامانه اطلاعات را تعیین کند. اگر نشانه مهر تاریخ و زمان برای یک سامانه اطلاعات لازم باشد، باید توسط یک واحد تأیید انطباق (ACU) یا توسط شخص ثالث معتمد مستقل بیرونی برای سامانه اطلاعات، فراهم شود.

۵-۷ خط‌سیر ممیزی

۵-۷-۱ کلیات

هر گونه رویداد همراه با سامانه اطلاعاتی یا همراه با چرخه عمر اسناد باید ثبت شود. گزارش رویداد به طور خودکار باید توسط سامانه اطلاعاتی با مهر زمان و تاریخ ایجاد شود (بند ۶-۵ را ببینید). توصیف کاملی از رویدادها باید به طور متوالی در گزارش مربوطه ذخیره شوند.

تمامی گزارشات همراه با همه اطلاعات مدیریتی مربوطه باید در دستورالعمل توصیف فنی تشریح شوند. گزارشات باید به آسانی دردسترس و خوانا باشند.

گزارشات باید بر یک مبنای منظم و براساس خط مشی بایگانی، همانند اسناد مربوطه، بر روی رسانه ذخیره سازی که فراهم کننده مشخصات یکسان از نگهداری و تمامیت است، بایگانی شوند.

گزارشات نباید برای کاربران و متصدیان معمولی در دسترس باشند. مدیریت گزارشات باید به کاربری که برای این وظیفه منتصب شده، محدود شود. ایجاد

گزارشات مستلزم ایجاد تصدیق الکترونیکی است. این تأیید انطباق‌ها باید همانند اسناد مربوطه در شرایط یکسان بایگانی شوند.

۵-۷-۲ نگهداری امن از خط‌سیر ممیزی

جدا از این که چه نوع رسانه‌ای برای نگهداری خط‌سیر ممیزی استفاده می‌شود، خط‌سیر ممیزی باید مدرکی دال بر تداوم ضبط رویدادهای سامانه اطلاعات را نشان دهد. گزارش رویدادها باید در شرایط امنیتی مشابه با اسناد، ذخیره و نگهداری شود.

۵-۷-۳ گزارشات چرخه عمر بایگانی

گزارشات چرخه عمر بایگانی‌ها می تواند کلی یا خاص هر موضوع باشد. این گزارشات باید شامل تأیید انطباق‌های الکترونیکی ، برای مثال، موارد زیر باشد:

۱- تأیید انطباق اسناد هم نمایه اولیه؛

۲- تأیید انطباق اصلاح دوره استمرار (برنامه زمانبندی نگهداری) اسناد هم نمایه، اگر وجود داشته باشد؛

۳- تأیید انطباق حذف، زود هنگام یا به‌موقع اسناد هم نمایه، اگر کاربرد داشته باشد؛

۴- تأیید انطباق بازگردانی اسناد هم نمایه، اگر کاربرد داشته باشد؛

۵- تأیید انطباق هرگونه ایجاد، اصلاح یا حذف یک نمایه سامانه بایگانی اگر کاربرد داشته باشد.

هنگام تشکیل گزارشات ایجاد، اصلاح یا حذف یک نمایه سامانه بایگانی، یا هنگامی که یک تأیید انطباق الکترونیکی جدید موضوعیت می‌یابد، گزارشات چرخه عمر بایگانی‌ها باید به موقع، بروز شود.

هر کاربر تأیید شده در نمایه سامانه بایگانی به عنوان یک کارور مجاز، باید قادر باشد، به بطور جزئی یا کلی، گزارشات چرخه عمر بایگانی‌ها را ببیند.

واحد بایگانی یک سازمان یا یک شخص ثالث، باید اعتباردهی کاربر را در یک نمایه سامانه بایگانی به عنوان یک کارور ارائه دهد که شامل همه وسایل ضروری برای کنترل تمامیت و اصل‌بودن همه یا بخشی از گزارشات است. بعد از هر بروز شدن، یا در هرزمانی، واحد بایگانی یک سازمان یا یک شخص ثالث، باید به اشخاص تأیید صلاحیت شده، اجازه کنترل تمامیت همه یا بخشی از گزارشات را بدهد.

۵-۷-۴ گزارش رویدادها

گزارش رویدادها باید منحصر به یک سامانه اطلاعات باشد و باید ثبت کند که چه کسی از آن استفاده کرده (کاربر انسانی یا کاربر سامانه‌ای خودکار)، چه زمانی از سامانه اطلاعات استفاده شده، چه‌کاری با سامانه اطلاعات و خروجی‌ها انجام شده است. گزارش رویدادها باید پیگیری کند که چه کسی به سامانه اطلاعات دسترسی داشته است، آیا کارکنان روش‌های اجرایی را رعایت کرده‌اند، یا آیا هر عمل انجام شده می‌تواند تصادفی، کلاهبرداری، بدخواهانه یا غیر مجاز باشد. گزارش رویدادها باید شامل سه بخش باشد:

الف- بخشی برای همه رویدادهای مربوط به کاربرد بایگانی؛

ب- بخشی برای همه رویدادهای مربوط به امنیت؛

پ- بخشی برای همه رویدادهای مربوط به سامانه اطلاعاتی.

عملکرد اصلی گزارش رویدادها برای تصدیق درونی است. این گزارشات باید اجازه بازنگری همه اطلاعات، پیام‌های خطا و سایر اخطارهای تولیدشده در طول عملیات سامانه اطلاعات، از قبیل عدم موفقیت در انجام وظیفه یا اجرا را بدهد. برای سامانه اطلاعاتی که از رسانه یکبار نوشتنی چند بار خواندنی استفاده می‌کند، گزارش رویدادها باید شروع به کار و توقف هر رسانه را ثبت کند. در رویدادی که یک رسانه در رسانه دیگری کپی شود، گزارش رویدادها باید این اقدام را ثبت کند.

اطلاعات در گزارش رویدادها باید مدرکی ارائه کند دال بر اینکه روش‌های اجرایی مشخص شده، دنبال شده اند و باید شامل حداقل اطلاعات زیر برای هر رویداد مهم باشد:

- تاریخ و زمان انجام عملیات مطابق با استاندارد ISO 8601 ؛

- عملیات انجام شده؛
- شناسایی اجزای فنی استفاده شده؛
- عنوان فرایندهای درگیر و شماره نگارش[1]؛
- شناسایی کاربر، اگر عملی باشد.

۶ ملاحظات رسانه ذخیره سازی

۶-۱ تعریف نوع رسانه

در جدول ۲ تعاریفی از انواع رسانه های متفاوت ارائه شده است.

جدول ۲- تعاریف انواع رسانه‌ها

نوع رسانه	تعریف
رسانه قابل حمل[2]	رسانه فیزیکی ثبت کننده اطلاعاتی است که می‌تواند از رانه جدا شود. فن‌آوری‌ها می‌تواند از نوع نوری یا مغناطیسی، بر روی لوح فشرده یا نوار باشد.
رسانه غیر قابل حمل	رسانه فیزیکی ثبت کننده اطلاعات که بخش یکپارچه‌ای از یک رانه هستند و نمی توانند از آن جدا شوند. فناوری، اغلب از نوع مغناطیسی بر روی لوح است.
یکبار نوشتنی چند بار خواندنی فیزیکی	اطلاعاتی که یک مرتبه با رسانه فیزیکی غیر قابل برگشت و فقط با یک مرتبه اصلاح رسانه نوشته می‌شود. بعد از این اصلاح، امکان حذف یا اصلاح اطلاعات وجود ندارد.
یکبار نوشتنی چند بار خواندنی منطقی	رسانه‌ای که از فناوری با قابلیت بازنویسی استفاده می‌کند، اما وسایل سخت‌افزاری یا نرم‌افزاری از هرگونه اصلاح یا حذف هرنوع اطلاعات ثبت‌شده جلوگیری می‌کند.
با قابلیت بازنویسی	بر روی این رسانه، اطلاعات می تواند بدون هیچگونه محدودیتی، ثبت، اصلاح یا حذف شود.

جدول ۳، بندهایی از این استاندارد، که استفاده از انواع متفاوت رسانه در یک سامانه اطلاعاتی مطابق با این استاندارد را توصیف می‌کنند، نشان می‌دهد.

جدول۳- استفاده از انواع رسانه‌های متفاوت

وضعیت رسانه	نوع رسانه		
	فقط با قابلیت خواندن فیزیکی	فقط با قابلیت خواندن منطقی	قابل بازنویسی
قابل حمل	بند ۷	بندهای ۷ و ۸	بندهای ۷ و ۹
غیر قابل حمل	-	بند۸	بند۹

1 - Version

2 - Removeable

۶-۲ نگهداری از رسانه‌های بایگانی

رسانه بایگانی، اعم از قابل حمل یا غیرقابل حمل، باید در محیطی سازگار با خصوصیات فیزیکی آن، همان طوری که توسط سازنده توصیف شده یا براساس استانداردهای کاربردی مربوطه، نگهداری شود. وضعیت داده های ثبت شده باید به طور مرتب کنترل شود. یک فرایند کیفی باید با کنترل‌ها و بررسی‌های دوره‌ای رسانه، در ارتباط باشد. این فرایند عامل کلیدی برای اطمینان از نگهداری از داده‌های ثبت شده بر روی رسانه است. انتقال داده های ثبت شده به رسانه جدید باید بر اساس عمر مورد انتظار رسانه قبلی، طبق توصیه سازنده ، انجام شود یا هنگامی که نتایج تولیدی توسط یک آزمون از رسانه، نشان‌دهنده نزدیک شدن به مشخصه‌های مرزی مقادیر توصیه شده آن است.

تغییر رسانه، باید نگهداری طولانی مدت از تمامیت و نیز دسترسی به اسناد را ضمانت کند.

۷ سامانه‌های استفاده کننده از رسانه‌های قابل حمل

۷-۱ کلیات

رسانه ذخیره‌سازی معمولاً به طور مستقیم توسط یک سامانه اطلاعات آدرس دهی نمی‌شود. اطلاعات در عمل بر روی فضای ذخیره سازی ثبت می‌شوند.

یک فضای ذخیره سازی می‌تواند شامل یک یا چند رسانه ذخیره‌سازی باشد و رسانه ذخیره‌سازی می‌تواند بخشی از یک یا چند فضای ذخیره‌سازی باشد.

رسانه ذخیره سازی یک موجودیت فیزیکی است، در حالی‌که فضای ذخیره سازی یک مفهوم مجازی منطقی است.

هنگامی که از رسانه نوری قابل حمل استفاده می‌شود، ساختارهای پرونده و حجم[1] آن باید با هر دو استاندارد ملی ایران ایزو به شماره ۱۳۴۹۰ یا ۸۱۷۱ مطابق باشند.

۷-۲ شروع به‌کار[2] فضاهای ذخیره سازی قابل حمل

هنگام ثبت کردن اسناد، تاریخچه پیکربندی سخت‌افزار مورد استفاده باید به عنوان فناوری‌هایی که در تکامل دائمی هستند، حفظ شود. فضاهای ذخیره سازی باید قبل از ثبت اولین سند نصب شوند اطلاعات این سند شامل موارد زیر است:

الف- عامل شناسایی منحصر به فرد رسانه؛

ب- تاریخ و زمان نصب؛

---

1 - Volume

2 - Initialization

نام سازمان؛

۳-۷ خاتمه کار فضاهای ذخیره‌سازی قابل حمل

هنگامی که یک فضا پر شد و بعد از این‌که آخرین سند ثبت شد، فضا باید در حد امکان نهایی‌سازی شود. نهایی‌سازی یک فضا باید از هرگونه نوشتن بیشتر بر روی این فضا جلوگیری کند. اساساً، اطلاعات زیر باید بعد از اطلاعات آخرین کاربر ثبت شود:

الف) تاریخ و زمان نهایی‌سازی؛

ب) تعداد پرونده‌های ذخیره شده بر روی رسانه.

۴-۷ برچسب گذاری رسانه با قابلیت یکبار نوشتن چند بار خواندن فیزیکی

هنگام استفاده از رسانه با قابلیت یکبار نوشتن چند بار خواندن فیزیکی، امنیت سامانه اطلاعات به شناسایی رسانه و وجود گزارش رویدادها که ثبت کننده هرگونه انتقال از این رسانه است، بستگی دارد.

به عنوان یک نتیجه، باید قادر باشیم تا هرگونه رسانه با قابلیت یکبار نوشتن چند بار خواندن فیزیکی را به طور مجزا شناسایی کنیم و روش‌ها و رویه‌های توانمندسازی تشخیص و یا پیشگیری از هرگونه جایگزینی رسانه را تعیین کنیم. روشی که این کار انجام می‌شود باید در دستورالعمل توصیف فنی، تشریح شود.

۸ سامانه‌های استفاده کننده از رسانه با قابلیت یکبار نوشتن چند بار خواندن منطقی

از آنجایی که رسانه با قابلیت یکبار نوشتن چند بار خواندن منطقی در کنار تعریف رسانه فیزیکی با قابلیت بازنویسی قرار دارد، سامانه‌های اطلاعات استفاده کننده از هر دو رسانه با قابلیت یکبار نوشتن چند بار خواندن منطقی قابل حمل و غیر قابل حمل، باید در محتوای این استاندارد، به عنوان سامانه اطلاعاتی استفاده کننده از رسانه با قابلیت بازنویسی مجدد، مدنظر قرار گیرد.

به علاوه، هنگام استفاده از رسانه با قابلیت یکبار نوشتن چند بار خواندن منطقی، الزامات بند ۷ باید به کار رود.

۹ سامانه های استفاده کننده از رسانه با قابلیت بازنویسی مجدد

۱-۹ کلیات

هنگامی که یک سامانه اطلاعاتی از رسانه با قابلیت بازنویسی مجدد قابل حمل یا غیر قابل حمل، استفاده می‌کند، حفظ تمامیت، متکی به قاعده‌ای است که وقتی اطلاعاتی وارد شد دیگر نمی‌تواند اصلاح شود، مگر این‌که با استفاده از فنون رمزی[1] و ایجاد تأیید انطباق های الکترونیکی، معلوم و مجاز بشود.

سه سطح امنیتی می‌تواند مبنا قرار گیرد: استاندارد، قوی و پیشرفته. این سطوح استفاده از فنون رمزی متمایزی چون توابع درهم‌سازی، مهرهای تاریخ و زمان و/یا امضاهای الکترونیکی را الزام می‌کند.

---

1 - Cryptographic techniques

هنگامی که یک سطح امنیت، استفاده از امضای رقمی را الزام می‌کند، امضا کننده ابزار ایجاد امضای رقمی را جهت داده و فعال می‌کند. امضاءکننده می‌تواند یک فرد، یک سازمان یا یک فرایند باشد. جایی‌که امضاءکننده یک فرایند است، امضای رقمی باید به طور خودکار در زمان وقوع عملیات مربوطه ایجاد شود.

امضای رقمی پیشرفته باید با الزامات زیر مطابق باشد:

الف- منحصراً به امضاءکننده پیوند داده شود؛

ب- قابلیت شناسایی امضاءکننده را داشته باشد؛

پ- با استفاده از وسایلی ایجاد شود که امضاءکننده بتواند آنرا بر قرار ساخته و تحت کنترل شخصی خود بگیرد و

پ- به داده‌ای پیوند شود که روشی را شرح می‌دهد که در آن هرگونه تغییر بعدی داده‌ها معلوم شود.

یادآوری- یک امضای رقمی پیشرفته، مطابق با تعریف ارائه شده توسط ETSI[1] (موسسه استانداردسازی مخابراتی اروپایی) در استاندارد ETSI 101 733 (CAdES) یا ETSI 101 903 (XAdES) است.

برای هریک از این سه سطح امنیت، یک تأیید انطباق الکترونیکی که تأییدکننده ذخیره‌سازی اولیه اسناد است، باید در خط‌سیر ممیزی نشر و ثبت شود. این تصدیق باید حداقل شامل اثرانگشت رقمی اسناد بایگانی شده و یک آدرس ذخیره‌سازی منطقی، مستقل از محل ذخیره‌سازی باشد. تأیید انطباق‌ها باید شواهدی ارائه دهند دال بر این‌که عملیات مربوطه، توسط شخص مجاز تقاضا شده و تحت کنترل کامل سامانه اطلاعاتی سازمان یا شخص ثالث است.

۹-۲ سطح امنیت استاندارد

در این سطح هر شخص یا فرایند مجاز با یک نمایه سامانه بایگانی برای انجام بهره‌برداری، باید حداقل با استفاده از یک شناسه و پسورد، مطابق با خط مشی امنیتی سازمان یا شخص ثالث معتبر شناخته شود.

به منظور این که از هرگونه اصلاح ورودی در گزارشات چرخه عمر بایگانی‌ها جلوگیری کنیم، گزارشات باید حداقل روزی یک‌مرتبه ممهور به مهر تاریخ و زمان شود، حتی اگر هیچ فعالیتی در طول این روز انجام نشود. تداوم گزارشات باید حفظ شود. این سطح امنیت باید از طریق خط‌سیرهای ممیزی مدیریت شده توسط سامانه اطلاعاتی یک سازمان یا یک شخص ثالث، پشتیبانی شود.

۹-۳ سطح امنیت قوی

در این سطح، شرایط زیر اضافه تر از سطح استاندارد هستند.

هر تأیید انطباق واردشده در گزارشات سامانه اطلاعات باید به طور الکترونیکی توسط واحد تأیید انطباق سامانه اطلاعاتی سازمان یا شخص ثالث، امضاء شود.

---

1 - European Telecommunications Standardization Institute

سامانه اطلاعاتی سازمان یا شخص ثالث باید برای هر خط مشی بایگانی، خط مشی امضا یا خط مشی‌های تعریف شده برای تأیید انطباق‌های الکترونیکی توسط واحد تأیید انطباق را، جزء به‌جزء شرح دهد.

۹-۴ سطح امنیت پیشرفته

در این سطح شرایط زیر اضافه‌تر از سطح قوی وجود دارد.

هر شخص مجاز به انجام کار توسط نمایه سامانه بایگانی باید تقاضاها را با استفاده از امضای رقمی پیشرفته، امضا کند. هر تأیید انطباق باید شامل تقاضای امضا شده، که شامل تأیید امضای اضافی دیگری، همان طور که در سطح امنیت قوی بیان شده، باشد.

خدمات بایگانی سازمان یا شخص ثالث باید برای هر خط مشی بایگانی خط‌مشی امضاء یا خط مشی‌هایی را تعیین کند که برای تقاضاهایی به کار می‌رود که به صورت الکترونیکی و توسط اشخاص مجاز، از طریق نمایه سامانه بایگانی، برای بهره‌برداری، امضا شده است.

۱۰ ضبط بایگانی

۱۰-۱ اسناد به صورت الکترونیکی ایجاد شده

۱۰-۱-۱ کلیات

اسناد دریافت شده توسط سامانه اطلاعاتی که به صورت الکترونیکی ایجاد شده، باید با استفاده از قالب پرونده استاندارد یا دارای استاندارد صنعتی نگهداری شود. مشخصات قالب‌ها باید بطور آزاد برای طول عمر کامل سند دردسترس باشد. در خط مشی بایگانی، استاندارد مرجع مرتبط با هرنوع متمایز از سند باید مورد ملاحظه قرار گیرد. این‌کار همچنین برای مشخصات قالب، به منظور حصول اطمینان از کاربرد طولانی مدت و ثبات محتوای اطلاعات کاربرد دارد.

۱۰-۱-۲ رویه‌ای برای ضبط بایگانی‌ها (هم‌نمایه‌سازی)

دو عملیات متمایز و مرتبط برای ضبط بایگانی‌ها الزامی است. ضبط پرونده‌های بایگانی در رسانه بایگانی و بروزکردن کاتولوگ‌ها با فراداده‌های همراه آن‌ها. ضبط فقط وقتی معتبر است که هر دو عملیات با موفقیت انجام شود.

فرایندهای کنترل و ضبط اسناد و فراداده‌های همراه آن‌ها باید تعیین شود و اسناد الکترونیکی باید با استفاده از شناسه های منحصر به فرد، تحویل رسانه ذخیره‌سازی شود. برای هر ذخیره‌سازی بایگانی، سامانه اطلاعات باید حداقل شامل موارد زیر باشد:

الف- با استفاده از هرآشکارساز خطا و کدهای مربوطه که ممکن است برای افزاره‌های مورد استفاده در دسترس باشد، صحت کیفیت سند ثبت شده بر روی رسانه بایگانی را کنترل نماید؛

ب- تأیید کند که سند جدید در فهرست سامانه اطلاعاتی، ثبت شده است؛

پ- ارتباط بین مکان فیزیکی سند و عامل شناسایی منطقی آن را محفوظ دارد.

۱۰-۱-۳ اسناد الکترونیکی علامت‌گذاری شده[1]

این اسناد، شامل اسناد ساخته شده از اجزای متنی و یا غیرمتنی، ساختاریافته توسط علامت‌گذاری استاندارد XML[2] (زبان علامت‌گذاری توسعه‌پذیر) می شود. این نوع سند می تواند به یک مدل منطقی ارجاع شده در شروع سند، اشاره کند. بایگانی این نوع سند باید شامل همه اجزای سازنده، به طور مثال نمودارهای توصیف فنی، جداول رمزی کردن، اسناد مرتبط و غیره شود.

۱۰-۱-۴ اسناد الکترونیکی استفاده کننده از یک قالب چیدمان

این حاکی از یک قالب رمزگذاری برای دیدن و چاپ‌کردن یک سند است. قالب‌های مورد استفاده برای اهداف بایگانی باید دارای استاندارد یا استاندارد صنعتی با مشخصات منتشرشده‌ای که آزادانه برای طول عمر کامل سند دردسترس است، باشد.

یادآوری- قالب‌های توصیف شده در استاندارد ایزو ۱۹۰۰۵ (همه بخش‌ها)، یا استاندارد ملی ایران به شماره ۲-۷۲۱۴، مطابق با این الزامات است.

۱۰-۱-۵ سایر قالب های اسناد الکترونیکی

اگر تصمیم گرفته شود که یک سند الکترونیکی در قالب اصلی آن نگه داری شود، و هنگامی که این مشخصه قالب به طور عمومی در دسترس نباشد، نگهداری سند در قالب اصلی آن، ممکن است مستلزم نگهداری ابزارهای سخت افزاری یا نرم افزاری مربوطه، برای دسترسی به اطلاعات، باشد.

۱۰-۱-۶ جریان چاپ

این زیربند، با پرونده‌هایی که به چاپگرهای با ظرفیت بالا فرستاده شده سرو کار دارد. چنین پرونده‌هایی همراه با این‌که داده‌ها چاپ می‌شوند، ممکن است شامل مراجعاتی به پرونده‌های بیرونی که"منابع" نامیده می‌شوند، باشند. چنین منابعی ممکن است شامل نویسه‌ها، تصاویر، رویهم‌ها[3]، فرم‌ها و غیره باشد. این منابع برای نمایش و ترجمه سند الکترونیکی لازم هستند.

این پرونده‌ها شامل سند و همه منابع مورد نیاز برای تبدیل هستند که باید تحت شرایط یکسان به منظور حفظ ارتباط بین همه اجزا، ذخیره شوند. برای این نوع سند الکترونیکی همه پرونده های ارجاع داده شده باید از یک قالب استاندارد یا دارای استاندارد صنعتی استفاده کنند. مجموعه پرونده‌های سازنده سند الکترونیکی باید اجازه بازگردانی سند چاپ شده اصلی را بدون انتقال بدهند.

۱۰-۱-۷ تصدیق اسناد الکترونیکی

حداقل برای موارد زیر، باید کنترل انجام شود:

1- Marked-up

2- Extensible markeup language

3- Overlays-

الف- کمیت و حجم اسناد ذخیره شده؛

ب- تطابق فراداده‌های همراه با قالب‌های تعیین شده؛

پ- به‌نوبت فقدان داده‌های کد(کدگذاری) شده یا مقادیر خوانا، که اجازه دهنده تفسیر کدها است.

کنترل‌های تکمیلی که می تواند تطابق اسناد ذخیره شده را با قالب‌های تعیین شده در خط مشی بایگانی تائید کند، باید ایجاد شود.

۱۰-۱-۸ کنترل تمامیت اسناد الکترونیکی انتقال داده شده از برنامه های کاربردی اصلی[۱]

تمامیت اسناد یا بسته های اسناد، دریافت شده از برنامه های کاربردی تولید بیرون باید قبل از قراردادن در سامانه اطلاعاتی، تصدیق شوند.

دو مورد باید مدنظر قرارگیرد:

- اگر اسناد یا بسته اسناد از قبل شامل مهر رقمی باشد، مهر باید هنگام پذیرفتن انتقالی به سامانه اطلاعات بررسی شود؛

- اگر اسناد یا بسته اسناد شامل هیچ افزاره اجازه دهنده چنین کنترلی نباشد، افزودن یک روش مناسب باید مدنظر قرار گیرد.

۱۰-۱-۹ ضبط فراداده

فراداده می‌تواند از چندین راه با سازگاری متقابل به دست آید.

الف- استخراج خودکار فراداده از سند؛

ب- استخراج خودکار فراداده از سامانه اطلاعاتی که سند الکترونیکی را ایجاد کرده؛

پ- ورود فراداده یا بهبود در هنگام ضبط در طی بهبودی.

رویه‌های ایجاد و کنترل فراداده باید در دستورالعمل توصیف فنی، تشریح شوند.

هنگام ضبط اسناد الکترونیکی، فراداده باید شامل اطلاعات زیر در مورد ایجاد یا اصل این اسناد باشد.

- شناسایی موجودیت آغازشدن انتقال اسناد؛
- شناسایی خدمت بایگانی دریافت کننده اسناد؛
- تاریخ و زمان ایجاد یا ورود بسته بایگانی منتقل شده؛
- فن تبدیل به کارگرفته شده برای اسناد اصلی اگر قالب اصلی اسناد مطابق با بند ۱۰-۱-۱ نباشد؛
- قالب رمزگذاری اسناد؛
- دوره نگهداری (برنامه زمان‌بندی نگهداری) و وضعیت نهایی اسناد؛
- حقوق دسترسی همراه با اسناد؛
- اندازه دسته بایگانی.

[3-] Source applications

۱۰-۱-۱۰ شاخص‌گذاری و جستجوی اسناد

اسناد الکترونیکی باید با استفاده از روشی که جستجو را برای سندی ویژه یا مجموعه‌ای از اسناد ویژه مقدور می‌سازد، رده‌بندی، شناسایی و شاخص‌گذاری شوند.

این شاخص‌ها باید از فراداده اسناد، ساخته شوند. شاخص‌گذاری اطلاعات باید توسط سامانه اطلاعاتی به عنوان شاخص خودکار و ساده، فقط با مراجعه کردن به اسناد، یا به عنوان بخشی از سامانه اطلاعات پیچیده‌تر (به عنوان مثال به عنوان بخشی از پایگاه داده بزرگتر) نگهداری شود.

سامانه اطلاعات باید به روشی طراحی شود که کاربر بدون این که به وی اخطار داده شود، سهواً، اقداماتی را که منجر به اصلاح یا ازدست دادن شاخص‌ها یا ارتباط بین آدرس‌های منطقی و آدرس‌های فیزیکی اسناد شود، انجام ندهد.

۱۰-۲ اسناد ریزفرم یا کاغذی

۱۰-۲-۱ افزاره های روبش‌کردن اسناد(روبشگر اسناد)

روبشگرهای اسنادی که از ابتدا برای کاغذ یا ریزفرم در نظر گرفته شدند باید به طور کامل توصیف شوند، شامل:

الف- مشخصات فیزیکی اسناد مورد استفاده توسط روبشگرها؛

ب- ظرفیت ضبط روبشگرها؛

پ- افزاره‌های نوری روبشگرها، اگر کاربرد داشته باشد، همراه با عملیات آن‌ها و سازوکارهای تنظیم کردن[1] در دسترس ؛

ت- سازوکارهای تنظیم‌کردن روبشگرها و عملیات مرتبط با آن‌ها.

۱۰-۲-۲ ویژگی‌های پردازش تصویر

برای این که تصاویر رقمی باکیفیتی را تولید کنیم یا برای این که اندازه پرونده‌ها را کاهش دهیم، ممکن است ضروری باشد تا از افزاره‌های سخت‌افزاری یا نرم افزاری که پردازش این تصاویر را بعد از رقمی‌سازی ، مقدور می‌سازد استفاده کنیم. اثرات هر پردازش و محدودیت‌های آن‌ها باید در دستورالعمل توصیف فنی بیان شود.

فراوان‌ترین روش‌ها عبارتند از:

الف- انتقال تصویر از رنگی یا طیف خاکستری به تک‌رنگ؛

ب- اریب زدایی؛

پ- حذف و پاک‌کردن نقاط/ پس زمینه؛

ت- حذف حاشیه سیاه؛

ث- حذف رویهمی‌ها[2]، لوگوها، نوشته‌ها ونقش‌های زمینه یا هرنوع اطلاعات غیرمرتبط دیگر؛

ج- حذف صفحات سفید.

1- Tuning

2- Overlays

همه این پردازش‌ها باید با ملاحظات دقیق انجام شود به طوری که دارای وابستگی به ثبات تصویر الکترونیکی در ارتباط با سند منبع باشد. به ویژه، رویه‌ای برای تبدیل تصویر رنگی یا طیف خاکستری به یک تصویر تک رنگ باید قبل از اجرا آزمون شود و درسطح جزئیات تائید اعتبار شود.

حذف نقاط می‌تواند منجر به حذف برخی اقلام اطلاعاتی از تصویر ، از قبیل یک کاما، یک تأکید[1] یا جزئی از یک نمودار شود. بنابراین، قبل از اجرا، این موارد باید آزمون شود. نتایج آزمون باید در دستورالعمل توصیف فنی ذخیره شود.

اگر ویژگی‌های عمل کننده در سامانه اطلاعات به طور کامل در دستورالعمل توصیف فنی بیان شود، نرم افزار مورد استفاده برای حذف رویهمی‌ها، با باقی نگه داشتن فقط محتوای متغیر، می تواند استفاده شود. بالاتر از آن، هنگام بازیابی یک سند، ادغام محتوای متغیر و رویهمی را الزام می‌کند، آنگاه هنگامی که صفحه اسکن و پردازش می شود، نسخه رویهمی مورد استفاده باید با رویهمی استخراج شده، یکسان باشد.

رویهمی‌ها به عنوان عناصر سند مد نظر قرار می‌گیرند و بنابراین باید در شرایط یکسان با سایر عناصر سند ذخیره شوند.

هنگامی که اجباری است کل اطلاعات را حفظ کنیم، توصیه می شود از چنین شیوه‌هایی استفاده نکنید. در سایر موارد، ضروری است، دلایل استفاده از چنین شیوه‌هایی را در دستورالعمل توصیف فنی بیان کنید.

حذف صفحه سفید، می تواند خطر بالقوه‌ای از فقدان اطلاعات را نمایش دهد. هنگام انجام این کار توصیه می‌شود، بررسی کنیم که آیا شیوه مورد استفاده قابل اعتماد است و صفحات شامل اطلاعات را حذف نمی-کند. دستورالعمل توصیف فنی باید روش‌های اجرایی مورد استفاده برای اطمینان از قابلیت اعتماد این عملیات را تشریح کند. همچنین توصیه می‌شود تا فرایندی برای شمارش تعداد صفحات حذف شده نسبت به تعداد صفحات باقی‌مانده انجام شود.

استفاده از صفحه مرجع آزمون (استاندارد ایران ایزو ۲-۱۲۶۵۳ و استاندارد بین المللی ISO 12653-1 -را ببینید)، اجازه اندازه‌گیری بی‌طرف سامانه اطلاعات و بررسی تأثیرات نرم افزار پردازش تصویر را می‌دهد.

۱۰-۲-۳ روش ضبط ریزفرم یا سند کاغذی

۱۰-۲-۳-۱ کلیات

هنگامی که ضبط سند ریزفرم یا کاغذی کامل شود، کاربر باید یک تأیید انطباق روبش ارائه دهد که حداقل نام کاربر، تاریخ روبش، زمان آغاز و پایان روبش، شناسه‌های اولین و آخرین سند روبش‌شده و تعداد صفحات روبش‌شده را اعلام نماید.

بعد از بررسی تصاویر روبش شده، یک تأیید انطباق اجازه باید توسط مالک یا مؤسسه مجاز از سوی مالک، صادر شود. اگر تأیید انطباق برای یک بسته از اسناد به کار رود، تعداد تصاویر و اسناد باید تعیین شود.

۱۰-۲-۳-۲ آماده‌سازی اسناد کاغذی

سازمان باید اطمینان یابد که کیفیت اسناد کاغذی که تولید می‌کند، با فنون روبش‌کردن یا ضبط ریزنگاره سازگار است. اسناد چروک یا پاره شده، اعم از این که توسط سازمان صادرشده باشد یا از منبع بیرونی

1- Accent

دریافت شده باشد، می تواند تعمیر مجدد[1] را قبل از رقمی‌سازی الزام کند. با این‌حال، به منظور بهبود خوانایی، متن اسناد نباید ویرایش یا اصلاح شود، به طوری‌که این‌کار می تواند تمامیت اسناد مرتبط با اسناد اصلی را تغییر دهد.

درحد ممکن، اقداماتی نظیر آن‌هایی که در استانداردهای ملی ایران به شماره‌های ۷۲۸۹ و ۱۳۳۸۹ تصریح شده، باید برای پردازش اسناد مورد نظر برای رقمی‌سازی، اجرا شود.

۱۰-۲-۳-۳ آماده‌سازی اسناد ریزفرم

اسناد ریزفرم، اگر ضروری باشد، باید قبل از رقمی‌سازی، عاری از گرد و غبار شوند. کاربر باید کنترل کند که هرگونه نقص یا خراش محدودکننده خوانایی، مرحله خواندن یا پردازش سند در تبدیل را غیر ممکن خواهد کرد.

۱۰-۲-۳-۴ روبش‌کردن سند ریزفرم یا کاغذی

دستورالعمل راهنمای کاربر باید همه جزئیات مربوط به روبش‌کردن سند، تنظیم روبشگر، فرایندهای ارتقای تصویر و عناصر متفاوتی از رویه روبش‌کردن را تعیین کند. هر فن پردازش مورد استفاده برای ارتقای اطلاعات، باید پیشاپیش به تصویب تهیه‌کننده پروژه، برسد و به طور کامل در دستورالعمل راهنمای سامانه روبش، توصیف بشود.

دستورالعمل راهنمای کاربر باید همه عناوین مربوط به عملیات مجاز در ارتباط با اصلاحات تصویر رقمی ایجاد شده توسط روبشگرهای سند را پوشش دهد.

۱۰-۲-۳-۵ تصدیق[2] اطلاعات روبش شده

دستورالعمل راهنمای کاربر سامانه روبش باید شامل یک رویه پوشش دهنده بازبینی روبش‌کردن باشد. بررسی‌های بازبینی باید حداقل برای موارد زیر به کار رود:

الف) کیفیت و تمامیت تصاویر مرتبط با اسناد منبع؛

ب) صحت شاخص‌گذاری اطلاعات اسناد روبش شده.

اگر کنترل‌های کیفیت توسط خود کاروران به منظور کاهش مردودی انجام شود، توصیه می‌شود که کنترل کیفیت نهایی توسط اشخاصی به غیر از کاروران انجام شود.

رویه‌های نمونه‌برداری برای عناصر فیزیکی مجزا باید با استاندارد ملی ایران به شماره ۶۶۶۵ (همه بخش‌ها) سازگار باشد.

۱۰-۲-۴ خط‌سیرهای ممیزی

۱۰-۲-۴-۱ شناسایی بسته یا سند

روبش‌های اسناد (کاغذ یا ریزفرم) باید شامل عناصر تاریخچه‌ی اطلاعاتی زیر باشد:

1- Reconditioning

2-Verification

الف- شناسه منحصر به فرد اسناد در سامانه اطلاعات؛

ب- تعداد صفحات سند.

بسته‌های سند (ریزفرم یا کاغذی) باید شامل عناصر تارخچه اطلاعاتی زیر باشد:

- شناسه بسته (این شناسه باید برای هر بسته منحصر به فرد باشد)؛
- تعداد اسناد یا حلقه های ریزفیلم یا ریزفیش در هر بسته؛
- تعداد صفحات روبش شده یا برای ریزفرم‌ها، تعداد فریم‌ها.

۱۰-۲-۴-۲ جزئیات فرایند ضبط سند

اطلاعات زیر، اگر قابل کاربرد باشد، باید در خط‌سیر ممیزی ثبت شود:

الف- شناسه پیام‌های دریافت شده از روبشگر (زمان و تاریخ شروع روبش، راه اندازی اولیه بسته برای سامانه‌های خودکار، پایان فرایند روبش و ...)؛

ب- شناسه تعداد بایت‌های ایجاد شده توسط فرایند روبش سند قبل و بعد از فشرده سازی (اگر از فشرده سازی استفاده شود).

۱۰-۲-۴-۳ داده‌های خط‌سیر ممیزی

یک ثبت تاریخچه از رویدادها باید شامل حداقل اطلاعات زیر باشد.

برای رقمی‌سازی اسناد کاغذی:

الف- شناسه اولین سند یا اولین بسته اسناد روبش‌شده و ذخیره شده؛

ب- شناسه آخرین سند یا آخرین بسته اسناد روبش‌شده و ذخیره شده؛

پ- تاریخ و زمان ورود و خروج هر کارور؛

ت- شناسه اولین سند یا بسته اسناد روبش‌شده و ذخیره شده توسط هر کارور؛

ث- شناسه آخرین سند یا بسته اسناد روبش‌شده و ذخیره شده توسط هر کارور؛

ج- تعداد کل صفحات پردازش شده؛

چ- تعداد کل صفحات پردازش نشده، شامل آن‌هایی که روبش آن‌ها به سبب کیفیت ضعیف سند (به طور مثال: تباین ضعیف رنگ[1]، خراش یا پارگی) غیرممکن باشد؛

ح- تعداد کل صفحات سفید، اگر داشته باشد.

برای رقمی‌سازی ریزفرم:

- شناسه اولین ریزفرم روبش شده و ذخیره شده؛
- شناسه آخرین ریزفرم روبش شده و ذخیره شده؛
- تاریخ و زمان ورود و خروج هر کاربر؛
- شناسه اولین ریزفرم روبش‌شده و ذخیره شده توسط هر کارور؛
- شناسه آخرین ریزفرم روبش‌شده و ذخیره شده توسط هر کارور؛
- تعداد کل فریم‌های ریزفرم پردازش شده؛

1- Weak contrast

- تعداد کل فریم‌های پردازش نشده، شامل آن‌هایی که به سبب کیفیت ضعیف ریزفرم‌ها، روبش آن‌ها غیرممکن است؛

۱۰-۳ اشیاء صوتی/ تصویری غیررقمی برروی رسانه‌های نواری[1]

۱۰-۳-۱ کلیات

این زیربند مربوط به سامانه اطلاعاتی است که افزاره‌هایی برای کدگذاری (رقمی‌سازی) ثبت نسخه اصلی صوتی و صوتی تصویری[2] دارد.

۱۰-۳-۲ آماده سازی رسانه‌های نوار اصلی[3]

قبل از کدگذاری (رقمی‌سازی) نوارهای مغناطیسی، این نوارها باید به منظور ارزیابی شرایط عملیاتی رسانه و ضبط کردن آن‌ها، کنترل شود.

این بررسی شامل موارد زیر است:

- وضعیت فیزیکی تعمیر ضبط‌ها؛
- کارایی‌های خواندن و
- سازمان‌دهی و کیفیت توالی‌های ثبت‌شده.

۱۰-۳-۳ رقمی‌سازی شیء صوتی تصویری و صوتی اصلی[4]

کیفیت نسخه رقمی اشیاء، توسط ویژگی‌های تجهیزات خواننده شیء اصلی و فرایند رقمی‌سازی (خصوصیات مبدل‌ها و روش‌های نمونه‌گیری/کدگذاری) تعیین خواهد شد. دربرخی موارد، رویه‌های برای تمیزکاری و نگهداری اسناد باید قبل از رویه‌های خواندن، اجرا شود. افزاره‌های خواندن باید با کیفیت بالا میزان شود (به طور مثال: تنظیم هدهای اصلی خواندن نوشتن ضبط نوار، ردگیری ثبت‌کننده ضبط تصویر).

ابزارهای استخراج اطلاعات، رقمی‌سازی و انتقال شرایط باید به طور کامل تشریح شود، شامل:

الف- مشخصات فیزیکی رسانه پشتیبانی‌شده برای افزاره‌های رقمی‌سازی ؛

ب- مشخصات و تنظیم ویژگی‌های افزاره‌های خواندن (شیارهایی صوتی، قالب تصویری غیررقمی مؤلفه یا ترکیب)؛

پ- مشخصات افزاره‌های رقمی‌ساز.

۱۰-۳-۴ پردازش اطلاعات صوتی تصویری و صوتی

هنگامی که نگهداری از تمامیت اطلاعات اجباری باشد، هرگونه پردازشی که منجر به اصلاح اطلاعات نسبت به اطلاعات اصلی شود، باید درحد ممکن مستثنی یا محدود شود.

1- Analogue audio/video objects on tape media

2- Audiovisual

3 - Preparation of original tape media

4- Original audio and audiovisual object digitization

هنگامی که اصلاح اطلاعات ممکن باشد، به منظور ارتقای کیفیت صوتی یا تصویری، ممکن است از نرم افزار پردازش استفاده شود که این نرم افزار مقرر می‌دارد که هرگونه کارکردی قبل از استفاده، آزمون و صحه-گذاری شده است. کارکردهای مورد استفاده توسط سامانه اطلاعات باید به طور کامل در دستورالعمل توصیف فنی بیان شود.

۱۰-۳-۴-۱ اشیاء صوتی

برای این نوع اشیاء، میزان سازی‌های معمول عبارتند از:

الف) میزان‌سازی سرعت ضبط؛

ب) تنظیم تعادل طیف؛

پ) تنظیم سطح صوت (تنظیم یا فشرده سازی پویا)

ت) حذف نقایص موقت؛

ث) کاهش نوفه[1] باند پهن؛

ج) انتخاب رمزگشا (فشرده سازی/ فشرده‌زدایی) برای اشیاء رقمی کدگذاری شده؛

چ) فراوانی طرزعمل نمونه‌گیری؛

هرگونه حذف "جای خالی" باید به دقت مدنظر قرار گرفته و اعتباردهی شود.

۱۰-۳-۴-۲ اشیاء تصویری

برای این نوع اشیاء، میزان‌کردن‌های معمول عبارتند از:

الف) تنظیم سطح سیاهی؛

ب) افزایش رنگ و درخشندگی[2]؛

پ) افزایش سیگنال تصویر؛

ت) کاهش نقص موقت؛

ث) ازهم جداکردن[3]

همه این فرایندها باید با ملاحظه دقیق اجرا شوند به طوری که بر ثبات توالی صدا یا تصویر رقمی، نسبت به نوع اصلی آن تأثیرگذار باشند.

۱۰-۳-۵ گزارش رویدادها

۱۰-۳-۵-۱ شناسایی شیء

برای هر شیء، اطلاعات زیر باید ثبت شود:

الف- شناسه منحصر به فرد شیء فیزیکی در سامانه اطلاعات؛

ب- شناسایی ورودی‌ها.

1- Noise

2- Luminance

3 - De- interlacing

۱۰-۳-۵-۲ شناسایی بسته های شیء

گزارشات برای بسته‌های روبش اشیاء (کاغذ یا ریزفرم) باید حاوی اطلاعات زیر باشد:

الف- شناسه بسته (این شناسه باید منحصر به فرد باشد)؛

ب- تعداد اشیاء، حلقه‌ها یا کارتریج‌ها[1] در هر بسته؛

پ- تعداد نوارها و ورودی‌های رقمی شده.

۱۰-۳-۵-۳ تصدیق رویه‌های ضبط و ذخیره سازی شیء

هنگام اجرای این رویه‌ها، اطلاعات زیر باید در گزارشات، ذخیره شود:

الف- افزاره‌های مورد استفاده برای عملیات (سازوکارهای خواندن، مبدل و ...) برروی قالب‌های منتخب و تنظیمات[2] ؛

ب- اسامی اشیاء رقمی، طول بخش‌های مربوطه[3] ؛

پ- کمیت بیت‌های ایجاد شده توسط رقمی‌کردن اشیاء یا دسته‌های اشیاء قبل و بعد از فشرده‌سازی متوالی (اگر باشد)؛

۱۰-۳-۵-۴ گزارش عملیات

یک گزارش عملیات باید، رد سابقه‌ای از همه عملیات انجام شده در روز فراهم کند، این گزارشات باید شامل حداقل اطلاعات زیر برای رقمی‌سازی اشیاء تصویری/ صوتی غیررقمی از نوار ضبط باشد:

- شناسه اولین شیء یا اولین دسته از اشیاء رقمی‌شده و ذخیره شده؛
- شناسه آخرین شیء یا آخرین دسته از اشیاء رقمی‌شده و ذخیره شده؛
- تاریخ و زمان ورود و خروج هر کاربر؛
- شناسه اولین شیء یا اولین دسته از اشیاء رقمی‌شده و ذخیره شده توسط هر کاربر؛
- شناسه آخرین شیء یا آخرین دسته از اشیاء رقمی‌شده و ذخیره شده توسط هر کاربر؛
- تعداد کل کاست‌های نواری یا کارتریج‌ها یا اقلام پردازش شده؛
- تعداد کل کاست‌ها یا ریل‌های پردازش نشده، شامل مواردی‌که رقمی‌کردن به سبب کیفیت ضعیف شیء (به طور مثال داشتن شیار، شکستگی یا تغییر شکل، سایش) غیر ممکن باشد.
- تعداد کل کاست‌های سفید و طول نوار ریل‌های سفید، اگر داشته باشد.

۱۰-۴ فنون فشرده‌کردن اطلاعات تصویر، تصویری و صوتی

۱۰-۴ -۱ انواع فشرده‌کردن

پرونده‌هایی که حاوی تصاویر رقمی از اشیاء غیررقمی باشند، می‌توانند به منظور کاهش فضای لازم برای ذخیره‌سازی، فشرده شوند.

دو روش فشرده‌کردن متفاوت وجود دارد: "بدون اتلاف[4]" یا "با اتلاف[5]" .

---

1 - Cartridges
2 - Settings
3- Associated sequence units
4 -Lossless
5- Losely

هرگاه یک فشرده‌کردن بدون اتلاف انجام شود، بعد از نافشرده‌کردن، تصویر ایجاد شده، دقیقاً ، بیت به بیت، یکسان با شیء اصلی است.
یک فشرده‌کردن با اتلاف هرگاه انجام شود، بعد از فشرده‌کردن ، تصویر ایجاد شده دقیقاً یکسان با شیء اصلی نیست. در این مورد، بخشی از اطلاعات شیء اصلی از دست می رود.

۱۰-۴ -۲ اسناد کاغذی یا ریزفرم

فشرده‌کردن با اتلاف باید فقط برای تصاویر از نوع عکس رنگی یا طیف‌خاکستری، هنگامی که بعد از یک چرخه فشرده‌کردن/ فشردگی زدایی ، منجر به حذف مشهود اطلاعات نمی شود، استفاده شود.
فشرده‌کردن با اتلاف نباید برای اسناد سیاه و سفید، که اغلب تحت عنوان اسناد اداری ارجاع می شود، و بیشتر حاوی ترسیمات خطی یا متن است، استفاده شود. برای این نوع سند، یک صفحه مرجع آزمون[1] باید استفاده شود (استاندارد ایران ایزو ۲-۱۲۶۵۳ و استاندارد بین المللی ISO 12653-1) را ببینید.
برخی فنون فشرده‌کردن، برپایی[2] پارامتر کیفیت را مجاز می‌کند. این پارامتر باید طوری برپا شود که هیچ فقدان آشکاری از اطلاعات بین تصویر اصلی و تصویری که چرخه فشرده‌کردن/ ذخیره‌کردن/ نافشرده‌کردن را طی کرده، وجود نداشته باشد.
سامانه‌های اطلاعات باید توانایی تصدیق را بعد از فشرده‌کردن پرونده‌هایی که حاوی تصاویر هستند، فراهم کنند.
نوع فشرده‌کردن و اگر مناسب باشد، پارامترهایی که برای فشرده‌کردن استفاده می‌شود، باید به عنوان بخش جامعی از پرونده حاوی تصویر رقمی ذخیره شود.
برای انتخاب هرگونه روش فشرده‌کردن، به منظور حل مشکل بایگانی، باید به استاندارد ISO/TR 12033، مراجعه شود.
هرگونه انتخابی که صورت گیرد، نوع فشرده‌کردن باید برمبنای استاندارد باشد و مشخصات آن‌ها آشکارا، قابل دستیابی باشد.

۱۰-۴ -۳ ثبت‌کردن اشیاء صوتی تصویری یا صوتی

معمولاً، اشیاء صوتی، نباید با استفاده از شیوه فشرده کردن با اتلاف پردازش شوند.
برای اشیاء تصویری، با درنظر گرفتن حجم ذخیره‌سازی دربرگرفته شده و پهنای باند دردسترس برای انتقال اطلاعات، معمولاً ضروری است فشرده‌کردن با اتلاف را اجرا کنیم.
برای هردو شیء صوتی تصویری و صوتی، قالب‌های استانداردشده ISO/MPEG باید استفاده شود. این استانداردها، گزینه‌هایی برای فنون فشرده‌کردن و قالبی که باید برای تبدیل‌کردن[3] اطلاعات براساس الزامات کیفیت، انتخاب شود، پیشنهاد می‌کنند.

۱۰-۵ قالب تبدیل

یک جدول با شرح جزئیات قالب های ورودی پذیرفته شده توسط سامانه اطلاعات باید ایجاد شود.

---

1 - Test target
2 - Setup
3 - REndering

قالب‌های رمزگذاری برمبنای مشخصات عمومی دردسترس (مبتنی بر استاندارد، هرگاه ممکن باشد) باید انتخاب شود. انتخاب یک قالب تبدیل باید براساس نوع سند الکترونیکی و مشخصه‌هایی که بعد از تبدیل نگهداری می شوند، یا نمی‌شوند، انجام شود. تعیین این‌که آیا نمود تصویری (نمایش) از اسناد مجبور است نگهداری شود، و آیا هیچ نوع ارتباطی با اسناد خارجی وجود دارد و آیا اجباری به نگهداری فرمول‌های ریاضی یا اسناد کلان داخلی وجود دارد یا نه، اهمیت دارد.

انتخاب یک قالب جدید برای نگهداری، و فنون تبدیل مرتبط، باید از حذف تصادفی اطلاعات مهم اجتناب کند. مشخصه‌های تبدیل و اجرا باید در گزارش رویدادها به همراه موارد زیر، کنترل و ثبت شود:

الف- نام برنامه (های) مورد استفاده برای تبدیل؛

ب- نام برنامه‌هایی که شناسایی و اعتباردهی قالب را مقدور می سازد؛

پ- نوع رویداد؛

ت- تاریخ تبدیل؛

ث- نام پرونده ورودی؛

ج- نام پرونده خروجی؛

چ- نمایش قالب؛

ح- خروجی عملیات (یعنی موفقیت یا شکست) و زمانی که شکست رخ می‌دهد، ثبت نتایج ناهنجار.

تبدیل‌های قالب ممکن است در تعداد مراحل متفاوت از فرایند بایگانی انجام شود: هنگامی که یک سند ضبط می‌شود، هنگامی که تبدیل بعد از بایگانی سند برنامه‌ریزی می‌شود، یا هنگامی که قالب رمزگذاری یک سند بایگانی شده منسوخ می‌شود و می تواند مشکلی را برای دسترسی نشان دهد.

دامنه فرایندهای مرتبط با قالب‌های سند الکترونیکی بایگانی شده، براساس توافقات بین مؤسس بایگانی و خدمات بایگانی، و درمورد خط مشی بایگانی قابل کاربرد، تغییر می‌کند.

درهنگام ورود به سامانه اطلاعات، گام‌های زیر انجام می‌شود:

- کنترل‌های قالب (یا عدم کنترل) در آغاز بایگانی (برمبنای جدول قالب‌های ورودی- سامانه قابل پذیرش)؛
- تبدیل‌های قالب (یا عدم تبدیل) در ورودی برمبنای نتایج کنترل‌ها، یا برمبنای شرایط قراردادی با ارجاع به جدول قالب‌های بایگانی هدف؛

بعد از ورود در سامانه اطلاعات، گام‌های زیر تقبل می شود:

- اعلام خطر به مالک (یا عدم اعلام خطر) اگر قالب کدگذاری منسوخ شده باشد؛
- تبدیل (یا عدم تبدیل) توسط سامانه اطلاعات، هنگامی که منسوخ‌شدن قالب گزارش شود.
- کنترل قالب باید با ابزاری انجام شود که اجازه شناسایی دقیق، توصیف و صحه‌گذاری قالب را می‌دهد.

۱۱ عملیات بایگانی

۱۱-۱ دامنه کاربرد

عملیات بایگانی به معنای دسترسی، بازگرداندن و وارهایی نهایی بایگانی‌هاست.

۱۱-۲ دسترسی

۱۱-۲-۱ کلیات

عملیات دسترسی باید برمبنای شرایط جستجو و انتقال بعدی اسناد الکترونیکی در قالب بایگانی خود باشد.
به علاوه، دسترسی می تواند شامل موارد زیر باشد:

الف- نمایش اسناد دریک صفحه نمایش؛

ب- چاپ یک نسخه از کاغذ یا فیلم؛

پ- پخش(نواختن) صوت در شرایط صوتی مناسب در رابطه با کیفیت اسناد؛

ت- نمایش تصاویر نمایشی در شرایط صوتی مناسب در رابطه با کیفیت اسناد؛

روش‌های مورد استفاده برای بازیابی و نمایش اسناد باید در دستورالعمل توصیف فنی بیان شود.
پردازش محتوای سند، نباید برای عملیات بازیابی و نمایش به استثنای نافشرده‌کردن، تفسیر قالب و اطمینان از پردازش فنی، همچنین هرگونه تنظیمات ضروری برای مشخصه‌های نرم‌افزاری یا فیزیکی افزاره‌های نمایش و بازیابی، مجاز شود.
اگر لازم باشد، تأیید انطباقی از انطباق نسخه انتقال یافته باید انجام شود. این تأیید انطباق باید علاوه بر نام شخصی که درخواست را صادر کرده و نام شخصی که تأیید انطباق را انجام داده، فراداده‌های مجاز برای شناسایی سند و ارائه یک خط‌سیر ممیزی از چرخه عمر سند در سامانه اطلاعات را، شامل شود.

۱۱-۲-۲ اسناد رقمی شده

برنامه‌های کاربردی دیدن و خواندن باید مستقل از ابزاری باشد که برای ایجاد اسناد بایگانی شده استفاده می‌شود. بنابراین یک سند الکترونیکی بایستی در یک محیط نرم‌افزاری و سخت‌افزاری متفاوت با محیط مورد استفاده برای دیدن و خواندن، ضبط شود.
اگر فرایند تبدیل رقمی برای سند با منشأء ریزفرم یا کاغذی، از نرم‌افزاری استفاده کند که همپوشانی‌ها یا هرگونه عناصر ثابت دیگر را حذف می‌کند، اصول ثبات سند در بازیابی و نمایش، الزام می‌کند که سند بازگردانده شده، محتوای ثابت را همراه با محتوای متغیر تجمیع کند. سامانه اطلاعات باید ضمانت کند که نسخه‌های عناصر ثابت یا رویهمی مورد استفاده با آن‌هایی که درطی رقمی‌سازی ضبط شده‌اند، یکسان هستند.

۱۱-۲-۳ اسناد الکترونیکی نشان‌دارشده

هنگامی که جداول کدگذاری مشخصی استفاده شوند، آن‌ها باید در طول دسترسی، دردسترس و قابل دستیابی باشند.
دسترسی به این اسناد باید با استفاده از دستورالعمل‌های چیدمان مربوطه انجام شود.

۱۱-۲-۴ اسناد الکترونیکی با استفاده از قالب چیدمان

فرایندهای دسترسی باید محدود به کنارهم قراردادن[1] اجزای متفاوت سند، براساس قوانین نمایش توصیف شده و رسانه نمایش مورد نظر، بدون هرگونه اقدام یا پردازش محتوا شود.

۱۱-۳ بازگردانی

بازگردانی بایگانی‌ها، اعم از کلی یا جزئی، به معنی انتقال اسناد بایگانی شده به صادرکننده آن‌ها یا به شخص ثالث منتصب برحسب وظیفه می‌باشد.

بازگردانی باید با انهدام (وارهایی) اسناد در سامانه اطلاعات، توأم باشد.

رویه بازگردانی و جزئیات فنی انتقال (قالب بازگردانی و رسانه انتخاب شده) باید در دستورالعمل توصیف فنی بیان شود.

۱۱-۴ وارهایی بایگانی‌ها

دوره نگهداری از اسناد بایگانی‌شده (برنامه زمان‌بندی نگهداری) باید در سامانه اطلاعات، یا با استفاده از سابقه دوره نگهداری فراداده برای هرسند بایگانی شده، یا با ارجاع دادن هرگونه سند بایگانی شده مربوط به یک جدول دوره نگهداری، مدیریت شود. سامانه اطلاعات باید اجازه اصلاح دوره نگهداری برای یک سند معین را بدهد.

تحت نظارت یک نماینده مجاز، و در انطباق با رویه‌های موجود، در پایان هردوره نگهداری، بایگانی‌ها باید حذف شوند. این عملیات باید اسناد را به طور قطع حذف کرده و به طور کامل غیرقابل دسترس سازد.

یادآوری- برای اطلاعات بیشتر به استاندارد ISO15489-1 و ISO 15489-2 یا مشخصات MoReq2 رجوع شود.

هنگامی که یک رسانه ذخیره‌سازی قابل حمل از بین می‌رود، فرایند باید درخصوص غیرقابل دسترس بودن کامل اطلاعات ثبت شده برروی رسانه اطمینان ایجاد کند.

هرگونه نگهداری فراداده‌ها و گزارشات یا خط‌سیرهای ممیزی مرتبط با بایگانی‌های حذف‌شده، باید در توافق قراردادی یا درخط مشی بایگانی تعیین شود.

۱۲ ارزیابی سامانه اطلاعات

۱۲-۱ کلیات

۱۲-۱-۱ ممیزی‌ها

1 - Assembly

سامانه اطلاعات و همه رویه‌های مرتبط باید به طور منظم ممیزی شود، به خصوص هنگامی که تغییرات اساسی در سامانه اطلاعات به وجود آید. این ممیزی‌ها می تواند یا توسط اشخاص داخلی سازمان پاسخگو برای اطلاعات (ممیزی داخلی) انجام شود و یا توسط اشخاص تعیین‌شده توسط یک شرکت[1] شخص ثالث (ممیزی بیرونی) اجرا گردد.
نتایج این ممیزی‌ها باید نگهداری شود.

۱۲-۱-۲ اهداف

ممیزی‌ها باید تصدیق کند که سامانه اطلاعات و رویه‌ها مطابق با این استاندارد ملی هستند. کنترل انطباق باید طراحی، اجرا، استفاده و همه رویه‌های عملیاتی سامانه را پوشش دهد.
به علاوه، ممیزی‌ها باید قادر باشد تا کارایی سامانه اطلاعاتی اجراشده و توانایی آن برای آدرس‌دهی اهداف و الزامات حوزه مرتبط فعالیت را اندازه‌گیری کند.
درپایان، ممیزی‌ها باید همه اطلاعات مفید برای بهبود مناسب انطباق سامانه اطلاعات را فراهم کند.

۱۲-۱-۳ مسئولیت‌های ممیز

ممیزان باید حداقل موارد زیر را رعایت کنند:
الف- الزامات را شفاف و مشخص نمایند؛
ب- عملیات ممیزی را آماده کرده و توسط کسانی که این کار به آن‌ها سپرده شده است، انجام دهند.
پ- نتایج را ثبت کنند؛
ت- نتایج ممیزی را گزارش دهند.
ممیزان باید بی‌طرف[2] بوده و عاری از هرگونه نفوذی باشند که بتواند بر واقعیات اثرگذارد.

۱۲-۱-۴ کارکنان مسئول ارزیابی

شرایط احراز، آموزش و تجربه هرممیز (اعم از فعال یا کمکی) باید توسط مسئول این موارد در سازمان، کنترل و پایش شود.
به ویژه این‌که، ممیزان باید با تجربه بوده و چندین سال اقدام حرفه‌ای در زمینه مدیریت اسناد، بایگانی الکترونیکی یا مدیریت سوابق داشته باشند. نسبت معنی‌داری از این تجربه باید در طراحی و مشاوره برای اجرای سامانه‌های اطلاعات وجود داشته باشد.
ممیزان داخلی یا خارجی باید مهارت‌های ضروری زیر را برای هدایت فرایند ممیزی داشته باشند:
الف- فنونی برای اندازه‌گیری، پرسش‌کردن، ارزیابی و نوشتن گزارش‌ها؛
ب- فنونی برای فرایندهای گوناگون ممیزی از قبیل برنامه‌ریزی، روش، سازماندهی، ارتباطات و مدیریت؛
مهارت‌های ممیزان باید مناسب برای پوشش همه نوع سند دربرگرفته شده در سامانه اطلاعات، شامل اسناد فنی مشخص از قبیل تصویری و صوتی باشد.

---

1 - Enterprice
2 - Impartial

۱۲-۱-۵ تصدیق مستندات

سازمان باید یک سامانه اطلاعات که اطمینان می‌دهد همه اسناد مرتبط با ممیزان می‌تواند تصدیق شود را حفظ کند و اطمینان حاصل کند که:

الف- نسخه‌های بروز از مستندات ضروری، به مقدار مناسب، در تمامی نقاطی که سامانه اطلاعات کار می-کنند، در دسترس هستند؛

ب- همه تغییرات یا اصلاحات مربوط به مستندات، به طور مناسب، مجاز و به روشی پردازش می‌شوند تا از اقدام سریع و مستقیم افراد درگیر اطمینان حاصل شود؛

پ- مستندات فاقد اعتبار، بلافاصله باطل می‌شوند و از تمام نقاط توزیع و مورد استفاده در سازمان جمع‌آوری و امحاء می‌شوند (به استثنای مستندات فاقد اعتباری که برای اهداف قانونی یا تاریخی نیاز به حفظ آن‌هاست، و باید به طور مناسب شناسایی و حفظ شوند).

۱۲-۱-۶ ارزیابی اسناد عملیاتی

سازمان باید همه نتایج عملیات ارزیابی را ثبت کند. اسناد باید فرایندهایی که برای هرعملیات ارزیابی کاربرد دارد را به کار برند.

همه اسناد باید به گونه مطمئن، برای یک دوره مناسب حفظ شوند.

۱۲-۲ ارزیابی داخلی

هنگامی که ارزیابی توسط کارکنان تحت اختیار سازمان انجام شود، سازمان باید توصیفی از سازمان را تهیه کند و قادر به ارائه آن باشد که به طور شفاف، نشان دهنده توزیع مسئولیت‌ها و ساختار سلسله مراتبی سازمان است، به ویژه این‌که، این توصیف نشان‌دهنده استقلال نقش‌های ممیزی و نقش های عملیاتی باشد.

۱۲-۳ ارزیابی بیرونی

سازمان‌های شخص ثالث که انجام‌دهنده ممیزی سامانه اطلاعات هستند، باید تجربه و مهارت‌های کافی و مؤثر در طراحی و اجرای سامانه اطلاعات برای نگهداری از اسناد را داشته باشند.

اشخاص انجام‌دهنده عملیات ارزیابی باید صلاحیت، آموزش و تجربه کافی برای ممیزی صحیح سامانه اطلاعات را داشته باشند.

سازمان‌های شخص ثالث، باید همه اقدامات ضروری در همه سطوح سازمان را برای اطمینان از محرمانگی اطلاعات جمع‌آوری شده در طول ممیزی، در نظر بگیرند.

۱۳ بایگانی شخص ثالث معتمد

۱۳-۱ فعالیت های ارائه دهنده خدمات بایگانی شخص ثالث معتمد

قوانین به کاررفته برای راه‌حل‌های داخلی، معادل با قواعد طرف‌های ثالث اجراکننده خدمات بایگانی الکترونیکی است. هنگامی که بایگانی‌ها تحت حفاظت یک خدمت‌دهنده بایگانی شخص ثالث مورد اعتماد قرار می گیرند، سازمان باید کنترل کند که شیوه‌ها و رویه‌های مورد استفاده در خصوص امنیت، تمامیت و نگهداری طولانی مدت از اسناد الکترونیکی اطمینان ایجاد می‌کنند و این که همه ساختارها، با تأیید انطباق های مربوطه ردگیری می‌شوند. پیوست پ، اصولی را برای شرایط پیشنهادی خدمات عمومی، ارائه می دهد.
قبل از هرگونه انتقال بایگانی‌ها به اشخاص ثالث معتمد، کنترل‌هایی باید برای اطمینان از موارد زیر انجام شود:

الف- شخص ثالث قادر باشد تا الزامات تعیین شده در این استاندارد را برآورده کند؛

ب- خط مشی بایگانی مورد استفاده توسط شخص ثالث، سازگار با خط مشی سازمان باشد؛

پ- رویه‌های امنیت شخص ثالث، سازگار با آن رویه‌ها در سازمان باشد.

شخص ثالث می‌تواند یا:

- درخصوص بایگانی اسناد الکترونیکی (پذیرش و ثبت همه اسناد الکترونیکی، ثبت عملیات بایگانی سند الکترونیکی و ذخیره‌سازی و فراداده‌های مرتبط) اطمینان ایجاد کند، تبدیل عملیات را انجام دهد، رویه‌های تکرار نسخه [1] را به کارگیرد، در خصوص دسترسی و بازگردانی اسناد، اطمینان ایجاد کند، یا:

- فقط مهرکردن‌های رقمی اسناد را ذخیره کند (پذیرش، بررسی‌ها و ثبت سند مرتبط با مهررقمی، ثبت عملیات)، در حالی که اسناد الکترونیکی ذخیره و نگهداری شده مطابق با این امضاها، تحت مسئولیت سازمان مشتری (مؤسس) باقی می‌ماند.

در هر دو مورد، شخص ثالث باید تأیید انطباق فعالیت‌های خود را ایجاد کند. نوع و تعداد انتقال این تأیید انطباق‌ها از شخص ثالث به مشتری (مبدأ) باید در قرارداد شخص ثالث تعیین شود.
شخص ثالث باید، نسخه‌هایی از این تأیید انطباق‌ها را در انطباق با مشخصات این استاندارد، نگهداری کند.
علاوه بر اجرای سامانه اطلاعات سازگار با این استاندارد، شخص ثالث باید:

۱- از شناسایی منحصر به فرد و موثق برای هریک از مشتریان خود اطمینان حاصل کند؛

۲- محرمانگی اسناد و فراداده‌های تحت حفاظت، به ویژه با استفاده از یک سامانه اطلاعات اجرا شده را ضمانت کند، به طوری‌که برای مشتری شخص ثالث ممکن نباشد که هیچگونه سند از دیگر مشتری شخص ثالث را بخواند، بنویسد، اصلاح یا حذف کند؛

۳- تأییدانطباق‌های هم‌نمایه را برای هرگونه عملیات ارائه دهد؛

۴- حذف‌همه سندها را بعد از آگاه‌سازی انجام دهد، و به طور کامل، تأیید انطباق‌های مناسب را ارائه دهد.

۵- یک خط‌سیر ممیزی چرخه عمر بایگانی، برای هر مشتری فراهم کند به طوری که مشتری بتواند آن را به عنوان مدرکی در مواقع اختلاف، ارائه دهد.

تبادل داده بین سازمان و شخص ثالث باید با استفاده از وسایلی چون، سندیت محکم، رمزدارکردن و کنترل تمامیت حفظ شود. شخص ثالث باید تعهد کند که هیچ‌گونه تحلیل و یا پردازشی (به طور مثال: تبدیل قالب)

---

1 - Replication

از اسناد الکترونیکی تحت حفاظت خود انجام نمی‌دهد مگر این که تقاضای شفافی از سوی مشتری وی (مبدأ) صورت گرفته باشد.
به دلایل محرمانگی، رمزدارکردن اولیه اسناد و فراداده‌ها، اگر مناسب باشد، می‌تواند توسط سازمان ضروری انگاشته شود. در این مورد، شرایط جستجو برای دسترسی به اسناد ممکن است محدود شود.

۱۳-۲ مدل قرارداد خدمت

۱۳-۲-۱ قرارداد خدمت

موارد زیر باید در قرارداد خدمت با هر ارائه دهنده خدمات بایگانی شخص ثالث معتمد، پوشش داده شود:
الف- رجوع به این استاندارد همراه با مشخصات الزامات پوشش داده شده؛
ب- رجوع به خط مشی بایگانی؛
پ- توصیف رویه‌های بایگانی؛
ت- توصیف ساختار سامانه اطلاعات؛
ث- رویه‌های برای دسترسی به جداول عملیات سامانه اطلاعات؛
ج- شیوه‌های مورد استفاده توسط شخص ثالث برای اطمینان از محرمانگی داده‌های سازمان؛
چ- روش‌ها و وسایل مورد استفاده برای هم‌نمایه‌کردن اسناد الکترونیکی و فراداده‌های آن‌ها توسط مشتری؛
ح- روش‌ها و وسایل درنظرگرفته‌شده برای اطمینان از تبدیل قالب، اگر کاربرد داشته باشد؛
خ- روش‌های اجرایی انتقال (انتقال فیزیکی)، اگر کاربرد داشته باشد؛
د- خط مشی‌های بیمه قرارداد بسته شده توسط شخص ثالث، که پوشش دهنده هرگونه خطرات مرتبط با فعالیت است.
اگرچه شروط قراداد خدمت ، بدون محدودیت، بین اشخاص ثبت می‌شوند، محتوای بندهای۱۳-۲-۲ تا ۱۳-۲-۱۳ باید پوشش داده شود.

۱۳-۲-۲ مدت قراداد خدمت

مدت قرارداد با شخص ثالث، به همراه شرایط فسخ و تجدید قرارداد، باید تعیین شود.

۱۳-۲-۳ دوره نگهداری

شخص ثالث در دوره نگهداری تعیین شده و تا جایی‌که روابط قرادادی ادامه‌دار اجازه می‌دهد باید متعهد به برنامه‌کاربردی بشود. شخص ثالث باید قادرباشد تا یک ظرفیت توانایی فنی و قراردادی برای بازگردانی و قابلیت تبادل راه‌حل‌های آن نشان دهد، به منظور این که از حفاظت از اسناد برای دوره توافق شده، اطمینان یابد.

۱۳-۲-۴ کیفیت خدمت

شخص ثالث باید متعهد به سطح معینی از کیفیت خدمت و پشتیبانی مشتری شود. این تعهد بستگی به سطح قابلیت دسترسی برای هم‌نمایه‌کردن و دسترسی به بایگانی‌ها دارد، و هنگامی که شرایط قراردادی محقق نشود، احتمالاً با جریمه همراه خواهد بود.

۱۳-۲-۵ امنیت و حفاظت از داده‌ها

شخص ثالث باید:

الف- همه اسناد الکترونیکی محرمانه توسط مشتری (مؤسس) و تحت حفاظت را برای دوره قرارداد و در شکل و قالب‌های توافق شده، نگهداری کند؛

ب- امنیت و تمامیت اسناد الکترونیکی شده را ضمانت کند؛

پ- متعهد به انجام همه انتقال‌های رسانه‌ای شود که ممکن است برای اطمینان از خوانایی اسناد الکترونیکی نیاز باشد؛

ت- یک خدمت دسترسی ایمن به همه اشیاء تحت حفاظت ارائه کند؛

ث- یک خط‌سیر ممیزی از همه عملیات مرتبط با اجرای خدمات تعیین شده در قراداد را نگهداری نماید؛

ج- امنیت و تمامیت چرخه عمر بایگانی و گزارش رویدادها را ضمانت کند.

۱۳-۲-۶ اطلاعات و مشاوره[1]

شخص ثالث باید به مشتری خود در مورد نیاز به حفظ سازگاری بین سامانه‌های اطلاعات خود مشتریان و اشیائی که تحت حفاظت از طرف مشتری، نگه داشته می‌شود، اطلاع دهد. ممکن است نیاز باشد شخص ثالث خدمات اضافه‌تری را برای رسیدگی به این موارد پیشنهاد دهد.
شخص ثالث باید هرگونه عملیات تبدیل یا تغییرات فنی در سامانه اطلاعات مورد استفاده و هرگونه تأثیری که ممکن است بر قابلیت دسترسی یا سازگاری با سخت افزار مشتری، یا با تبادل، یا نگهداری از داده‌های تحت حفاظت داشته باشد را، به مشتری اعلان کند.

۱۳-۲-۷ انتقال و استمرار

اگر اسناد الکترونیکی تحت حفاظت یک مشتری، به شخص ثالث دیگری انتقال داده شود، این مجموعه باید بتواند اطمینان دهد، که اسناد هم در طی انتقال و هم بعد از عمل انتقال، خصوصیات اصلی خود را حفظ می‌کنند. این بدین معنی است که:

- شخص ثالث باید تمامیت و انتقال کامل همه بایگانی‌ها و همه داده‌های مرتبطی که تحت حفاظت نگه می‌دارد را، حفظ کند.

---

1 - Counsel

- در همه موقعیت‌ها، شخص ثالث باید اطلاعات و داده های فنی را به روشی نگه‌داری کند که مشتری آن شخص، یا هر طرفی که توسط مشتری منصوب شده باشد، بتواند آن اطلاعات را بازیابی کند و بدین ترتیب، این‌کار را در یک دوره زمانی مطلوب ، انجام دهد.

۱۳-۲-۸ قابلیت انتقال[1]

در هنگام پایان قرارداد، یا اگر شخص ثالث عملیات را متوقف کند، شخص ثالث باید قادر باشد تا همه اسناد الکترونیکی و عناصر مربوطه را به طور کامل و در شرایط فنی مشابه با زمان دریافت در سامانه اطلاعات، بازگرداند. شخص ثالث نباید از اسناد بازگردانی شده، نگهداری و نسخه‌برداری کند.
بازگردانی گزارش رویدادها یا خط‌سیرهای ممیزی باید تعیین شود.
شرایط این انتقال باید به مشتری اجازه دهد، با انتفاع از یک ضمانت قراردادی که طی آن، خدمت بیرونی می‌تواند به شخص ثالث دیگری انتقال داده شده یا به سامانه اطلاعات داخلی برگردانده شود، استقلال خود را درخصوص شخص ثالث حفظ کند.
این تدارک باید حداقل موارد زیر را شامل شود:
الف- استفاده شخص ثالث از استاندارد بازاری و وضعیت ابزارهای فنی هنری (معماری، سخت افزار و نرم افزار، قرارداد، پروتکل و ...)؛
ب- سازماندهی انتقال اسناد به مشتری داخلی سامانه اطلاعات (بازگرداندن) یا به شخص ثالث دیگر؛
پ- ذخیره‌سازی اطلاعات و داده‌های فنی، به‌طوری‌که قابل بازیافت در یک مکان یا از طریقی‌که قابل دسترسی توسط مشتری سیستم یا هر طرفی که توسط مشتری تعیین شده است، باشد[2]؛
ت- هزینه برگشت‌پذیری؛
ث- زمان لازم برای انجام همه عملیات برگشت پذیری از زمان درخواست؛
ج- نگهداری منظم از همه عناصر مرتبط با برگشت‌پذیری.

۱۳-۲-۹ بازگردانی[3]

در پایان تعهدات نگهداری طی قرارداد، شخص باید متعهد به بازگرداندن همه بایگانی‌ها به مشتری خود باشد و نباید هیچ‌نسخه‌ای از آن‌ها را نگه‌داری کند. با این وجود، اگر به طور ویژه، مشتری بخواهد، نگهداری از بایگانی‌ها می تواند توسط شخص ثالث برای یک دوره اضافه‌تر تمدید شود.

۱۳-۲-۱۰ داده های خصوصی و محرمانگی

شخص ثالث باید رازداری نسبت به اطلاعاتی که نزد وی به امانت سپرده شده و هرگونه اطلاعات دیگری که ممکن است در طی روابط قراردادی وی با مشتریانش، مشهود شده باشد را ضمانت کند.

---

1 - Transferability
2 - Recovery
3 - Restitution

این اطلاعات می تواند از دسترسی به اسناد یا از عملیات بر روی اسنادی که تحت حفاظت نگه‌داری شده، یا از دانشی که درباره سامانه اطلاعات سازمان، خواه این دانش ناشی از مشاهدات خودش باشد یا توسط مشتری وی تأمین شده باشد، به دست آید.

شخص ثالث باید همه معیارهای ضروری برای اطمینان از محرمانگی اطلاعاتی که وی در طی فعالیت‌های مربوط به عملیات‌نگهداری بدست می‌آورد را در نظر بگیرد.

چنین اطلاعاتی فقط باید به اشخاصی که از طرف مشتری منصوب شده‌اند، انتقال داده شود، به استثنای موقعیت‌هایی که از نظر قانونی، انتقال این اطلاعات به شخص دیگری الزامی باشد.

۱۳-۲-۱۱ بیمه حرفه‌ای[1]

شخص ثالث باید قرارداد بیمه‌ای داشته باشد که همه خطرات مرتبط با مسئولیت مدنی[2] وی را پوشش دهد. این بیمه باید یک ضمانت مالی به نسبت سطح تعهدات، ارائه دهد.
شخص ثالث باید این بیمه را تا زمانی که قرارداد خدمت کاربرد دارد، حفظ کند.
شخص ثالث ممکن است به دنبال بیمه اضافه‌تر برای حفاظت در برابر خرابی سامانه اطلاعات باشد.

۱۳-۲-۱۲ پیمان‌کار فرعی[3]

هنگامی که شخص ثالث طرح‌ریزی کند تا از خدمات پیمان‌کار فرعی استفاده کند، باید به کارفرما اطلاع دهد. در این مورد، مسئولیت شخص ثالث برای خدمات ارائه شده به مشتری باقی می‌ماند.

۱۳-۲-۱۳ ارزیابی

ضوابط مرتبط با ممیزی‌های ارزیابی باید مطابق با این استاندارد باشد (به بند ۱۲ رجوع شود).

۱۴ ارائه دهندگان خدمت

۱۴-۱ کلیات

این بند به راه‌حل‌های بایگانی، برای مواردی که ارائه بعضی خدمات توسط پیمان‌کاران فرعی به غیر از طرف های ثالث ، انجام می شود، می‌پردازد. در پیوست پ، اصولی را برای شرایط عمومی خدمت پیشنهاد شده، شده است.
سازمان اجراکننده خدمات سامانه اطلاعات، مسئول کل سامانه باقی می‌ماند و باید اطمینان یابد که همه خدمات ارائه شده توسط پیمان‌کاران فرعی، مطابق با این استاندارد و براساس حقوقی است که آن‌ها عهده‌دار شده‌اند.

1- Professional insurance
2 - Civil liability
3- Subcontracting

سند مشخصات که تعریف‌کننده الزامات است باید توسط شخص مجاز به پیمان‌کار فرعی منتخب داده شود. پیمان کار فرعی باید این به مشخصات متهد باشد.
رویه‌ها و عملیات اجراشده توسط پیمان‌کار فرعی باید به طور منظم کنترل شده و بر یک مبنای منظم بازرسی شود.

۱۴-۲ موافقت‌نامه پیمان‌کار فرعی

قبل از به کارگیری خدمات پیمان کار فرعی، موارد زیر باید تأیید شود:
- پیمان‌کار فرعی قادر باشد تا الزامات این استاندارد را برای خدماتی که ارائه می‌شود، برآورده کند؛
- رویه‌های پیمان‌کار فرعی مطابق با خط مشی بایگانی سازمان مؤسس باشد؛
- داده‌های خط‌سیر ممیزی ایجادشده توسط پیمان‌کار فرعی، قابل استفاده برروی سامانه اطلاعات سازمان مؤسس باشد؛
- خط مشی‌های امنیتی پیمان‌کار فرعی سازگار با خط مشی‌های امنیتی سازمان مؤسس باشد.

۱۴-۳ قرارداد با پیمان‌کار فرعی

قرارداد باید حداقل اطلاعات زیر را شامل شود:

الف- رجوع به این استاندارد ملی؛

ب- توصیف رویه‌های مورد استفاده؛

پ- توصیف ساختار مورد استفاده در ارتباط با خدمات ارائه شده؛

ت- معیار مورد استفاده برای کنترل کیفیت؛

ث- دسترسی به گزارش رویدادهای سامانه اطلاعات پیمان‌کار فرعی؛

ج- اقدامات درنظر گرفته شده برای اطمینان از محرمانگی و امنیت داده‌های تحت حفاظت[1]؛

چ- فنون و رسانه مورد استفاده برای انتقال اسناد الکترونیکی و فراداده‌های مرتبط بین سازمان مؤسس و پیمان‌کار فرعی؛

ح) فنون مورد استفاده برای تبدیل قالب، اگر کاربرد داشته باشد؛

خ) شرایط برای انتقال سند، اگر کاربرد داشته باشد؛

د) خط‌مشی‌بیمه پیمان‌کار فرعی که پوشش دهنده صدمات مرتبط با کار مرتبط است.

۱۴-۴ انتقال داده در سرتاسر شبکه‌های مخابراتی

1 - Custody

هنگامی که از شبکه‌های باز برای انتقال سند بین مالک و پیمان‌کار فرعی استفاده می‌شود، شیوه‌های مناسب برای سندیت، تمامیت و محرمانگی داده‌ها باید مورد استفاده قرار گیرد.

پیوست الف

(اطلاعاتی)

خط مشی بایگانی

یک خط مشی بایگانی، شرایط امنیتی، فنی، عملیاتی، عملکردی و قانونی الزامات را برای یک سامانه اطلاعات داخلی یا بیرونی، که شامل مقاصد، اهداف و تعهدات سامانه است، توصیف می‌کند.

خط مشی باید جزئیات زیر را تعیین کند:

الف) خدمات ارائه شده به هم‌نمایه‌کنندگان یا کاربران برای هم‌نمایه‌کردن یا بازگردانی یک بایگانی، شامل محدوده خدمات، سطح خدمت، انواع بایگانی، قالب‌های سند الکترونیکی، شرایط انتقال، حجم انتقال، تکرار هم‌نمایه‌سازی‌ها و از این قبیل.

ب) تعهدات الزام‌آور برای همه طرف‌ها، در وهله نخست در مورد خود خدمات بایگانی به تنهایی. تعهدات در خصوص طرف‌های دیگر باید حداقل الزامات را برای اجرای خدمات بایگانی که مطابق با خط مشی بایگانی است، نشان دهد.

پ) ویژگی‌های عملیات اجرا شده به منظور ارائه این خدمات (انبارش، ذخیره‌سازی و ...) و سازماندهی عملیات مرتبط (ارتباط بین عملیات، تبدیل داده و ...).

ت) قواعد کاربردی امنیت براساس هر سطح از خدمت و وظیفه، برمبنای شرایط سازمانی، فنی و عملی.

یک خط مشی بایگانی، بالاتر از چارچوب عملکرد کلی است، و بنابراین، باید مستقل از فنون خاص مورد استفاده برای اهداف اجرایی عملیات خاص باشد.

یک خط مشی بایگانی، سندی است که به همه طرف‌های درگیر (اعم از داخلی یا بیرونی نسبت به خدمت)، توصیف شفافی از تعهدات خدمت بایگانی را ارائه می‌دهد. این عمل موجب ملاحظات عملی برای اجرا و تحویل، شامل موارد زیر خواهد شد:

- هم‌نمایه‌سازی بایگانی؛
- شناسایی و سندیت منبع بایگانی؛
- دسترس‌پذیری بایگانی؛
- بازیابی و نمایش بایگانی‌ها؛
- بازگردانی بایگانی‌ها؛
- تمامیت بایگانی‌ها؛
- خوانایی بایگانی‌ها؛
- نگهداری طولانی مدت از بایگانی‌ها؛

- قابلیت ردیابی عملیات هم‌نمایه‌سازی، بازگردانی و امحاء؛
- ایجاد تأیید انطباق‌ها؛
- تداوم کسب‌وکار و یا جبران فاجعه ناشی از عوامل غیرمترقبه یا از روی بدخواهی؛
- انهدام داوطلبانه بایگانی.

پیوست ب

(اطلاعاتی)

اعلانیه شیوه‌های بایگانی

یک اعلانیه از شیوه‌های بایگانی، فنون و فرایندهای مورد استفاده برای برآورده‌کردن اهداف امنیتی خط‌مشی بایگانی را توضیح می‌دهد.

یک اعلانیه خط‌مشی بایگانی، باید توصیف کند که چطور خدمت بایگانی سازمان، و یا ارائه‌دهنده خدمت بایگانی شخص ثالث، الزامات خط مشی بایگانی در ارتباط با جنبه‌های محیطی، مواد، فرایندها، عملیات و فنی را برآورده می‌کند.

یک اعلانیه خط مشی بایگانی، باید موارد زیر را توصیف کند:

- فرایندهای عملیاتی خدمت بایگانی اجرا شده، و
- قواعد امنیتی توصیف شده در خط‌مشی بایگانی، برحسب مشخصه‌های امنیتی عملیاتی درخصوص اجزای گوناگون خدمت بایگانی و کارهایی که برای اجرای این مشخصه‌ها مورد نیاز است.

این استانداردها و قواعد، باید به طور شفاف در اعلانیه خط مشی بایگانی، توصیف شوند به ویژه اگر، به تنهایی، مختص خط‌مشی بایگانی باشند. این اعلانیه، درصورت مناسب‌بودن، می‌تواند به خط‌مشی امنیتی عمومی‌تر سند که پوشش‌دهنده سامانه اطلاعات است، اشاره کند.

اعلانیه شیوه بایگانی، باید حداقل شامل توصیف کامل و جامعی از شیوه‌ها باشد، و باید ارتباط بین قواعد توصیف شده در خط‌مشی بایگانی که اعلانیه به آن اشاره می‌کند و با استانداردها و شیوه‌های عملیاتی، را برقرار کند.

در حالی که یک خط‌مشی بایگانی مستقل از جنبه‌های خاص محیط عملیاتی یک سامانه اطلاعات، ایجاد می شود، یک اعلانیه شیوه بایگانی، با توجه به ساختار سازمان، فرایندهای عملیاتی و محیط فیزیکی خدمت بایگانی سازمان یا ارائه دهنده خدمت بایگانی شخص ثالث، نوشته می شود.

یک اعلانیه شیوه بایگانی، همیشه توسط تأمین‌کننده خدمت، یعنی خدمت بایگانی سازمان یا شخص ثالث ارائه‌دهنده خدمت بایگانی، ارائه می‌شود.

یک اعلانیه شیوه بایگانی، دراصل، یک سند داخلی محرمانه درخصوص فقط خدمت بایگانی است. با این وجود، برای تکمیل خط‌مشی بایگانی، یک خدمت بایگانی می‌تواند خلاصه‌ای از بیانیه خط‌مشی بایگانی خود را انتشار دهد.

یک اعلانیه شیوه بایگانی، توصیف می‌کند که چطور خدمت بایگانی سازمان یا ارائه‌دهنده خدمت شخص ثالث، قادر است وظایف خود را به طور رضایت‌بخش اجرا کند. این کار به ویژه، در طی هر ارزیابی مفید است به طوری که کار ممیز را تسهیل کرده و زمان ممیزی را کاهش می‌دهد.

پیوست پ

(اطلاعاتی)

شرایط کلی خدمت

کاربران خدمات بایگانی، ممکن است فقط به خط مشی بایگانی سازمان دسترسی داشته باشند. بدین دلیل ممکن است برای این کاربران مشکل باشد، تا اطلاعات را تفسیر کنند.

براین اساس به نظر می رسد، مفید باشد تا به کاربران یک سند مکمل ساده شده‌ای ارائه دهیم که بتواند به آن‌ها در شفاف‌سازی و فهم اطلاعات ضروری که به منظور تصمیم‌گیری در مورد موضوعات اعلان‌شده‌ی در حال تحقیق، نیاز دارند، کمک کند.

شرایط کلی خدمت باید شامل ارجاعاتی به دستورالعمل دردسترس کاربر باشد. به منظور حفظ شفافیت و خوانایی، این دستورالعمل‌ها باید فقط وظایفی را توصیف کنند که برای عملیات پشتیبانی ضروری است، هرچند اگر مفید به نظر بیاید، آن‌ها می توانند به دستورالعمل‌های کلی‌تری نیز ارجاع دهند.

خدمات بایگانی سازمان و یا شخص ثالث ارائه‌دهنده خدمت بایگانی، باید شرایط کلی خدمت خود را در دسترس کاربران قرار دهد.