INSO
20342
1st.Edition
2016

جمهوری اسلامی ایران
Islamic Republic of Iran
سازمان ملی استاندارد ایران
Iranian National Standardization Organization

استاندارد ملی ایران
۲۰۳۴۲
چاپ اول
۱۳۹۴

حفاظت داده‌ها- سامانهٔ مدیریت اطلاعات شخصی

Data protection – Personal information management system

ICS: 01.140.30; 03.100.99; 35.020

به نام خدا

آشنایی با سازمان ملی استاندارد ایران

مؤسسهٔ استاندارد و تحقیقات صنعتی ایران به موجب بند یک مادهٔ ۳ 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 حوزه‌های مختلف در کمیسیون‌های فنی مرکب از کارشناسان سازمان، صاحب نظران مراکز و مؤسسات علمی، پژوهشی، تولیدی و اقتصادی آگاه و مرتبط انجام می‌شود و کوششی همگام با مصالح ملی و با توجه به شرایط تولیدی، فنّاوری 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، 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 تعیین شده 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 بین المللی استاندارد (ISO)[1]،کمیسیون بین المللی الکتروتکنیک (IEC)[2] و سازمان بین‌المللی اندازه شناسی 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 پیش‌بینی شده در قانون، برای حمایت از مصرف کنندگان، حفظ سلامت و ایمنی فردی و عمومی، حصول اطمینان از کیفیت محصولات و ملاحظات زیست‌محیطی 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 درجه-بندی 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 نظام 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

«حفاظت داده‌ها-سامانهٔ مدیریت اطلاعات شخصی»

رئیس:	**سمت و/یا نمایندگی**
قیصری، تقی (فوق‌لیسانس مهندسی‌مکانیک)	شرکت خدمات فنی و مهندسی سرمد
دبیر:	
معین، فروزان (فوق‌لیسانس روابط بین‌الملل)	ادارهٔ استاندارد مراغه
اعضاء: (اسامی به ترتیب حروف الفبا)	
آل‌احمدی، ام‌البنین (فوق‌لیسانس شیمی‌تجزیه)	انجمن صنفی مدیران کنترل کیفی و مسئولین فنی صنایع استان آذربایجان شرقی
اسماعیل‌پور، شاهرخ (فوق‌لیسانس مدیریت اجرایی)	ادارهٔ کل استاندارد استان آذربایجان شرقی
بحری‌لاله، سپیده (فوق‌لیسانس فنّاوری اطلاعات)	ادارهٔ کل استاندارد استان آذربایجان شرقی
بدرزاده، فریبا (فوق‌لیسانس کامپیوتر، شبکه)	ادارهٔ کل استاندارد استان آذربایجان شرقی
تفسیری، حامد (لیسانس کامپیوتر، سخت‌افزار)	شرکت پگاسوس
جاودانی، بهاره (فوق‌لیسانس مهندسی الکترونیک)	شرکت معیار آزمای ارس
حسین‌زاده، ملیحه (دکترای پزشکی)	شرکت اسلوب آفرینان آریا آذربایجان

رضوی، محمدباقر (لیسانس حقوق)	ادارۀ کل استاندارد استان آذربایجان‌شرقی
سالک‌زمانی، لیلا (فوق‌لیسانس زبان و ادبیات فرانسه)	کارشناس استاندارد
سالک‌زمانی، مریم (فوق‌لیسانس علوم تغذیه)	ادارۀ کل استاندارد استان آذربایجان‌شرقی
وظیفه‌خورانی، بهروز (فوق‌لیسانس مدیریت صنعتی)	ادارۀ کل استاندارد استان آذربایجان‌شرقی
ولی‌پور، جواد (دکترای شیمی‌تجزیه)	دانشگاه صنعتی سهند

فهرست مندرجات

عنوان	ادامهٔ فهرست مندرجات	صفحه

پیش گفتار

استاندارد «حفاظت داده‌ها-سامانهٔ مدیریت اطلاعات شخصی» که پیش‌نویس آن در کمیسیون‌های فنی مربوط توسط سازمان ملی استاندارد ایران مربوط تهیه و تدوین شده است و در صدوشصت‌وهشتمین اجلاسیهٔ کمیته ملی استاندارد اسناد و تجهیزات اداری و آموزشی مورخ ۱۳۹۴/۱۰/۱۶ مورد تصویب قرار گرفته است، اینک به استناد بند یک ماده ۳ قانون اصلاح قوانین و مقررات موسسه 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 زمینهٔ صنایع، علوم و خدمات، استانداردهای ملی ایران در مواقع لزوم تجدید نظر خواهد شد و هر پیشنهادی که برای اصلاح و تکمیل این استانداردها ارائه شود، هنگام تجدیدنظر در کمیسیون فنی مربوط مورد توجه قرار خواهد گرفت. بنابراین، باید همواره از آخرین تجدیدنظر استانداردهای ملی استفاده کرد.

منبع و ماخذی که برای تهیه این استاندارد مورد استفاده قرار گرفته به شرح زیر است:

BS 10012:2009, Data protection –Specification for a personal information management system

مقدمه

۰-۱ سامانهٔ مدیریت اطلاعات شخصی (PIMS)[1]

هدف از تدوین این استاندارد، قادر ساختن سازمان‌ها به قرار دادن PIMS، به‌عنوان بخشی از زیرساخت کلی آمریت[2] اطلاعات‌شان است تا چارچوبی را برای حفظ و بهبود انطباق با قانون حفاظت داده‌ها[3] و به‌آموخت‌ها[4] فراهم کند.

یادآوری-در حال حاضر، «قانون جرائم رایانه‌ای»، مصوب ۱۳۸۸/۳/۵ مجلس شورای اسلامی، مرتبط‌ترین قانون حفاظت داده‌ها در کشور است. لایحهٔ مالکیت فکری که در سال ۹۳ از سوی دولت به مجلس شورای اسلامی تقدیم شده است، هنوز به تصویب نرسیده است. ازاین‌رو، لازم است در صورت تصویب و ابلاغ «قانون حفاظت داده‌ها» چه به صورت مستقل و چه در بطن سایر قوانین مصوب، به آن قوانین استناد شود.

۰-۲ اصول حفاظت داده‌ها

در حفاظت داده‌ها پیروی از اصول حفاظت هفت‌گانهٔ زیر لازم است:

اصل اول: پردازش عادلانه و قانونمند؛

اصل دوم: به‌دست آمده تنها برای اهداف مشخص‌شده و خودداری از پردازش بعدی به شیوه‌ای ناسازگار با آن اهداف؛

اصل سوم: کافی، مرتبط و به‌اندازهٔ لازم؛

اصل چهارم: دقیق و روزآمد؛

اصل پنجم: نگهداری نکردن بیش‌تر از مدت زمان ضروری؛

اصل ششم: پردازش همسو با حقوق تعریف‌شدهٔ قانونی برای افراد، از جمله حق دسترسی آنها؛

اصل هفتم: نگه‌داشت امن؛

اصل هشتم: انتقال ندادن به کشورهای خارج از جمهوری اسلامی ایران، بدون حفاظت کافی.

استثنائاتی از این اصول در موارد زیر، مجاز دانسته می‌شود:

- مستثنی بودن از اصول عدم افشا؛
- مستثنی بودن از مقرره‌های راجع به اطلاعات اشخاص؛
- مستثنی بودن از پردازش برای اهداف تاریخی و/یا تحقیقاتی؛
- استثنائات متفرقه، مانند سوابق و مراجع تحصیلی و کاری محرمانه و اوراق امتحانی[5].

۰-۳ اطلاع‌رسانی

جز در موارد استثنائی، سازمان‌ها باید در مورد پردازش اطلاعات برای حصول اطمینان از جریان آزاد[6] اطلاعات، اطلاع‌رسانی کنند.

1-Personal information management system
2-Governance
3-Data protection legislation
4-Good practice
5-Exam scripts
6-Openness

حفاظت داده‌ها-سامانهٔ مدیریت اطلاعات شخصی

۱ هدف و دامنه کاربرد

هدف از تدوین این استاندارد، تعیین الزاماتی برای سامانهٔ مدیریت اطلاعات شخصی (PIMS) است که چارچوبی را برای حفظ و بهبود انطباق با قوانین حفاظت داده‌ها و به‌آموخت‌ها فراهم می‌کند.

یادآوری- در این استاندارد، چرخهٔ «برنامه‌ریزی، اجرا، بررسی، اقدام اصلاحی (PDCA)[1] » کاربرد دارد. برای آگاهی‌های بیشتر به پیوست اطلاعاتی الف مراجعه شود.

این استاندارد، برای همهٔ سازمان‌ها صرف نظر از اندازه و زمینهٔ فعالیت‌ای که دارند، کاربرد دارد. این استاندارد، در سازمان‌هایی با مسئولیت آغاز، اجرا و حفظ PIMS قابل به‌کارگیری است. این استاندارد زمینهٔ مشترکی را برای مدیریت اطلاعات شخصی، برای اعتمادآفرینی در خصوص مدیریت آنها، و برای امکان‌پذیر کردن ارزیابی اثربخش انطباق با قانون حفاظت داده‌ها و به‌آموخت‌ها توسط ارزیابان درون‌سازمانی و برون‌سازمانی، هر دو، فراهم می‌آورد.

۲ اصطلاحات وتعاریف

در این استاندارد، اصطلاحات و تعاریف زیر به کار می‌رود.

۲-۱

ممیزی

بررسی نظام‌مند برای تعیین این که فعالیت‌ها و نتایجِ مرتبط، مطابق با ترتیبات برنامه‌ریزی‌شده هستند یا نه و این که ترتیبات یادشده به طور اثربخشی اجرا می‌شوند یا نه و برای دستیابی به خط‌مشی و اهداف سازمان، مناسب هستند یا نه.

یادآوری- ممیزی می‌تواند برای بازنگری مدیریتی و دیگر مقاصد درون‌سازمانی، توسط خود سازمان، یا از جانب آن، انجام شود.

۲-۲

شخص

فردی که اطلاعات شخصی مربوط به اوست.

۲-۳

سامانهٔ مدیریتی

سامانهٔ مدیریتی، سامانه‌ای است برای تعیین خط‌مشی و اهداف و دستیابی به آن اهداف.

۲-۴

عدم انطباق

برآورده نشدن الزام، عدم انطباق نامیده می‌شود.

1-Plan-Do-Check-Act

۵-۲

سازمان

شخصیت حقوقی[1] که اطلاعات را پردازش می‌کند.

مثال: اشخاص حقیقی، تجار منفرد، شرکت‌ها، شراکت‌ها، شرکت‌های سهامی، شرکت‌های بخش عمومی، انجمن‌های داوطلبانه و خیریه.

۶-۲

اطلاعات شخصی

داده‌های شخصی مربوط به یک شخص زندهٔ دارای هویت، اطلاعات شخصی نامیده می‌شود.

۷-۲

خط‌مشی مدیریت اطلاعات شخصی

بیانیه‌ای از مقاصد و جهت‌گیری کلی سازمان که به‌طور رسمی توسط مدیریت ارشد برای حفظ و بهبود انطباق با قانون حفاظت داده‌ها و به‌آموخت‌ها تصویب شده است.

یادآوری- در ادامهٔ متن استاندارد، صرفا از واژهٔ خط‌مشی استفاده شده است.

۸-۲

سامانهٔ مدیریت اطلاعات شخصی

PIMS

بخشی از چارچوب کلی مدیریتی که برای تعیین، پیاده‌سازی، بهره‌برداری، پایش، بازنگری، و بهبود مدیریت اطلاعات شخصی به کار می‌رود.

۹-۲

روش اجرایی/شیوه‌نامه

مجموعهٔ مدونی از اقداماتی که شیوه‌ای رسمی یا پذیرفته‌شده برای انجام کاری هستند.

۱۰-۲

فرآیند

مجموعه اقداماتی که به منظور دستیابی به نتیجهٔ معین انجام می‌شود.

۱۱-۲

پردازش

کسب، ثبت یا نگه‌داشت اطلاعات شخصی یا انجام یک یا مجموعه‌ای از عملیات بر روی اطلاعات شخصی، پردازش نامیده می‌شود.

1-Legal entity

یادآوری- پردازش شامل جمع‌آوری، سازمان‌دهی، تنظیم[1]، تغییر، افشا، به‌اشتراک‌گذاری، انتشار، تطبیق[2]، ترکیب، توقیف[3]، پاک کردن و امحای[4] اطلاعات شخصی است.

۱۲-۲

اطلاعات شخصی حساس

منظور، اطلاعات فردی مربوط به موارد زیر است:

الف- منشاء نژادی یا قومی؛

ب- عقاید سیاسی؛

پ- اعتقادات مذهبی یا سایر؛

ت- عضویت در اتحادیهٔ صنفی؛

ث- سلامت یا بیماری فیزیکی یا روانی؛

ج – زندگی خانوادگی؛

چ–ارتکاب یا اتهام ارتکاب هر گونه جرم، از جمله سوابق رسیدگی قضایی، فیصلهٔ دعوی یا محکومیت دادگاهی در فرآیند چنین رسیدگی‌هایی به هر جرم مرتکب‌شده یا ادعای ارتکاب جرم توسط فرد.

۱۳-۲

سامانه

مجموعه‌ای از عناصر که دارای ارتباط درونی یا تعامل است.

۱۴-۲

کارکنان

افرادی که تحت کنترل سازمان به کار مشغول‌اند.

مثال: کارمندان، کارکنان موقتی، پیمان‌کاران، داوطلبان و مشاوران.

۳ طرح‌ریزی برای سامانهٔ اطلاعات شخصی

هدف، طرح‌ریزی برای اجرای سامانهٔ مدیریت اطلاعات شخصی است که هدایت و پشتیبانی از انطباق با قانون حفاظت داده‌ها و به‌آموخت‌ها را فراهم می‌کند.

۳-۱ ایجاد و مدیریت PIMS

سازمان باید PIMS مدونی را مطابق با بندهای ۳-۲ تا ۳-۷ ایجاد کند، پیاده‌سازی کند، برقرار نگه دارد و به طور مداوم بهبود بخشد.

۳-۲ دامنهٔ کاربرد و اهداف PIMS

سازمان باید دامنهٔ کاربرد PIMS را تعریف و اهداف مدیریت اطلاعات شخصی را با توجه به موارد زیر تعیین کند:

1-Adapting
2-Aligning
3-Blocking
4-Destroying

الف- الزاماتِ مدیریت اطلاعات شخصی؛
ب- اهداف و تعهدات[1] سازمانی؛
پ- سطح ریسک قابل قبول در سازمان؛
ت- وظایف قابل اعمال قانونی، مقرراتی، قراردادی و/یا حرفه‌ای؛ و
ث- منافع افراد و سایر ذی‌نفعان[2] کلیدی.

۳-۳ خط‌مشی مدیریت اطلاعات شخصی

سازمان باید اطمینان حاصل کند که تیم مدیریت ارشد وظیفهٔ صدور و برقراری خط‌مشی را به انجام رسانده است، خط‌مشی‌ای که چارچوب شفافی را تعیین می‌کند و پشتیبانی از مدیریت انطباق با قانون حفظ داده‌ها و به‌آموخت‌ها و تعهد به آن را به اثبات می‌رساند.

یادآوری- مدیریت ارشد می‌تواند شامل هیأت‌امنا/ مدیران، مدیر ارشد و کارکنان رده بالا، شرکای سازمان یا مالک شرکت تجاری منفرد باشد.

خط‌مشی باید تبیین‌گر پوشش برای حوزه‌های زیر باشد:
الف- کل سازمان؛
ب- بخش مشخصی از آن.
خط‌مشی باید به همهٔ کارکنان ابلاغ شده باشد.

۴-۳ محتوای خط‌مشی

خط‌مشی باید تعهد سازمان را برای انطباق با قانون حفاظت داده‌ها و به‌آموخت‌ها، از جمله موارد زیر را بیان کند:
الف- پردازش اطلاعات شخصی فقط در مواردی که این کار به شدت برای اهداف مشروع سازمانی ضرورت دارد؛
ب- جمع‌آوری صرفا حداقل اطلاعات شخصی مورد نیاز برای این اهداف و خودداری از پردازش مازاد اطلاعات شخصی؛
پ- ارائهٔ اطلاعات روشن به افراد دربارهٔ چگونگی استفاده از اطلاعات شخصی آنها و این که توسط چه کسانی استفاده خواهد شد؛
ت- پردازش صِرف اطلاعات شخصی مربوط و کافی؛
ث- پردازش اطلاعات شخصی به‌طور عادلانه و قانونمند (به بند ۴-۷ مراجعه شود)؛
ج- حفظ موجودی مقوله‌هایی از اطلاعات شخصی پردازش‌شده توسط سازمان (به بند ۴-۲ مراجعه شود)؛
چ- نگه‌داشت اطلاعات شخصی دقیق و در صورت لزوم، روزآمد؛
ح- حفظ اطلاعات شخصی تنها تا زمانی که به دلایل قانونی یا اهداف مشروع سازمانی لازم است؛
خ- احترام به حقوق افراد در رابطه با اطلاعات شخصی آنها، از جمله حق دسترسی؛
د- نگه‌داشت امن همهٔ اطلاعات شخصی؛

1-Obligations
2-Stakeholders

ذ- انتقال اطلاعات شخصی به خارج از کشور تنها در شرایطی که از حفاظت کامل آنها اطمینان حاصل شده باشد؛

یادآوری- این استاندارد می‌تواند به مقیاس اتحادیه‌های اقتصادی و تجاری که کشور جمهوری اسلامی ایران عضوی از آنهاست تعمیم داده شود. در صورت اقتضا و در شرایطی که از این استاندارد در مقیاس اتحادیهٔ بین‌الممالک استفاده شود، هنگام استناد به مواد و مفادی از این استاندارد که به محدودهٔ کشوری اشاره شده است، واژهٔ «کشور» بایستی به واژهٔ «اتحادیه» تغییر داده شود.

ر- استفاده از استثنائات و معافیت‌های مختلف مجاز طبق قانون حفاظت داده‌ها؛

ز- تدوین و پیاده‌سازی PIMS برای امکان‌پذیر کردن پیاده‌سازی خط‌مشی؛

ژ- حسب اقتضا، مشخص کردن ذی‌نفعان درون‌سازمانی و برون‌سازمانی و میزان مشارکت این ذی‌نفعان در آمریت PIMS سازمانی؛ و

س- مشخص کردن کارکنان با مسئولیت و پاسخ‌گویی خاص برای PIMS (به بند ۳-۵ مراجعه شود).

۳-۵ مسئولیت و پاسخ‌گویی

یکی از اعضای تیم مدیریت ارشد باید پاسخ‌گوی مدیریت اطلاعات شخصی درون سازمان باشد تا از این رهگذر انطباق با قانون حفاظت داده‌ها و به‌آموخت‌ها بتواند اثبات شود (همچنین به بند ۴-۱-۱ مراجعه شود). چنین پاسخ‌گویی باید شامل موارد زیر باشد:

الف- تصویب خط‌مشی توسط تیم مدیریت ارشد؛

ب- تکوین و پیاده‌سازی PIMS برابر آن چه در خط‌مشی الزام شده است؛

پ- امنیت و مدیریت ریسک در ارتباط با انطباق با خط‌مشی (همچنین به بند ۴-۱۳-۱ مراجعه شود).

یک یا چند نفر از کارکنان واجد شرایط یا باتجربه باید برای عهده‌دار شدن مسئولیت بی‌وقفه و هرروزه برای انطباق سازمان با خط‌مشی منصوب شوند (همچنین به بند ۴-۱-۲ مراجعه شود).

همهٔ کارکنان از طریق پیاده‌سازی فرآیندها و روش‌های اجرایی سازمان، پای‌بندی به الزامات، به‌سازی مناسب کارکنان[1]، یا روش‌های اجرایی موجود برای پاسخ‌گویی به عدم انطباق‌ها موظف به رعایت خط‌مشی هستند.

۳-۶ تدارک منابع

سازمان باید منابع مورد نیاز را برای ایجاد، پیاده‌سازی، عمل و برقرار نگهداشتن PIMS تعیین و فراهم کند.

۳-۷ نهادینه‌سازی PIMS در فرهنگ سازمان

برای حصول اطمینان از اینکه مدیریت اطلاعات شخصی، بخشی از ارزش‌های اصلی سازمان و مدیریت اثربخش خواهد شد، سازمان باید:

الف- موجبات آگاهی همهٔ کارکنان را دربارهٔ PIMS از طریق آموزش مستمر و برنامه‌های آگاه‌سازی فراهم کند، آگاهی آنها را ارتقا دهد و حفظ کند؛

ب- فرآیندی را برای ارزیابی اثربخشی آگاه‌سازی از PIMS ایجاد کند؛

پ- اهمیت موارد زیر را به اطلاع همهٔ کارکنان برساند:

- برآورده کردن اهداف PIMS؛

1-Appropriate worker development

- انطباق با خط‌مشی؛
- بهبود مداوم خط‌مشی؛

ت- حصول اطمینان از این که همه کارکنان از این که چگونه آنها در دستیابی به اهداف PIMS مشارکت دارند، و همچنین از عواقب ناشی از عدم انطباق‌ها آگاه هستند.

۴ پیاده‌سازی و اجرای PIMS

۴-۱ انتصابات کلیدی

هدف از انتصابات کلیدی، حصول اطمینان از این امر است که سازمان کارکنان پاسخ‌گو و مسئول را طبق آن چه در خط‌مشی سازمان مشخص شده است، منصوب می‌کند.

۴-۱-۱ مدیریت ارشد

یکی از اعضای تیم مدیریت ارشد باید به عنوان پاسخ‌گو برای مدیریت اطلاعات شخصی در سازمان مشخص شود به طوری انطباق با قانون حفاظت داده‌ها و به‌آموخت‌ها بتواند قابل اثبات شود.

۴-۱-۲ مسئولیت هرروزه برای انطباق با خط‌مشی

یک یا چند نفر از کارکنان واجد شرایط یا با تجربه باید به عنوان مسئول انطباق با خط‌مشی به طور بی‌وقفه و هرروزه مشخص شوند. این مسئولیت را می‌توان، بسته به اندازه سازمان و ماهیت پردازش اطلاعات شخصی، به صورت تمام‌وقت یا پاره‌وقت تعیین کرد.

فرد (افراد) منصوب باید مسئولیت‌های زیر را عهده‌دار باشند:

الف- مسئولیت کلی برای انطباق با خط‌مشی؛

ب- تدوین و بازنگری خط‌مشی؛

پ- حصول اطمینان از پیاده‌سازی خط‌مشی؛

ت- بازنگری مدیریتیِ خط‌مشی (به بند ۵-۲ مراجعه شود)؛

ث- آموزش و آگاهی مستمر حسب آن‌چه در خط‌مشی الزام شده است (به بند ۴-۳ مراجعه شود)؛

ج- تصویب روش‌های اجرایی برای مواقعی که اطلاعات شخصی پردازش می‌شود، مانند:

- مدیریت و ابلاغ اعلامیه‌های حریم خصوصی[1] (به بند ۴-۷-۱ مراجعه شود)؛
- رسیدگی به درخواست‌های افراد (به بند ۴-۱۲-۱ مراجعه شود)؛
- جمع‌آوری و کار با اطلاعات شخصی (به بند ۴-۷-۱ مراجعه شود)؛
- رسیدگی به شکایت‌ها (به بند ۴-۱۲-۲ مراجعه شود)؛
- مدیریت حوادث امنیتی[2] (به بند ۴-۱۳-۶ مراجعه شود)؛
- برون‌سپاری و برون‌مرزسپاری[3](به بند ۴-۱۴ مراجعه شود)؛

چ- ارتباط با افرادی که مسئول مدیریت ریسک و موضوعات امنیتی در درون سازمان هستند (به بند ۴-۱۳ مراجعه شود)؛

1-Privacy notices
2-Security incidents
3-Off-shoring

ح- ارائهٔ مشاوره و راهنمایی در مورد مسائل حفاظت داده‌ها؛
خ- تفسیر و استفاده از استثنائات مختلف قابل اعمال برای پردازش اطلاعات شخصی (به مقدمه و بند ۴-۸-۱ مراجعه شود)؛
د- ارائهٔ مشاوره در رابطه با پروژه‌های به‌اشتراک‌گذاری داده‌ها (از جمله موضوعات امنیتی در مواقعی که داده‌ها خارج از محل فعالیت هستند) (به بند ۴-۸-۳ مراجعه شود)؛
ذ- حصول اطمینان از دسترسی سازمان به مدارک روزآمد قانونی و راهنماهای مناسب مربوط به قانون حفاظت داده‌ها (به بند ۴-۵ مراجعه شود)؛
ر- بررسی و مراقبت مداوم از این که PIMS مطابق تغییرات قوانین، آیین‌نامه‌ها، و فنّاوری روزآمد شده است (به بند ۴-۵ مراجعه شود)؛
ز- تکمیل، ارائه و مدیریت اعلان‌ها برای سازمان تنظیم مقررات و حفاظت اطلاعات اشخاص حقیقی و حقوقی[1] حسب اقتضای قانون حفاظت داده‌ها (به بند ۴-۶ مراجعه شود)؛
ژ- پیاده‌سازی شیوه‌نامه‌های مربوط به پردازش اطلاعات شخصی اشاره‌شده در بخش‌نامه‌های توصیه‌ای یا اجباری قابل اِعمال در سازمان، حسب اقتضا.

۴-۱-۳ نمایندگان حفاظت داده‌ها

هرگاه سازمان دارای بخش‌ها یا سامانه‌های مختلفی برای پردازش اطلاعات شخصی باشد، سازمان باید تعیین کند که آیا ایجاد شبکه‌ای از نمایندگان حفاظت داده‌ها لازم است یا نه به‌طوری‌که:
الف- نشان‌دهندهٔ بخش‌ها یا سامانه‌هایی باشند که در زمینهٔ مدیریت اطلاعات شخصی به عنوان موارد با ریسک بالا شناخته شده‌اند (برای آگاهی از نمونه‌های اطلاعات شخصی متعلق به مقوله‌های با ریسک بالا به بند ۴-۲-۲ مراجعه شود)؛ و
ب- به کارکنان دارای مسئولیت روزمره برای انطباق با خط‌مشی کمک کند.

۴-۲ مشخص کردن و ثبت کاربری‌های اطلاعات شخصی

هدف از این کار، حصول اطمینان از این امر است که سازمان مقوله‌های اطلاعات شخصی را که پردازش می‌کند، و سطح ریسک مربوط به پردازش این اطلاعات را، درک می‌کند.

۴-۲-۱ کلیات

فهرستی از مقوله‌های اطلاعات شخصی پردازش‌شده توسط سازمان باید حفظ شود. در این فهرست باید اهداف مورد نظر برای کاربری هر کدام از مقوله‌های اطلاعات شخصی نیز، درج شود.
یادآوری- این فهرست بایستی اطلاعات لازم را برای اعلان صحت پردازش اطلاعات به سازمان تنظیم مقررات و حفاظت اطلاعات اشخاص حقیقی و حقوقی فراهم کند.
سازمان باید محل‌ها و مسیرهایی از فرآیندهای سازمانی را که اطلاعات شخصی در آنها گردش می‌کنند ثبت کند.

1-Information Commissioner
نهادی دولتی که مسئول تنظیم مقررات و نظارت بر اجرای قوانین و مقررات «آزادی اطلاعات» و «حفاظت داده‌های شخصی» در معنای گستردهٔ آن است. در حال حاضر، چنین نهادی در کشور تأسیس نشده و بخش‌هایی از رسالت و وظایف قانونی آن را به‌ترتیب «پلیس فتا» و «سازمان تنظیم مقررات و ارتباطات رادیویی» به عهده دارند.

۴-۲-۲ اطلاعات شخصی در معرض ریسک بالا

این فهرست (به بند ۴-۲-۱ مراجعه شود) باید امکان تعیین هویت و مستندسازی صریح مقوله‌های اطلاعات شخصی در معرض ریسک بالای پردازش‌شده توسط سازمان را میسر سازد.

مقوله‌های اطلاعات شخصی در معرض ریسک بالا می‌تواند شامل موارد زیر باشد:

الف- اطلاعات شخصی حساس؛

ب- حساب بانکی شخصی و دیگر اطلاعات مالی؛

پ- شناسه‌های ملی، مانند شمارهٔ بیمهٔ تأمین اجتماعی؛

ت- اطلاعات شخصی مربوط به بزرگسالان و کودکان آسیب‌پذیر؛

ث- ریزاطلاعات مربوط به سوابق فعالیت و کار افراد؛

ج- اظهارات حساس که می‌تواند بر موقعیت افراد تاثیر منفی بگذارد.

یادآوری- در مواردی که حجم بالایی از اطلاعات شخصی پردازش می‌شود، سطح ریسک می‌تواند افزایش یابد.

۴-۳ آموزش و آگاه‌سازی

هدف از آموزش و آگاه‌سازی، حصول اطمینان از این نکته است که همهٔ کارکنان از مسئولیت‌های خود در هنگام پردازش اطلاعات شخصی آگاه هستند.

سازمان باید اطمینان حاصل کند که کارکنان دارای مسئولیت بی‌وقفه و هرروزه برای امکان‌پذیر کردن اثبات انطباق با قانون حفاظت داده‌ها و به‌آموخت‌ها (به بند ۴-۱-۲ مراجعه شود) قادر به اثبات شایستگی خود در درک خود قانون حفاظت داده‌ها و به‌آموخت‌ها هستند و از چگونگی پیاده‌سازی این امر در سازمان آگاه‌اند.

سازمان همچنین باید اطمینان حاصل کند که این کارکنان همچنان در مورد مسائل مربوط به مدیریت اطلاعات شخصی، حسب اقتضا، از طریق تماس با نهادهای برون‌سازمانی مطلع می‌مانند.

سازمان باید قادر به اثبات این امر باشد که همهٔ کارکنان مسئولیت خود را در خصوص حصول اطمینان از محافظت و پردازش اطلاعات شخصی مطابق با روش‌های اجرایی قابل اعمال، با ملحوظ کردن الزامات امنیتیِ مرتبط، درک می‌کنند.

به همهٔ کارکنان باید آموزش داده شود تا قادر به پردازش اطلاعات شخصی مطابق با روش‌های اجرایی قابل اعمال باشند. این آموزش باید با نقش هر کدام از آنها در سازمان مرتبط باشد.

۴-۴ ارزیابی ریسک

هدف از ارزیابی ریسک حصول اطمینان از این امر است که سازمان از هر گونه ریسک همراه با پردازش انواع خاصی از اطلاعات شخصی آگاه است.

سازمان باید فرآیندی را برای ارزیابی سطح ریسک مرتبط با پردازش اطلاعات شخصی افراد، به اجرا بگذارد. چنین ارزیابی‌هایی باید شامل پردازش انجام‌شده توسط سازمان‌های دیگر باشد. سازمان باید به منظور کاهش احتمال عدم انطباق با خط‌مشی، هر گونه ریسکی را که در ارزیابی ریسک مشخص می‌شود، مدیریت کند.

فرآیند ارزیابی ریسک باید آن دسته از روش‌های اجرایی را دربرگیرد که به موجب آن‌ها هر گونه پردازش اطلاعات شخصی می‌تواند موجب ایراد خسارت و/یا ناراحتی در افراد شود، به‌طوری‌که این روش‌های اجرایی

برای بازنگری توسط افراد مسئول و پاسخ‌گو برای مدیریت اطلاعات شخصی (به بند ۵-۳ مراجعه شود) برجسته شوند.

یادآوری- روش‌شناسی[1] ارزیابی ریسک خود سازمان می‌تواند برای این منظور استفاده شود. از سایر منابع معتبر نیز می‌توان بهره برد.

۴-۵ روزآمدسازی PIMS

هدف از روزآمدسازی PIMS ارزیابی این نکته است که آیا PIMS همچنان به ارائهٔ زیرساخت لازم برای حفظ و بهبود انطباق با قانون حفاظت داده‌ها و به‌آموخت‌ها، قادر است یا نه.

کارکنان دارای مسئولیت روزمره برای انطباق با خط‌مشی (به بند ۴-۱-۲ مراجعه شود) باید به طور مداوم ارزیابی کنند که آیا PIMS همچنان قادر به اثبات انطباق با قانون حفاظت داده‌ها و به‌آموخت‌ها است یا نه؛ تا در صورت لزوم، بتوانند تغییراتی در سامانه بدهند.

این ارزیابی باید هر گاه که تغییراتی در الزامات و/یا فنّاوری سازمان رخ می‌دهد، بازنگری PIMS را دربرگیرد.

۴-۶ اطلاع‌رسانی

هدف از اطلاع‌رسانی، حصول اطمینان از این امر است که سازمان، جزئیات پردازش اطلاعات شخصی را حسب الزام «سازمان تنظیم مقررات و حفاظت اطلاعات اشخاص حقیقی و حقوقی»، اطلاع‌رسانی می‌کند.

سامانهٔ مدیریت اطلاعات شخصی باید حاوی شیوه‌نامه‌هایی باشد که روش اجرایی اطلاع‌رسانی را فعال می‌سازند (مگر این که سازمان از چنین الزامی معاف باشد) و اطمینان می‌دهند که چنین اطلاع‌رسانی‌هایی دقیق و روزآمد می‌مانند.

۴-۷ پردازش عادلانه و قانونمند

هدف از پردازش عادلانه و قانونمند، حصول اطمینان از این نکته است که اطلاعات شخصی به طور عادلانه و قانونمند پردازش می‌شوند و زمینه‌های قانونی برای پردازش اطلاعات شخصی به‌وضوح قبل از پردازش آنها، مشخص شده است.

۴-۷-۱ جمع‌آوری و پردازش اطلاعات شخصی

سامانهٔ مدیریت اطلاعات شخصی باید حاوی آن عده از شیوه‌نامه‌هایی باشد که موجب حصول اطمینان از موارد زیر شود:

الف- پردازش عادلانه و قانونی اطلاعات شخصی توسط سازمان؛

ب- پردازش اطلاعات شخصی فقط در موارد موجه؛

پ- پردازش اطلاعات حساس شخصی فقط در مواقع ضروری برای اهداف سازمان و منطبق با بندهای مرتبط «قانون حفاظت اطلاعات اشخاص حقیقی و حقوقی»؛

ت- هر فردی که اطلاعات شخصی را برای سازمان ارائه می‌کند «اعلامیهٔ حریم خصوصی» یا بیانیهٔ برخط حریم خصوصی به وی، یا به طور کامل یا به صورت اختصار همراه با پیوند[2] یا مرجعی به اعلامیهٔ کاملی که به‌وضوح حامل اطلاعات زیر است، عرضه می‌شود:

1-Methodology
2-Link

- هویت سازمان؛
- اهدافی که اطلاعات شخصی بدان منظور پردازش خواهند شد؛
-اطلاعاتی دربارهٔ افشای اطلاعات شخصی به اشخاص ثالث؛
- اطلاعات در مورد حق فرد از دسترسی به اطلاعات شخصی مربوط به خود؛
- این که آیا اطلاعات شخصی در خارج به کشورهای بدون حفاظت کافی از داده‌ها منتقل خواهد شد یا نه؛
- جزئیات چگونگی تماس با سازمان برای درخواست مرتبط با پردازش اطلاعات شخصی؛
- جزئیات همهٔ فنّاوری‌های مورد استفاده در وب‌گاه، مانند کوکی‌ها[1]، برای جمع‌آوری اطلاعات شخصی دربارهٔ افراد؛
- هر گونه اطلاعات دیگری که موجب پردازش عادلانهٔ اطلاعات خواهد بود.

هرگاه اطلاعات شخصی برای اهداف بازاریابی جمع‌آوری شود یا ممکن است در آینده برای این اهداف مورد استفاده قرار گیرد، PIMS باید شیوه‌نامه‌هایی را به کار گیرد تا اطمینان حاصل کند که اعتراض افراد به چنین بازاریابی‌هایی، به وضوح به آنها توضیح داده شده است.

سامانهٔ مدیریت اطلاعات شخصی باید شیوه‌نامه‌هایی را به کار گیرد که اثبات می‌کند هرگاه پردازشی مبتنی بر رضایت بوده است و سپس از رضایت در آن مورد اعلام انصراف شده است، پردازش مبتنی بر رضایت مذکور متوقف خواهد شد.

مواردی که در آن سایر بخشنامه‌ها یا قوانین، به‌صراحت و روشنی رضایت برای بازاریابی را به عنوان شرطی الزامی مقرر کرده‌اند، PIMS باید شیوه‌نامه‌هایی برای جلب رضایت در این موارد داشته باشد.

هرگاه اطلاعات شخصی حساس برای هدف(های) خاصی جمع‌آوری می‌شود، PIMS باید شیوه‌نامه‌هایی تدوین کند تا اطمینان حاصل شود که اعلامیهٔ حریم خصوصی به‌صراحت هدف(ها)یی را که اطلاعات شخصی حساس ممکن است برای آن(ها) مورد استفاده قرار گیرند، بیان می‌دارد.

سامانهٔ مدیریت اطلاعات شخصی باید شیوه‌نامه‌هایی را به کار گیرد که از بازنگری و به‌روزآوری و رسمیت بخشیدن به روش‌های جدید جمع‌آوری داده توسط مسئول صلاحیت‌دار و باتجربه (بند ۴-۱-۲) اطمینان حاصل شود و به نوبهٔ خود این اطمینان را ایجاد کند که می‌توان انطباق چنین روش‌هایی را با به‌آموخت‌ها و قوانین حفاظت داده‌ها اثبات کرد.

۴-۷-۲ سوابق اعلامیه‌ها و بیانیه‌های حریم خصوصی

سامانهٔ مدیریت اطلاعات شخصی باید شیوه‌نامه‌هایی را برای حفظ سوابق اعلامیه‌های حریم خصوصی و بیانیه‌های برخط حریم خصوصی به کار گیرد. این سوابق باید حداقل تا زمانی که اطلاعات شخصی مرتبط با آن حفظ می‌شوند، نگه‌داری شوند.

۴-۷-۳ زمان ارائهٔ اعلامیه‌ها و بیانیه‌های حریم خصوصی

سامانهٔ مدیریت اطلاعات شخصی باید شیوه‌نامه‌هایی را به کار گیرد تا اطمینان حاصل شود در مواردی که سازمان، اطلاعات شخصی را به طور مستقیم از فردی جمع‌آوری می‌کند، هر گونه اعلامیهٔ حریم خصوصی یا

1-Cookies

بیانیهٔ برخط حریم خصوصی لازم به فرد ارائه یا قبل از جمع‌آوری هر گونه اطلاعات شخصی در دسترس فرد قرار داده شده است.

۴-۷-۴ دستیابی‌پذیری اعلامیه‌ها و بیانات حریم خصوصی

سامانهٔ مدیریت اطلاعات شخصی باید شیوه‌نامه‌هایی را به کار گیرد تا اطمینان حاصل شود که محتوای هر گونه اعلامیهٔ حریم خصوصی یا بیانیهٔ برخط حریم خصوصی به شیوه‌ای ارائه شده است که اجازه می‌دهد به‌راحتی توسط مخاطبان مورد نظر درک شود و برای آنان دستیابی‌پذیر باشد.

یادآوری-اعلامیه‌های حریم خصوصی مورد نظر برای استفاده در جمع‌آوری اطلاعات شخصی از بزرگسالان آسیب‌پذیر، افراد مبتلا به مشکلات یادگیری یا کودکان، لازم است با زبان و قالبی که به‌آسانی برای این افراد قابل درک و دستیابی‌پذیر باشد، ارائه شود.

۴-۷-۵ اشخاص ثالث

سامانهٔ مدیریت اطلاعات شخصی باید شیوه‌نامه‌هایی را به کار گیرد تا اطمینان حاصل شود که اطلاعات شخصی از اشخاص ثالث به طور عادلانه و قانونمند جمع‌آوری می‌شود.

سامانهٔ مدیریت اطلاعات شخصی باید شیوه‌نامه‌هایی را به کار گیرد تا اطمینان حاصل شود که در مواقع ضروری، اعلامیهٔ حریم خصوصی، و حسب اقتضا، بیانیهٔ برخط حریم خصوصی (به بند ۴-۷-۱ مراجعه شود)، در اختیار فرد قرار می‌گیرد مگر این که انجام این کار متضمن کار خارج از قاعده[1] باشد.

یادآوری- «کار خارج از قاعده» در این بافتار صرفا به معنی «کار زیاد» نیست، زیرا این امکان وجود دارد در مواردی که احتمال ایراد آثار زیان‌بار برای فرد وجود دارد، سازمان ملزم شود برای تامین اعلامیه‌های حریم خصوصی کار زیادی انجام دهد و در صورت لزوم، بیانیه‌های برخط حریم خصوصی تهیه کند..

۴-۸ پردازش اطلاعات شخصی برای اهداف مشخص

هدف از این امر، حصول اطمینان از این نکته است که اطلاعات فقط برای یک یا چند هدف مشخص‌تر جمع شده است، و پردازش بیشتری به طریقی که با آن هدف یا اهداف ناسازگار باشد، نخواهد یافت.

۴-۸-۱ زمینه‌های پردازش

سامانهٔ مدیریت اطلاعات شخصی باید شیوه‌نامه‌هایی را به کار گیرد تا اطمینان حاصل شود که پردازش اطلاعات شخصی به شیوه‌ای انجام نخواهد شد که نقض (یا احتمال نقض) هرگونه تعهدات قانونی، از جمله مقررات قانونی، رویّهٔ قضایی، یا ضوابط قراردادی را در پی داشته باشد.

سامانهٔ مدیریت اطلاعات شخصی باید شیوه‌نامه‌هایی را به کار گیرد تا اطمینان حاصل شود که اطلاعات شخصی جمع‌آوری‌شده برای اهداف تعیین‌شده، در راه هدف ناسازگار دیگری استفاده نخواهد شد، مگر این که:

الف- معافیت‌های مربوط قانونی قابل اعمال باشد؛

ب- افرادی که اطلاعات شخصی‌شان قرار است برای هدف جدیدی پردازش شود، رضایت‌شان را برای هدف جدید اعلام کرده باشند.

1 -Disproportionate effort

سامانهٔ مدیریت اطلاعات شخصی باید شیوه‌نامه‌هایی را به کار گیرد تا اطمینان حاصل کند در مواردی که اطلاعات حساس شخصی قرار است که برای هدف ناسازگار جدیدی مورد استفاده قرار گیرد، رضایت صریح و روشن فرد برای این کار، قبل از پردازش، گرفته شده است، مگر این که استثنائات قانونی مربوط قابل اعمال باشد.

۴-۸-۲ رضایت به اهداف جدید

سامانهٔ مدیریت اطلاعات شخصی باید شیوه‌نامه‌هایی را به کار گیرد تا اطمینان حاصل شود که هرگونه رضایت برای اهداف جدید آزادانه و آگاهانه گرفته شده است.

سامانهٔ مدیریت اطلاعات شخصی باید شیوه‌نامه‌هایی را به کار گیرد تا اطمینان حاصل کند که:

الف- دلالت‌های مثبت رضایت فرد در مورد استفاده از اطلاعات شخصی آنها برای هدف جدید به دست آمده است؛

ب- سوابق رضایت به دست آمده برای هدف جدید حفظ شده است.

۴-۸-۳ به‌اشتراک‌گذاری داده‌ها

سامانهٔ مدیریت اطلاعات شخصی باید شیوه‌نامه‌هایی را به کار گیرد تا اطمینان حاصل کند در مواردی که سازمان اطلاعات شخصی را با یک سازمان دیگر به اشتراک می‌گذارد، مسئولیت‌ها برای هر دو طرف با توجه به اطلاعات شخصی به طور رسمی در یک موافقت‌نامه یا قرارداد مکتوب، حسب اقتضا، مستند شده است.

سامانهٔ مدیریت اطلاعات شخصی باید شیوه‌نامه‌هایی را به کار گیرد تا اطمینان حاصل کند در مواردی که سازمان دیگری از اطلاعات شخصی برای آن اهداف خود استفاده خواهد کرد:

الف- موافقت‌نامه یا قرارداد مکتوب هر دو، اهدافی را که ممکن است اطلاعات برای آن استفاده شود و هر گونه محدودیت یا قیود در استفادهٔ بیشتر از اطلاعات شخصی برای اهداف دیگر را توصیف می‌کند؛ و

ب- سازمان دیگر تعهد یا شواهد دیگری را از تعهد خود به پردازش اطلاعات به شیوه‌ای که ناقض مقررات نباشد، فراهم می‌کند.

سامانهٔ مدیریت اطلاعات شخصی باید شیوه‌نامه‌هایی را به کار گیرد تا اطمینان حاصل شود هر گاه که ممکن باشد، هرگونه پردازش جدید که متضمن به‌اشتراک‌گذاری اطلاعات شخصی با اشخاص ثالث است، با اطلاع‌رسانی‌های سازمانی (به بند ۴-۶ مراجعه شود) و با شرایط اعلامیهٔ حریم خصوصی یا بیانیهٔ برخط حریم خصوصی [به قسمت ت بند ۴-۷-۱) مراجعه شود] ارائه‌شده به فرد، سازگار است.

در مواردی که این امر ممکن نیست، سازمان باید اطمینان حاصل کند که:

- دارای مبنای قانونی برای به‌اشتراک‌گذاری داده‌هاست؛

- در صورت لزوم، رضایت فرد برای به‌اشتراک‌گذاری داده‌ها گرفته شده است.

در مواردی که به‌اشتراک‌گذاری داده‌ها با اشخاص ثالث، بدون رضایت فرد مجاز است، PIMS باید اطمینان حاصل کند که شیوه‌نامه‌هایی را به کار گرفته است تا اطمینان حاصل کند که سابقهٔ قابل ممیزی از پروتکل‌ها و کنترل‌ها برای به‌اشتراک‌گذاری این داده‌ها مستند شده است.

در مواردی که به‌اشتراک‌گذاری داده‌ها با یک شخص ثالث، مثلاً به لحاظ قانونی، مورد نیاز است، PIMS باید شیوه‌نامه‌هایی را به کار گیرد تا اطمینان حاصل کند که پروتکل‌ها و کنترل‌ها برای به‌اشتراک‌گذاری داده‌ها مستند شده است.

۴-۸-۴ تطبیق داده‌ها[1]

در مواردی که اطلاعات شخصی با اطلاعات شخصی دیگری، مثلاً به منظور ارتقای سوابق تحصیلی و کاری تطبیق داده می‌شود، PIMS باید شیوه‌نامه‌هایی را به کار گیرد تا اطمینان حاصل کند که اطلاعات شخصی تطبیق‌داده‌شده، تنها برای اهداف بیان‌شده و سازگار با الزام قانونی یا در مواردی که رضایت گرفته شده است، مورد استفاده قرار می‌گیرد.

۴-۹ کافی، مرتبط، و غیراضافی

هدف، حصول اطمینان از کافی بودن، مرتبط بودن، و اضافی نبودن اطلاعات شخصی است.

۴-۹-۱ کفایت

سامانهٔ مدیریت اطلاعات شخصی باید شیوه‌نامه‌هایی را به کار گیرد تا اطمینان حاصل کند که اطلاعات شخصی جمع‌آوری شده توسط سازمان برای اهداف سازمان کافی است.

سامانهٔ مدیریت اطلاعات شخصی باید شیوه‌نامه‌هایی برای بازنگری‌های منظم فنّاوری و فرآیندهای مربوط به پردازش اطلاعات شخصی به کار گیرد تا اطمینان حاصل کند که اطلاعات همچنان برای آن اهداف مناسب هستند.

۴-۹-۲ مرتبط و غیراضافی

سامانهٔ مدیریت اطلاعات شخصی باید شیوه‌نامه‌هایی را به کار گیرد تا اطمینان حاصل کند که:

الف- سازمان، برای برای آورده کردن اهداف قانونی خود، حداقل اطلاعات شخصی مورد نیاز را پردازش می‌کند.

ب- اطلاعات زاید شخصی را که برای اهداف مذکور مرتبط نیست، پردازش نمی‌کند، مگر این که تدارک این اطلاعات اختیاری بوده است و تنها با رضایت افراد پردازش می‌شود.

پ- سامانه‌ها و فرآیندهای جدید متضمن پردازش اطلاعات شخصی به منظور حصول اطمینان از این که اطلاعات تحت پردازش مرتبط و غیراضافی هستند، بازنگری می‌شوند.

در مواردی که پردازش اطلاعات شخصی، برای اهداف سازمان، مرتبط یا ضروری نیست، PIMS باید اطمینان حاصل کند که اطلاعات شخصی پردازش نمی‌شود.

۴-۱۰ درستی

هدف، حصول اطمینان از دقیق بودن و، در صورت لزوم، نگهداشت روزآمد اطلاعات شخصی است.

سامانهٔ مدیریت اطلاعات شخصی باید شیوه‌نامه‌هایی را به کار گیرد تا از حفظ یکپارچگی و درستی اطلاعات شخصی تحت پردازش اطمینان حاصل کند.

سامانهٔ مدیریت اطلاعات شخصی باید شیوه‌نامه‌هایی را به کار گیرد تا اجازه دهد افراد صحت اطلاعات شخصی خود را زیر سؤال ببرند و در صورت لزوم مسئول مرتبط را وادار به اصلاح آن کنند. در مواردی که

1-Data matching

در مواردی که افراد ادعاهایی مانند کار در یک شرکت را برای درج در سوابق خود می‌کنند، برای جلوگیری از ایراد زیان به عموم ناشی از احتمال ادعای کذب، ممکن است مراجعه به لیست بیمهٔ آن شرکت برای تطبیق ادعاهای آن فرد با داده‌های شخص حقیقی یا حقوقی دیگر لازم باشد.

اطلاعات شخصی نادرست و غیرقابل تصحیح است، به عنوان مثال در مورد یک سابقهٔ تاریخی، PIMS باید شیوه‌نامه‌هایی برای ثبت نادرستی‌های گزارش‌شده و حسب اقتضا، ثبت اطلاعات درست شخصی، به‌کار گیرد.
سامانهٔ مدیریت اطلاعات شخصی باید شیوه‌نامه‌هایی را به کار گیرد تا مشخص کند آیا اطلاعات مذکور واقعاً نادرست است یا نه.
سامانهٔ مدیریت اطلاعات شخصی باید شیوه‌نامه‌هایی را به کار گیرد تا اطمینان حاصل شود که کارکنان از اهمیت ثبت اطلاعات شخصیِ درست مطلع هستند و فقط از اطلاعات شخصی روزآمد برای گرفتن تصمیمات مهم در مورد افراد استفاده می‌کنند.
سامانهٔ مدیریت اطلاعات شخصی باید شیوه‌نامه‌هایی برای موارد زیر به کار گیرد:
الف- اطلاع‌رسانی به اشخاص ثالث دربارهٔ این که سازمان به آنها اطلاعات شخصی نادرست یا غیرروزآمد فرستاده است مبنی بر نادرست یا غیرروزآمد بودن اطلاعات و این که برای تصمیم‌گیری دربارهٔ افراد ذی‌ربط، از اطلاعات مزبور استفاده نکند؛ و
ب- ارسال هر گونه اصلاحات اطلاعات شخصی به اشخاص ثالث در موارد مقتضی.
سامانهٔ مدیریت اطلاعات شخصی باید شیوه‌نامه‌هایی را برای بازنگری سامانه‌ها و فرآیندهای مربوط به پردازش اطلاعات شخصی در موارد زیر به کارگیرد:
- تایید این نکته که سامانه‌ها یا فرآیندهای مزبور تا آنجا که ممکن است از ثبت اطلاعات شخصی نادرست یا غیرروزآمد جلوگیری می‌کنند، و
- اجازهٔ اصلاحات در مورد اطلاعات شخصی نادرست یا غیرروزآمد را میسر می‌سازند.

۴-۱۱ نگهداری و وارهایی[1]

هدف، حصول اطمینان از نگه نداشتن اطلاعات شخصی بیشتر از مدت زمان ضروری است.
سامانهٔ مدیریت اطلاعات شخصی باید برنامه‌های زمان‌بندی حفظ اطلاعات شخصی تنظیم کند که باید:
الف- شامل حداقل دورهٔ نگهداری الزام شده توسط قانون، و همچنین سازمان باشد؛
ب- شفاف‌سازی توجیه و مبنای مدت زمان نگهداری؛ و
پ- مستندسازی هر نوع توجیه قابل اعمال برای حفظ اطلاعات شخصی به مدتی طولانی‌تر از حداقل مدتِ نگهداری اعلام شده، به عنوان مثال که هرگاه که ممکن است برای اهداف تاریخی و/یا پژوهشی حفظ شود.
سامانهٔ مدیریت اطلاعات شخصی باید شیوه‌نامه‌هایی برای پیاده‌سازی برنامه‌های زمانی حفظ اطلاعات شخصی و اطلاع‌رسانی به همهٔ کارکنان ذی‌ربط دربارهٔ آنها به کار گیرد.
سامانهٔ مدیریت اطلاعات شخصی باید شیوه‌نامه‌هایی را به کار گیرد تا اطمینان حاصل کند که اطلاعات شخصی بیشتر از مدتی که برای وارهایی آن در نظر گرفته شده است، باقی نمی‌مانند.
سامانهٔ مدیریت اطلاعات شخصی باید شیوه‌نامه‌هایی برای وارهایی را به کار گیرد یا به آنها ارجاع دهد که به روش‌های زیرکنترل می‌شوند:
- با استفاده از فرآیندهای تصویب‌شده؛
- در سطح امنیتی مناسب با حساسیت اطلاعات شخصی؛

1-Disposal

- سازگار با ارزیابی ریسک امنیت اطلاعات سازمانی.

یادآوری- در برخی موارد، ممکن است وارهایی اطلاعات شخصی از طریق انتقال آن به بایگانی راکد انجام گیرد.

۴-۱۲ حقوق افراد

هدف، حصول اطمینان از در دسترس بودن روش‌های اجرایی برای ممکن کردن محترم شمردن حقوق افراد است.

۴-۱۲-۱ کلیات

سامانهٔ مدیریت اطلاعات شخصی باید دربرگیرندهٔ روش‌های اجرایی برای حصول اطمینان از این نکته باشد که حقوق افراد در رابطه با اطلاعات شخصی آنها محترم شمرده می‌شود و درخواست‌ها برای اعمال چنین حقوقی در حدود زمانی قانونی مورد رسیدگی قرار می‌گیرند.

یادآوری- چنین حقوقی شامل دسترسی به اطلاعات، اعتراض به پردازش، و بازنگری پردازش خودکار است.

۴-۱۲-۲ شکایت‌ها و اعتراض‌ها[1]

PIMS باید شیوه‌نامه‌ای به کار گیرد تا اطمینان حاصل کند که شکایت‌ها دربارهٔ پردازش اطلاعات شخصی به‌درستی مورد رسیدگی قرار می‌گیرند. این شیوه باید حاوی تمهیداتی برای رسیدگی به اعتراض افراد در مورد روش رسیدگی به شکایت‌های خود باشد.

۴-۱۳ مسائل امنیتی

هدف، حصول اطمینان از این امر است که اطلاعات شخصی در برابر از بین رفتن یا آسیب دیدن و پردازش غیرمجاز یا غیرقانونی، با اجرای اقدامات امنیتی مناسب فنی و سازمانی محافظت می‌شوند.

۴-۱۳-۱ کنترل‌های امنیتی

سامانهٔ مدیریت اطلاعات شخصی باید کنترل‌های امنیتی زیر را حسب اقتضا مشخص کند:

الف- نوع اطلاعات شخصی در حال پردازش؛ و

ب- ریسک خسارت یا ناراحتی به افراد در صورتی که در مورد حفاظت اطلاعات تعلل شود (به بند ۴-۴ مراجعه شود).

یادآوری ۱- ارزیابی ریسک (بند ۴-۴) سطح مناسب کنترل را تعیین خواهد کرد. الزامات امنیتی بیش از حد یا کمتر از حد زیان‌بار خواهد بود.

در صورت پردازش اطلاعات شخصی پرریسک (به بند ۴-۲-۲ مراجعه شود)، PIMS باید اطمینان حاصل کند که اقدامات امنیتی مشخص و اجراشده متناسب با ریسک‌های ارزیابی‌شده هستند، و به‌همین صورت باقی می‌مانند.

یادآوری ۲- در موارد مقتضی، سازمان می‌تواند خواهان انطباق با استاندارد ایران-ایزو-آی‌ای‌سی ۲۷۰۰۱ باشد. صدور گواهینامه ۲۷۰۰۱ توسط نهاد برون‌سازمانی به منظور اثبات انطباق، می‌تواند گزینه‌ای در این باره باشد.

1-Appeals

۴-۱۳-۲ ذخیره‌سازی و جابه‌جایی[1]

سامانهٔ مدیریت اطلاعات شخصی باید شیوه‌نامه‌هایی را به کار گیرد تا اطمینان حاصل کند که اطلاعات شخصی با اقدامات احتیاطی متناسب با محرمانگی و حساسیت آنها به طور امنی ذخیره شده و به کار گرفته می‌شود.

۴-۱۳-۳ انتقال

سامانهٔ مدیریت اطلاعات شخصی باید شیوه‌نامه‌هایی را به کار گیرد تا اطمینان حاصل کند که در مواردی که اطلاعات شخصی به طریق الکترونیکی یا دستی در سازمان انتقال می‌یابد یا به دیگر سازمان‌ها منتقل می‌شود، این انتقال با تمهیدات مناسب تعریف‌شده توسط سازمان به منظور حفاظت اطلاعات در هنگام انتقال، به طور امن انجام می‌شود.

۴-۱۳-۴ کنترل‌های دسترسی

سامانهٔ مدیریت اطلاعات شخصی باید شیوه‌نامه‌هایی را به کار گیرد تا اطمینان حاصل کند که در مواردی که دسترسی کارکنان به اطلاعات شخصی مجاز است، این دسترسی محدود به کارکنانی است که چنین دسترسی‌هایی بخشی از نقش آنهاست. سامانهٔ مدیریت اطلاعات شخصی باید شیوه‌نامه‌هایی را به کار گیرد تا اطمینان حاصل کند که برای کارکنان روشن شده است که هرگاه دسترسی به لحاظ قانونی برایشان مجاز است، فقط برای مقاصد کاری است و دسترسی به اطلاعات فقط باید برای اهداف قانونی صورت پذیرد.

هرگاه اطلاعات شخصی پرریسک پردازش می‌شود (به بند ۴-۲-۲ مراجعه شود)، PIMS باید شیوه‌نامه‌هایی را به کار گیرد تا اطمینان حاصل کند که کنترل‌های دسترسی با حساسیت این اطلاعات متناسب است.

سامانهٔ مدیریت اطلاعات شخصی باید شیوه‌نامه‌هایی را به کار گیرد تا اطمینان حاصل کند که همهٔ دسترسی‌ها به اطلاعات شخصی، پایش می‌شود و مطابق ارزیابی ریسک امنیت اطلاعات سازمان مورد ارزیابی قرار می‌گیرد.

۴-۱۳-۵ ارزیابی‌های امنیتی

سامانهٔ مدیریت اطلاعات شخصی باید شیوه‌نامه‌هایی را به کار گیرد تا اطمینان حاصل کند که ارزیابی‌های امنیتی به طور ادواری انجام می‌شود.

این ارزیابی‌ها باید ثابت کند که آیا کنترل‌های امنیتی موجود کافی هستند یا نه و توصیه‌هایی برای بهبودها در مواقع ضروری ارائه دهد.

در این ارزیابی‌ها باید ریسک ایراد خسارت، مخاطره و/یا ناراحتی افراد در صورت حادثهٔ امنیتی لحاظ شود.

۴-۱۳-۶ مدیریت حوادث امنیتی

سامانهٔ مدیریت اطلاعات شخصی باید شیوه‌نامه‌هایی را به کار گیرد:

الف- که حوادث امنیتی دربرگیرندهٔ اطلاعات شخصی را ارزیابی و مدیریت کند، از جمله روش‌های اجرایی برای کاهش خسارت ناشی از هرگونه حادثهٔ امنیتی؛

ب- برای مستندسازی هرگونه حادثهٔ امنیتی، از جمله ارزیابی چگونگی رخ دادن حادثه، اقدام اصلاحی انجام شده، و آنچه می‌توان از حادثه یاد گرفت؛

1-Handling

پ- برای اتخاذ تصمیمات در مورد این که حادثهٔ امنیتی به نهادهای مقرراتی ذی‌ربط ارجاع داده شود یا به افراد اطلاع‌رسانی شود؛

ت- برای حفظ سوابق هر گونه ارجاع و اطلاعیه‌های صادرشده.

۴-۱۴ افشا برای اشخاص ثالث

هدف، حصول اطمینان از این امر است که افشای اطلاعات برای اشخاص ثالث در انطباق با قانون حفاظت داده‌ها و به‌آموخت‌ها مدیریت می‌شود.

PIMS باید شیوه‌نامه‌هایی را به کار گیرد تا اطمینان حاصل کند که اشخاص ثالث شواهد زیر را ارائه می‌کنند:

الف- حق خود برای دسترسی به اطلاعات شخصی؛ و

ب- در صورت لزوم، هویت‌شان.

سامانهٔ مدیریت اطلاعات شخصی باید شیوه‌نامه‌هایی را به کار گیرد تا اطمینان حاصل شود که بررسی‌هایی به منظور حصول اطمینان از وجود زمینه‌های قانونی برای افشای اطلاعات به شخص ثالث انجام می‌گیرد. فقط حداقل مقدار اطلاعات شخصی لازم باید برای اشخاص ثالث افشا شود.

سامانهٔ مدیریت اطلاعات شخصی باید شیوه‌نامه‌هایی برای نگهداری سوابق افشای اطلاعات شخصی به کار گیرد. این سوابق باید اثبات کند که افشا قانونمند بوده است بود و باید سازمان را به حفظ روند افشای اطلاعات شخصی قادر سازد.

۴-۱۵ پردازش تحت قرارداد

هدف، حصول اطمینان از این نکته است که اطلاعات شخصی پردازش‌شده توسط یک سازمان دیگر به نمایندگی از سازمان در انطباق با قانون حفاظت داده‌ها و به‌آموخت‌ها مدیریت می‌شود.

سامانهٔ مدیریت اطلاعات شخصی باید شیوه‌نامه‌هایی را به کار گیرد تا اطمینان حاصل کند که هرگاه اطلاعات از طرف آن سازمان توسط سازمان(های) دیگر پردازش می‌شود:

الف-سازمان فقط سازمان‌های دیگری را انتخاب خواهد کرد که می‌توانند امنیت فنی، فیزیکی و سازمانی فراهم کنند که تامین‌کنندهٔ الزامات سازمان برای همه اطلاعات شخصی که آنها از طرف او پردازش خواهند کرد، باشند؛

ب- ارزیابی امنیتی مناسب به عنوان بخشی از فعالیت لازم قبل از مشارکت سازمان دیگر، انجام می‌شود و در صورت لازم، به دلیل ماهیت اطلاعات شخصی تحت پردازش یا به دلیل شرایط خاص پردازش، ممیزی ترتیبات امنیتی سازمان دیگر قبل از ورود به قرارداد انجام می‌شود؛

پ- هنگامی که سازمان‌های دیگر انتخاب می‌شود، سازمان موافقت‌نامهٔ مکتوب را برای ارائه خدمات به صورتی که مشخص شده است آماده می‌کند و در دسترس قرار می‌دهد و از سازمان دیگر می‌خواهد امنیت مقتضی را برای اطلاعات شخصی که پردازش خواهد کرد، تامین کند؛

ت- قرارداد با سازمان دیگر ممیزی‌های منظم از ترتیبات امنیتی سازمان دیگر را در طول دوره‌ای که سازمان دیگر به اطلاعات شخصی دسترسی دارد، میسر می‌سازد؛

ث- سازمان دیگر به موجب قرارداد متعهد است برای استفاده از پیمانکاران فرعی ردهٔ پایین‌تر برای پردازش اطلاعات شخصی، از خود سازمان مجوز بگیرد؛

ج- عقد قرارداد با پیمانکاران فرعی (ردهٔ ۳) سازمان دیگر (ردهٔ ۲) الزام می‌کند که پیمانکاران فرعی (ردهٔ ۳) دست‌کم با امنیت و تمهیداتی در سطح سازمان دیگر (ردهٔ ۲) انطباق داشته باشند؛

چ- عقد قرارداد با سازمان(های) دیگر (که به هر پیمانکار فرعی رده‌های دیگر نیز تسری می‌یابد) مشخص می‌کند که هنگامی که قرارداد منقضی می‌شود، اطلاعات شخصی مربوط یا امحا خواهد شد یا به سازمان دیگر که توسط سازمان به عنوان مشخص شده است، منتقل می‌شود.

۴-۱۶ نگهداری

سامانهٔ مدیریت اطلاعات شخصی باید شیوه‌نامه‌هایی را به کار گیرد تا اطمینان حاصل کند که روش‌های اجرایی و تجهیزات فنّاوری برای حصول اطمینان از عملکرد صحیح و مناسب خود نگهداری می‌شوند. این روش‌های اجرایی باید اطمینان دهد که چنین نگهداشتی طرح‌ریزی شده و به صورتی منظم، و زمان‌بندی‌شده انجام می‌شوند.

۵ پایش و بازنگری PIMS

هدف، حصول اطمینان از پایش و بازنگری اثربخشی و کارایی PIMS است.

۵-۱ ممیزی داخلی

۵-۱-۱ طرح‌ریزی ممیزی

با رعایت خط‌مشی، باید یک برنامهٔ ممیزی که اثربخشی و کارایی پردازش اطلاعات شخصی را توسط سازمان پایش و بازنگری می‌کند، طرح‌ریزی، اجرا، و برقرار نگه داشته شود.

برنامهٔ ممیزی هم باید هرگونه پردازش اطلاعات شخصی پرریسک را به‌صراحت (به بند ۴-۲-۲ مراجعه شود) پوشش دهد و باید هر گونه پردازش اطلاعات شخصی توسط سازمان‌های دیگر (به بند ۴-۱۶ مراجعه شود) را نیز شامل شود.

۵-۱-۲ انتخاب ممیزان

باید با انتخاب مناسب ممیزان و منش ممیزی‌ها، از عینی و بی‌طرف بودن برنامهٔ ممیزی اطمینان حاصل شود.

یادآوری- در سازمان‌های بزرگتر و سازمان‌هایی که اطلاعات شخصی پرریسک را پردازش می‌کنند، (به بند ۴-۲-۲ مراجعه شود) بایستی ممیزی‌های منظم توسط اشخاص برون‌سازمانی مورد نظر قرار گیرد.

۵-۱-۳ الزامات ممیزی

ممیزی باید در فواصل برنامه‌ریزی‌شده انجام شود تا تعیین کند که آیا PIMS:

الف- مطابق با خط‌مشی و روش‌های اجرایی تعیین‌شده صورت می‌پذیرد یا نه؛

ب- مطابق با الزامات فنّاوری اجرا و نگهداری می‌شود یا نه.

گزارش‌های ممیزی حاوی شرحی از هرگونه انحراف قابل توجهی از خط‌مشی و/یا روش‌های اجرایی ایجاد شده باید به مدیریت ارائه شود.

گزارش‌های ممیزی همچنین باید موضوعات مربوط به فنّاوری یا فرآیندهایی را مشخص کند که می‌تواند بر انطباق با خط‌مشی تاثیر بگذارد.

۵-۲ بازنگری مدیریتی

بازنگری مدیریتی PIMS باید در فواصل منظم، برنامه‌ریزی‌شده، و نیز هنگامی که تغییرات عمده صورت می‌گیرد، انجام شود تا از تداوم مناسب بودن، کفایت و اثربخشی سامانه اطمینان حاصل شود.

بازنگری مدیریتی باید بر اساس داده‌ها و اطلاعات زیر انجام شود:

الف- بازخورد کاربران PIMS؛

ب- ریسک‌های مشخص شده و تأکید شده توسط کارکنان؛

پ- نتایج ممیزی‌ها؛

ت- سوابق بازنگری روش‌های اجرایی؛

ث- نتایج حاصل از ارتقا و/یا جایگزینی‌های فنّاوری؛

ج- درخواست‌های رسمی برای ارزیابی توسط نهادهای مقرراتی؛

چ- رسیدگی به شکایات؛

ح- نقض‌ها/ حوادث امنیتی رخ داده.

بازنگری مدیریتی باید اطلاعات دقیقی را در مورد تغییرات بالقوهٔ PIMS مانند تغییرات خط‌مشی، روش‌های اجرایی و/یا فنّاوری را که می‌تواند بر انطباق تأثیر بگذارد، ارائه کند.

هر گاه تغییرات عمده‌ای در PIMS انجام شود، ممیزی باید در اسرع وقت پس از انجام تغییرات انجام شود.

۶ بهبود PIMS

هدف، حصول اطمینان از بهبود اثربخشی و کارایی PIMS از طریق اجرای اقدامات اصلاحی است.

۶-۱ اقدامات پیشگیرانه و اصلاحی

۶-۱-۱ کلیات

سازمان باید PIMS را از طریق به‌کارگیری اقدامات پیشگیرانه و اصلاحی بهبود بخشد.

همهٔ تغییرات و/یا بهبود پیشنهادی باید قبل از اجرا ارزیابی شود تا اطمینان حاصل شود که الزامات خط‌مشی برآورده می‌شوند. تغییراتی که می‌تواند بر توانایی اثبات انطباق با قانون حفاظت داده‌ها و به‌آموخت‌ها (مانند تبدیل اطلاعات شخصی به یک قالب جدید ذخیره‌سازی پرونده[1]) باید برای تعیین این که آیا بر انطباق تاثیر خواهند گذاشت یا نه، بازنگری شوند.

فهرست و ماهیت تغییرات ناشی از اقدامات پیشگیرانه و اصلاحی باید مستند شوند و مطابق با برنامهٔ زمان‌بندی‌شده انجام شوند.

۶-۱-۲ اقدامات پیشگیرانه

سازمان باید در خصوص محافظت در برابر عدم‌انطباق‌های بالقوه، به منظور جلوگیری از وقوع آنها، اقداماتی را انجام دهد. یک روش اجرایی باید ایجاد شود تا:

1-File

الف- عدم انطباق‌های بالقوه و علل آنها را مشخص کند؛

ب- اقدام پیشگیرانهٔ مورد نیاز را تعیین و اجرا کند؛

پ- نتایج اقدام انجام‌شده و بازنگری آن را، ثبت کند؛

ت- تغییرات ریسک‌ها را مشخص کند؛

ث- اطمینان حاصل کند که همهٔ افرادی که لازم است از عدم انطباق بالقوه و اقدام پیشگیرانه مطلع باشند، در دسترس هستند.

۶-۱-۳ اقدامات اصلاحی

یک روش اجرایی باید ایجاد شود تا بر اساس آن هرگاه عدم انطباقی مشخص می‌شود، آن را بازنگری و، بر اساس ارزیابی ریسک یکی از اقدامات زیر انجام شود:

الف- علت عدم انطباق رفع شود؛

ب- میزان عدم انطباق کاهش یابد؛

پ- هرگاه ارزیابی ریسک مشخص کند که اطمینانی به کاهش میزان عدم انطباق وجود ندارد، وضعیت به طور مشروح مستند شود.

ارزیابی ریسک باید در فواصل زمانی منظم انجام شود تا تعیین کند که آیا شرایط تغییر کرده است یا نه و آیا عدم انطباق نیاز به اصلاح دارد یا نه (به بند ۴-۴ مراجعه شود).

سازمان باید اطمینان حاصل کند که همهٔ ریسک‌هایی که اخیراً در مورد اطلاعات شخصی (یا از درون سازمان یا در چشم‌انداز ملی گسترده‌تر) مشخص شده‌اند، با استفاده از روش‌های اجرایی کنش‌گرایانه[1] مانند ارزیابی‌های پی‌آمدهای نقض حریم خصوصی ارزیابی می‌شوند.

۶-۲ بهبود مداوم

سازمان باید به طور مداوم اثربخشی PIMS را از طریق نتایج ممیزی، اقدامات پیشگیرانه و اصلاحی، و بازنگری مدیریت بهبود بخشد.

شکایت‌ها، حوادث امنیتی، درخواست دسترسی سوژه و مسائل دیگر باید به عنوان کمک در بهبود اثربخشی PIMS به کار رود.

1-Proactive procedures

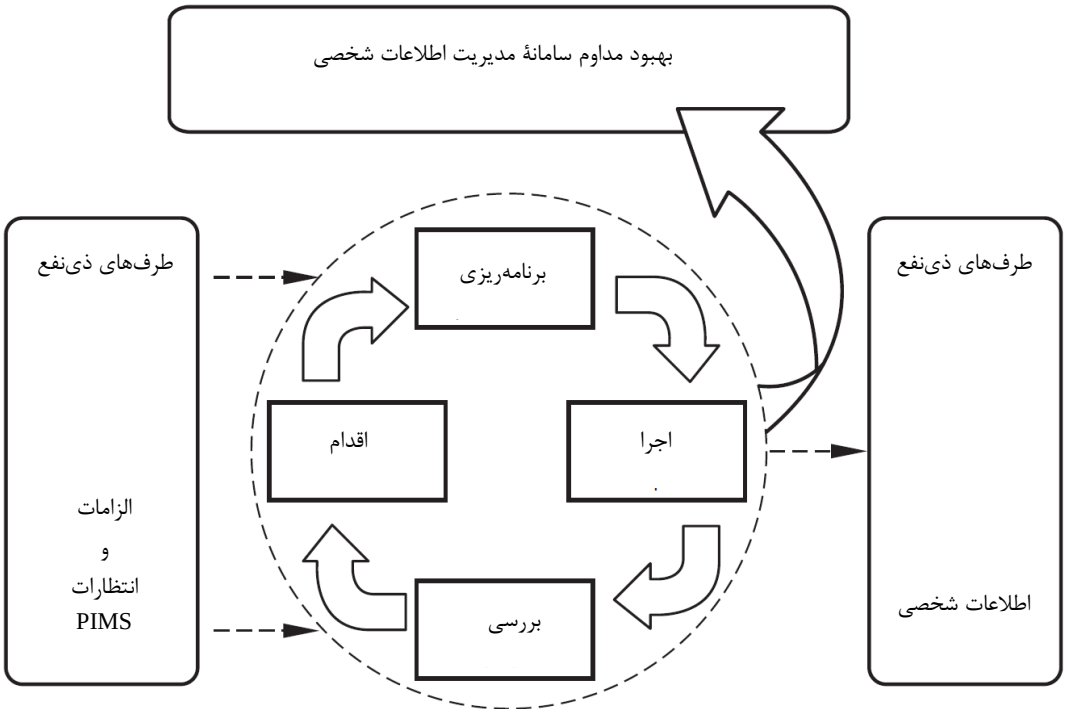
پیوست الف
(اطلاعاتی)
چرخهٔ برنامه‌ریزی-اجرا-بررسی-اقدام (PDCA)

در این استاندارد از چرخهٔ «برنامه‌ریزی-اجرا-بررسی-اقدام» (PDCA) برای ایجاد، اجرا، بهره‌برداری، پایش، اجرا و حفظ و بهبود اثربخشی PIMS سازمان استفاده می‌شود. این امر موجب حصول اطمینان از میزان همخوانی با دیگر استانداردهای سامانهٔ مدیریت می‌شود و از این طریق از اجرای سازگار و یکپارچه و عملیات سامانه‌های مدیریتی مرتبط پشتیبانی می‌کند.

سایر استانداردهای سامانه‌های مدیریتی عبارتند از:

- ایزو ۹۰۰۱ (سیستم مدیریت کیفیت)؛
- ایزو ۱۴۰۰۱ (سیستم مدیریت زیست‌محیطی)؛
- ایزو-آی‌ای‌سی ۲۷۰۰۱ (سیستم‌های اطلاعات مدیریت امنیت).
- ایزو-آی‌ای‌سی ۲۰۰۰۰ (مدیریت خدمات IT).

در شکل الف۱ چگونگی استفاده از الزامات مختلف این استاندارد به عنوان درون‌دادها در PIMS نشان داده شده است و این که از طریق اقدامات و فرآیندهای ضروری، پیامدهای حفاظت داده‌ها (به عنوان مثال اطلاعات شخصی مدیریت‌شده) حاصل می‌شود که آن الزامات را تامین می‌کند.



برنامه‌ریزی	به منظور طرح‌ریزی برای اجرای PIMS	بند ۳
اجرا	به منظور پیاده‌سازی و اجرای PIMS	بند ۴
بررسی	به منظور پایش و بازنگری PIMS	بند ۵
اقدام	به منظور بهبود PIMS	بند ۶

شکل الف۱- چرخهٔPDCA به‌کاربرده‌شده برای سامانهٔ مدیریت اطلاعات شخصی

پیوست ب

(اطلاعاتی)

کتاب‌نامه

[۱] استاندارد ایران-ایزو ۹۰۰۰، سیستم‌های مدیریت کیفیت - مبانی و واژگان

[۲] استاندارد ایران-ایزو ۹۰۰۱، سیستم‌های مدیریت کیفیت -الزامات

[۳] استاندارد ایران-ایزو ۱۴۰۰۱، سیستم‌های مدیریت زیست محیطی -مشخصات همراه با راهنمای استفاده

[۴] استاندارد ملی ایران شماره ۱-۱۶۳۴۷، فنّاوری اطلاعات - مدیریت خدمات قسمت ۱- الزامات سامانه مدیریت خدمات

[۵] استاندارد ملی ایران شماره ۲-۱۶۳۴۷، فناوری اطلاعات- مدیریت خدمات-قسمت ۲: راهنمای کاربرد سامانه‌های مدیریت خدمت

[۶] استاندارد ملی ایران شماره ۳-۱۶۳۴۷، فناوری اطلاعات- مدیریت خدمات- قسمت ۳: راهنمایی برای تعریف دامنه و کاربردپذیری استاندارد ملی ایران شماره‌ی ۱-۱۶۳۴۷

[۷] استاندارد ملی ایران شماره ۲۷۰۰۱، فناوری اطلاعات- فنون امنیتی- سیستم های مدیریت امنیت اطلاعات- الزامات

[8] GREAT BRITAIN. Data Protection Act 1998, London: The Stationery Office. 1998.

[9] PARLIAMENT AND COUNCIL OF THE EUROPEAN COMMUNITY. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. *OJ L 281, 23.11.1995, p. 31–50 (ES, DA, DE, EL, EN, FR, IT, NL, PT, FI, SV).*

[10] GREAT BRITAIN. Freedom of Information Act 2000, London: The Stationery Office. 2000.

[11] INFORMATION COMMISSIONER'S OFFICE.4) *Data Protection Technical Guidance: Determining what information is 'data' for the purposes of the DPA*. 2009.

[12] INFORMATION COMMISSIONER'S OFFICE. *Data Protection Technical Guidance: Determining what is personal data*. 2007.

[13] INFORMATION COMMISSIONER'S OFFICE. *Data Protection Audit Manual*. 2001.

[14] INFORMATION COMMISSIONER'S OFFICE. *Data Protection Act 1998: Legal Guidance.*

[15] PARLIAMENT AND COUNCIL OF THE EUROPEAN COMMUNITY. Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC. *OJ L 105, 13.4.2006, p. 54–63 (ES, CS, DA, DE, ET, EL, EN, FR, IT, LV, LT, HU, MT, NL, PL, PT, SK, SL, FI, SV).*

[16]BIP 0012, *Data Protection: Guide to practical implementation* European Standards Committee CEN/ISSS Personal data protection audit framework