INSO-ISO-IEC- TR

27015

1st.Edition
Identical with
ISO/IEC TR 27015:
2012
Feb.2014

جمهوری اسلامی ایران
Islamic Republic of Iran

سازمان ملی استاندارد ایران
Iranian National Standards Organization

استاندارد ایران-ایزو-آی ای سی- تی آر
۲۷۰۱۵
چاپ اول
اسفند ۱۳۹۲

فناوری اطلاعات — فنون امنیتی — راهنماهای مدیریت امنیت اطلاعات برای خدمات مالی

Information technology — Security techniques — Information security management guidelines for financial services

ICS: 35.040

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.

این گونه سازمان ها و مؤسسات را بر اساس ضوابط نظام تأیید صلاحیت ایران ارزشیابی می‌کند و در صورت احراز شرایط لازم، گواهینامهٔ تأیید صلاحیت به آن ها اعطا و بر عملکرد آن ها 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

« فن‌آوری اطلاعات - فنون امنیتی - راهنماهای مدیریت امنیت اطلاعات برای خدمات مالی »

رئیس :	**سمت و/ یا نمایندگی**
ایزدپناه، سحرالسادات (فوق لیسانس مهندسی فناوری اطلاعات)	کارشناس مسؤل سازمان فناوری اطلاعات ایران
دبیر:	
میر اسکندری، سید محمدرضا (لیسانس مهندسی کامپیوتر نرم افزار)	مدیرکل اداره خدمات ارزش افزوده سازمان فناوری اطلاعات
اعضاء : (اسامی به ترتیب حروف الفبا)	
خوشنویسان، نازنین (فوق لیسانس MBA)	پژوهش‌گر دانشگاه شهید بهشتی
ده موبد، بیژن (لیسانس مهندسی کامپیوتر نرم‌افزار)	نماینده شرکت خدمات انفورماتیک
سجادیه، علیرضا (فوق لیسانس مهندسی کامپیوتر)	مدیرعامل شرکت پردازشگران
سراج زاده، هادی (فوق لیسانس فناوری اطلاعات)	پژوهش‌گر دانشگاه شهید بهشتی
سعیدی، عذراء (فوق لیسانس مهندسی مخابرات)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات
سوزنگر، علی (لیسانس مهندسی کامپیوتر)	رئیس هیات مدیره شرکت اینفوامن
طی نیا، رضا (فوق لیسانس مدیریت فناوری اطلاعات)	مدیر عامل شرکت کاربرد سیستم
فولادیان، مجید (فوق لیسانس مهندسی مخابرات)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات
قسمتی، سیمین (فوق لیسانس فناوری اطلاعات)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات

ناظمی، اسلام
(دکترای مهندسی کامپیوتر)
استادیار دانشگاه شهید بهشتی

نصیری آسایش، حمید رضا
(فوق لیسانس فناوری اطلاعات)
پژوهش‌گر دانشگاه شهید بهشتی

یوسف زاده، سمیرا
(فوق لیسانس مهندسی کامپیوتر نرم‌افزار)
پژوهش‌گر دانشگاه شهید بهشتی

فهرست مندرجات

عنوان **صفحه**

پیش‌گفتار

استاندارد « فناوری اطلاعات - فنون امنیتی - راهنماهای مدیریت امنیت اطلاعات برای خدمات مـالی » کـه پیش نویس آن در کمیسیون های مربوط توسط سازمان فناوری اطلاعات ایران تهیه و تدوین شده است و در سیصد و بیست و سومین اجلاس کمیته ملی استاندارد رایانه و فرآوری داده مورخ ۹۲/۱۱/۲۸ مـورد تصـویب 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 می شود .

برای حفظ همگامی و هماهنگی با تحولات و پیشرفت های ملی و جهانی در زمینه صنایع ، علوم و خدمات ، استانداردهای ملی ایران در مواقع لزوم تجدید نظر خواهد شد و هر پیشنهادی که برای اصلاح و تکمیل ایـن استانداردها ارائه شود ، هنگام تجدید نظر در کمیسیون فنی مربوط مورد توجه قرار خواهد گرفت . بنابراین ، باید همواره از آخرین تجدید نظر استانداردهای ملی استفاده کرد .

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

ISO/IEC TR 27015: 2012, Information technology — Security techniques — Information security management guidelines for financial services

مقدمه

پیشرفت‌های مستمر در فناوری اطلاعات منجر به افزایش وابستگی سازمان‌های ارائه دهنده خدمات مالی به دارایی‌های پردازش اطلاعات آن‌ها شده است. در نتیجه، مدیریت، مشتریان و سازمان های ذیصلاح در تنظیم مقررات، انتظارات مربوط به حفاظت موثر از امنیت اطلاعات مرتبط با این دارایی‌ها و اطلاعات پردازش شده را تشدید کرده‌اند.

از آنجایی‌که استاندارد ملی ایران به شماره ۲۷۰۰۱: سال ۱۳۸۷، استاندارد ملی ایران به شماره ۲۷۰۰۲: سال ۱۳۸۷، اطلاعات مدیریت امنیت و کنترل‌ها، را مشخص می‌کند، این کار را به یک شکل تعمیم یافته انجام می‌دهد.

سازمان‌های ارائه دهنده خدمات مالی از نیازهای امنیت اطلاعات و محدودیت‌های خاص چه در سازمان خود یا در زمان تراکنش‌های مالی با شرکای تجاری که نیاز به سطح بالایی از اعتماد بین ذی‌نفعان مرتبط دارد، برخوردار می باشند.

این استاندارد ملی مکملی برای مجموعه استانداردهای خانواده ISO/IEC 27000[1]، است که برای سازمان-هایی که خدمات مالی ارائه می‌دهند، استفاده می‌شود. به‌ویژه، راهنمایی‌های مندرج در این استاندارد ملی مکملی بر کنترل‌های امنیت اطلاعات می‌باشد که در استاندارد ملی ایران به شماره ۲۷۰۰۲: سال ۱۳۸۷، تعریف شده است.

توصیه می‌شود، اصطلاح «خدمات مالی» به عنوان خدمات در مدیریت، سرمایه‌گذاری، انتقال، یا اعطای تسهیلات برداشت شود، که توسط سازمان‌هایی که تخصص‌های مالی را به جای فروش محصولات فیزیکی (یعنی هر کسی در «کسب‌وکار پول») ارائه می‌دهند، تهیه و تدارک دیده شود.

با استفاده از این استاندارد ملی، علاوه بر پیاده‌سازی استاندارد ملی ایران به شماره ۲۷۰۰۱: سال ۱۳۸۷ و استاندارد ملی ایران به شماره ۲۷۰۰۲: سال ۱۳۸۷، سازمان‌هایی که خدمات مالی ارائه می‌دهند، ممکن است سطح بالاتری از اعتماد درون سازمان با مشتریان و شرکای کسب‌وکار خود ایجاد کنند. به‌ویژه، زمانی که بتوان نشان داد هدایت بخش خاص برای مدیریت امنیت اطلاعات اقتباس شده است.

این استاندارد ملی نشان‌دهنده آخرین پیشرفت‌ها است و با هدف صدور گواهی تهیه نشده است.

---

۱ - استاندارد بین‌المللی ISO/IEC 27000:2009، با شماره ملی ۲۷۰۰۰ در سال ۱۳۹۱ منتشر شده است.

فناوری اطلاعات ـ فنون امنیتی ـ راهنماهای مدیریت امنیت اطلاعات برای خدمات مالی

۱ هدف و دامنه کاربرد

هدف از تدوین این استاندارد، تعیین راهنمای امنیت اطلاعاتی است که مکمل و افزوده‌ای بر کنترل‌های امنیت اطلاعات تعریف شده در استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۸۷، برای راه‌اندازی، پیاده‌سازی، نگهداری و بهبود امنیت اطلاعات درون سازمان‌هایی ارائه کننده خدمات مالی، است

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 محسوب می شوند.

در صورتی که به مدرکی با ذکر تاریخ انتشار ارجاع داده شده باشد، اصلاحیه‌ها و تجدید نظرهای بعدی آن مورد نظر این استاندارد ملی ایران نیست. در مورد مدارکی که بدون ذکر تاریخ انتشار به آن‌ها ارجاع داده شده است، همواره آخرین تجدید نظر و اصلاحیه‌های بعدی آن‌ها مورد نظر است.

استفاده از مراجع زیر برای این استاندارد الزامی است:

۲-۱ استاندارد ملی ایران شماره ۲۷۰۰۰: سال ۱۳۹۱، فناوری اطلاعات - فنون امنیتی – سامانه‌های مدیریت امنیت اطلاعات - مرور کلی و واژگان

۳ اصطلاحات، تعاریف و کوته‌نوشت‌ها

۳-۱ اصطلاحات و تعاریف

در این استاندارد علاوه بر اصطلاحات و تعاریف تعیین شده و در استاندارد ملی ایران به شماره ۲۷۰۰۰: سال ۱۳۹۱، اصطلاحات و تعاریف زیر نیز به‌کار می‌رود:

۳-۱-۱

خدمات مالی [1]

خدمات مورد استفاده در مدیریت، سرمایه‌گذاری، انتقال یا اعطای تسهیلات است.

۳-۲ کوته‌نوشت‌ها

ماشین تحویل‌دار خودکار	Automatic Teller Machines	ATM

1 - Financial services

COBIT	Control Objectives for Information Technology	اهداف کنترلی برای فناوری اطلاعات
OTP	One-Time Password	اسم‌رمز یک بار مصرف
PCI-DSS	Payment Card Industry - Data Security Standard	صنعت کارت پرداخت - استاندارد امنیت داده
POS	Point Of Sale	نقطه فروش
SST	Self Service Terminal	پایانه خودخدمتی

٤ ساختار این استاندارد ملی

راهنمای امنیت اطلاعات مکمل و افزوده‌ای بر کنترل‌های امنیت اطلاعات از استاندارد ملی ایران به شماره ۲۷۰۰۲: سال ۱۳۸۷را در بندهای ۵ تا ۱۵ ارائه می‌کند.

٥ خط‌مشی امنیتی[1]

هیچ راهنمای افزوده‌ای برای سازمان‌های ارائه دهنده خدمات مالی وجود ندارد.

٦ سازمان امنیت اطلاعات

٦-١ سازمان داخلی

٦-١-١ تعهد مدیریت به امنیت اطلاعات

هیچ راهنمای افزوده‌ای برای سازمان‌های ارائه دهنده خدمات مالی وجود ندارد.

٦-١-٢ هماهنگی امنیت اطلاعات

هیچ راهنمای افزوده‌ای برای سازمان‌های ارائه دهنده خدمات مالی وجود ندارد.

٦-١-٣ تخصیص مسؤولیت‌های امنیت اطلاعات

کنترل ۶-۱-۳ از استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۸۷ به شرح زیر تکمیل می‌شود:

راهنمای پیاده‌سازی

توصیه می‌شود سازمانی که خدمات مالی ارائه می‌دهد قوانین و مقررات به همراه چارچوب‌های صنعت مرتبط و موارد زیر را در تعریف نقش‌های امنیت اطلاعات و الزامات مسؤولیت‌ها مورد توجه قرار دهد.

همچنین توصیه می‌شود سازمانی که خدمات مالی ارائه می‌دهد، برای اطمینان از پیاده‌سازی محلی، الزامات مرتبط و توصیه‌نامه‌هایی که توسط شرکای بین‌المللی در رابطه با تعریف آن از نقش و مسؤولیت‌های امنیت شرح داده شده است را مورد توجه قرار دهد.

مثال‌هایی از چارچوب‌هایی که به طور کلی توسط سازمان‌های ارائه کننده خدمات مالی استفاده شده و اطلاعاتی در مورد تخصیص نقش و مسؤولیت‌های امنیت اطلاعات را ارائه می‌کنند، به شرح زیر است:

---

1 - Security Policy

الف- PCI-DSS با زیربند زیر فهرست شده است:

۱- PCI زیربند ۱۲-۵ مسؤولیت‌های مدیریت امنیت اطلاعات تخصیص داده شده.

ب- COBIT با زیربند زیر فهرست شده است:

۲- زیربند ۴-۰ تعریف سازمان فناوری اطلاعات و روابط

۳- زیربند ۴-۴ نقش‌ها و مسؤولیت‌ها.

۴-زیربند ۴-۶ مسؤولیت برای امنیت منطقی و فیزیکی.

برای اطمینان از انطباق با تغییرات در الزامات و توصیه‌نامه‌هایی که به واسطه قوانین، مقررات، چارچوب‌های صنعت و شرکا مشخص شده است، نقش‌ها و مسؤولیت‌های تعیین شده‌ی امنیت اطلاعات باید به صورت منظم بازنگری شود.

٦-١-٤ فرایند مجوزدهی برای تسهیلات پردازش کننده اطلاعات

هیچ راهنمای افزوده‌ای برای سازمان‌های ارائه دهنده خدمات مالی وجود ندارد.

٦-١-٥ توافق‌نامه‌های محرمانگی[1]

هیچ راهنمای افزوده‌ای برای سازمان‌های ارائه دهنده خدمات مالی وجود ندارد.

٦-١-٦ برقراري ارتباط با صاحبان اختیار[2]

هیچ راهنمای افزوده‌ای برای سازمان‌های ارائه دهنده خدمات مالی وجود ندارد.

٦-١-٧ برقراري ارتباط با گروه‌هاي خاص موردنظر

کنترل ۶-۱-۷ از استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۸۷، به شرح زیر تکمیل می‌شود:

راهنمای پیاده‌سازی

علاوه بر راهنمایی ارائه شده در استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۸۷، توصیه می‌شود عضویت در گروه‌های خاص موردنظر یا انجمن‌ها به عنوان وسیله‌ای برای مورد زیر در نظر گرفته شود:

الف- به اشتراک‌گذاشتن و تبادل محرمانه اطلاعات در مورد فعالیت‌های مجرمانه و کلاهبرداری‌های اخیر

٦-١-٨ بازنگري مستقل امنیت اطلاعات

هیچ راهنمای افزوده‌ای برای سازمان‌های ارائه دهنده خدمات مالی وجود ندارد.

---

1 - Confidentiality agreements

2 - Contact with authorities

٦-٢ طرف‌هاي خارجی[1]

٦-٢-١ شناسایی مخاطره‌های مرتبط با طرف‌هاي خارجی

کنترل ۶-۲-۱ از استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۸۷، به شرح زیر تکمیل می‌شود:

راهنمای پیاده‌سازی

علاوه بر راهنمایی‌هایی که در استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۸۷، ارائه شده است، هنگام شناسایی مخاطره‌های مرتبط با دسترسی طرف خارجی، موضوع‌های زیر باید توسط سازمانی که ارائه دهنده خدمات مالی است، در نظر گرفته شود:

الف- الزامات قانونی و مقرراتی، همراه با تعهدات قراردادی که به طرف خارجی مستقر در کشورهای دیگر تحمیل شده و می‌تواند اطلاعات مشتری و اطلاعات مالی را برای طرف سوم (به عنوان مثال سازمان اصلی مادر، نمایندگی یا مقام دولتی) بدون اطلاع قبلی به سازمان، افشا نماید. این مساله می‌تواند منجر به افشای غیرمجاز اطلاعات و نقض‌های امنیتی قابل توجه شود.

٦-٢-٢ نشانی‌دهي امنیت هنگام تعامل داشتن با مشتریان

کنترل ۶-۲-۲ از استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۸۷، به شرح زیر تکمیل می‌شود:

راهنمای پیاده‌سازی

توصیه می‌شود علاوه بر راهنمایی‌هایی که در استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۸۷، ارائه شده است، اصول زیر برای نشانی‌دهی امنیت هنگام تعامل با مشتریان در نظر گرفته شود:

الف- به منظور بالا بردن آگاهی مشتریان، سازمان باید خدمات مشاوره امنیت اطلاعاتی را پیرامون تهدیدهایی (در مورد اسب‌های تروا[2]، حمله صیادی[3]، تماس‌های کلاهبرداری[4]...) که ممکن است مخاطره‌های امنیت اطلاعات برای آن‌ها ایجاد کند، ارائه نماید.

توصیه می‌شود این مشاوره درخور نیازهای مشتری و متناسب با نیازهای ارتباطی فنی انتخاب شود تا از موثر بودن آگاهی بخشی به مشتری، اطمینان حاصل گردد.

به منظور اطمینان از موثر و مناسب باقی ماندن مشاوره امنیت اطلاعات ارائه شده به مشتریان، برای رُخنما[1] مخاطره سازمان و نشانی‌دهی تهدیدهای امنیتی جدید، سازمان باید به صورت مرتب این خدمات مشاوره را بازنگری کند.

1- External Parties

2 - Trojans

۱- برنامه رایانه که با تابعی به ظاهر مفید که به طور پنهانی دارای توابعی است که علیه سامانه عمل می‌کند.

3 - Phishing

۲ – روشی در سرقت اطلاعات است که هدف آن اغفال کاربران جهت دزدیدن اطلاعات خصوصی است.

4 - Fraudulent calls

مثال‌هایی از مشاوره امنیت اطلاعات داده شده به طور معمول عبارتند از:

۱- به کار بردن کنترل‌های مناسب (مانند حفاظت به کمک اسم‌رمز، آنتی ویروس) برای تامین امنیت رایانه‌های شخصی و دیگر افزاره‌ها که برای دسترسی به خدمات بانکداری اینترنتی استفاده می‌شود.

۲- عدم افشای اطلاعات مشتری و اطلاعات مالی(به عنوان مثال شماره کارت پرداخت) در موارد غیر ضروری و جایی که یکپارچگی[۲] گیرنده مورد تردید است.

۳- از بین بردن امن کارت‌های پرداخت منقضی شده یا غیر قابل استفاده.

مثال‌هایی از توصیه‌نامه‌هایی که می‌توان به مشتری ارائه داد:
الف- برش صحیح کارت پرداخت[۳].

ب- استفاده از خُردکننده برای از بین بردن کارت پرداخت.

پ- اطمینان از نابود شدن تراشه[۴] و نوار مغناطیسی کارت پرداخت.

ت- استفاده از چندین سطل زباله واقع در مکان‌های مختلف برای دور انداختن قطعات کارت.

ث- پرهیز از به کارگیری سطل بازیافت[۵] برای دور انداختن قطعات کارت، به دلیل امکان مداخله بالقوه انسانی در مراکز بازیافت.

۴- انجام اقدامات حفاظتی هنگام انجام فعالیت‌های بانکی، برای اطمینان از اینکه هیچ‌کسی قادر به مشاهده یا دسترسی به اعتبارنامه کاربر[۶] یا دیگر اطلاعات امنیتی فناوری اطلاعات نیست.

۵- استفاده از سازوکارهای اصالت‌سنجی امن مانند استفاده از اسم‌رمز قوی، کدهای شماره شناسایی شخصی(PIN Codes)[۷] یا تأیید اعتبار دو عاملی در هر جا که در دسترس است.

۶- پرهیز از به کارگیری اسم‌رمز یکسان برای دسترسی به خدمات بانکداری اینترنتی که توسط سازمان‌های مختلف ارائه شده است.

۷- پرهیز از به کارگیری PIN Codeیکسان برای همه کارت‌های پرداخت.

---

1 - profile
2 - Integrity

٦- شامل کارت خرید، هدیه بن کارت

4 - Chip
5 - Recycling bin
6 - User credentials
7 - PIN codes

۸- یادآوری به مشتریان که سازمان درخواست‌های دریافت اطلاعات اصالت‌سنجی (مانند اسم‌رمز، PIN Code) را انجام نمی‌دهد.

۹- اطلاع رسانی به مشتریان برای پایش منظم تراکنش‌ها و صورت حساب‌ها.

۱۰- اطلاع رسانی به مشتری در مورد رویه قابل انجام هنگام شک به کلاهبرداری و سرقت هویت (حتی تلاش وابسته به آن).

به منظور کاهش مخاطره‌ای که هدف آن کلاه‌برداری است، ممکن است سازمان، مقایسه گسترده و منظم مشتری با همتایان خود و با انجمن صنعت خدمات مالی را سودمند یابد.

ب- توصیه می‌شود موارد زیر از طرف سازمان به اطلاع مشتریان برسد:

۱- معرفی یک رابط تماس اختصاصی امنیتی، که مشتریان هر گونه مسائل مربوط به امنیت اطلاعات یا نگرانی‌های خود در رابطه با استفاده از خدمات مالی ارائه شده توسط سازمان را با او در میان بگذارند.

۲- اقداماتی که باید توسط مشتری صورت پذیرد در زمانی که اطلاعات اصالت‌سنجی مشتری (به عنوان مثال اسم‌رمز، PIN Code) به خطر بیافتد، حتی اگر این مساله نتیجه خطای خود مشتری باشد.

۳- روش ارائه گزارش در خصوص رویدادهای غیرمنتظره هنگام تلاش برای دستیابی به خدمات مالی ارائه شده توسط سازمان.

پ- توصیه می‌شود سازمان موارد زیر را هنگام ایجاد سامانه تراکنش‌های بر خط (به طور مثال خدمات بانکداری اینترنتی) برای مشتریان، زیر نظر داشته باشد:

۱- شرایط و ضوابط استفاده از سامانه تراکنش بر خط. توصیه می‌شود توجه ویژه‌ای در به رسمیت شناختن قانونی تراکنش‌های انجام شده در راستای مقررات اعمال شود.

۲- بیانیه روشن در مورد نقش‌ها و مسؤولیت‌ها همچنین تعهدهایی که به سازمان و مشتری ارجاع داده می‌شود.

۳- بیانیه روشن در مورد حفظ حریم خصوصی و پایش نحوه استفاده مشتری، از جمله پایش کلاهبرداری در سامانه تراکنش بر خط، با هدف تامین حفاظت از منافع مشتری و سازمان.

۴- تخصیص حقوق دسترسی بر اساس اصول زیر استوار است:

الف- مشتری خود را بشناسید: این اصل توسط تنظیم کنندگان مقررات مورد استفاده قرار می‌گیرد تا نگرش خود به موسسات مالی را از دیدگاه آگاهی از فعالیت‌های مشتریان بیان کنند.

ب- نیاز به دانستن: این اصل قدرت دسترسی به اطلاعات و منابع مربوط به پردازش اطلاعات در سطحی که برای تحقق فعالیت‌های خاص زیاد مورد نیاز نیست را محدود می‌کند

پ- کنترل دوگانه: این اصل به حفظ یکپارچگی فرآیند و مبارزه با تحریف عملکرد نیاز سامانه به (الگوریتم، زمان، منابع و دیگر موارد) پشتیبان‌گیری از عملیات تا اتمام تراکنش‌های خاص می‌پردازد.

۵- ایجاد موارد زیر:

الف- روش‌های قوی اصالت‌سنجی کاربر (به عنوان مثال نمودافزار[1] OTP، گواهی کاربر).

ب- سامانه درستی‌سنجی برای حصول اطمینان از درستی اعتبارنامه کاربر حاضر و ابزار ارائه شده.

پ- درستی‌سنجی سطح به رسمیت شناختن صاحبان اختیار گواهی‌دار[2].

۶- شناسه کاربر به صورت منحصر به فرد به هر یک از مشتریان اختصاص داده شده است.

۷- سازوکارهای اطلاع‌رسانی برای آگاهی دادن به مشتریان (به صورت منظم، به طور مداوم و یا در صورت درخواست) در مورد تمام عملیات انجام شده از طرف آن‌ها.

سایر اطلاعات

در حالی که مشتریان بسیاری از صنایع یا ارائه‌دهندگان خدمات ممکن همان ذی‌نفعان کسب‌وکار باشند، به طور کلی در محتوای خدمات مالی، سازمان وظیفه‌ی ارائه مشاوره به مشتریان خود برای اقدامات حفاظتی مناسب را دارد. اگر نقض یا ضرری رخ دهد، ممکن است سازمان با خطر آسیب مالی یا اعتبار روبرو شود.

۶-۲-۳ نشانی‌دهی امنیت در توافق‌نامه‌های طرف سوم

کنترل ۶-۲-۳ از استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۸۷، به شرح زیر تکمیل می‌شود:

راهنمای پیاده‌سازی

توصیه می‌شود علاوه بر راهنمایی‌هایی که در استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۸۷، ارائه شده است، اگر دامنه کاربرد به خدمات مالی که توسط سازمان ارائه می‌شود مرتبط باشد، موارد زیر برای رسیدگی به توافق‌نامه تامین‌کننده در نظر گرفته شود:

1 - Token
2 - Certificate Authorities

الف- یک نقطه تماس مجاز که باید به درخواست های سازمان رسیدگی نماید.

ب- تهیه‌ی مدارک دارایی که ممکن است تامین‌کننده، در دوره اجرای توافق‌نامه ایجاده کرده باشد.

پ-اطلاع رسانی به موقع درباره تغییرات امنیتی داخل دارایی تامین‌کننده که تحویل خدمات مالی سازمان را پشتیبانی می‌کند.

ت- تضمین در مورد اینکه اطلاعات سازمان که در دسترس تامین‌کننده است فقط تحت شرایط و ضوابط مشخص شده در قرارداد، پردازش خواهد شد.

ث- تضمینی در مورد اینکه تغییرات پیمانکاران فرعی یا محل ذخیره‌سازی اطلاعات پردازش شده سازمان (به عنوان مثال برون‌سپاری) به سازمان ابلاغ خواهد شد و می‌توان به تایید قبلی که با سازمان انجام شده بود، به‌ویژه هنگامی که شامل پردازش اطلاعات سازمان می‌شود ارجاع داده شود.

ج- تضمین رخدادی[1] که در دوره اجرای توافق‌نامه تامین‌کننده پدیدار می‌شود و به موقع به سازمان گزارش داده خواهد شد و تحقیقات مناسب توسط تامین کننده به انجام خواهد رسید

چ-دخالت تامین‌کننده در مورد یک حادثه یا یک رویداد مشکوک ممکن است فراتر از مرزهای سازمان برود. توصیه می‌شود توجه لازم برای اطمینان از واکنش تامین‌کننده در توانمندی آن در پایش یا لغو یک تراکنش مالی که در میان سازمان‌های مختلفی توزیع شده است، انجام شود، به‌ویژه اگر در مورد قانونی بودن آن تردیدی وجود داشته باشد.

ح- حق موارد زیر را داشته باشد:

۱- ممیزی پیمانکاران فرعی به همان سطح تعریف شده برای تامین‌کننده.

۲- دسترسی به اطلاعات تامین‌کننده و عملیات و پیمانکاران فرعی آن به واسطه تنظیم‌کننده‌های سازمان.

۷ مدیریت دارایی

۷-۱ مسؤولیت دارایی

۷-۱-۱ دفتر دارایی‌ها

کنترل ۷-۱-۱ از استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۸۷، به شرح زیر تکمیل می‌شود:

راهنمای پیاده‌سازی

مراقبت از موارد زیر توسط سازمان توصیه می‌شود:

1 - Incident

الف- دارایی‌های خاص مورد استفاده در محتوای ارائه خدمات مالی، مانند افزاره پرداخت (ATM، SST، POS)، کارت‌های پرداخت (بدهکاری، اعتبار، کارت اعتباری[1]) و سامانه‌های درون‌بانکی ذخیره شده در مکان مشخص یا نامشخص در دفتر دارایی‌های آن گنجانده شده است.

ب- فهرست موجودی کارت‌های پرداخت که توسط تامین‌کننده، نگهداری می‌شود (مانند ارائه‌دهنده خدمات پرداخت، که تصویب پرداخت با کارت‌های پرداخت صادر شده توسط سازمان و از طرف آن را انجام می‌دهد) همواره درست است و شامل وضعیت درست (معتبر یا لغو شده) کارت‌های پرداخت صادر شده است، تا از پردازش پرداخت‌های انجام شده با کارت پرداخت غیرمجاز جلوگیری کند.

۷-۱-۲ مالکیت دارایی[2]

هیچ راهنمای افزوده‌ای برای سازمان‌های ارائه دهنده خدمات مالی وجود ندارد.

۷-۱-۳ استفاده قابل قبول از دارایی‌ها[3]

کنترل ۷-۱-۳ از استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۸۷، به شرح زیر تکمیل می‌شود:

راهنمای پیاده‌سازی

سازمانی که خدمات مالی ارائه می‌دهد همچنین باید متعهد شود که قوانین مربوط به اداره و دسترسی یکنواختی‌ها و هر گونه اقلام نماهای دیگر، از جمله قالب پیش‌چاپ شده، به منظور جلوگیری از استفاده غیرمجاز از آن‌ها برای ارتکاب کلاهبرداری یا فعالیت‌های مجرمانه ایجاد شده است.

۷-۲ طبقه‌بندي اطلاعات

هیچ راهنمای افزوده‌ای برای سازمان‌های ارائه دهنده خدمات مالی وجود ندارد.

۸ امنیت منابع انسانی
۸-۱ پیش از اشتغال[4]
۸-۱-۱ نقش‌ها و مسؤولیت‌ها

هیچ راهنمای افزوده‌ای برای سازمان‌های ارائه دهنده خدمات مالی وجود ندارد.

1 - Prepaid Card
2 - Ownership of Assets
3 - Acceptable Use of Assets
4 - Prior to employment

۸-۱-۲ گزینش[1]

کنترل ۸-۱-۲ از استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۸۷، به شرح زیر تکمیل می‌شود:

راهنمای پیاده‌سازی

سازمان ارائه‌دهنده خدمات مالی، نیاز دارد از جرایم سازمان‌یافته[2] که ممکن است کارکنانی در فرآیندهای کلیدی کسب‌وکار جای دهند آگاهی داشته باشد.

به‌ویژه، عملیات خاص، با اطمینان اینکه بررسی پیشینه[3] با جزییات کامل تا جایی که قانون اجازه می‌دهد اعمال شده است. مثال‌هایی از این عملیات در زیر آورده شده است:

الف- همه کارکنان به اطلاعات مالی و اطلاعات مشتری دسترسی دارند (به عنوان مثال اطلاعات مربوط به کارت پرداخت، اسم‌رمز مشتریان، PIN Code)

ب- سرپرستان[4] سامانه، مسؤول پردازش اطلاعات مشتری و اطلاعات مالی هستند.

پ-متولیان امنیتی مسؤول مدیریت کلیدهای رمزنگاری که برای اهداف زیر استفاده می‌شود هستند:

۱-انتقال و ذخیره‌سازی اطلاعات مربوط به مشتری و اطلاعات مالی.

۲-اصالت سنجی تراکنش مالی.

۳-اسم‌رمز مشتری، PIN Code یا مدیریت اصالت‌سنجی دو عاملی.

۸-۱-۳ ضوابط و شرایط استخدام

کنترل ۸-۱-۳ از استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۸۷، به شرح زیر ارتقا یافته است:

راهنمای پیاده‌سازی

همچنین توصیه می‌شود شرایط و ضوابط استخدام نیز ترکیبی از خط‌مشی مرخصی که به سازمان و کارمند تامین‌کنندگان که فعالیت‌های مالی حساس را به انجام می‌رساند، اعمال شود.

به عنوان سنجه ضد-کلاهبرداری خط‌مشی مرخصی باید یک دوره حداقل مرخصی (به عنوان مثال ۱۰ روز متوالی کاری در هر سال تقویمی) را به منظور حصول اطمینان از اینکه فعالیت‌های مالی حساس همواره و فقط توسط همان شخص انجام نمی‌شود، به اجرا درآورد.

۸-۲ حین خدمت

۸-۲-۱ مسؤولیت‌های مدیریت

هیچ راهنمای افزوده‌ای برای سازمان‌های ارائه دهنده خدمات مالی وجود ندارد.

---

1 - Screening
2 - Organized Crime
3 - Background Checks
4 - Administrators

۸-۲-۲ آگاه‌سازی، تحصیل و آموزش امنیت اطلاعات

کنترل ۸-۲-۲ از استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۸۷، به شرح زیر ارتقا یافته است:

راهنمای پیاده‌سازی

سازمان ارائه دهنده خدمات مالی باید توجه داشته باشد که قوانین و مقررات آن، همراه با بیانیه تنظیم-کنندگان، نیازمند مسائل خاص (مانند استفاده از تلفن برای انتشار اطلاعات مالی و اطلاعات مشتری، برنامه-های ضد پول‌شویی[1]) برای مشخص کردن آگاه‌سازی امنیت و فعالیت‌های آموزش به سازمان است.

آگاهی رسانی امنیت اطلاعات نیز باید موضوع‌های خاص مانند مهندسی اجتماعی[2]، صیادی، بردارهای برخط حمله[3]، کارت‌های دستکاری سامانه و مخرب نرم‌افزار را مشخص کند.

۸-۳ خاتمه استخدام یا تغییر در شغل

راهنمای اضافه برای سازمان‌های ارائه دهنده خدمات مالی وجود ندارد.

۹ امنیت فیزیکی و محیطی

۹-۱ نواحی امن

۹-۱-۱ حصار امنیت فیزیکی

هیچ راهنمای افزوده‌ای برای سازمان‌های ارائه دهنده خدمات مالی وجود ندارد.

۹-۱-۲ کنترل مدخل فیزیکی

هیچ راهنمای افزوده‌ای برای سازمان‌های ارائه دهنده خدمات مالی وجود ندارد.

۹-۱-۳ ایمن‌سازی دفاتر، اتاق‌ها و تسهیلات

هیچ راهنمای افزوده‌ای برای سازمان‌های ارائه دهنده خدمات مالی وجود ندارد.

۹-۱-٤ محافظت در برابر تهدیدهای خارجی و محیطی

هیچ راهنمای افزوده‌ای برای سازمان‌های ارائه دهنده خدمات مالی وجود ندارد.

۹-۱-۵ کار در نواحي امن

کنترل ۹-۱-۵ از استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۸۷، به شرح زیر تکمیل می‌شود:

راهنمای پیاده‌سازی

---

1 - Money laundering
2 - Social Engineering
3 - Online Vectors of Attack

توصیه می‌شود که برای جلوگیری از ثبت‌های غیرمجاز یا انتقال اطلاعات، استفاده از افزاره‌های تلفن همراه به خصوص در مناطق کلیدی پردازش کسب‌وکار و در جاهایی که شماره کارت پرداخت یا دیگر اطلاعات مربوط به مشتری در دسترس است یا پردازش شده است، محدود شده باشد.

۹-۱-۶ دسترسی عمومی، نواحی تحویل و بارگیری

۹-۲ امنیت تجهیزات

۹-۲-۱ استقرار و حفاظت تجهیزات

کنترل ۹-۲-۱ از استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۸۷، به شرح زیر تکمیل می‌شود:

راهنمای پیاده‌سازی

برای محافظت از افزاره‌های پرداخت (به عنوان مثال ATM، SST، POS) که در خارج از محل سازمان واقع شده‌اند، پردازش اطلاعات مالی یا اطلاعات مشتری یا دارایی‌های مادی در برابر تغییر غیرمجاز، باز کردن و سرقت باید توجه ویژه شود. اقدامات امنیتی پیاده‌سازی شده باید شامل، به عنوان مثال، شاسی(چارچوب) ساخته شده و ثابت، سازوکار تخریب خودکار و همچنین حفاظت از هر گونه کابل کشی باشد.

۹-۲-۲ بهره‌برداری پشتیبانی

هیچ راهنمای افزوده‌ای برای سازمان‌های ارائه دهنده خدمات مالی وجود ندارد.

۹-۲-۳ امنیت کابل‌کشی

هیچ راهنمای افزوده‌ای برای سازمان‌های ارائه دهنده خدمات مالی وجود ندارد.

۹-۲-۴ نگهداری تجهیزات

هیچ راهنمای افزوده‌ای برای سازمان‌های ارائه دهنده خدمات مالی وجود ندارد.

کنترل ۹-۲-۴ از استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۸۷، به شرح زیر تکمیل می‌شود:

راهنمای پیاده‌سازی

علاوه بر راهنمایی که در استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۸۷، ارائه شده، همچنین توصیه می‌شود سازمان ایجاد کنترل دوگانه برای نگهداری از افزاره‌های پرداخت (به عنوان مثال ATM، SST، POS) را در نظر بگیرد.

۹-۲-۵ امنیت تجهیزات خارج از محل

هیچ راهنمای افزوده‌ای برای سازمان‌های ارائه دهنده خدمات مالی وجود ندارد.

۹-۲-۶ امحاء یا استفاده مجدد از تجهیزات به صورت امن

کنترل ۹-۲-۶ از استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۸۷، به شرح زیر تکمیل می‌شود:

راهنمای پیاده‌سازی

توصیه می‌شود که از نابودی امن، حذف یا رونویسی پیش از امحاء اطلاعات ذخیره شده مشتری و اطلاعات مالی در مولفه‌های حافظه (مانند افزاره‌های خودپرداز، SST، دیسک‌های سخت، حافظه داخلی POS) افزاره‌های پرداخت اطمینان حاصل نمود.

۹-۲-۷ خروج اموال

هیچ راهنمای افزوده‌ای برای سازمان‌های ارائه دهنده خدمات مالی وجود ندارد.

۱۰ مدیریت ارتباطات و عملیات

۱۰-۱ روش‌های اجرایی عملیاتی و مسؤولیت‌ها

۱۰-۱-۱ روش‌های اجرایی عملیاتی مدون

هیچ راهنمای افزوده‌ای برای سازمان‌های ارائه دهنده خدمات مالی وجود ندارد.

۱۰-۱-۲ مدیریت تغییر

هیچ راهنمای افزوده‌ای برای سازمان‌های ارائه دهنده خدمات مالی وجود ندارد.

۱۰-۱-۳ تفکیک وظایف

کنترل ۱۰-۱-۳ از استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۸۷، به شرح زیر تکمیل می‌شود:

راهنمای پیاده‌سازی

تفکیک وظایف باید در محدوده سامانه تراکنش‌های مالی اعمال شود تا اطمینان حاصل شود که نه تنها شروع یک رویداد، از جمله تراکنش مالی، از پردازش یا مجوز آن جدا است بلکه این شروع از درستی‌سنجی آن هم جدا است. سازمان باید حداقل از کنترل دوگانه مدیریت تراکنش‌های مالی اطمینان داشته باشد، یعنی پردازش اطلاعات مالی یا تراکنش و درستی‌سنجی نتیجه‌ی فرآیند انجام شده توسط کارکنان مختلف یا فرآیندهای خودکار باشد.

۱۰-۱-٤ جداسازی تسهیلات توسعه، آزمون و عملیاتی

هیچ راهنمای افزوده‌ای برای سازمان‌های ارائه دهنده خدمات مالی وجود ندارد.

۱۰-۲ مدیریت تحویل خدمت طرف سوم

هیچ راهنمای افزوده‌ای برای سازمان‌های ارائه دهنده خدمات مالی وجود ندارد.

۱۰-۳ طرح‌ریزی و پذیرش سامانه

۱۰-۳-۱ مدیریت ظرفیت

کنترل ۱۰-۳-۱ از استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۸۷، به شرح زیر تکمیل می‌شود:

راهنمای پیاده‌سازی

توصیه می‌شود توجه شود که از تعریف نیازمندی‌های ظرفیت برای دارایی‌های که در ادامه آورده شده‌اند کـه یا اجرا یا برای استقرار طرح‌ریزی شده‌اند اطمینان حاصل شود:

الف- خدمات بانکداری اینترنتی، که مبتنی بر الزامات کسب‌وکار که در زیر آورده شده‌اند مورد توجه است:
۱- تعداد تراکنش‌های جاری و مورد انتظار.
۲- دوره اوج، صعود ناگهانی جاری و مورد انتظار در تراکنش‌ها.
۳- تعداد مشتریان جاری.
۴- رشد مورد انتظار در تعداد مشتریان.
۵- اطمینان از در دسترس بودن خدمات بانکداری اینترنتی حتی در زمانی که با نرخ بالای دسترسی مشتریان مواجه هستند.

ب- افزاره‌های پرداخت (به عنوان مثال ATM، SST، POS) که پردازش اطلاعات مشتری و اطلاعات مالی را انجام می‌دهند.

۱۰-۳-۲ پذیرش سامانه

هیچ راهنمای افزوده‌ای برای سازمان‌های ارائه دهنده خدمات مالی وجود ندارد.

۱۰-٤ حفاظت در برابر بدافزارها و کدهای سیار[1]

۱۰-٤-۱ کنترل‌هایی در برابر کدهای مخرب

کنترل ۱۰-۴-۱ از استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۸۷، به شرح زیر تکمیل می‌شود:

راهنمای پیاده‌سازی

بررسی‌های انجام شده جهت تشخیص کدهای مخرب و اصلاح نرم‌افزار باید دربرگیرنده افزاره‌هـای پرداخـت (به عنوان مثال ATM، SST، POS) که پردازش اطلاعات مشتری و اطلاعات مالی را انجام می‌دهند و اغلـب کمتر مورد توجه کدهای مخرب قرار می‌گیرند باشد.

۱۰-٤-۲ کنترل‌هایی در برابر بدافزارها

هیچ راهنمای افزوده‌ای برای سازمان‌های ارائه دهنده خدمات مالی وجود ندارد.

۱۰-۵ نسخ پشتیبان

هیچ راهنمای افزوده‌ای برای سازمان‌های ارائه دهنده خدمات مالی وجود ندارد.

۱۰-٦ مدیریت امنیت شبکه

هیچ راهنمای افزوده‌ای برای سازمان‌های ارائه دهنده خدمات مالی وجود ندارد.

1 - Mobile Code

۱۰-۷ سامان‌دهی محیط

۱۰-۷-۱ مدیریت محیط‌های ذخیره‌سازی قابل جابجایی

هیچ راهنمای افزوده‌ای برای سازمان‌های ارائه دهنده خدمات مالی وجود ندارد.

۱۰-۷-۲ امحاء محیط‌های ذخیره‌سازی

کنترل ۱۰-۷-۲ از استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۸۷، به شرح زیر تکمیل می‌شود:

راهنمای پیاده‌سازی

توصیه می‌شود توجه شود تا از روش دسترسی امن برای همه نوع دارایی‌ها، پردازش اطلاعات مشتری و اطلاعات مالی (به عنوان مثال اطلاعات مربوط به کارت پرداخت، اسم‌رمز مشتریان، PIN Code) به همراه دارایی‌های خاص مورد استفاده کارت‌های پرداخت مانند نوار ماشین تحریر، اطمینان حاصل شود.

۱۰-۷-۳ روش‌های اجرایی سامان‌دهی اطلاعات

کنترل ۱۰-۷-۳ از استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۸۷، به شرح زیر تکمیل می‌شود:

راهنمای پیاده‌سازی

همچنین توصیه می‌شود سازمان اطمینان یابد که روش‌های اجرایی جابجایی اطلاعات اداره کردن امحاء چک و دفترچه سپرده، چک و کارت‌های پرداخت (بدهی، اعتبار، کارت اعتباری) و دیگر انواع ثابت چاپ شده را نشانی‌دهی می‌کند.

۱۰-۷-٤ امنیت مستندات سامانه

هیچ راهنمای افزوده‌ای برای سازمان‌های ارائه دهنده خدمات مالی وجود ندارد.

۱۰-۸ تبادل اطلاعات

هیچ راهنمای افزوده‌ای برای سازمان‌های ارائه دهنده خدمات مالی وجود ندارد.

۱۰-۹ خدمات تجارت الکترونیک

۱۰-۹-۱ تجارت الکترونیک

هیچ راهنمای افزوده‌ای برای سازمان‌های ارائه دهنده خدمات مالی وجود ندارد.

۱۰-۹-۲ تراکنش‌های بر خط[1]

هیچ راهنمای افزوده‌ای برای سازمان‌های ارائه دهنده خدمات مالی وجود ندارد.

1 - On-line

۱۰-۹-۳ اطلاعات در دسترس عموم

هیچ راهنمای افزوده‌ای برای سازمان‌های ارائه دهنده خدمات مالی وجود ندارد.

۱۰-۹-٤ خدمات بانکداری اینترنتی

کنترل

خدمات بانکداری اینترنتی باید از دسترس غیرمجاز و تغییر حفاظت شود تا جلوی مشتری‌های غیرمجاز و افشای اطلاعات مالی و تراکنش‌های مالی گرفته شود.

راهنمای پیاده‌سازی

سازمان باید ملاحظات امنیتی زیر را برای حفاظت از خدمات بانکداری اینترنتی رعایت کند:

الف- اطلاع رسانی فعال‌سازی خدمات بانکداری اینترنتی به مشتری که از کانال ارتباطی و رسانه‌هایی که قبلا برقرار شده است استفاده می‌کند، مانند گزارش مالی حساب بانک که بر روی کاغذ چاپ شده است.

ب- محدودیت‌های مالی پیشگیرانه، مانند، حدود میان‌بانکی، حدود اختیاری.

پ-اعتبارنامه جدا برای کاربران دارنده حساب مشترک با تعریف اولیه امتیازهای دسترسی مشترک که بیان کننده‌ی قدرت امضا است.

ت- افشای محدود اطلاعات مشتری و مالی، از قبیل شناسه کاربری، نام و شماره حساب به جز اهداف کسب-وکار معتبر و اقداماتی که مشتری انجام می‌دهد.

ث- تایید اقدامات مشتری تنها در صورتی که طی همان جلسه کاربر بدون اختلال یا قطع ارتباط ارائه شده باشد. در صورت اختلال در نشست[1] کاربر یا قطع ارتباط مشتری، برای دسترسی به خدمات بانکداری اینترنتی، باید دوباره اصالت‌سنجی کاربر اعمال گردد.

سایر اطلاعات

سامانه‌های اطلاعات مشتریان میزبانی رابط وب برای خدمات بانکداری اینترنتی، اگر چه به خطر افتند، به جهت کاهش مخاطره رخنه در اطلاعات نباید اطلاعات مالی یا اطلاعات مشتریان را ذخیره کنند.

1 - Session

۱۰-۱۰ پایش[1]

۱۰-۱۰-۱ واقعه‌نگاري ممیزي[2]

هیچ راهنمای افزوده‌ای برای سازمان‌های ارائه دهنده خدمات مالی وجود ندارد.

۱۰-۱۰-۲ پایش کاربرد سامانه

کنترل ۱۰-۱۰-۲ از استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۸۷، به شرح زیر تکمیل می‌شود:

راهنمای پیاده‌سازی

علاوه بر مناطق ارائه شده در استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۸۷، برای فعالیت‌های پایش تسهیلات فردی، توصیه می‌شود نواحی زیر نیز در نظر گرفته شود:

الف- رویدادهای غیرعادی مربوط به اطلاعات مشتری و اطلاعات مالی، به همراه تراکنش‌هایی که توسط مشتریان انجام شده، از جمله:

۱- تراکنش‌های غیر معمول (مانند انتقال پول به حساب بانکی ناشناخته در صلاحدید دادگاه‌های خارجی).

۲- اقدامات کاربر در خارج از ساعات استفاده استاندارد.

۳- اجرای اقدامات کاربر با سرعت غیرطبیعی که برای شناسایی مداخله‌های غیر انسانی کاربرد دارد.

۴- اقدامات کاربران با پرش از فعالیت‌های استاندارد در فرآیند تراکنش‌های بر خط.

۵- تکراری بودن جلسات کاربران

۱۰-۱۰-۳ حفاظت از اطلاعات ثبت شده وقایع

هیچ راهنمای افزوده‌ای برای سازمان‌های ارائه دهنده خدمات مالی وجود ندارد.

۱۰-۱۰-٤ ثبت وقایع سرپرست و متصدی

هیچ راهنمای افزوده‌ای برای سازمان‌های ارائه دهنده خدمات مالی وجود ندارد.

۱۰-۱۰-٥ واقعه‌نگاری اشکال

هیچ راهنمای افزوده‌ای برای سازمان‌های ارائه دهنده خدمات مالی وجود ندارد.

۱۰-۱۰-٦ همزمان‌سازی ساعت

هیچ راهنمای افزوده‌ای برای سازمان‌های ارائه دهنده خدمات مالی وجود ندارد.

۱۱ کنترل دسترسی

هیچ راهنمای افزوده‌ای برای سازمان‌های ارائه دهنده خدمات مالی وجود ندارد.

---

1 - Monitoring
2 - Audit logging

۱۲ اکتساب، توسعه و نگهداری سامانه‌های اطلاعاتی

۱-۱۲ الزامات امنیتی سامانه‌های اطلاعاتی

۱-۱-۱۲ تحلیل و مشخصات الزامات امنیتی

کنترل ۱۲-۱-۱ از استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۸۷، به شرح زیر تکمیل می‌شود:

راهنمای پیاده‌سازی

توصیه می‌شود سازمان الزامات امنیتی زیر را هنگام طراحی سامانه‌ی تراکنش‌های مالی جدید یا هنگام اعمال تغییرات به سامانه‌ی موجود در نظر داشته باشد:

الف- حفاظت اطلاعات تراکنش‌های مالی، از تغییر غیرمجاز، کلاهبرداری، آدرس‌دهی مجدد و تخریب.

ب- بازیابی اطلاعات تراکنش‌های مالی در مورد تغییر غیرمجاز، کلاهبرداری، آدرس‌دهی مجدد و تخریب.

پ-بررسی انطباق خودکار هنگام آغاز، پردازش، انتقال و ذخیره‌سازی تراکنش‌های مالی.

ت- امکان ردیابی کلاهبرداری در تراکنش‌های مالی محتمل کلاهبرداری به صادرکننده.

ث- اصالت‌سنجی موارد زیر:

۱- کارخواه خودکار (ایستگاه‌های کاری و کارسازها) و شرکت‌کنندگان در تبادل تراکنش‌های مالی.

۲- پیام‌های پرداخت‌ها و دریافت‌های الکترونیکی ورودی و خروجی.

ج- تحویل پیام‌های پرداخت الکترونیکی به شرکت‌کنندگان در تبادل تراکنش‌های مالی.

چ-مغایرت‌گیری مالی[1] پیام‌های خروجی پرداخت الکترونیکی با پیام‌های مشابه ورودی و پیام‌های پردازش پرداخت الکترونیکی مربوطه در پرداخت‌های بین بانکی.

ح- اصالت‌سنجی کاربر برای دسترسی به پارامترهای حساس یا انجام اقدامات حساس مانند دفترداری مضاعف[2]، مغایرت‌گیری، ایجاد محدودیت ارزش برای عملیات مالی.

خ- تفکیک وظایف در طول جریان تراکنش‌ها و مصوبه‌های پرداخت.

۲-۱۲ پردازش صحیح در برنامه‌های کاربردی

هیچ راهنمای افزوده‌ای برای سازمان‌های ارائه دهنده خدمات مالی وجود ندارد.

1 - Reconciliation
2 - Double Entry

۱۲-۳ کنترل‌های رمزنگاشتی

۱۲-۳-۱ خط‌مشی استفاده از کنترل‌های رمزنگاشتی

کنترل ۱۲-۳-۱ از استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۸۷، به شرح زیر تکمیل می‌شود:

راهنمای پیاده‌سازی

هنگام توسعه خط‌مشی رمزنگاری علاوه بر راهنمایی‌های ارائه شده در استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۸۷، توصیه می‌شود موارد زیر در نظر گرفته شود:

الف- سازمان باید هر زمان که اطلاعات مشتری و اطلاعات مالی ذخیره یا پردازش می‌شود، بررسی نظام‌مند و اعمال کنترل‌های رمزنگاری را برای اطمینان از محرمانگی و یکپارچگی به عنوان یک اصل کلی انطباق دهد.

ب- دسترسی به این اطلاعات در قالب‌های واضح فقط برای اهداف کسب‌وکار معتبر مقدور باشد و باید با الزاماتی که به‌واسطه قوانین و مقرراتی که برای سازمان تعیین شده مطابقت داشته باشد.

پ- رویکرد و روش‌های منظم ارزشیابی کیفیت و قدرت الگوریتم‌های رمزبندی مورد استفاده در کنترل رمزنگاری به منظور کشف نقاط ضعف مربوط به مراحل اولیه و جلوگیری از استفاده نامناسب یا نادرست از الگوریتم‌های رمزبندی، با تغییر بر اساس مدیریت کلیدهای رمزنگاشتی (به عنوان مثال افزایش فراوانی تغییر یا به‌روزرسانی کلیدهای رمزنگاری) می‌باشد.

هنگام تعریف و تخصیص نقش‌ها و مسؤولیت‌ها برای مدیریت کلیدهای رمزتگاشتی باید اطمینان حاصل نمود که متولیان امنیتی امتیازهایی در استفاده از کلیدهای رمزنگاشتی تولید شده ندارند.

کلیدهای رمزنگاشتی درگیر در سامانه‌های پردازش تراکنش مالی یا ذخیره‌سازی اطلاعات مشتری و اطلاعات مالی ممکن است توسط متولیان امنیتی چندگانه نگهداری شود، که به ترتیب یک بخش خاص از کلیدهای رمزنگاشتی را داشته باشند.

۱۲-۳-۲ مدیریت کلید

هیچ راهنمای افزوده‌ای برای سازمان‌های ارائه دهنده خدمات مالی وجود ندارد.

۱۲-٤ امنیت پرونده‌های سامانه

۱۲-٤-۱ کنترل نرم‌افزارهای عملیاتی

کنترل ۱۲-۴-۱ از استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۸۷، به شرح زیر تکمیل می‌شود:

راهنمای پیاده‌سازی

علاوه بر راهنمایی‌های ارائه شده در استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۸۷، توصیه‌نامه‌های زیر برای به حداقل رساندن مخاطره خرابی سامانه‌های عامل باید در نظر گرفته شود:

الف- اصالت سنجی تغییرهای ارائه شده توسط فروشندگانی که نرم‌افزارهای کاربردی و سامانه‌عامل افزاره-های پرداخت (به عنوان مثال ATM، SST، POS) را تهیه می‌کنند، قبل از اینکه به صورت گسترده و با موفقیت مورد آزمایش قرار گیرد باید بررسی شود (به عنوان مثال استفاده از امضای دیجیتال(رقمی)، الگوریتم درهم‌ساز).

۱۲-٤-۲ حفاظت از داده آزمایشی سامانه

هیچ راهنمای افزوده‌ای برای سازمان‌های ارائه دهنده خدمات مالی وجود ندارد.

۱۲-٤-۳ کنترل دسترسی به کد منبع برنامه

هیچ راهنمای افزوده‌ای برای سازمان‌های ارائه دهنده خدمات مالی وجود ندارد.

۱۲-۵ امنیت در فرآیندهای توسعه و پشتیبانی

۱۲-٦ مدیریت آسیب‌پذیری فنی

۱۳ مدیریت رخداد امنیت اطلاعات

هیچ راهنمای افزوده‌ای برای سازمان‌های ارائه دهنده خدمات مالی وجود ندارد.

۱٤ مدیریت تداوم کسب‌وکار

۱٤-۱ جنبه‌های امنیت اطلاعات مدیریت تداوم کسب‌وکار

۱٤-۱-۱ لحاظ کردن امنیت اطلاعات در فرآیند مدیریت تداوم کسب‌وکار

هیچ راهنمای افزوده‌ای برای سازمان‌های ارائه دهنده خدمات مالی وجود ندارد.

۱٤-۱-۲ تداوم کسب‌وکار و ارزیابی مخاطره

کنترل ۱۴-۱-۲ از استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۸۷، به شرح زیر تکمیل می‌شود:

راهنمای پیاده‌سازی

هنگام ارزشیابی مخاطره‌های تداوم کسب‌وکار برای بررسی وابستگی‌های خارجی فرآیندهای کسب‌وکار باید توجه کافی داشت، به عنوان مثال موارد زیر تدارک دیده شود:

الف- اطلاعات مالی که توسط شرکای کسب‌وکار، پیمانکاران یا تامین‌کنندگان منتقل می‌شود.

ب- خدمات مالی (مانند بانکداری اینترنتی، کارت پردازش، مدیریت پول نقد) تدارک یافته.

۱٤-۱-۳ توسعه و پیاده‌سازی طرح‌های تداوم دربرگیرنده امنیت اطلاعات

کنترل ۱۴-۱-۳ از استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۸۷، به شرح زیر تکمیل می‌شود:

راهنمای پیاده‌سازی

طرح‌های تداوم کسب‌وکار که توسط سازمان توسعه یافته است باید وابستگی‌های خارجی زیر را به عنوان بخشی از روند بهبود و ترمیم فعالیت‌های کسب‌وکار مشخص کند:

الف- اطلاعات مالی که توسط شرکای کسب‌وکار، پیمانکاران یا تامین‌کنندگان منتقل می‌شود.

ب- خدمات مالی دریافتی (مانند بانکداری اینترنتی، کارت پردازش، مدیریت پول نقد) که با بررسی بدترین حالت فرانامه‌ها برای حصول اطمینان از تداوم این خدمات در صورتی که اختلالی تاثیرگذار بر فعالیت‌های تامین‌کننده وارد آید.

۱۴-۱-۴ چارچوب طرح‌ریزی تداوم کسب‌وکار

هیچ راهنمای افزوده‌ای برای سازمان‌های ارائه دهنده خدمات مالی وجود ندارد.

۱۴-۱-۵ آزمایش، نگهداری و ارزیابی مجدد طرح‌های تداوم کسب‌وکار

هیچ راهنمای افزوده‌ای برای سازمان‌های ارائه دهنده خدمات مالی وجود ندارد.

۱۵ انطباق

۱۵-۱ انطباق با الزامات قانونی

هیچ راهنمای افزوده‌ای برای سازمان‌های ارائه دهنده خدمات مالی وجود ندارد.

۱۵-۲ انطباق با خط‌مشی‌ها و استانداردهای امنیتی و انطباق فنی

۱۵-۲-۱ انطباق خط‌مشی‌ها و استانداردهای امنیتی

هیچ راهنمای افزوده‌ای برای سازمان‌های ارائه دهنده خدمات مالی وجود ندارد.

۱۵-۲-۲ بررسی انطباق فنی

کنترل ۱۵-۲-۲ از استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۸۷، به شرح زیر تکمیل می‌شود:

راهنمای پیاده‌سازی

در بررسی انطباق فنی باید به سامانه‌های تراکنش مالی برخط (مانند خدمات بانکداری اینترنت) که به صورت منظم انجام می‌شود توجه شود، به‌ویژه برای اطمینان از اجرای درست و توجه به مطابقت با قوانین و مقررات، اگر این سامانه‌ها در دسترس مشتریان هستند یا حاوی اطلاعات مالی و اطلاعات مشتری هستند.

۱۵-۲-۳ پایش انطباق

کنترل

توصیه می‌شود سازمان اطمینان حاصل کند که الزامات قانونی نظم‌دهنده و قراردادی مربوطه، به صورت دوره‌ای در مقابل چارچوب مدیریت امنیت اطلاعات برای حصول اطمینان از پایش انطباق بررسی می‌شود.

راهنمای پیاده‌سازی

فرایند پایش انطباق باید به طور منظم برای انجام یک نگاشت بین موارد زیر تعریف شود:

الف- الزامات حقوقی، نظم‌دهنده و قراردادی قابل اعمال بر امنیت اطلاعات،

ب- اطلاعات چارچوب مدیریت امنیت سازمان، از جمله اهداف کنترل‌های امنیتی، کنترل‌ها، خط‌مشی‌ها، استانداردها و هر گونه نیازمندی‌های امنیتی دیگر که توسط سازمان اجرا شده است.

باید نگاشت را به طور منظم برای نشان دادن قانون قابل اجرا و در چارچوب مدیریت امنیت اطلاعات انجام داد، به عنوان مثال در ارزشیابی مخاطره، کاهش و هنگامی که تغییرات قابل توجهی رخ می‌دهد. مثال‌های عدم موفقیت با قوانین قابل اجرا باید توسط سازمان شناسایی و به کار گرفته شود.

کتابنامه

[۱] استاندارد ملی ایران شماره ۲۷۰۰۳: سال ۱۳۸۹، فناوری اطلاعات - فنون امنیتی - راهنمای اجرای سامانه مدیریت امنیت اطلاعات

[۲] استاندارد ملی ایران شماره ۲۷۰۰۵: سال ۱۳۹۲، فناوري اطلاعات - فنون امنيتي - مدیریت مخاطرات امنیت اطلاعات

[۳] استاندارد ملی ایران شماره ۲٤۷٦۲: سال ۱۳۸۸، فناوری اطلاعات - فنون امنیتی - رهنمودهایی برای سرویس‌های بازیابی از حادثه در فناوری ارتباطات و اطلاعات

[۴] استاندارد ملی ایران شماره ۲۷۰۳۱: سال ۱۳۹۲، فناوري اطلاعات -فنون امنيتي -راهنماهايي براي آمادگي فناوري اطلاعات و ارتباطات به منظور تداوم کسب و کار

[۵] استاندارد ملی ایران شماره ۲۷۰۳۵: سال ۱۳۹۲، فناوري اطلاعات – فنون امنيتي – مدیریت رخداد امنیت اطلاعات

[۶] استاندارد ملی ایران شماره ۲۷۰۰۱: سال ۱۳۸۷، فناوري اطلاعات - فنون امنيتي - سامانه هاي مديريت امنيت اطلاعات - الزامات

[۷] استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۸۷، فناوري اطلاعات - فنون امنيتي - آیین کارمدیریت امنیت اطلاعات

[8] ISO/IEC 27004:2009, Information technology — Security techniques — Information security management — Measurement

[9] ISO/TR 13569:2005, Financial services -- Information security guidelines

[10] ISO/IEC 27033-1:2009, Information technology — Security techniques — Network security — Part 1: Overview and concepts

[11] ISO/IEC 27033-2:2012, Information technology — Security techniques — Network security — Part 2: Guidelines for the design and implementation of network security

[12] ISO/IEC 27033-3:2010, Information technology — Security techniques — Network security — Part 3: Reference networking scenarios — Threats, design techniques and control issues

[13] Payment Card Industry (PCI) Data Security Standard, Requirements and Security Assessment Procedures (version 1.2).

[14] COBIT – Control Objectives for Information Technology – Version 4.1 – IT Governance Institute and Information Systems Audit and Control Association (ISACA).