شماره: ۰۰/۱۹۱۰۱۲
تاریخ: ۱۴۰۰/۰۷/۰۶
پیوست: دارد (۲۷ صفحه)

بانک مرکزی جمهوری اسلامی ایران

بسمه تعالی

جهت اطلاع مدیران عامل محترم بانک‌های دولتی، غیردولتی، شرکت دولتی پست‌بانک، موسسات اعتباری غیربانکی و بانک مشترک ایران ـ ونزوئلا ارسال می‌شود

با سلام؛

احتراماً، همان‌گونه که مستحضرند، توسعه روزافزون فناوری اطلاعات و زیرساخت‌های ارتباطی، نقش تعیین‌کننده‌ای در کسب و کار بانکی داشته و تغییرات فراوانی را در خدمات بانکداری طی سال‌های اخیر موجب شده است. گسترش و تنوع بسترها و خدمات بانکی مبتنی بر فناوری اطلاعات و رشد فزاینده تراکنش‌های بانکداری الکترونیکی، افزایش ریسک‌های مرتبط علی‌الخصوص ریسک عملیاتی که از جمله مهمترین منابع ایجادکننده آن، ریسک فناوری اطلاعات می‌باشد را در پی داشته است. در این میان توجه ویژه به مقوله ارتقاء امنیت زیرساخت‌ها و فرآیندهای حوزه فناوری اطلاعات با هدف کاهش ریسک‌ها و چالش‌های این حوزه، امری ضروری و اجتناب‌ناپذیر می‌باشد.

بر این اساس حوزه نظارت بانک مرکزی با هدف ارائه چارچوب مناسب در جهت ایجاد بستر امن و کاهش ریسک‌های مترتب در حوزه فناوری اطلاعات، اقدام به تدوین ضوابطی تحت عنوان «حداقل الزامات ناظر بر ریسک فناوری اطلاعات مؤسسات اعتباری» نموده که مراتب در هجدهمین جلسه مورخ ۱۴۰۰/۰۵/۳۱ کمیسیون مقررات و نظارت مؤسسات اعتباری، طرح و به تصویب رسیده و مورد تأیید رییس کل محترم بانک مرکزی قرار گرفته است.

با عنایت به مراتب فوق، ضمن ابلاغ ضوابط مزبور به شرح پیوست، به استحضار می‌رساند حداقل الزامات یادشده با بهره‌گیری از آخرین استانداردها و مراجع معتبر بین‌المللی مانند ISO، Deloitte وGartner و نیز استفاده از تجارب بهینه روز دنیا و همچنین دریافت نظرات کارشناسان، مدیران و خبرگان مطلع فناوری اطلاعات شبکه بانکی کشور در قالب ۱۰ موضوع تخصصی حوزه فناوری اطلاعات تدوین شده است.

برخی از مهم‌ترین اهداف و ویژگی‌های ضوابط حداقل الزامات ابلاغی به شرح زیر می‌باشد:

- **حرکت به سمت استقرار استانداردهای روز دنیا در حوزه فناوری اطلاعات شبکه بانکی کشور؛**
- **افزایش ضریب امنیت اطلاعات و کاهش ریسک‌های فناوری اطلاعات مؤسسات اعتباری؛**
- **کاهش سوء استفاده‌های احتمالی و جلوگیری از هدررفت منابع موجود در شبکه بانکی کشور؛**
- **یکپارچگی سیاست‌های ابلاغی در نظارت بر ریسک فناوری اطلاعات مؤسسات اعتباری.**

همچنین خاطر نشان می‌سازد رعایت مفاد بخشنامه‌های شماره ۹۷/۴۹۷۵۱ مورخ ۹۷/۰۲/۲۰ با موضوع «الزامات سازمان‌دهی امنیت اطلاعات در بانک‌ها و مؤسسات اعتباری»، شماره ۹۷/۴۹۴۸۸ مورخ ۱۳۹۷/۰۲/۲۰ درخصوص «الزامات گزارش‌دهی رخدادهای امنیت اطلاعات بانکی» و شماره ۹۹/۳۱۱۴۱۷ مورخ ۹۹/۱۰/۰۱ تحت عنوان «احراز

هویت قوی در خدمات بانکداری الکترونیکی از راه دور» که پیشتر توسط معاونت فناوری‌های نوین این بانک به شبکه بانکی ابلاغ شده است، در راستای انطباق با ضوابط ابلاغی پیوست ضروری می‌باشد.

شایان ذکر است به منظور گزارش‌دهی دوره‌ای و سیستمی در خصوص نحوه عملکرد مؤسسات اعتباری در زمینه اجرای مفاد حداقل الزامات، فرم‌های متناظر در کارتابل «مهتاب» ایجاد و در دسترس شبکه بانکی قرار خواهد گرفت. بدیهی است آن بانک/مؤسسه اعتباری موظف است در بازه‌های زمانی معین، گزارش‌ها و اطلاعات اقدامات خود در چارچوب ضوابط «**حداقل الزامات ناظر بر ریسک فناوری اطلاعات مؤسسات اعتباری**» را در کارتابل مهتاب بارگذاری و به این بانک ارسال نماید.

با عنایت به موارد فوق ضروری است به منظور تطبیق حداکثری حوزه فناوری اطلاعات آن بانک/مؤسسه اعتباری با مفاد «**حداقل الزامات ناظر بر ریسک فناوری اطلاعات مؤسسات اعتباری**»، اقدامات و تمهیدات لازم به عمل آمده و برنامه زمان‌بندی دقیق بر اساس مهلت زمانی مندرج در ماده (۱۲۷) حداقل الزامات یادشده، به این مدیریت کل ارائه گردد.

در خاتمه ضمن تأکید مجدد بر مسئولیت هیأت مدیره در مدیریت مؤثر ریسک فناوری اطلاعات، خواهشمند است دستور فرمایند، مراتب به قید تسریع به تمامی واحدهای ذی‌ربط آن بانک/مؤسسه اعتباری ابلاغ شده و بر حسن اجرای آن نظارت دقیق به عمل آید./۵۳۳۲۵۹۷

مدیریت‌کل نظارت بر بانک‌ها و موسسات اعتباری
اداره ارزیابی سلامت نظام بانکی
عبدالمهدی ارجمندنژاد سید علی‌اکبر میرعمادی
۸۴۱۶ ۳۲۱۵-۰۹

بانک مرکزی جمهوری اسلامی ایران

حداقل الزامات ناظر بر ریسک فناوری اطلاعات مؤسسات اعتباری

مدیریت کل نظارت بر بانک‌ها و مؤسسات اعتباری
اداره ارزیابی سلامت نظام بانکی

گروه نظارت بر ریسک فناوری اطلاعات

ویرایش ۱/۰
مرداد ماه ۱۴۰۰

شناسنامه سند	
سند	حداقل الزامات ناظر بر ریسک فنـاوری اطلاعـات مؤسسـات اعتبـاری
اداره تهیه‌کننده	اداره ارزیابی سلامت نظام بانکی
گروه تهیه‌کننده	نظارت بر ریسک فناوری اطلاعات
تاریخ	۱۴۰۰/۰۵/۳۱
نام فایل	CBI_Ver۱.۰_BanksITMinimumObligations

فهرست مطالب

بسمه تعالی

به استناد مفاد بند (ب) ماده (۱۱)، بند (۲) ماده (۱٤) و ماده (۳۷) قانون پولی و بانکی کشور و مفاد بند (الف) ماده (٤۹) قانون برنامه پنجم توسعه کشور، به منظور حصول اطمینان از صحت عملکرد مؤسسات اعتباری در حوزه فناوری اطلاعات، «حداقل الزامات ناظر بر ریسک فناوری اطلاعات مؤسسات اعتباری» که از این پس به اختصار «الزامات» نامیده می‌شود، به شرح زیر تدوین می‌گردد:

فصل اول – تعاریف

ماده ۱- در این الزامات اصطلاحات در معانی مشروح زیر به کار می‌رود:

۱-۱- مؤسسه اعتباری: بانک یا مؤسسه اعتباری غیربانکی که به موجب قانون و یا با مجوز بانک مرکزی تأسیس شده و تحت نظارت بانک مرکزی می‌باشد؛

۱-۲- هیئت مدیره: گروهی متشکل از اشخاص حقیقی منتخب سهامداران مؤسسه اعتباری که مسئولیت سیاست‌گذاری و نظارت بر نحوه اداره، حسن اجرای قوانین و مقررات و مدیریت ریسک مؤسسه اعتباری را بر عهده دارد؛

۱-۳- خدمات بانکداری الکترونیکی: عبارت است از انواع خدمات بانکی و اعتباری از طریق درگاه‌های الکترونیکی؛

۱-٤- سامانه: مجموعه‌ای از نرم‌افزار و سخت‌افزار برای ارائه خدمات بانکداری؛

۱-۵- کاربر: تمامی بهره‌برداران سامانه اعم از درون‌سازمانی و برون‌سازمانی؛

۱-٦- کمیته عالی فناوری اطلاعات: کمیته‌ای است تخصصی ذیل هیئت مدیره مؤسسه اعتباری که به منظور یاری رسانیدن به آن‌ها در امر سیاست‌گذاری و راهبری حوزه فناوری اطلاعات تشکیل شده، در چارچوب حداقل وظایف و اختیارات تعیین شده در این الزامات انجام وظیفه می‌نماید؛

۱-۷- واحد حسابرسی فناوری اطلاعات: واحدی است تخصصی ذیل کمیته عالی فناوری اطلاعات که به منظور یاری رسانیدن به این کمیته در امر حسابرسی حوزه فناوری اطلاعات تشکیل شده، در چارچوب حداقل وظایف و اختیارات تعیین شده در این الزامات انجام وظیفه می‌نماید؛

فصل دوم – معماری و ساختار سازمانی

ماده ۲- مؤسسه اعتباری موظف است معماری فناوری اطلاعات را بر مبنای توگف[۱]، بایان[۲] و چارچوب ملی معماری سازمانی ایران و یا ترکیبی از آنها و در حوزه سرویس با رویکرد معماری سرویس‌گرا[۳]، طراحی و تدوین نماید.

---

[۱] TOGAF
[۲] BIAN
[۳] SOA

ماده ۳- مؤسسه اعتباری مکلف است طرح جامع فناوری اطلاعات[1] مؤسسه اعتباری را تصویب و در فواصل زمانی مناسب به‌روزرسانی نماید.

ماده ٤- مؤسسه اعتباری موظف است ساختار سازمانی و شرح وظایف و اختیارات حوزه فناوری اطلاعات مؤسسه اعتباری را جهت دستیابی به معماری فناوری اطلاعات موضوع ماده (۲) این الزامات تصویب و اجرا نماید.

ماده ٥- مؤسسه اعتباری مکلف است در ساختار سازمانی خود، معاونتی را با عنوان «معاونت فناوری اطلاعات» تحت نظر مستقیم مدیرعامل (پیوست) ایجاد نماید. معاون فناوری اطلاعات مؤسسه اعتباری باید واجد حداقل شرایط زیر باشد:

٥-۱-حداقل ۸ سال سابقه کار مرتبط با فناوری اطلاعات در حوزه بانکی؛

٥-۲- تحصیلات دانشگاهی، حداقل کارشناسی ارشد در رشته‌های مهندسی کامپیوتر، مهندسی فناوری‌اطلاعات، علوم کامپیوتر و مدیریت فناوری‌اطلاعات؛

٥-۳- احراز صلاحیت توسط مراجع ذی‌صلاح.

ماده ٦- هیئت مدیره موظف است به منظور انجام صحیح و دقیق وظایف خود در حوزه فناوری اطلاعات کمیته‌ای تحت عنوان «کمیته عالی فناوری اطلاعات» را ایجاد نماید(پیوست).

ماده ۷- وظایف و مسئولیت‌های «کمیته عالی فناوری اطلاعات» به شرح زیر است:

۷-۱- تدوین اهداف کلان، سیاست‌گذاری، برنامه‌ریزی و راهبری سرمایه‌گذاری و توسعه خدمات فناوری اطلاعات و نظارت بر حسن اجرای آن‌ها؛

۷-۲- نظارت بر حسن اجرای مقررات ابلاغی از سوی بانک مرکزی (از جمله این الزامات) در حوزه فناوری اطلاعات؛

۷-۳- نظارت بر اجرای صحیح و به‌موقع مصوبات هیئت مدیره در حوزه فناوری اطلاعات؛

۷-٤- ارائه نظر مشورتی در خصوص موضوعات ارجاعی از سوی هیئت مدیره در حوزه فناوری اطلاعات؛

۷-٥- نظارت بر فرآیند حسابرسی فناوری اطلاعات در مؤسسه اعتباری؛

۷-٦- نظارت بر فرآیندها و منابع فناوری اطلاعات از منظر توجیه اقتصادی، کارآیی و اثر بخشی؛

۷-۷- نظارت بر فرآیند مدیریت ریسک‌های فناوری اطلاعات در مؤسسه اعتباری؛

۷-۸- نظارت بر حسن اجرای تمامی فرآیندهای امنیت اطلاعات مؤسسه اعتباری؛

۷-۹- تدوین برنامه‌های کلان آموزشی و پژوهشی در جهت توسعه فناوری اطلاعات با رویکردهای *تخصصی*.

[1] IT Master Plan

ماده ۸- کمیته عالی فناوری اطلاعات، باید ویژگی‌های زیر را داشته باشد:

۸-۱- رئیس، نایب رئیس و اعضای آن توسط هیئت مدیره انتخاب شوند؛

۸-۲- رئیس آن باید از میان اعضای غیراجرایی هیئت مدیره انتخاب شود و دارای آشنایی کافی با فناوری اطلاعات و عملیات بانکی باشد؛

۸-۳- تعداد اعضای «کمیته عالی فناوری اطلاعات» می‌بایست حداقل ۵ نفر و فرد باشد؛

۸-٤- دو نفر از اعضای هیئت مدیره با احتساب رئیس کمیته در آن عضویت داشته باشند؛

۸-۵- اکثریت اعضای آن باید دارای تخصص و تجربه لازم در زمینه فناوری اطلاعات بوده و حداقل یک نفر از اعضاء از خارج موسسه اعتباری انتخاب شود؛

۸-٦- رئیس هیئت مدیره نمی‌تواند همزمان به ریاست کمیته عالی فناوری اطلاعات انتخاب شود؛

۸-۷- مدت تصدی مسئولیت اعضای کمیته عالی فناوری اطلاعات با اتمام مدت تصدی مسئولیت اعضای هیئت مدیره پایان می‌یابد. انتصاب مجدد هریک از اعضاء بلامانع است؛

۸-۸- معاون فناوری اطلاعات مؤسسه اعتباری به‌عنوان دبیر کمیته و بدون حق رأی در جلسات کمیته حضور داشته باشد؛

۸-۹- در صورت لزوم، کمیته می‌تواند از کارشناسان دارای دانش و مهارت‌های تخصصی مورد نیاز (از داخل و خارج از مؤسسه اعتباری) به منظور مشاوره، دعوت به‌عمل آورد.

ماده ۹- مؤسسه اعتباری می‌تواند در راستای وظایف نظارتی کمیته عالی فناوری اطلاعات، واحدی را تحت عنوان «واحد حسابرسی فناوری اطلاعات» ذیل کمیته مزبور با شرح وظایف زیر تشکیل دهد:

۹-۱- تهیه برنامه جامع حسابرسی فناوری اطلاعات مؤسسه اعتباری و هدایت و راهبری فرآیندهای مرتبط بر اساس آخرین نسخه چارچوب حسابرسی فناوری اطلاعات ایساکا[۱]؛

۹-۲- حسابرسی فناوری اطلاعات حداقل شامل فرآیندها، اسناد، قراردادها، معاملات، پروژه‌ها و گزارش‌های تهیه شده مربوط به حوزه فناوری اطلاعات مؤسسه اعتباری؛

۹-۳- ارزیابی دوره‌ای میزان انطباق عملکرد فناوری اطلاعات مؤسسه اعتباری با مفاد الزامات و ارائه گزارش به معاونت نظارت بانک مرکزی و کمیته عالی فناوری اطلاعات در مقاطع ٦ ماهه؛

۹-٤- ارزیابی میزان تحقق سیاست‌ها و برنامه‌های مؤسسه اعتباری و مصوبات هیئت مدیره در حوزه فناوری اطلاعات و ارائه گزارش به کمیته عالی فناوری اطلاعات؛

۹-۵- ارزیابی فرآیندهای فناوری اطلاعات از منظر توجیه اقتصادی، کارایی و اثربخشی؛

۹-٦- ارزیابی کارآمدی منابع فناوری اطلاعات از قبیل نیروی انسانی، تجهیزات و سامانه‌ها؛

[۱] ISACA IT Audit Framework (ITAF™)

۹-۷- نظارت بر حسابرسی فناوری اطلاعات خارجی (برون سپاری شده)؛

۹-۸- دریافت و بررسی پیشنهادها و توصیه‌های حسابرسان مستقل در ارتباط با حوزه فناوری اطلاعات و پیگیری آن‌ها؛

۹-۹- انجام حسابرسی‌های موردی در صورت لزوم بنا به درخواست معاونت نظارت بانک مرکزی و یا کمیته عالی فناوری اطلاعات مؤسسه اعتباری؛

۹-۱۰-انجام فعالیت‌های پژوهشی در حوزه حسابرسی فناوری اطلاعات.

ماده ۱۰- مؤسسه اعتباری موظف است «تیم پاسخ به رخداد[۱]» را زیرمجموعه معاونت فناوری اطلاعات به همراه تبیین مسئولیت‌ها و شرح وظایف، مطابق با دستورالعمل‌های کمیته پدافند غیرعامل کشوری تعیین نماید.

فصل سوم –خط‌مشی‌ها/سیاست‌ها و برنامه‌ها

ماده ۱۱- مؤسسه اعتباری مکلف است خط‌مشی‌ها/سیاست‌ها و برنامه‌های حوزه فناوری اطلاعات مشتمل بر برون‌سپاری، امنیت، مدیریت شناسایی و تایید مشتریان، سامانه جامع بانکداری متمرکز، سامانه‌های بانکداری الکترونیکی، مدیریت ریسک، شبکه و ارتباطات و مرکز داده را در چارچوب مفاد این الزامات تدوین، تصویب و به ارکان ذی‌ربط ابلاغ نماید.

ماده ۱۲- مؤسسه اعتباری موظف است طرح کنترل و مدیریت رخدادها و حوادث غیرمترقبه[۲] را تهیه و در بازه‌های زمانی مناسب بازنگری نموده و مورد آزمون قرار دهد. طرح یاد شده باید حداقل دارای ویژگی‌های زیر باشد:

۱۲-۱- امکان کشف سریع منشاء؛

۱۲-۲- توانایی ارزیابی دامنه رخداد و شدت بالقوه آن؛

۱۲-۳- امکان گزارش‌دهی سریع به هیئت مدیره در صورت بروز ریسک شهرت یا زیان مالی؛

۱۲-٤- امکان اطلاع‌رسانی مناسب به مشتریان؛

۱۲-٥- امکان بازیابی اطلاعات و خدمات در کمترین زمان ممکن؛

۱۲-٦- امکان دسترسی مشتریان به خدمات کلیدی بانکداری الکترونیکی.

ماده ۱۳- مؤسسه اعتباری موظف است کاتالوگ خدمات فناوری اطلاعات[۳] و همچنین دارایی‌های مرتبط با فناوری اطلاعات را مشخص و مکتوب نماید. بدین منظور مؤسسه اعتباری می‌تواند از فرآیند مدیریت کاتالوگ خدمات و مدیریت دارایی‌ها در آخرین ویرایش چارچوب ITIL[۴] استفاده نماید.

---

[۱] CIRT (Computer Incident Response Team)
[۲] DRP (Disaster Recovery Plan)
[۳] IT Service Catalog
[۴] ITIL (Information Technology Infrastructure Library)

ماده ١٤- مؤسسه اعتباری موظف است در تهیه برنامه تداوم کسب‌وکار[1] حداقل موارد زیر را پوشش داده، آنها را در بازه‌های زمانی مناسب بازنگری نموده و مورد آزمون قرار دهد:

١-١٤- خدمات فناوری اطلاعات مؤسسه اعتباری، امکان تداوم در شرایط عادی و اضطراری را داشته باشند؛

٢-١٤- خدمات فناوری اطلاعات مؤسسه اعتباری، برای مواقع بحرانی و اوج کاری از نظر کارآیی مورد آزمون و بهینه‌سازی قرار گیرند؛

٣-١٤- خدمات فناوری اطلاعات مؤسسه اعتباری، از قابلیت مقیاس‌پذیری[2] برخوردار باشند؛

٤-١٤- امکان دسترسی به خدمات بانکداری الکترونیکی برای مشتریان در تمامی ساعات شبانه‌روز و هفت روز هفته (٢٤×٧) فراهم شود.

ماده ١٥- مؤسسه اعتباری موظف است از میزان وقفه احتمالی که در اثر تغییر، به‌روزرسانی و اصلاح سامانه‌های بانکداری به وجود می‌آید تخمین مناسبی داشته باشد. در صورت احتمال بروز هرگونه وقفه در خدمات، تأمین شرایط زیر ضروری است:

١-١٥- حداقل یک هفته کاری قبل از ایجاد هرگونه وقفه با ذکر دقیق زمان و مدت احتمالی وقفه، اطلاع‌رسانی کافی و شفاف به مشتریان صورت گیرد؛

٢-١٥- تغییرات به‌گونه‌ای برنامه‌ریزی شود که زمان شروع وقفه و حتی‌المقدور مدت آن در ساعات غیراداری یا تعطیل باشد؛

٣-١٥- برای ارائه خدمات بانکداری الکترونیکی، واحد امداد مشتریان با توان پاسخگویی مناسب راه‌اندازی شود؛

٤-١٥- روش‌های مناسب جبران خسارت ناشی از عدم خدمت‌رسانی به کاربران به دلیل نقص یا توقف سامانه‌های خدمات بانکداری الکترونیکی و دیگر ریسک‌های ممکن در این حوزه پیاده‌سازی شود.

ماده ١٦- مؤسسه اعتباری موظف است به منظور ارتقاء دانش و مهارت کارکنان در سطوح مختلف، برنامه‌های آموزشی لازم را به صورت مستمر اجرا نماید.

فصل چهارم – برون‌سپاری

ماده ١٧- مؤسسه اعتباری موظف است دستورالعمل برون‌سپاری خدمات فناوری اطلاعات را بر اساس آخرین ویرایش استاندارد ISO ٣٧٥٠٠ تدوین نموده و به تصویب هیئت مدیره برساند. دستورالعمل یاد شده باید شامل حداقل موارد زیر باشد:

١-١٧- شرح نیازمندی‌ها؛

[1] BCP (Business Continuity Plan)
[2] Scalability

۱۷-۲- جدول و معیار ارزیابی و انتخاب پیمانکار؛

۱۷-۳- طرح توجیهی؛

۱۷-٤- شاخص‌های کلیدی عملکرد مرتبط با برون‌سپاری؛

۱۷-٥- تهیه و نحوه انتشار درخواست پیشنهاد[۱]؛

۱۷-٦- نحوه بررسی پاسخ شرکت‌کنندگان مناقصه؛

۱۷-۷- نحوه ارزیابی شرکت‌کنندگان؛

۱۷-۸- معیارهای نهایی انتخاب پیمانکار؛

۱۷-۹- موارد مرتبط با تدارکات، خرید و قرارداد؛

۱۷-۱۰- حدود اختیارات و مسئولیت‌ها در فرآیند برون‌سپاری؛

۱۷-۱۱- رویه‌های نظارت بر روابط برون‌سپاری.

ماده ۱۸- مؤسسه اعتباری مجاز به دریافت خدمات فناوری اطلاعات از شرکت‌ها و پیمانکاران برون‌سازمانی بدون عقد قرارداد نمی‌باشد.

ماده ۱۹- مؤسسه اعتباری موظف است در برون‌سپاری پروژه‌های فناوری اطلاعات مفاد ضوابط بالادستی را رعایت نماید.

ماده ۲۰- مؤسسه اعتباری مکلف است قبل از انعقاد هرگونه قرارداد برون‌سپاری در خصوص هر بخش از خدمات فناوری‌اطلاعات به شرکت‌های داخلی و خارجی، نسبت به رعایت حداقل موارد زیر اطمینان حاصل نماید:

۲۰-۱- وجود فرآیند مناسب تصمیم‌گیری در ارتباط با مدیریت ریسک‌های ناشی از برون‌سپاری؛

۲۰-۲- احراز هویت کامل شرکت تأمین‌کننده خدمات و برخورداری شرکت از صلاحیت‌های عمومی، مالی، فنی و توانایی ارائه خدمات پشتیبانی و اخذ تأییدیه از مراجع ذیصلاح امنیتی؛

۲۰-۳- به‌کارگیری روش‌های مناسب و کافی برای بررسی پیشنهادهای اولیه شرکت تأمین‌کننده خدمات فناوری اطلاعات با نظرداشت شاخص‌های فنی و عملکردی و معیارهای لازم جهت انتخاب صحیح آن‌ها؛

۲۰-٤- برخورداری از منابع، تخصص و فرآیند کاری لازم برای نظارت مؤثر بر رعایت مفاد قراردادهای برون‌سپاری؛

۲۰-٥- اخذ تأییدیه از معاونت نظارت بانک مرکزی مبنی بر عدم وجود منع مقرراتی در خصوص انعقاد قرارداد برون‌سپاری با شرکت تأمین‌کننده خدمات فناوری اطلاعات.

---

[۱] Request for Proposal (RFP)

ماده ۲۱- مؤسسه اعتباری موظف است برای تمامی فرآیندهای برون‌سپاری حوزه فناوری اطلاعات، سند توافقنامه سطح خدمات[۱] داشته باشد. بدین منظور استفاده از آخرین ویرایش چارچوب ITIL پیشنهاد می‌شود.

ماده ۲۲- مؤسسه اعتباری مکلف است اطمینان حاصل نماید که روش‌های حفظ اطلاعات مشتریان توسط تأمین‌کنندگان خدمات با سیاست‌های مؤسسه اعتباری و ضوابط بانک مرکزی مطابقت دارد.

ماده ۲۳- مؤسسه اعتباری موظف است تمامی تضامین لازم را برای تأمین امنیت اطلاعات و داده‌ها و جلوگیری از افشاء هر نوع اطلاعات مرتبط، پیش از واگذاری خدمات و پروژه‌ها به شرکت تأمین‌کننده خدمات، اخذ نماید.

ماده ۲٤- مؤسسه اعتباری مکلف است در تمامی قراردادها با شرکت تأمین‌کننده خدمات، توافقنامه محرمانگی امضاء نموده و در متن قرارداد نیز این موضوع را به شکل شفاف تبیین نماید.

ماده ۲۵- مؤسسه اعتباری موظف است در متن قراردادهای برون‌سپاری حداقل موارد زیر را لحاظ نماید:

۱-۲۵- ضرورت انطباق سامانه‌ها و خدمات فناوری اطلاعات مؤسسه اعتباری با ضوابط بانک مرکزی در حداقل زمان ممکن؛

۲-۲۵- ممنوعیت واگذاری تمام/بخشی از خدمات فناوری اطلاعات عهده شرکت تامین‌کننده خدمات به اشخاص ثالث؛

۳-۲۵- لزوم تصریح مالکیت مؤسسه اعتباری بر داده‌های ذخیره شده در پایگاه‌های داده؛

٤-۲۵- تعیین مسئولیت‌ها و تعهدات طرفین قرارداد در خصوص بروز هرگونه وقفه و یا اختلال در ارائه خدمات و دسترسی غیرمجاز به اطلاعات و حساب مشتریان و لزوم اطلاع‌رسانی سریع به ذینفعان توسط شرکت تأمین‌کننده خدمات؛

۵-۲۵- درج تمامی خدمات درخواستی، فعالیت‌ها به همراه نمودار روند و فرآیند انجام آن، برنامه زمان‌بندی و حداقل سطح خدمت‌رسانی خدمات فناوری اطلاعات به‌طور شفاف؛

٦-۲۵- پیش‌بینی مسئولیت‌های تأمین‌کنندگان خدمات متناسب با نیاز مؤسسه اعتباری با نظرداشت محرمانگی داده‌ها و مستندات، تبیین و خسارات احتمالی به شکل دقیق؛

۷-۲۵- تعیین شرایط پوشش احتیاطی و حقوق مؤسسه اعتباری در بازیابی داده‌ها بعد از انقضاء یا خاتمه قرارداد؛

۸-۲۵- تعیین حدود نظارت مؤسسه اعتباری بر عملکرد شرکت تأمین‌کننده خدمات در چارچوب موضوع قرارداد منعقده و شرایط فسخ قرارداد؛

---

[۱] SLA (Service Level Agreement)

۹-۲۵- تعیین و درج جریمه و یا وجه التزام مشخص در صورت تخطی شرکت تأمین‌کننده خدمات از شرایط قرارداد، فرار از مسئولیت و یا عدم انجام تعهدات؛

۱۰-۲۵- امکان انجام بازرسی توسط معاونت نظارت بانک مرکزی در مواقع لزوم از شرکت تأمین‌کننده خدمات در حدود خدمات برون سپاری شده.

ماده ۲۶- مؤسسه اعتباری موظف است در صورت عدم پوشش ضوابط بانک مرکزی در قراردادهای قبلی منعقده، از طریق انعقاد الحاقیه و یا متمم نسبت به رعایت کامل ضوابط مزبور اقدام نماید.

ماده ۲۷- در صورت تخطی شرکت تأمین‌کننده خدمات فناوری اطلاعات از ضوابط ابلاغی بانک مرکزی، تمدید یا انعقاد مجدد قرارداد مؤسسه اعتباری با شرکت مزبور ممنوع می باشد.

فصل پنجم– امنیت

ماده ۲۸- مؤسسه اعتباری مکلف است، نظام مدیریت امنیت اطلاعات را پیاده‌سازی نموده و گزارش‌های لازم را به‌صورت دوره‌ای به «کمیته عالی فناوری اطلاعات» ارائه دهد.

ماده ۲۹- مؤسسه اعتباری موظف است استاندارد مرجع ISO ۲۷۰۰۱ را پیاده‌سازی نموده و مستندات و مدارک معتبر در این زمینه اخذ نماید.

ماده ۳۰- مؤسسه اعتباری مکلف است به منظور دریافت خدمات مشاوره‌ای پیاده‌سازی مدیریت امنیت اطلاعات ISO ۲۷۰۰۱، صرفاً با شرکت‌هایی که مجوز سازمان فناوری اطلاعات (نما) در زمینه مشاوره را دارند قرارداد منعقد نماید. اخذ مجوز صلاحیت از مراجع ذی‌صلاح امنیتی در فرآیند عقد قرارداد الزامی است.

ماده ۳۱- مؤسسه اعتباری موظف است به منظور ارتقاء سطح امنیت در حوزه پرداخت از استاندارد PCIDSS[۱] استفاده نموده و تمامی ضوابط مرتبط با این استاندارد را اجرا نماید.

ماده ۳۲- مؤسسه اعتباری موظف است گزارش‌های رخدادها و حوادث امنیتی را به محض وقوع به معاونت نظارت بانک مرکزی اعلام نماید.

ماده ۳۳- مؤسسه اعتباری مکلف است با هدف حصول اطمینان از اعمال کنترل‌های امنیت اطلاعات، اقدامات زیر را انجام دهد:

۱-۳۳- تصویب و ابلاغ سیاست‌ها و فرآیندهای مدیریت امنیت اطلاعات مشتمل بر رویه‌ها و دستورالعمل‌های مدون و مکتوب در مورد سطوح دسترسی افراد به داده‌ها و اطلاعات عملیات بانکی، میزان مخاطره مرتبط با داده‌ها و نحوه مدیریت این مخاطرات و ارزیابی و بازنگری آن‌ها به صورت ادواری؛

[۱] Payment Card Industry Data Security Standard

۲-۳۳- تبیین و تفکیک مسئولیت‌های مدیریت و کارکنان و کنترل‌های آن‌ها بر اساس سیاست‌های امنیتی مؤسسه اعتباری؛

۳-۳۳- ارزیابی و بازنگری منظم و مستمر معیارها و کنترل‌های امنیتی؛

٤-۳۳- تصویب رویه‌ها و دستورالعمل‌های مربوط به شناسایی نیازهای مرتبط با اطلاع‌رسانی و آموزش کاربران.

ماده ۳٤- مؤسسه اعتباری مکلف است موضوع صیانت و حفظ امنیت اطلاعات را در ضوابط مربوط به نحوه جذب، نگهداری، جابجایی، اخراج، بازنشستگی و یا هر نوع خاتمه خدمت کارکنان را مدنظر قرار دهد.

ماده ۳۵- مؤسسه اعتباری موظف است به منظور اطمینان از تقسیم وظایف مناسب و حفظ امنیت اطلاعات، موارد زیر را رعایت نماید:

۱-۳۵- اصل کنترل دو نفره (دوگانه) در فرآیند تراکنش‌های مالی توسط کارکنان مؤسسه اعتباری و تأمین‌کنندگان خدمات؛

۲-۳۵- تفکیک وظایف بین مسئول ورود داده‌ها و اطلاعات و مسئول بررسی و تأیید صحت آن‌ها؛

۳-۳۵- تفکیک وظایف مسئولین طراحی و پیاده‌سازی از راهبری سامانه‌های بانکداری الکترونیکی؛

٤-۳۵- تفکیک وظایف مسئولین پردازش اطلاعات از مسئولین پایش آن‌ها.

ماده ۳٦- مؤسسه اعتباری موظف است برای ایجاد و ارتقاء امنیت فیزیکی لازم جهت جلوگیری از دسترسی غیرمجاز به تجهیزات کامپیوتری و شبکه‌های ارتباطی تدابیر مناسب اتخاذ نماید. این تدابیر حداقل شامل موارد زیر باشد:

۱-۳٦- ایجاد حفاظ مناسب برای درب‌ها، راه‌اندازی تجهیزات ثبت و کنترل تردد افراد مانند درب‌های کنترل شده با کارت، اثر انگشت یا سایر روش‌های احراز هویت و یا در صورت لزوم راه‌اندازی نگهبانی به منظور ثبت ورود و خروج دستی؛

۲-۳٦- ایجاد مکان‌های امن برای حفاظت سامانه‌ها و منابع آن با رعایت کمترین حساسیت برای بازدیدکنندگان؛

۳-۳٦- اطلاع کارکنان مؤسسه اعتباری از وجود و جزئیات اماکن موضوع بند قبل صرفاً براساس درجه نیاز آن‌ها به این اطلاعات؛

٤-۳٦- فرآیندی به منظور مدیریت ورود/خروج و امحای تجهیزات و اطلاعات طراحی و پیاده‌سازی شود؛

۵-۳٦- نصب و آزمون سیستم‌های مناسب کنترلی تشخیص و اعلام نفوذ در محل به گونه‌ای صورت پذیرد که تمامی درب‌های نفوذ به داخل (داکت‌ها و کانال‌های هواساز، مجاری موجود در کف یا سقف کاذب یا تونل‌های دسترسی به سایت و نظایر آن) از حیث نفوذ، محافظت گردد؛

٦-٣٦- ساختمان‌ها، کانال‌های فاضلاب و سایر مجراهای طبیعی یا شهری که پتانسیل امکان نفوذ به سایت امن را فراهم می‌آورد باید از حیث نفوذ مورد بررسی قرار گیرد؛

٧-٣٦- دسترسی‌ها اعم از موفق و ناموفق جهت ورود به سایت امن باید به‌طور فیزیکی یا الکترونیکی، ثبت شده و در مکان امن با رعایت طبقه‌بندی نگهداری گردد؛

٨-٣٦- تمامی نقاط حساس از جمله درب ورودی سایت، باید از طریق دوربین مداربسته توسط واحدهای ذی‌ربط مانند اداره انتظامات/حراست کنترل شود؛

٩-٣٦- محافظت فیزیکی از دسترسی به کابل‌ها، جعبه‌های تقسیم و داکت‌های انتقال کابل به شکل مناسبی انجام شود.

ماده ٣٧- مؤسسه اعتباری مکلف است سازوکار لازم برای امن‌سازی شبکه داخلی و ارتباطات برون‌سازمانی از طریق شبکه‌های عمومی مانند اینترنت را پیاده نماید.

ماده ٣٨- مؤسسه اعتباری موظف است ارتباطات میان دستگاه‌های مدیریت شبکه و تجهیزات آن مانند مسیریاب‌ها[١] و دیواره‌های‌آتش[٢] برای حفاظت جریان داده‌ها را رمزگذاری نماید.

ماده ٣٩- مؤسسه اعتباری مکلف است دسترسی به داده‌ها، منابع و یا خدمات برای تمامی پایانه‌های شبکه داخلی را صرفاً براساس سیاست‌ها و طرح کنترل سطوح دسترسی کارکنان تعیین نماید.

ماده ٤٠- مؤسسه اعتباری موظف است ترتیبی اتخاذ نماید تا پایانه‌های متصل به شبکه پس از گذشت زمان مشخصی از عدم استفاده توسط کاربران به صورت خودکار از شبکه، قطع و غیرفعال گردد و برای اتصال دوباره، کاربران ملزم به انجام عملیات احراز هویت مجدد باشند.

ماده ٤١- مؤسسه اعتباری مکلف است سازوکار مناسب و امن به منظور مدیریت هرگونه اتصال خارج از شبکه داخلی را تهیه و اجرا نماید. استفاده از روش‌های مناسب احراز هویت[٣]، مجازسازی[٤] و کنترل دسترسی باید در اولویت باشد.

ماده ٤٢- مؤسسه اعتباری موظف است اتصال هرگونه تجهیزات شبکه‌ای بیرونی (مانند WiMAX و مودم‌های اینترنتی) که ارتباط به زیرساخت شبکه‌ای دیگر (علی‌الخصوص ارتباط اینترنتی) را تأمین می‌کنند به شبکه داخلی غیرممکن نماید.

ماده ٤٣- مؤسسه اعتباری مکلف است با بهره‌برداری از ابزارهایی نظیر UTM[٥] و دیواره آتش، نقل و انتقال اطلاعات شبکه سازمانی را به/از بیرون کنترل، نظارت و مدیریت نماید.

---

[١] Router
[٢] Firewall
[٣] Authentication
[٤] Authorization
[٥] Unified Threat Management

ماده ٤٤- مؤسسه اعتباری موظف است ضمن راه‌اندازی دیواره‌های آتش بیرونی، اقدام به طراحی و استقرار DMZ[1] برای سرویس‌دهنده‌ها جهت کنترل و تفکیک جریان داده‌ها میان شبکه‌های خارجی، داخلی و ارتباطات اینترنتی خود نماید.

ماده ٤٥- مؤسسه اعتباری مکلف است مکانیزم‌های دفاعی دیواره‌های آتش را به صورت دوره‌ای و با زمان‌بندی مشخص، به‌روزرسانی نماید. توانایی به‌روزرسانی و بهبود دیواره‌های آتش بر مبنای پیشرفت‌های فناوری توسط فروشندگان و یا ارایه دهندگان خدمات، قبل از تهیه و خرید باید مورد ارزیابی قرار گیرد.

ماده ٤٦- مؤسسه اعتباری مکلف است طی یک فرآیند زمان‌بندی‌شده اقدام به اجرای آزمون نفوذ به‌منظور پویش[2] و شناسایی آسیب‌پذیری‌های سامانه‌های خود نماید و روش‌های مقابله با آسیب‌پذیری‌ها به شکل مناسبی شناسایی و اعمال گردد.

ماده ٤٧- مؤسسه اعتباری موظف است فرآیندی تعریف نماید که طی آن Log ورود به سامانه‌ها در ساعات غیراداری را در ابتدای روز کاری بعد با استفاده از ابزارهای تحلیل Log مورد بررسی و تحلیل قرار دهد.

ماده ٤٨- مؤسسه اعتباری مکلف است داده‌های حساس و محرمانه (به تشخیص مؤسسه اعتباری) را با استفاده از الگوریتم‌های رمزنگاری معتبر رمزگذاری نموده و بر روی پایگاه‌های داده امن قرار دهد. همچنین از ذخیره داده‌های محرمانه بر روی سرویس‌دهنده کاربردی/وب خودداری نماید.

ماده ٤٩- مؤسسه اعتباری موظف است ترتیبی اتخاذ نماید که داده‌های محرمانه بر روی سرویس‌دهنده پایگاه داده مجزا ذخیره گردد. بسته نرم‌افزاری پایگاه داده‌های تهیه شده توسط مؤسسه اعتباری باید حاوی تمامی ماژول‌های امنیتی و مدیریتی لازم برای ایجاد امنیت در سطح پایگاه داده برای ذخیره و بازیابی اطلاعات به صورت امن باشد.

ماده ٥٠- مؤسسه اعتباری مکلف است طراحی سازوکار کنترل دسترسی کاربران به پایگاه داده‌های مورد استفاده را به ترتیبی انجام دهد که کاربران صرفاً براساس سطوح تعریف شده امکان دسترسی به مجموعه مشخصی از اطلاعات (جداول اطلاعاتی خاص) را داشته باشند.

ماده ٥١- مؤسسه اعتباری موظف است هرگونه نرم‌افزار یا سرویس بدون کاربرد یا اضافی بر روی سرویس‌دهنده‌ها را غیر فعال نماید.

ماده ٥٢- مؤسسه اعتباری مکلف است به منظور جلوگیری از سوءاستفاده‌های حاصل از ایجاد تغییرات در منابع نرم‌افزاری، پیکربندی و سخت‌افزاری، رویه مدیریت تغییرات[3] را به صورت یکپارچه و قابل پیگرد، تدوین و پیاده‌سازی نماید.

---

[1] DeMilitarized Zone
[2] Scan
[3] Change Management

ماده ۵۳- مؤسسه اعتباری موظف است از اطلاعات با اهمیت سرویس‌دهندگان، نسخه پشتیبان کامل و قابل بازگشت تهیه نماید. آزمون‌های لازم به منظور بازیابی اطلاعات پشتیبان باید انجام پذیرد.

ماده ٥٤- مؤسسه اعتباری مکلف است ترتیبی اتخاذ نماید که دسترسی به سرویس‌دهنده‌ها چه از لحاظ فیزیکی و چه از لحاظ پیکربندی صرفاً برای افراد مجاز قابل تعریف و اعمال باشد.

ماده ٥٥- مؤسسه اعتباری موظف است ترتیبی اتخاذ نماید که نام‌های کاربری پیش‌فرض برای تمامی تجهیزات کامپیوتری و ارتباطی، غیرفعال شده یا به شکل امن، تغییر یابد.

ماده ٥٦- مؤسسه اعتباری مکلف است نرم‌افزارهای طراحی شده را به لحاظ امنیتی و صحت عملکرد، مورد ارزیابی قرار داده و گزارش‌ها و مستندات لازم را تهیه نماید.

ماده ۵۷- مؤسسه اعتباری موظف است محرمانه بودن اطلاعات مشتریان را (به طور خاص تراکنش‌های بانکداری الکترونیکی) حین ذخیره‌سازی یا انتقال اطلاعات در سامانه‌ها و شبکه داخلی یا خارج از مؤسسه اعتباری تضمین نماید.

ماده ۵۸- مؤسسه اعتباری مکلف است برای حصول اطمینان از حفظ اطلاعات مشتریان از روش‌های رمزنگاری، پروتکل‌های خاص و سایر کنترل‌های امنیتی استفاده نموده و آن‌ها را به صورت ادواری مورد بازبینی و به‌روزرسانی قرار دهد.

ماده ۵۹- مؤسسه اعتباری موظف است برای انتقال اطلاعات حساس خصوصاً میان سرویس‌دهنده‌ها و تجهیزات مشتریان از روش‌های رمزگذاری شناخته شده و معتبر بین‌المللی به شکل انتها به انتها[1] استفاده نماید.

ماده ٦٠- مؤسسه اعتباری مکلف است به منظور افزایش اثربخشی فناوری رمزگذاری مورد استفاده، نسبت به بکارگیری روش‌های مدیریت کلیدهای رمزگذاری اقدام نماید. استفاده از کلید رمزگذاری مشترک برای بیش از یک برنامه ممنوع است.

ماده ٦١- مؤسسه اعتباری موظف است به منظور پایش، مدیریت و کنترل مؤثر رخدادهای امنیتی، مرکز عملیات امنیت[2] با حداقل وظایف زیر ایجاد نماید:

١-٦١- شناسایی، مدیریت و پایش لحظه‌ای آسیب‌پذیری‌ها، تهدیدات و حملات امنیتی به منابع و تجهیزات رایانه‌ای و ارتباطی در کمترین زمان ممکن به صورت ٢٤×٧؛

٢-٦١- جمع‌آوری و آنالیز ترافیک شبکه و تولید گزارش‌های امنیتی در سطوح مختلف ؛

٣-٦١- ایجاد نقطه تماس متمرکز برای رسیدگی به مشکلات امنیتی ذینفعان؛

٤-٦١- پردازش رخدادهای امنیتی و پاسخ‌دهی به مشکلات مرتبط.

---

[1] End to End

[2] SOC (Security Operations Center)

ماده ٦٢- مؤسسه اعتباری مکلف است ترتیبی اتخاذ نماید که ارزیابی چک‌لیست‌های امنیتی لازم برای تمامی کارکنان و تأمین‌کنندگان خدمات که به نقاط حساس دسترسی دارند، انجام شود.

ماده ٦٣- مؤسسه اعتباری موظف است برای مدیریت عملیات مالی و ارائه خدمت به مشتریان از نرم‌افزارهای نسخه اصلی[1] و با مجوز استفاده نماید.

ماده ٦٤- مؤسسه اعتباری مکلف است از نرم‌افزار و نسخه‌های معتبر سیستم‌عامل در سرویس‌دهنده‌ها استفاده نماید. ریسک استفاده از نسخه‌های دستکاری شده سیستم‌عامل و نرم‌افزارهای کاربردی بر عهده مؤسسه اعتباری می‌باشد.

ماده ٦٥- مؤسسه اعتباری موظف است در شبکه داخلی خود فرآیند به‌روزرسانی و نصب آخرین وصله‌ها[2] را برای تجهیزات، سیستم عامل‌ها و نرم‌افزارهای کاربردی پیاده‌سازی نماید.

ماده ٦٦- مؤسسه اعتباری مکلف است توصیه‌های امنیتی لازم را با توجه به ماهیت خدمات بانکداری الکترونیکی ارائه شده به مشتریان در اختیار آن‌ها قرار دهد. این اطلاع‌رسانی حداقل باید موارد زیر را در برگیرد:

١-٦٦- انتخاب نام کاربری و گذرواژه مناسب؛

٢-٦٦- اهمیت حفظ اطلاعات شخصی از جمله شناسه کاربری و گذرواژه؛

٣-٦٦- استفاده از آنتی‌ویروس‌ها در هنگام بهره برداری از خدمات بانکداری الکترونیکی؛

٤-٦٦- اطلاع‌رسانی درخصوص تارنماها[3] و پست‌های الکترونیکی جعلی، Phishing و نظایر آن؛

٥-٦٦- عدم استفاده از کامپیوترها و شبکه‌های عمومی پرخطر برای استفاده از خدمات بانکداری الکترونیکی؛

٦-٦٦- خروج صحیح از صفحات تارنمای سامانه بانکداری الکترونیکی مؤسسه اعتباری.

فصل ششم – مدیریت شناسایی و تأیید مشتریان

ماده ٦٧- ارائه هرگونه خدمات بانکداری الکترونیکی به اشخاص حقیقی و حقوقی منوط به رعایت کامل ضوابط شناسایی مشتریان ابلاغی از سوی بانک مرکزی می‌باشد.

ماده ٦٨- به منظور پذیرش مشتریان غیرحضوری، مؤسسه اعتباری باید از اصالت هویت مشتری، اطمینان حاصل نماید.

ماده ٦٩- به منظور دسترسی به خدمات بانکداری الکترونیکی لازم است مؤسسه اعتباری حداقل یک یا ترکیبی از روش‌ها یا ابزارهای احراز هویت الکترونیکی از قبیل موارد زیر را به‌کار گیرد:

١-٦٩- کلمه عبور، شماره شناسایی؛

---

[1] Original
[2] Patch
[3] Web Site

۲-٦۹- کارت، شناسه فیزیکی الکترونیکی، امضاء دیجیتال و توکن[1] امنیتی؛

۳-٦۹- خصوصیات منحصر به فرد زیستی مانند اثر انگشت و عنبیه چشم؛

٤-٦۹- سایر روش‌های متناسب با فناوری روز.

ماده ۷۰- فهرست تمام کاربران مجاز به دسترسی به سامانه‌های بانکداری الکترونیکی تعیین شده و دسترسی به هیچ‌یک از سامانه‌های مبتنی بر تراکنش و تبادل اطلاعات (مالی – هویتی) بدون احراز هویت امکان‌پذیر نباشد.

ماده ۷۱- تعریف مجوز کاربری، حق دسترسی، ورود کاربر جدید و تغییر سطح دسترسی به سامانه‌های بانکداری الکترونیکی باید توسط افراد مسئول صورت گرفته و به طور مرتب و به موقع تحت بازرسی و بازنگری قرار گیرد.

ماده ۷۲- کنترل سطح دسترسی برای هر کاربر و گروه کاربران باید براساس هویت و شناسه‌های منحصر به فرد، وظایف و مسئولیت‌ها، زمان و نوع تراکنش تعیین شود.

ماده ۷۳- پایگاه داده مربوط به مجوز کاربری و شناسایی و احراز هویت مشتریان باید در مقابل نفوذ، دسترسی‌های غیرمجاز، کدهای مخرب، ویروس و حملات خرابکارانه، مقاوم‌سازی شود.

ماده ۷٤- ضروری است هرگونه تلاش برای نفوذ (موفق یا ناموفق) در پایگاه داده، طی فرآیند بازبینی و آزمون مداوم، کشف، اصلاح، به‌روزرسانی و مستند شود.

ماده ۷۵- مؤسسه اعتباری موظف است سیاست‌های تغییر دوره‌ای و موردی گذرواژه کاربران و تعیین حداکثر مدت مجاز استفاده از آن را تدوین و اجرا نماید.

ماده ۷٦- روش‌های احراز هویت، مجازسازی و تأیید اصالت مشتریان از طریق سامانه باید به طور مستمر تحت پایش و بازنگری قرار گرفته، به‌گونه‌ای که مؤسسه اعتباری نسبت به موارد زیر اطمینان حاصل نماید:

۱-۷٦- شیوه‌های شناسایی و تأیید مشتری در سامانه بانکداری الکترونیکی باید به‌گونه‌ای باشد که امکان ورود کاربران غیرمجاز به سامانه با استفاده از هویت مشتریان بانکی را ناممکن سازد؛

۲-۷٦- هنگام کار با سامانه بانکداری الکترونیکی، چنانچه کاربر برای مدت معینی از سامانه استفاده ننماید لازم است برای ادامه کار، مجدداً عملیات احراز هویت انجام شود.

ماده ۷۷- مؤسسه اعتباری موظف است جهت اطلاع‌رسانی به مشتریان، حداقل موارد زیر را در تارنمای خود درج نماید:

۱-۷۷- نام، نشانی و تلفن دفتر مرکزی مؤسسه اعتباری (دفاتر منطقه‌ای یا نمایندگی‌ها در صورت وجود) و واحدهای امداد مشتریان؛

[1] Token

۷۷-۲- معرفی بانک مرکزی به عنوان مقام ناظر بر مؤسسه اعتباری؛

۷۷-۳- مشخص نمودن فرآیند طرح و رسیدگی به شکایت مشتریان؛

۷۷-٤- استفاده از روش‌هایی برای آموزش مشتریان در خصوص کاربری، نکات امنیتی ـ حفاظتی و مسئولیت‌های حقوقی طرفین درخصوص استفاده از خدمات بانکداری الکترونیکی؛

۷۷-۵- مشخص نمودن سطح خدمت‌رسانی به مشتریان برای هر یک از خدمات بانکداری الکترونیکی؛

۷۷-٦- توصیه و آموزش‌های لازم به مشتریان درخصوص مخاطرات ناشی از ورود عوامل نفوذی، آلودگی ویروسی، جعل هویت و موارد مشابه.

فصل هفتم – طراحی، نگهداری و مدیریت سامانه جامع بانکداری متمرکز[۱]

ماده ۷۸- مؤسسه اعتباری موظف است نسبت به استقرار سامانه جامع بانکداری متمرکز با دارا بودن حداقل ویژگی‌های عملکردی زیر اقدام نماید:

۷۸-۱- مدیریت اطلاعات پایه و پیکربندی سیستم؛

۷۸-۲- مدیریت مشتریان؛

۷۸-۳- مدیریت ذینفع واحد؛

۷۸-٤- مدیریت خزانه‌داری و صندوق؛

۷۸-۵- مدیریت تحویلداری و پرداخت؛

۷۸-٦- مدیریت سپرده؛

۷۸-۷- مدیریت حسابداری و دفترکل؛

۷۸-۸- مدیریت اعتبارات و تعهدات؛

۷۸-۹- مدیریت چک؛

۷۸-۱۰- مدیریت عملیات ارزی؛

۷۸-۱۱- مدیریت پشتیبانی اطلاعات و گزارش‌ها؛

۷۸-۱۲- نظارت و بازرسی؛

۷۸-۱۳- مدیریت کارت؛

۷۸-۱٤- مدیریت سوئیچ و درگاه‌های فیزیکی الکترونیکی؛

۷۸-۱۵- مدیریت بانکداری مدرن؛

۷۸-۱٦- بانکداری باز؛

۷۸-۱۷- پشتیبانی فنی [۲].

---

[۱] Core Banking

[۲] Help Desk

۱۸-۷۸- سایر ضوابط و سیستم‌های مورد نیاز براساس بخشنامه‌های ابلاغی معاونت نظارت بانک مرکزی.

ماده ۷۹- سامانه جامع بانکداری متمرکز باید حداقل دارای ویژگی‌های فنی زیر باشد:

۱-۷۹- ماژولار و یکپارچه باشد؛

۲-۷۹- دارای پایگاه داده مشترک و متمرکز باشد؛

۳-۷۹- مبتنی بر مدیریت فرآیندهای کسب و کار باشد؛

٤-۷۹- از کد نویسی امن و امضای دیجیتال استفاده نماید؛

۵-۷۹- پایگاه داده و سرورهای کاربردی به سیستم‌عامل، سکوی[۱] نرم‌افزاری و سخت‌افزاری خاص وابستگی نداشته باشد؛

٦-۷۹- منطبق بر قوانین رمزنگاری باشد به‌گونه‌ای که انتخاب الگوریتم رمزنگاری، متناسب با کاربرد آن انجام شود؛

۷-۷۹- قابلیت تعریف کدینگ‌های متفاوت مالی و حسابداری و ثبت هم‌زمان تراکنش‌های مالی در آن وجود داشته باشد به‌گونه‌ای که نتایج صحیح را با دقت مورد نیاز، فرآهم نماید؛

۸-۷۹- تمامی عملیات سامانه، ثبت و مدیریت گردد؛

۹-۷۹- زمان پردازش و توان عملیاتی قابل قبولی داشته باشد؛

۱۰-۷۹- عملیات تعریف شده را در شرایط معین و برای یک دوره زمانی مشخص، اجرا نماید؛

۱۱-۷۹- امکان تصحیح خطا در بهترین حالت و کمترین زمان میسر باشد؛

۱۲-۷۹- در صورت بروز خطاهای سخت‌افزاری و یا نرم‌افزاری، دارای قابلیت تحمل‌پذیری خطا[۲] بوده و افزونگی اجزاء نداشته باشد؛

۱۳-۷۹- امکان ایجاد و اجرای معیارهای آزمون برای بررسی تحقق آن‌ها وجود داشته باشد به‌گونه‌ای که قابلیت اجرای انواع آزمون فراهم باشد؛

۱٤-۷۹- قبل و بعد از پیاده‌سازی سامانه و به‌روزرسانی نسخه‌های جدید و وصله‌های الحاقی، تحت آزمون‌های بار[۳]، بحران[٤]، پایداری[۵]، نفوذپذیری[٦] و امنیت قرار گیرد؛

۱۵-۷۹- به صورت منظم قابل توسعه و ارتقاء باشد؛

۱٦-۷۹- امکان مدیریت دسترسی افراد و سایر سیستم‌ها، متناسب با نوع و سطح اختیار آن‌ها فراهم شود به‌گونه‌ای که حفاظت سامانه از اطلاعات و داده‌ها به شکل جامع صورت پذیرد؛

---

[۱] Platform
[۲] Fault tolerance
[۳] Load test
[٤] Stress test
[۵] Stability test
[٦] Penetration Test

۷۹-۱۷- قابلیت ارتباط و یکپارچه شدن با سایر سامانه‌های نرم‌افزاری موجود را داشته باشد؛

۷۹-۱۸- دارای واسط کاربری واحد با قابلیت سفارشی‌سازی باشد؛

۷۹-۱۹- دارای قابلیت طبقه‌بندی اطلاعات متناسب با کاربرد باشد؛

۷۹-۲۰- امکان توسعه هوشمندی صفحات در نقاط ورود داده به منظور جلوگیری از اشتباه کاربر وجود داشته باشد؛

۷۹-۲۱- توصیف کامل کدهای خطا و مراحل بازیابی آن قابل انجام باشد.

ماده ۸۰- مؤسسه اعتباری مکلف است در طراحی سامانه بانکداری متمرکز از معماری سرویس‌گرا استفاده نماید به‌گونه‌ای که تغییر در یک مؤلفه کمترین تأثیر را در سایر مؤلفه‌ها داشته باشد.

ماده ۸۱- مؤسسه اعتباری موظف است مستندات مربوط به طراحی، نصب و راه‌اندازی، تغییرات و ارتقاء و روابط پایگاه‌های داده سامانه جامع عملیات بانکداری را تهیه و نگهداری نماید.

ماده ۸۲- مؤسسه اعتباری مکلف است فرآیند پشتیبان‌گیری از اطلاعات سامانه جامع عملیات بانکداری را به صورت دوره‌ای انجام دهد.

ماده ۸۳- مؤسسه اعتباری موظف است درصورت نیاز به تفویض اختیار کاربران، دسترسی موقت به سامانه جامع عملیات بانکداری را به صورت سیستمی تعیین و پایش نماید.

ماده ۸٤- مؤسسه اعتباری مکلف است در صورت برون‌سپاری تمام و یا بخشی از عملیات طراحی، پیاده‌سازی، نگهداری و پشتیبانی سامانه جامع بانکداری متمرکز، کلیه موارد الزام شده در این فصل را در متن قرارداد خود با پیمانکار به نحو مقتضی درج و بر حسن اجرای آن نظارت نماید.

فصل هشتم – طراحی، نگهداری و مدیریت سامانه‌های بانکداری الکترونیکی

ماده ۸۵- ارائه خدمات بانکداری الکترونیکی باید مطابق با استانداردها و ضوابط بانک مرکزی باشد.

ماده ۸٦- تمامی تراکنش‌های انجام شده در سامانه‌های بانکداری الکترونیکی اعم از درون و برون‌سازمانی به‌گونه‌ای ثبت و نگه‌داری شود که قابلیت بازیابی، پردازش و ردیابی آن‌ها در کوتاه‌ترین زمان ممکن، میسر باشد.

ماده ۸۷- سامانه‌های بانکداری الکترونیکی اعم از درون و برون سازمانی به‌گونه‌ای طراحی و پیاده‌سازی شود که تراکنش‌ها و مستندات تولید شده آن، قابلیت طرح و دفاع در محاکم قضایی را داشته باشد.

ماده ۸۸- سامانه‌های بانکداری الکترونیکی باید به‌گونه‌ای طراحی و پیاده‌سازی شود تا هرگونه تلاش جهت دسترسی غیرمجاز و یا مداخله غیرمسئولانه در سامانه را ردیابی، ثبت و گزارش نماید.

ماده ۸۹- انتقال، پردازش و نگهداری داده‌ها، اطلاعات و اسناد بانکداری الکترونیکی باید به‌گونه‌ای صورت گیرد که در مقابل هرگونه دسترسی غیرمجاز محافظت شود.

ماده ۹۰- به منظور مقابله با سوء استفاده‌های احتمالی، درگاه‌های پرداخت جعلی مشابه درگاه مؤسسه اعتباری، شناسایی و به منظور اقدامات حقوقی و قضائی، به مراجع قضائی معرفی شود.

ماده ۹۱- خدمات بانکداری الکترونیکی باید بنا به درخواست مشتری و براساس قرارداد منعقده بین مؤسسه اعتباری و مشتری ارائه شود. لازم است در متن قرارداد موارد زیر به طور شفاف تبیین شود:

۹۱-۱- مدت اعتبار قرارداد و روش‌های تمدید آن؛

۹۱-۲- تعیین محدوده زمانی مشخص ارائه خدمات بانکداری الکترونیکی به مشتری؛

۹۱-۳- تأکید بر استفاده از ابزارهای احراز هویت صرفاً برای کاربری شخصی مشتری؛

۹۱-٤- ذکر خدمات قابل ارائه توسط مؤسسه اعتباری و اخذ تأیید از مشتری؛

۹۱-٥- نحوه اطلاع‌رسانی مشتری به مؤسسه اعتباری در صورت بروز هرگونه مشکل یا احتمال سوء استفاده از اطلاعات کاربری یا حساب وی؛

۹۱-٦- اخطار و پیامدهای ناشی از قراردادن اطلاعات کاربری یا حساب در اختیار افراد غیر توسط مشتری.

ماده ۹۲- سامانه‌های بانکداری الکترونیکی باید به‌گونه‌ای طراحی شوند که:

۹۲-۱- احتمال انجام تراکنش‌های ناخواسته توسط کاربران مجاز به حداقل برسد؛

۹۲-۲- اطلاع‌رسانی به موقع به کاربران هنگام انجام تراکنش با استفاده از ابزارهای اطلاع‌رسانی از قبیل پیامک انجام شود؛

۹۲-۳- هر یک از طرفین انجام‌دهنده تراکنش‌ها به طور دقیق یکدیگر را مورد شناسایی قرار دهند؛

۹۲-٤- اصالت داده‌ها و محرمانه نگه‌داشتن اطلاعات کلیدی مؤسسه اعتباری لحاظ شود.

ماده ۹۳- مؤسسه اعتباری باید به منظور پشتیبانی و حفاظت از داده‌ها و سامانه‌های بانکداری الکترونیکی تدابیر امنیتی لازم را اعمال نماید. این تدابیر باید به صورت دوره‌ای مورد بازبینی قرار گیرد. به همین منظور ضروری است:

۹۳-۱- تمامی سامانه‌ها و پشتیبان آن‌ها باید در داخل کشور قرار داشته باشد؛

۹۳-۲- از تمامی داده‌های عملیات بانکداری الکترونیکی، نسخه‌های پشتیبان تهیه شود؛

۹۳-۳- حداقل یک نسخه پشتیبان قابل اتکاء با امکان جایگزینی سریع با پایگاه داده اصلی در سایت عملیاتی وجود داشته باشد؛

۹۳-٤- حداقل یک نسخه پشتیبان داده در محلی مجزا از سایت عملیاتی، نگهداری شود؛

۹۳-٥- رسانه‌های پشتیبان‌گیری با توجه به میزان اهمیت اطلاعات ذخیره شده، از طریق قراردادن گذرواژه‌ها یا روش‌های مناسب دیگر، امن‌سازی شود؛

۹۳-٦- فرآیندهای کنترل دسترسی بر روی نسخه‌های پشتیبان، اعمال شده و نباید در دسترس افراد غیرمجاز قرار گیرد؛

۹۳-۷- رویه امحاء و دفع تجهیزات سخت‌افزاری، نرم‌افزاری، مستندات و نسخ پشتیبان به دقت تدوین و اجرا گردد.

ماده ۹٤- مؤسسه اعتباری موظف است اقدامات لازم جهت مقابله با تهدیدهای امنیتی (درون‌سازمانی/برون‌سازمانی) سامانه‌های بانکداری الکترونیکی را به شرح زیر انجام دهد:

۹٤-۱- استفاده از نرم‌افزارهای ضد بدافزار، پایش امنیتی، تشخیص و جلوگیری از نفوذ در تمامی سرویس‌دهنده‌های سامانه‌های بانکداری الکترونیکی؛

۹٤-۲- استفاده از دیواره آتش نرم‌افزاری و سخت‌افزاری به‌منظور حفاظت سامانه‌های بانکداری الکترونیکی؛

۹٤-۳- انجام آزمون‌های امنیتی نظیر آزمون بحران، آزمون پایداری و نفوذپذیری داخلی و خارجی به شبکه‌ها و سامانه‌ها، به‌صورت دوره‌ای و موردی توسط گروه‌های مستقل از گروه‌های امنیتی درون‌سازمانی؛

۹٤-٤- انجام اقدامات اصلاحی مورد نیاز بر مبنای نتایج آزمون‌های بند ۹٤-۳.

فصل نهم – مدیریت ریسک

ماده ۹۵- مؤسسه اعتباری موظف است یکی از استانداردهای سری ISO ۳۱۰۰۰، ISO ۲۷۰۰۵ و یا چارچوب ریسک فناوری اطلاعات ایساکا را به عنوان مرجع پیاده‌سازی مدیریت ریسک فناوری اطلاعات استفاده نماید.

ماده ۹٦- مؤسسه اعتباری مکلف است برنامه‌های منظم سالانه برای مدیریت ریسک فناوری اطلاعات داشته باشد.

ماده ۹۷- مؤسسه اعتباری موظف است برنامه و راهکارهای مدیریت ریسک فناوری اطلاعات را همسو با برنامه تداوم کسب و کار و برنامه مقابله با حوادث غیرمترقبه مؤسسه اعتباری،تهیه و تدوین نماید.

ماده ۹۸- مؤسسه اعتباری مکلف است قبل از ارائه هر نوع خدمت جدید فناوری اطلاعات نسبت به شناسایی و ارزیابی ریسک ناشی از ارائه یا انتشار خدمات جدید اقدام نماید.

ماده ۹۹- مؤسسه اعتباری موظف است در صورت تحمیل هرگونه زیان ناشی از ارائه خدمات جدید فناوری اطلاعات، پوشش بیمه‌ای متناسب را برای مشتریان مؤسسه اعتباری پیش بینی نماید.

ماده ۱۰۰- مؤسسه اعتباری مکلف است برنامه‌های اجرایی مرتبط با ریسک‌های شناسایی شده را به ترتیب اهمیت و اولویت، به شکل مداوم مورد پایش قرار دهد.

ماده ۱۰۱- مؤسسه اعتباری موظف است برنامه‌های آموزشی شناسایی و سنجش ریسک‌های مرتبط با فناوری اطلاعات را در تمامی سطوح مؤسسه تدوین و اجرا نماید.

فصل دهم – شبکه و ارتباطات

ماده ۱۰۲- مؤسسه اعتباری موظف است استاندارد و یا چارچوب‌های منطبق و یا مرتبط با پنج لایه پروتکل TCP/IP و یا هفت لایه OSI در حوزه شبکه و ارتباطات را پیاده‌سازی و اجرا نماید.

ماده ۱۰۳- مؤسسه اعتباری مکلف است سامانه مدیریت شبکه بر مبنای چارچوب FCAPS [۱] را طراحی و پیاده‌سازی نماید.

ماده ۱۰٤- مؤسسه اعتباری موظف است شبکه داخلی خود را به شکل Core-Distribution-Access طراحی و لایه‌بندی نموده و تجهیزات پشتیبان لازم به منظور حداقل نمودن قطعی شبکه را پیکربندی و آماده بهره‌برداری نماید.

ماده ۱۰۵- مؤسسه اعتباری مکلف است مرکز عملیات شبکه [۲] را به منظور پایش، کنترل و مدیریت رخدادهای شبکه ارتباطی به صورت متمرکز پیاده‌سازی نماید.

ماده ۱۰٦- مؤسسه اعتباری موظف است فهرست کامل و دقیق همه تجهیزات شبکه و ارتباطات را به شکل مدون، مصور و مکتوب تهیه و نگهداری نماید.

ماده ۱۰۷- مؤسسه اعتباری مکلف است مستندات مربوط به طراحی و معماری شبکه را به شکل دقیق، کامل و مکتوب تدوین نماید.

ماده ۱۰۸- مؤسسه اعتباری موظف است فرآیند مستندسازی اتصالات مسیریاب، سوئیچ و دروازه [۳] را به شکل مکتوب و مصور انجام دهد.

ماده ۱۰۹- مؤسسه اعتباری مکلف است مستند و نقشه دقیق شبکه‌های محلی و گسترده و همچنین نحوه ارتباط شعب و ساختمان‌ها با یکدیگر را به شکل مکتوب تهیه نماید.

ماده ۱۱۰- مؤسسه اعتباری موظف است فرآیندی به منظور به‌روزرسانی IOS [٤] سوئیچ‌ها و مسیریاب‌های خود از طریق دریافت آخرین نسخه IOS از سازنده تجهیزات، تدوین و اجرا نماید.

ماده ۱۱۱- مؤسسه اعتباری مکلف است مدیریت تغییرات پیکربندی در حوزه شبکه را در قالب سامانه مدیریت تغییرات، راه‌اندازی نماید.

ماده ۱۱۲- مؤسسه اعتباری موظف است با توجه به شرایط پیکربندی شبکه از تکنیک‌هایی مانند VLAN برای جداسازی منطقی و ارتقاء امنیت شبکه استفاده نماید.

---

[۱] FCAPS (Fault, Configuration, Accounting, Performance, Security) Management
[۲] NOC (Network Operations Center)
[۳] Gateway
[٤] IOS (Internetwork Operating System)

ماده ۱۱۳- مؤسسه اعتباری مکلف است خطوط ارتباطی غیرفعال و بلااستفاده را مسدود و از معماری شبکه حذف نماید.

ماده ۱۱٤- مؤسسه اعتباری موظف است به منظور حداقل سازی قطعی شبکه از خطوط ارتباطی پشتیبان استفاده نماید.

ماده ۱۱۵- مؤسسه اعتباری مکلف است از نیروی انسانی متخصص و آموزش دیده کافی با مدارک تخصصی معتبر در زمینه مدیریت، راهبری و نظارت شبکه‌های کامپیوتری استفاده نماید.

فصل یازدهم – مرکز داده

ماده ۱۱٦- مؤسسه اعتباری موظف است نسبت به فراهم نمودن مراکز داده زیر اقدام نماید:

۱-۱۱٦- مرکز داده اصلی؛

۲-۱۱٦- مرکز داده بحران با قابلیت جایگزینی سریع با مرکز داده اصلی؛

۳-۱۱٦- مرکز داده پشتیبان با قابلیت جایگزینی با رعایت فاصله جغرافیایی مناسب.

ماده ۱۱۷- مؤسسه اعتباری موظف است قراردادهای خدمات مراکز داده استیجاری را در قالب توافق‌نامه سطح خدمت، حداقل در سطح Tier۲ در استاندارد TIA۹٤۲ تدوین نماید.

ماده ۱۱۸- مؤسسه اعتباری مکلف است به منظور طراحی، پیاده‌سازی و مدیریت مراکز داده از چارچوب معرفی شده توسط سازمان فناوری اطلاعات ایران با عنوان DC-۱۰۰ استفاده نماید به گونه ای که تمامی ضوابط در سطوح و رتبه‌های مختلف مراکز داده منطبق بر یکی از سطوح تعریف شده در چارچوب مذکور باشد.

ماده ۱۱۹- مؤسسه اعتباری موظف است در بهره‌برداری از خدمات مراکز داده اصلی، پشتیبان و بحران موضوعات: حفاظتی و حراستی، قرارداد مالکیت داده، دسترسی به اطلاعات و داده‌ها و امنیت فیزیکی را به شکل کامل و دقیق منظور نماید.

ماده ۱۲۰- مؤسسه اعتباری موظف است به منظور مقابله با خطرات احتمالی، مراکز داده پشتیبان و بحران را به‌گونه‌ای طراحی و پیاده‌سازی نماید که در هر دو سطح داده و سرویس، پشتیبان وجود داشته باشد.

ماده ۱۲۱- مؤسسه اعتباری موظف است در مراکزداده موارد زیر را رعایت نماید:

۱-۱۲۱- در نظر گرفتن تهدیدات و حوادث قهری برای انتخاب محل؛

۲-۱۲۱- رعایت ملاحظات کمیته پدافند غیرعامل کشوری در تمامی مراحل ساخت یا برون‌سپاری؛

۳-۱۲۱- رعایت ملاحظات ارتفاع تا سطح زمین، استحکام و استتار مرکز داده؛

٤-۱۲۱- اعمال سیاست‌های مدیریت دسترسی به بخش‌های مختلف مرکز داده.

ماده ۱۲۲- مؤسسه اعتباری موظف است تمامی قراردادهای مرتبط با مراکز داده را با رعایت بندهای بخش برون‌سپاری این الزامات منعقد نماید.

فصل دوازدهم – سایر

ماده ۱۲۳- مؤسسه اعتباری موظف است سامانه‌های متناظر با بخشنامه‌های ابلاغی بانک مرکزی را با رعایت مهلت زمانی مقرر، به قید تسریع پیاده‌سازی نماید.

ماده ۱۲٤- مؤسسه اعتباری باید حداقل هر دو سال یکبار پروژه خودارزیابی فناوری اطلاعات و یا ارزیابی بلوغ فناوری اطلاعات کل مؤسسه اعتباری را انجام دهد. این ارزیابی باید حداقل شامل موارد زیر باشد:

۱-۱۲٤- سامانه عملیات بانکداری؛

۲-۱۲٤- ریسک فناوری اطلاعات؛

۳-۱۲٤- امنیت فناوری اطلاعات؛

٤-۱۲٤- شبکه و زیرساخت؛

٥-۱۲٤- مرکز داده.

ماده ۱۲٥- عدم رعایت مفاد الزامات موجب اعمال اقدامات انضباطی زیر در مورد مؤسسه اعتباری متخلف و مدیران آن می‌گردد:

۱-۱۲٥- اعمال مجازات‌های انتظامی موضوع ماده (٤٤) قانون پولی و بانکی کشور؛

۲-۱۲٥- اعمال مجازات‌های انتظامی موضوع بند (الف) ماده (١٤) قانون برنامه پنج‌ساله ششم توسعه اقتصادی، اجتماعی و فرهنگی جمهوری اسلامی ایران.

ماده ۱۲٦- تشخیص موارد تخلف از الزامات با بانک مرکزی بوده و با متخلفین، مطابق با قوانین و مقررات رفتار خواهد شد.

ماده ۱۲۷- مؤسسه اعتباری موظف است برنامه زمان‌بندی ۲٤ ماهه به منظور تطبیق حوزه فناوری اطلاعات با مفاد الزامات را حداکثر ظرف مدت ۳ ماه از تاریخ ابلاغ به معاونت نظارت بانک مرکزی ارائه دهد. بدیهی است شروع برنامه زمان‌بندی در بازه زمانی ۳ ماهه پس از ابلاغ الزامات قابل پذیرش است.

«حداقل الزامات ناظر بر ریسک فناوری اطلاعات مؤسسات اعتباری» در ۱۲۷ ماده در جلسه مورخ ۱٤۰۰/٥/۳۱ کمیسیون مقررات و نظارت مؤسسات اعتباری به تصویب رسید و از تاریخ ابلاغ آن به مؤسسات اعتباری، لازم‌الاجرا می‌باشد.

پیوست

نمودار جایگاه

کمیته عالی فناوری اطلاعات/ واحد حسابرسی فناوری اطلاعات / معاونت فناوری اطلاعات

در ساختار سازمانی مؤسسه اعتباری