شماره بخشنامه : 191012-00

تاریخ : ۱۴۰۰/۰۷/۰۶

موضوع	19- بخشنامه شماره 00/191012 مورخ 1400/07/06; ابلاغ بخشنامه «حداقل الزامات ناظر بر ریسک فناوری اطلاعات مؤسسات اعتباری»

شماره : تاریخ :
۰۰٫۱۹۱۰۱۲
۱۴۰۰٫۰۷٫۰۶ پوست دارد (۲۷) صفحه)
بانک مرکزی جمهوری اسلامی ایران
ریتالی

جهت اطلاع مدیران عامل محترم بانکهای دولتی غیر دولتی شرکت دولتی پست بانک موسسات اعتباری غیربانکی و بانک مشترک ایران - ونزوئلا ارسال میشود
با سلام
احتراماً، همان گونه که مستحضرند توسعه روز افزون فناوری اطلاعات و زیر ساختهای ارتباطی نقش تعیین کننده ای 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 ریسک های مرتبط علی الخصوص ریسک عملیاتی که از جمله مهمترین منابع ایجاد کننده آن ریسک فناوری اطلاعات میباشد را در پی داشته است. در این میان توجه ویژه به مقوله ارتقاء امنیت زیر ساختها و فرایندهای حوزه فناوری اطلاعات با هدف کاهش ریسکها و چالشهای این حوزه امری ضروری و اجتناب ناپذیر 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 بهره گیری از آخرین استانداردها و مراجع معتبر بین المللی مانند Deloitte ISO و Gartner 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 استفاده های احتمالی و جلوگیری از هدر رفت منابع موجود در شبکه بانکی کشور
یکپارچگی سیاستهای ابلاغی در نظارت بر ریسک فناوری اطلاعات مؤسسات اعتباری
همچنین خاطر نشان میسازد رعایت مفاد بخشنامه های شماره ۹۷٫۴۹۷۵۱ مورخ ۹۷٫۰۲٫۲۰ با موضوع «الزامات سازمان دهی امنیت اطلاعات در بانکها و موسسات اعتباری شماره ۹۷٫٤۹٤۸۸ مورخ ۱۳۹۷٫۰۲٫۲۰ در خصوص الزامات گزارش دهی رخدادهای امنیت اطلاعات بانکی و شماره ۹۹٫۳۱۱۴۱۷ مورخ ۹۹٫۱۰٫۰۱ تحت عنوان احراز
بانک مرکزی جمهوری اسلامی ایران

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 گزارش دهی دوره ای 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 بازه های 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 زمان بندی دقیق بر اساس مهلت زمانی مندرج در ماده (۱۲۷) حداقل الزامات یاد شده به این مدیریت کل ارائه گردد.
در خاتمه ضمن تأکید مجدد بر مسئولیت هیات مدیره در مدیریت مؤثر ریسک فناوری اطلاعات خواهشمند است. دستور فرمایند مراتب به قید تسریع به تمامی واحدهای ذی ربط آن بانک مؤسسه اعتباری ابلاغ شده و بر حسن اجرای آن نظارت دقیق به عمل آید. ۵۳۳۲۵۹۷

مدیریت کل نظارت بر بانکها و موسسات اعتباری
اداره ارزیابی سلامت نظام بانکی
عبدالمهدی ارجمند نژاد سید علی اکبر میرعمادی
۰۹-۳۲۱۵
تهران بلوار میرداماد، پلاک ۱۹۸ تلفن: ۱۹۵۱ کد پستی: ۳۱- ۱۵۴۹۶ فاس : ۶۷۳۵۶۷۴ عربات اینترنتی: www.cbi.ir
.

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

حداقل الزامات ناظر بر ریسک فناوری اطلاعات مؤسسات اعتباری مدیریت کل نظارت بر بانکها و مؤسسات اعتباری اداره ارزیابی سلامت نظام بانکی

شناسنامه سند

حداقل الزامات ناظر بر ریسک فناوری اطلاعات مؤسسات اعتباری
فهرست مطالب
فصل اول - تعاریف .
فصل دوم - معماری و ساختار سازمانی
فصل سوم خط مشی ها سیاستها و برنامه ها .

فصل چهارم - برون سپاری.....
فصل پنجم امنیت فصل ششم - مدیریت شناسایی و تأیید مشتریان فصل هفتم - طراحی نگهداری و مدیریت سامانه جامع بانکداری متمرکز فصل هشتم - طراحی نگهداری و مدیریت سامانه های بانکداری الکترونیکی فصل نهم - مدیریت ریسک
فصل دهم - شبکه و ارتباطات .
فصل یازدهم - مرکز داده .
فصل دوازدهم - سایر.....
پیوست.

بسمه تعالی
به استناد مفاد بند (ب) ماده (۱۱) بند (۲) ماده (۱۴) و ماده (۳۷) قانون پولی و بانکی کشور و مفاد بند (الف) ماده (٤٩) 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 می گردد
فصل اول - تعاریف
ماده ۱ در این الزامات اصطلاحات در معانی مشروح زیر به کار می رود
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 سیاست گذاری 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 درگاه های الکترونیکی
۱-٤- سامانه مجموعه ای از نرم افزار و سخت افزار برای ارائه خدمات بانکداری
۱-۵- کاربر تمامی بهره برداران سامانه اعم از درون سازمانی و برون سازمانی
۱-٦- کمیته عالی فناوری اطلاعات کمیته ای است تخصصی ذیل هیئت مدیره مؤسسه اعتباری که به منظور یاری رسانیدن به آنها در امر سیاست گذاری و راهبری حوزه فناوری اطلاعات تشکیل شده در چارچوب حداقل وظایف و اختیارات تعیین شده در این الزامات انجام وظیفه می نماید؛
۱- 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 می نماید؛
فصل دوم - معماری و ساختار سازمانی
ماده ۲ مؤسسه اعتباری موظف است معماری فناوری اطلاعات را بر مبنای توگف بایان و چارچوب ملی
معماری سازمانی ایران و یا ترکیبی از آنها و در حوزه سرویس با رویکرد معماری سرویس گرا طراحی و تدوین نماید.
TOGAF
BIAN SOA
ماده ۳- مؤسسه اعتباری مکلف است طرح جامع فناوری اطلاعات مؤسسه اعتباری را تصویب و در فواصل زمانی مناسب به روزرسانی نماید.
ماده - 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 ۵ مؤسسه اعتباری مکلف است در ساختار سازمانی خود معاونتی را با عنوان معاونت فناوری اطلاعات تحت نظر مستقیم مدیر عامل (پیوست) ایجاد نماید معاون فناوری اطلاعات مؤسسه اعتباری باید واجد حداقل شرایط زیر باشد:
ه-1 - حداقل ۸ سال سابقه کار مرتبط با فناوری اطلاعات در حوزه بانکی
۵-۲- تحصیلات دانشگاهی حداقل کارشناسی ارشد در رشته های مهندسی کامپیوتر مهندسی فناوری اطلاعات علوم کامپیوتر و مدیریت فناوری اطلاعات
احراز صلاحیت توسط مراجع ذی صلاح.
ماده - هیئت مدیره موظف است به منظور انجام صحیح و دقیق وظایف خود در حوزه فناوری اطلاعات کمیته ای 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 سیاست گذاری برنامه ریزی و راهبری سرمایه گذاری 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
نظارت بر اجرای صحیح و به موقع مصوبات هیئت مدیره در حوزه فناوری اطلاعات
۷-٤- ارائه نظر مشورتی در خصوص موضوعات ارجاعی از سوی هیئت مدیره در حوزه فناوری اطلاعات
۷-۵- نظارت بر فرآیند حسابرسی فناوری اطلاعات در مؤسسه اعتباری
۷-٦- نظارت بر فرآیندها و منابع فناوری اطلاعات از منظر توجیه اقتصادی کارایی و اثر بخشی
--- نظارت بر فرآیند مدیریت ریسکهای فناوری اطلاعات در مؤسسه اعتباری
--- نظارت بر حسن اجرای تمامی فرآیندهای امنیت اطلاعات مؤسسه اعتباری
۷-۹ تدوین برنامه های کلان آموزشی و پژوهشی در جهت توسعه فناوری اطلاعات با رویکردهای تخصصی

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 غیر اجرایی هیئت مدیره انتخاب شود و دارای آشنایی کافی با فناوری اطلاعات و عملیات بانکی باشد؛
- تعداد اعضای کمیته عالی فناوری اطلاعات میبایست حداقل ۵ نفر و فرد باشد؛
-- 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؛
---- رئیس هیئت مدیره نمیتواند همزمان به ریاست کمیته عالی فناوری اطلاعات انتخاب شود؛
مدت تصدی مسئولیت اعضای کمیته عالی فناوری اطلاعات با اتمام مدت تصدی مسئولیت اعضای هیئت مدیره پایان می یابد انتصاب مجدد هر یک از اعضاء بلامانع است
--- معاون فناوری اطلاعات مؤسسه اعتباری به عنوان 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 به عمل 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
۹-۲- حسابرسی فناوری اطلاعات حداقل شامل فرآیندها اسناد قراردادها ،معاملات پروژه ها و گزارشهای تهیه شده مربوط به حوزه فناوری اطلاعات مؤسسه اعتباری
۹-۳ ارزیابی دوره ای 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 ۶ ماهه؛
--- ارزیابی میزان تحقق سیاستها و برنامه های مؤسسه اعتباری و مصوبات هیئت مدیره در حوزه فناوری اطلاعات و ارائه گزارش به کمیته عالی فناوری اطلاعات
- ارزیابی فرآیندهای فناوری اطلاعات از منظر توجیه اقتصادی کارایی و اثربخشی
۹-٦- ارزیابی کارآمدی منابع فناوری اطلاعات از قبیل نیروی انسانی تجهیزات و سامانه ها؛
ISACA IT Audit Framework (ITAFT™)
۹-۷- نظارت بر حسابرسی فناوری اطلاعات خارجی برون سپاری شده
۹-۸ دریافت و بررسی پیشنهادها و توصیه های 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 را زیر مجموعه معاونت فناوری اطلاعات به همراه تبیین مسئولیتها و شرح وظایف مطابق با دستورالعملهای کمیته پدافند غیر عامل کشوری تعیین نماید.
فصل سوم خط مشی ها ر سیاست ها و برنامه ها
ماده ۱۱ مؤسسه اعتباری مکلف است خط مشی ها سیاستها و برنامه های حوزه فناوری اطلاعات مشتمل بر برون سپاری امنیت مدیریت شناسایی و تایید مشتریان سامانه جامع بانکداری متمرکز سامانه های بانکداری الکترونیکی مدیریت ریسک شبکه و ارتباطات و مرکز داده را در چارچوب مفاد این الزامات تدوین تصویب و به ارکان ذی ربط ابلاغ نماید.
است طرح کنترل و مدیریت رخدادها و حوادث غیر مترقبه را تهیه و در بازه های زمانی مناسب بازنگری نموده و مورد آزمون قرار دهد. طرح یاد شده باید حداقل دارای ویژگی های زیر باشد
۱۳-۱- امکان کشف سریع منشاء
۱۲-۲- توانایی ارزیابی دامنه رخداد و شدت بالقوه آن
۱۳-۳- امکان گزارش دهی سریع به هیئت مدیره در صورت بروز ریسک شهرت یا زبان مالی
۱۲-٤- امکان اطلاع رسانی مناسب به مشتریان
۱۲-۵- 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 و همچنین دارایی های 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 استفاده نماید.
CIRT (Computer Incident Response Team)
DRP (Disaster Recovery Plan)
IT Service Catalog
ITIL (Information Technology Infrastructure Library)
Ik
لم

ماده ١٤ مؤسسه اعتباری موظف است در تهیه برنامه تداوم کسب و کار حداقل موارد زیر را پوشش داده آنها را در بازه های زمانی مناسب بازنگری نموده و مورد آزمون قرار دهد
١٤-١ خدمات فناوری اطلاعات مؤسسه اعتباری امکان تداوم در شرایط عادی و اضطراری را داشته باشند؛
١٤-٢ خدمات فناوری اطلاعات مؤسسه اعتباری برای مواقع بحرانی و اوج کاری از نظر کارایی مورد آزمون و بهینه سازی قرار گیرند؛
١٤-٣ خدمات فناوری اطلاعات مؤسسه اعتباری از قابلیت مقیاس پذیری برخوردار باشند؛
١٤-٤ امکان دسترسی به خدمات بانکداری الکترونیکی برای مشتریان در تمامی ساعات شبانه روز و هفت روز هفته (٧٢٤) فراهم شود.
ماده ١٥ مؤسسه اعتباری موظف است از میزان وقفه احتمالی که در اثر تغییر به روزرسانی و اصلاح سامانه های بانکداری به وجود میآید تخمین مناسبی داشته باشد. در صورت احتمال بروز هرگونه وقفه در خدمات تأمین شرایط زیر ضروری است
١٥-١ حداقل یک هفته کاری قبل از ایجاد هرگونه وقفه با ذکر دقیق زمان و مدت احتمالی وقفه اطلاع رسانی کافی و شفاف به مشتریان صورت گیرد؛
١٥-٢ تغییرات به گونه ای برنامه ریزی شود که زمان شروع وقفه و حتی المقدور مدت آن در ساعات غیر اداری یا تعطیل باشد؛
١٥- برای ارائه خدمات بانکداری الکترونیکی واحد امداد مشتریان با توان پاسخگویی مناسب راه اندازی شود؛
١٥-٤ روشهای مناسب جبران خسارت ناشی از عدم خدمت رسانی به کاربران به دلیل نقص یا توقف سامانه های خدمات بانکداری الکترونیکی و دیگر ریسکهای ممکن در این حوزه پیاده سازی شود.
ماده ١٦ مؤسسه اعتباری موظف است به منظور ارتقاء دانش و مهارت کارکنان در سطوح مختلف برنامه های آموزشی لازم را به صورت مستمر اجرا نماید.
فصل چهارم - برون سپاری
ماده ١٧ مؤسسه اعتباری موظف است دستورالعمل برون سپاری خدمات فناوری اطلاعات را بر اساس آخرین ویرایش استاندارد ISO ٣٧٥٠٠ تدوین نموده و به تصویب هیئت مدیره برساند. دستور العمل یاد شده باید شامل حداقل موارد زیر باشد
١٧-١ شرح نیازمندی ها
BCP (Business Continuity Plan) Scalability
لم
١٧-٢ جدول و معیار ارزیابی و انتخاب پیمانکار
١٧-٣ طرح توجیهی
١٧-٤- شاخصهای کلیدی عملکرد مرتبط با برون سپاری
١٧-٥- تهیه و نحوه انتشار درخواست پیشنهاد ؛
١٧-٦- نحوه بررسی پاسخ شرکت کنندگان مناقصه
١٧-٧- نحوه ارزیابی شرکت کنندگان
١٧-٨ معیارهای نهایی انتخاب پیمانکار
١٧-٩ موارد مرتبط با تدارکات خرید و قرارداد
١٧-١٠- حدود اختیارات و مسئولیتها در فرآیند برون سپاری
١٧-١١- رویه های نظارت بر روابط برون سپاری
ماده ١٨ مؤسسه اعتباری مجاز به دریافت خدمات فناوری اطلاعات از شرکتها و پیمانکاران برون سازمانی بدون عقد قرارداد نمی باشد.
ماده ١٩ مؤسسه اعتباری موظف است در برون سپاری پروژه های فناوری اطلاعات مفاد ضوابط بالادستی را رعایت نماید.
ماده ٢٠ مؤسسه اعتباری مکلف است قبل از انعقاد هرگونه قرارداد برون سپاری در خصوص هر بخش از خدمات فناوری اطلاعات به شرکتهای داخلی و خارجی نسبت به رعایت حداقل موارد زیر اطمینان حاصل نماید
٢٠ - ١ وجود فرآیند مناسب تصمیم گیری در ارتباط با مدیریت ریسکهای ناشی از برون سپاری
٢٠-٢- احراز هویت کامل شرکت تأمین کننده خدمات و برخورداری شرکت از صلاحیت های عمومی مالی فنی و توانایی ارائه خدمات پشتیبانی و اخذ تأییدیه از مراجع ذیصلاح امنیتی
٢٠-٣ به کارگیری روشهای مناسب و کافی برای بررسی پیشنهادهای اولیه شرکت تامین کننده خدمات فناوری اطلاعات با نظر داشت شاخصهای فنی و عملکردی و معیارهای لازم جهت انتخاب صحیح آنها
٢٠- برخورداری از منابع تخصص و فرآیند کاری لازم برای نظارت موثر بر رعایت مفاد قراردادهای برون سپاری
٢٠-٥- اخذ تاییدیه از معاونت نظارت بانک مرکزی مبنی بر عدم وجود منع مقرراتی در خصوص انعقاد قرارداد برون سپاری با شرکت تأمین کننده خدمات فناوری اطلاعات
(Request for Proposal (RFP
ماده ٢١ مؤسسه اعتباری موظف است برای تمامی فرآیندهای برون سپاری حوزه فناوری اطلاعات سند توافقنامه سطح خدمات داشته باشد. بدین منظور استفاده از آخرین ویرایش چارچوب ITIL پیشنهاد می شود.
ماده ٢٢ مؤسسه اعتباری مکلف است اطمینان حاصل نماید که روشهای حفظ اطلاعات مشتریان توسط تأمین کنندگان 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 داده ها و جلوگیری از افشاء هر نوع اطلاعات مرتبط پیش از واگذاری خدمات و پروژه ها به شرکت تأمین کننده خدمات اخذ نماید.
ماده ۲۴ مؤسسه اعتباری مکلف است در تمامی قراردادها با شرکت تامین کننده 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 برون سپاری حداقل موارد زیر را لحاظ نماید
۲۵-۱ ضرورت انطباق سامانه ها و خدمات فناوری اطلاعات مؤسسه اعتباری با ضوابط بانک مرکزی در حداقل زمان ممکن
۲۵-۲ ممنوعیت واگذاری تمام بخشی از خدمات فناوری اطلاعات عهده شرکت تامین کننده خدمات به اشخاص ثالث؛
۲۵-۳- لزوم تصریح مالکیت مؤسسه اعتباری بر داده های ذخیره شده در پایگاه های داده
۲۵٤ تعیین مسئولیتها و تعهدات طرفین قرارداد در خصوص بروز هرگونه وقفه و یا اختلال در ارائه خدمات و دسترسی غیر مجاز به اطلاعات و حساب مشتریان و لزوم اطلاع رسانی سریع به ذینفعان توسط شرکت تأمین کننده خدمات
۲۵-۵ درج تمامی خدمات درخواستی فعالیتها به همراه نمودار روند و فرآیند انجام آن برنامه زمان بندی و حداقل سطح خدمت رسانی خدمات فناوری اطلاعات به طور شفاف
۲۵-٦- پیش بینی مسئولیتهای تأمین کنندگان خدمات متناسب با نیاز مؤسسه اعتباری با نظر داشت محرمانگی داده ها و مستندات تبیین و خسارات احتمالی به شکل دقیق
۲۵-۷- تعیین شرایط پوشش احتیاطی و حقوق مؤسسه اعتباری در بازیابی داده ها بعد از انقضاء یا خاتمه قرار داد؛
۲۵-۸ تعیین حدود نظارت مؤسسه اعتباری بر عملکرد شرکت تأمین کننده خدمات در چارچوب موضوع قرارداد منعقده و شرایط فسخ قرارداد؛
SLA (Service Level Agreement).
۲۵-۹- تعیین و درج جریمه و یا وجه التزام مشخص در صورت تخطی شرکت تأمین کننده خدمات از شرایط قرارداد فرار از مسئولیت و یا عدم انجام تعهدات
۲۵-۱۰ امکان انجام بازرسی توسط معاونت نظارت بانک مرکزی در مواقع لزوم از شرکت تأمین کننده 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 تامین کننده خدمات فناوری اطلاعات از ضوابط ابلاغی بانک مرکزی تمدید یا انعقاد مجدد قرارداد مؤسسه اعتباری با شرکت مزبور ممنوع می باشد.
پنجم - امنیت
ماده ۲۸ مؤسسه اعتباری مکلف است نظام مدیریت امنیت اطلاعات را پیاده سازی نموده و گزارشهای لازم را به صورت دوره ای به کمیته عالی فناوری اطلاعات ارائه دهد.
ماده ۲۹ مؤسسه اعتباری موظف است استاندارد مرجع ISO ۲۷۰۰۱ را پیاده سازی نموده و مستندات و مدارک معتبر در این زمینه اخذ نماید.
ماده ۳۰ مؤسسه اعتباری مکلف است به منظور دریافت خدمات مشاوره ای پیاده سازی 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 ذی صلاح امنیتی در فرآیند عقد قرارداد الزامی است.
ماده ۳۱ مؤسسه اعتباری موظف است به منظور ارتقاء سطح امنیت در حوزه پرداخت از استاندارد PCIDSS 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:
۳۳-۱- تصویب و ابلاغ سیاستها و فرآیندهای مدیریت امنیت اطلاعات مشتمل بر رویه ها و دستورالعملهای مدون و مکتوب در مورد سطوح دسترسی افراد به داده ها و اطلاعات عملیات بانکی میزان مخاطره مرتبط با داده ها و نحوه مدیریت این مخاطرات و ارزیابی و بازنگری آنها به صورت ادواری
Payment Card Industry Data Security Standard
۳۳-۲- تبیین و تفکیک مسئولیتهای مدیریت و کارکنان و کنترلهای آنها بر اساس سیاستهای امنیتی مؤسسه اعتباری
۳۳-۳ ارزیابی و بازنگری منظم و مستمر معیارها و کنترلهای امنیتی
۳۳٤ تصویب رویه ها و دستورالعملهای مربوط به شناسایی نیازهای مرتبط با اطلاع رسانی 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
۳۵-۱ اصل کنترل دو نفره (دوگانه در فرآیند تراکنشهای مالی توسط کارکنان مؤسسه اعتباری و تأمین کنندگان خدمات
۳۵-۲- تفکیک وظایف بین مسئول ورود داده ها و اطلاعات و مسئول بررسی و تأیید صحت آنها
۳۵-۳ تفکیک وظایف مسئولین طراحی و پیاده سازی از راهبری سامانه های بانکداری الکترونیکی
۳۵-٤- 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 غیر مجاز به

تجهیزات کامپیوتری و شبکه های ارتباطی تدابیر مناسب اتخاذ نماید. این تدابیر حداقل شامل موارد زیر باشد:
۳۶-۱- ایجاد حفاظ مناسب برای دربها راه اندازی تجهیزات ثبت و کنترل تردد افراد مانند دربهای کنترل شده با کارت اثر انگشت یا سایر روشهای احراز هویت و یا در صورت لزوم راه اندازی نگهبانی به منظور ثبت ورود و خروج دستی
۳۶-۲- ایجاد مکانهای امن برای حفاظت سامانه ها و منابع آن با رعایت کمترین حساسیت برای بازدید کنندگان
۳۶-۳- اطلاع کارکنان مؤسسه اعتباری از وجود و جزئیات اماکن موضوع بند قبل صرفاً بر اساس درجه نیاز آنها به این اطلاعات
۳۶-٤- فرایندی به منظور مدیریت ورود خروج و امحای تجهیزات و اطلاعات طراحی و پیاده سازی شود؛
۳۶-۵- نصب و آزمون سیستمهای مناسب کنترلی تشخیص و اعلام نفوذ در محل به گونه ای صورت پذیرد که تمامی دربهای نفوذ به داخل داکت ها و کانالهای هواساز مجاری موجود در کف یا سقف کاذب یا تونلهای دسترسی به سایت و نظایر آن از حیث نفوذ، محافظت گردد؛

۳۶-٦- ساختمانها کانالهای فاضلاب و سایر مجراهای طبیعی یا شهری که پتانسیل امکان نفوذ به سایت امن را فراهم می آورد باید از حیث نفوذ مورد بررسی قرار گیرد؛
۳۶-۷ دسترسی ها اعم از موفق و ناموفق جهت ورود به سایت امن باید به طور فیزیکی یا الکترونیکی ثبت شده و در مکان امن با رعایت طبقه بندی نگهداری گردد؛
۳۶-۸ تمامی نقاط حساس از جمله درب ورودی سایت باید از طریق دوربین مداربسته توسط واحدهای ذی ربط مانند اداره انتظامات حراست کنترل شود؛
۳۶-۹- محافظت فیزیکی از دسترسی به کابلها جعبه های تقسیم و داکتهای انتقال کابل به شکل مناسبی انجام شود.
ماده ۳۷ مؤسسه اعتباری مکلف است سازوکار لازم برای امن سازی شبکه داخلی و ارتباطات برون سازمانی از طریق شبکه های عمومی مانند اینترنت را پیاده نماید.
ماده ۳۸ مؤسسه اعتباری موظف است ارتباطات میان دستگاههای مدیریت شبکه و تجهیزات آن مانند مسیریابها و دیواره های آتش برای حفاظت جریان داده ها را رمزگذاری نماید.
ماده ۳۹ مؤسسه اعتباری مکلف است دسترسی به داده ها منابع و یا خدمات برای تمامی پایانه های شبکه داخلی را صرفا بر اساس سیاستها و طرح کنترل سطوح دسترسی کارکنان تعیین نماید.
ماده ٤۰ مؤسسه اعتباری موظف است ترتیبی اتخاذ نماید تا پایانه های متصل به شبکه پس از گذشت زمان مشخصی از عدم استفاده توسط کاربران به صورت خودکار از شبکه قطع و غیر فعال گردد و برای اتصال دوباره کاربران ملزم به انجام عملیات احراز هویت مجدد باشند.
ماده ٤۱ 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 مجاز سازی و کنترل دسترسی باید در اولویت باشد.
ماده ٤۲ مؤسسه اعتباری موظف است اتصال هرگونه تجهیزات شبکه ای بیرونی مانند WiMAX و مودم های اینترنتی که ارتباط به زیر ساخت شبکه ای دیگر علی الخصوص ارتباط اینترنتی را تأمین می کنند به شبکه داخلی غیر ممکن نماید.
ماده ٤۳ مؤسسه اعتباری مکلف است با بهره برداری از ابزارهایی نظیر UTM و دیواره آتش نقل و انتقال اطلاعات شبکه سازمانی را به از بیرون کنترل نظارت و مدیریت نماید.
Router
Firewall.
Authentication
Authorization
Unified Threat Management
ماده ٤٤ مؤسسه اعتباری موظف است ضمن راه اندازی دیواره های آتش بیرونی اقدام به طراحی و استقرار DMZ برای سرویس دهنده ها جهت کنترل و تفکیک جریان داده ها میان شبکه های خارجی داخلی و ارتباطات اینترنتی خود نماید.
ماده ٤۵ مؤسسه اعتباری مکلف است مکانیزمهای دفاعی دیواره های آتش را به صورت دوره ای و با زمان بندی مشخص به روز رسانی نماید توانایی به روزرسانی و بهبود دیواره های 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 فرایند زمان بندی شده اقدام به اجرای آزمون نفوذ به منظور پویش و شناسایی آسیب پذیریهای سامانه های خود نماید و روشهای مقابله با آسیب پذیری ها به شکل مناسبی شناسایی و اعمال گردد.
ماده ٤۷ مؤسسه اعتباری موظف است فرآیندی تعریف نماید که طی آن Log ورود به سامانه ها در ساعات غیر اداری را در ابتدای روز کاری بعد با استفاده از ابزارهای تحلیل Log مورد بررسی و تحلیل قرار دهد.
ماده ٤۸ مؤسسه اعتباری مکلف است داده های حساس و محرمانه به تشخیص مؤسسه اعتباری را با استفاده از الگوریتم های رمزنگاری معتبر رمزگذاری نموده و بر روی پایگاههای داده امن قرار دهد. همچنین از ذخیره داده های محرمانه بر روی سرویس دهنده کاربردی وب خودداری نماید.
ماده ٤۹ مؤسسه اعتباری موظف است ترتیبی اتخاذ نماید که داده های محرمانه بر روی سرویس دهنده پایگاه داده مجزا ذخیره گردد بسته نرم افزاری پایگاه داده های 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 ۵۰ مؤسسه اعتباری مکلف است طراحی سازوکار کنترل دسترسی کاربران به پایگاه داده های مورد استفاده را به ترتیبی انجام دهد که کاربران صرفاً بر اساس سطوح تعریف شده امکان دسترسی به مجموعه مشخصی از اطلاعات جداول

اطلاعاتی خاص را داشته باشند.
ماده ۵۱ مؤسسه اعتباری موظف است هر گونه نرم افزار یا سرویس بدون کاربرد یا اضافی بر روی سرویس دهنده ها را غیر فعال نماید.
۵۲ مؤسسه اعتباری مکلف است به منظور جلوگیری از سوء استفاده های حاصل از ایجاد تغییرات در منابع نرم افزاری پیکربندی و سخت افزاری رویه مدیریت تغییرات را به صورت یکپارچه و قابل پیگرد تدوین و پیاده سازی نماید.
DeMilitarized Zorse
Scan
Change Management
ماده ۵۳ مؤسسه اعتباری موظف است از اطلاعات با اهمیت سرویس دهندگان 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 سرویس دهنده ها چه از لحاظ فیزیکی و چه از لحاظ پیکربندی صرفاً برای افراد مجاز قابل تعریف و اعمال باشد.
ماده ۵۵ مؤسسه اعتباری موظف است ترتیبی اتخاذ نماید که نامهای کاربری پیش فرض برای تمامی تجهیزات کامپیوتری و ارتباطی غیر فعال شده یا به شکل امن تغییر یابد.
ماده ٥٦ مؤسسه اعتباری مکلف است نرم افزارهای 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 ذخیره سازی یا انتقال اطلاعات در سامانه ها 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 پروتکل های خاص و سایر کنترلهای امنیتی استفاده نموده و آنها را به صورت ادواری مورد بازبینی و به روز رسانی قرار دهد.
ماده ۵۹ مؤسسه اعتباری موظف است برای انتقال اطلاعات حساس خصوصاً میان سرویس دهنده ها و تجهیزات مشتریان از روشهای رمزگذاری شناخته شده و معتبر بین المللی به شکل انتها به انتها استفاده نماید.
ماده ٦۰ مؤسسه اعتباری مکلف است به منظور افزایش اثر بخشی 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 ٦۱ مؤسسه اعتباری موظف است به منظور پایش مدیریت و کنترل موثر رخدادهای امنیتی مرکز عملیات امنیت یا حداقل وظایف زیر ایجاد نماید
٦۱-۱- شناسایی مدیریت و پایش لحظه ای آسیب پذیریها تهدیدات و حملات امنیتی به منابع و تجهیزات رایانه ای و ارتباطی در کمترین زمان ممکن به صورت ۷۲٤
٦۱-۲- جمع آوری و آنالیز ترافیک شبکه و تولید گزارشهای امنیتی در سطوح مختلف :
٦۱-۳- ایجاد نقطه تماس متمرکز برای رسیدگی به مشکلات امنیتی ذینفعان
٦۱-٤ پردازش رخدادهای امنیتی و پاسخ دهی به مشکلات مرتبط
End to End
(SOC (Security Operations Center
ماده ٦۲ مؤسسه اعتباری مکلف است ترتیبی اتخاذ نماید که ارزیابی چک لیستهای امنیتی لازم برای تمامی کارکنان و تأمین کنندگان خدمات که به نقاط حساس دسترسی دارند، انجام شود.
ماده ٦۳ مؤسسه اعتباری موظف است برای مدیریت عملیات مالی و ارائه خدمت به مشتریان از نرم افزارهای نسخه اصلی و با مجوز استفاده نماید.
ماده ٦٤ مؤسسه اعتباری مکلف است از نرم افزار و نسخه های معتبر سیستم عامل در سرویس دهنده ها استفاده نماید. ریسک استفاده از نسخه های دستکاری شده سیستم عامل و نرم افزارهای کاربردی بر عهده مؤسسه اعتباری میباشد.
ماده ٦٥ مؤسسه اعتباری موظف است در شبکه داخلی خود فرآیند به روز رسانی و نصب آخرین وصله ها را برای تجهیزات سیستم عاملها و نرم افزارهای کاربردی پیاده سازی نماید.
ماده ٦٦ مؤسسه اعتباری مکلف است توصیه های امنیتی لازم را با توجه به ماهیت خدمات بانکداری الکترونیکی ارائه شده به مشتریان در اختیار آنها قرار دهد. این اطلاع رسانی حداقل باید موارد زیر را در برگیرد
٦٦-۱- انتخاب نام کاربری و گذرواژه مناسب
٦٦-۲- اهمیت حفظ اطلاعات شخصی از جمله شناسه کاربری و گذرواژه
٦٦-۳- استفاده از آنتی ویروسها در هنگام بهره برداری از خدمات بانکداری الکترونیکی
٦٦-٤- اطلاع رسانی در خصوص تارنماها و پستهای الکترونیکی جعلی Phishing و نظایر آن؛
٦٦-٥- عدم استفاده از کامپیوترها و شبکه های عمومی پرخطر برای استفاده از خدمات بانکداری الکترونیکی؛
٦٦-٦- خروج صحیح از صفحات تارنمای سامانه بانکداری الکترونیکی مؤسسه اعتباری
فصل ششم - مدیریت شناسایی و تأیید مشتریان
ماده ٦۷ ارائه هرگونه خدمات بانکداری الکترونیکی به اشخاص حقیقی و حقوقی منوط به رعایت کامل ضوابط شناسایی مشتریان ابلاغی از سوی بانک مرکزی میباشد.
ماده ۶۸ به منظور پذیرش مشتریان غیر حضوری مؤسسه اعتباری باید از اصالت هویت مشتری اطمینان حاصل نماید.
ماده ۶۹ 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 به کار گیرد
۶۹-۱- کلمه عبور شماره شناسایی

Original
Patch
Web Site
لم
۶۹-۲- کارت شناسه فیزیکی الکترونیکی امضاء دیجیتال و توکن امنیتی
۶۹-۳- خصوصیات منحصر به فرد زیستی مانند اثر انگشت و عنبیه چشم؛
۶۹٤ سایر روشهای متناسب با فناوری روز
ماده ۷۰ فهرست تمام کاربران مجاز به دسترسی به سامانه های بانکداری الکترونیکی تعیین شده و دسترسی به هیچ یک از سامانه های مبتنی بر تراکنش و تبادل اطلاعات مالی - هویتی بدون احراز هویت
امکان پذیر نباشد.
ماده ۷۱ تعریف مجوز کاربری حق دسترسی ورود کاربر جدید و تغییر سطح دسترسی به سامانه های 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 بر اساس هویت و شناسه های 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 دسترسی های غیر مجاز کدهای مخرب ویروس و حملات خرابکارانه مقاوم سازی شود.
ماده ۷٤ ضروری است هرگونه تلاش برای نفوذ موفق یا ناموفق در پایگاه داده طی فرآیند بازبینی و آزمون مداوم کشف اصلاح به روز رسانی و مستند شود.
ماده ۷۵ مؤسسه اعتباری موظف است سیاستهای تغییر دوره ای و موردی گذرواژه کاربران و تعیین حداکثر مدت مجاز استفاده از آن را تدوین و اجرا نماید.
ماده ۷۶ روشهای احراز هویت مجازسازی و تأیید اصالت مشتریان از طریق سامانه باید به طور مستمر تحت پایش و بازنگری قرار گرفته به گونه ای که مؤسسه اعتباری نسبت به موارد زیر اطمینان حاصل نماید
۷۶-۱- شیوه های شناسایی و تأیید مشتری در سامانه بانکداری الکترونیکی باید به گونه ای باشد که امکان ورود کاربران غیر مجاز به سامانه با استفاده از هویت مشتریان بانکی را ناممکن سازد؛
۷۶-۲ هنگام کار با سامانه بانکداری الکترونیکی چنانچه کاربر برای مدت معینی از سامانه استفاده ننماید لازم است برای ادامه کار مجددا عملیات احراز هویت انجام شود.
ماده ۷۷ مؤسسه اعتباری موظف است جهت اطلاع رسانی به مشتریان حداقل موارد زیر را در تارنمای خود درج نماید
۷۷-۱ نام نشانی و تلفن دفتر مرکزی مؤسسه اعتباری دفاتر منطقه ای یا نمایندگیها در صورت وجود و واحدهای امداد مشتریان
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 - حفاظتی و مسئولیت های حقوقی طرفین در خصوص استفاده از خدمات بانکداری الکترونیکی
۷۷-۵- مشخص نمودن سطح خدمت رسانی به مشتریان برای هر یک از خدمات بانکداری الکترونیکی
۷۷-۶- توصیه و آموزشهای لازم به مشتریان در خصوص مخاطرات ناشی از ورود عوامل نفوذی، آلودگی ویروسی جعل هویت و موارد مشابه
فصل هفتم - طراحی نگهداری و مدیریت سامانه جامع بانکداری متمرکز
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
۷-٤- مدیریت خزانه داری و صندوق؛
۷۸-۵ مدیریت تحویلداری و پرداخت
۷۸-۶ مدیریت سپرده
۷۸-۷- مدیریت حسابداری و دفتر کل
۷۸-۸- مدیریت اعتبارات و تعهدات
۷۸-۹ مدیریت چک
۷۸-۱۰- مدیریت عملیات ارزی
۷۸-۱۱ مدیریت پشتیبانی اطلاعات و گزارشها
۷۸ - ۱۳ 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 ..
Core Banking Help Desk
۷۸-۱۸- سایر ضوابط و سیستمهای مورد نیاز بر اساس بخشنامه های ابلاغی معاونت نظارت بانک مرکزی
ماده ۷۹ سامانه جامع بانکداری متمرکز باید حداقل دارای ویژگی های فنی زیر باشد
۷۹-۱- ماژولار و یکپارچه باشد؛
۷۹-۲ دارای پایگاه داده مشترک و متمرکز باشد؛
۷۹-۳- مبتنی بر مدیریت فرایندهای کسب و کار باشد؛
۷۹-۴- از کد نویسی امن و امضای دیجیتال استفاده نماید؛
۷۹-۵- پایگاه داده و سرورهای کاربردی به سیستم عامل سکوی نرم افزاری و سخت افزاری خاص وابستگی نداشته باشد؛
۷۹٦- منطبق بر قوانین رمزنگاری باشد به گونه ای که انتخاب الگوریتم رمزنگاری متناسب با کاربرد آن انجام شود؛
۷۹-۷- قابلیت تعریف کدینگهای متفاوت مالی و حسابداری و ثبت هم زمان تراکنشهای مالی در آن وجود داشته باشد به گونه ای که نتایج صحیح را با دقت مورد نیاز فراهم نماید
۷۹-۸- تمامی عملیات سامانه ثبت و مدیریت گردد؛
۷۹-۹- زمان پردازش و توان عملیاتی قابل قبولی داشته باشد؛
۷۹-۱۰- عملیات تعریف شده را در شرایط معین و برای یک دوره زمانی مشخص اجرا نماید؛
۷۹-۱۱ امکان تصحیح خطا در بهترین حالت و کمترین زمان میسر باشد؛
۷۹-۱۲- در صورت بروز خطاهای سخت افزاری و یا نرم افزاری دارای قابلیت تحمل پذیری خطا بوده و افزونگی اجزاء نداشته باشد؛
۷۹-۱۳- امکان ایجاد و اجرای معیارهای آزمون برای بررسی تحقق آنها وجود داشته باشد به گونه ای که قابلیت اجرای انواع آزمون فراهم باش