بانک مرکزی جمهوری اسلامی ایران

حداقل الزامات امنیت اطلاعاتی شرکت‌های صرافی

شناسه سند:	BIS RG 100-14
نسخه سند:	Release 1.0
طبقه‌بندی:	عادی
تعداد صفحات:	۱۴
تاریخ ویرایش:	۱۴۰۲/۰۴/۱۸

فهرست مطالب

۱- مقدمه

صرافی‌ها، شرکت‌هایی هستند که با مجوز بانک مرکزی تأسیس شده و فعالیت ایشان در زمینه خریدوفروش ارز، عملیات مربوط به حواله‌های ارزی از طریق مؤسسات اعتباری و همچنین ارائه خدمات ارزی برون‌مرزی از طریق کارگزاران در چارچوب قوانین و مقررات ارزی توسعه‌یافته است. شرکت‌های صرافی که از سامانه‌های حاکمیتی بانک مرکزی ج.ا.ا (از جمله: پنجره واحد مجوزهای بانکی، سنا و نیما) به‌منظور ثبت اطلاعات معاملات ارزی استفاده می‌کنند، ملزم به تأمین امنیت دارایی‌های متصل به شبکه صرافی هستند؛ لذا، ضروری است الزامات امنیتی در راستای کاهش مخاطرات پردازش، ذخیره‌سازی و انتقال اطلاعات کسب‌وکار صرافی‌ها در بهره‌برداری از سامانه حاکمیتی بانک مرکزی ج.ا.ا تدوین گردد؛ بنابراین، در راستای اجرای وظایف نظارتی بانک مرکزی ج.ا.ا و لزوم رعایت الزامات امنیتی در صرافی‌ها، سند «حداقل الزامات امنیتی شرکت‌های صرافی» که از این پس به اختصار «سند» نامیده می‌شود به شرح ذیل تدوین می‌گردد.

۱-۱- هدف

هدف نهایی مجموعه کنترل‌های این سند، کمک به امن‌سازی محیط داخلی شرکت‌های صرافی و ارتقاء امنیت محیط کاربری خدمات ارائه‌شده از سوی بانک مرکزی ج.ا.ا به شرکت‌های صرافی می‌باشد. بر این اساس، سند حاضر ضمن فراهم آوردن مبنایی برای ممیزی امنیت اطلاعات در تمامی شرکت‌های صرافی، در راستای کاهش مخاطرات مرتبط با موارد ذیل تدوین شده است:

الف) بهره‌برداری امن از سامانه‌های حاکمیتی بانک مرکزی ج.ا.ا شامل و نه محدوده به پنجره واحد مجوزهای بانکی و سامانه‌های سنا و نیما؛

ب) پردازش، ذخیره‌سازی و انتقال اطلاعات موجود در صرافی‌ها؛

ج) استفاده امن از شبکه نورنتا.

۱-۲- دامنهٔ کاربرد

دامنه کاربرد سند حاضر، تمامی شرکت‌های صرافی اعم از سهامی خاص (بانکی) و تضامنی دارای مجوز معتبر از بانک مرکزی ج.ا.ا است.

۱-۳- تعاریف

الف) اطلاعات (حساس) معاملات صرافی: تمامی اقلام اطلاعاتی که برای انجام یک معامله در سامانه سنا توسط شرکت صرافی ثبت می‌گردد و همچنین سایر اقلام اطلاعاتی که منجر به شناسایی اطلاعات طرفین معامله و آسیب به کسب‌وکار صرافی می‌شود که از این پس به اختصار «اطلاعات حساس» نامیده می‌شود.

ب) اماکن حساس: شامل محل‌هایی هستند که دسترسی غیرمجاز به آن‌ها می‌تواند پیامدهای امنیتی و یا کسب-وکاری قابل‌توجهی را برای شرکت صرافی ایجاد نماید.

ج) مدیریت آسیب‌پذیری: شامل اقداماتی به‌منظور شناسایی، ارزیابی و اولویت‌بندی آسیب‌پذیری‌های امنیتی و نیز پیاده‌سازی راه‌کارهایی به‌منظور برطرف‌سازی آسیب‌پذیری‌های شناسایی شده است.

د) شرکت صرافی: شرکتی که با مجوز بانک مرکزی تأسیس شده و موضوع فعالیت آن انجام هر یک از فعالیت‌های خریدوفروش ارز، عملیات مربوط به حواله‌های ارزی از طریق مؤسسات اعتباری و ارائه خدمات ارزی برون‌مرزی از طریق کارگزاران در چارچوب قوانین و مقررات ارزی می‌باشد.

ه) سیستم/سامانه: مجموعه‌ای سخت‌افزاری/نرم‌افزاری مستقل از منابع اطلاعاتی که برای پردازش، نگهداری، استفاده، به اشتراک‌گذاری، انتشار یا توزیع اطلاعات سازمان‌دهی شده است.

و) دارایی: هر آنچه برای شرکت صرافی دارای ارزش اطلاعاتی است. ازجمله دارایی‌ها عبارت‌اند از: اطلاعات، اسناد، کارکنان، اماکن فیزیکی و زیرساخت فناوری اطلاعات (سخت‌افزار، نرم‌افزار و شبکه).

ز) ایستگاه‌های کاری: منظور دستگاه‌های دارای قابلیت پردازش (به‌طورمعمول رایانه همراه یا شخصی) است که برای نگهداری یا به‌کارگیری زیرساخت دسترسی به خدمات بانک مرکزی ج.ا.ا توسط کاربران نهایی یا راهبران سیستم‌ها به کار گرفته می‌شوند. ایستگاه کاری متصدیان می‌تواند با توجه به مقتضیات شرکت صرافی، اختصاصی یا عمومی باشد. در این سند، واژه «ایستگاه‌کاری» بدون ذکر نوع آن، به هر دو نوع ایستگاه کاری اختصاصی (مختص به دریافت خدمات از بانک مرکزی ج.ا.ا) و عمومی (برای انجام امور دیگر کسب‌وکار صرافی) دلالت دارد.

ح) موجودیت‌های متصل به شبکه صرافی: تمامی دارایی‌هایی که به شبکه صرافی متصل شده‌اند. این دارایی‌ها شامل و نه محدود به ایستگاه‌های‌کاری، سرورها (نظیر سرور سیستم حسابداری، سرور اتوماسیون اداری، سرور دامین، فایل سرور و سایر سرورهای داخلی صرافی)، دوربین‌های نظارتی و تجهیزات مرتبط با آن، اماکن فیزیکی، شبکه‌ها، تجهیزات شبکه، برنامه‌های کاربردی، تجهیزات ذخیره‌ساز، کاربران و راهبران است.

ط) مرکز کاشف: مرکزی است برای کنترل امنیت، رصد و پایش فضای سایبری و تبادل اطلاعاتِ نظام بانکی کشور که مسئولیت ایجاد آن بر اساس مصوبه یک هزار و یک‌صد و پنجاه و یکمین جلسه شورای پول و اعتبار مورخ ۱۳۹۱/۰۹/۰۷ بر عهده «بانک مرکزی» نهاده شده است. بر اساس «مادهٔ ۸ مقررات ناظر بر فعالیت مرکز کاشف» شرکت مدیریت امن الکترونیکی «کاشف»، به نمایندگی از بانک مرکزی ج.ا.ا. مسئولیت ایجاد، راهبری و اجرای وظایف محول شده به «مرکز کاشف» را بر عهده دارد.

۲- شرح الزامات شرکت‌های صرافی

۲-۱- فرآیندهای امنیت اطلاعات

۲-۱-۱- خط‌مشی‌ها و روش‌های اجرایی امنیت اطلاعات باید مستند شده و در بازه‌های زمانی منظم مورد بازبینی و به‌روزرسانی قرار گیرد. این خط‌مشی‌ها و روش‌های اجرایی شامل و نه محدود به موارد ذیل است:

أ. امنیت شبکه: حداقل شامل الزاماتی در خصوص سازوکارهای امنیتی مورد نیاز برای حفاظت از شبکه داخلی، گسترده و اینترنت شرکت صرافی و موجودیت‌های شبکه صرافی؛

ب. مدیریت پیکربندی موجودیت‌های شبکه: حداقل شامل الزاماتی جهت پیکربندی امن تجهیزات پردازش، ذخیره‌سازی و انتقال اطلاعات و نیز ابزارهای امنیتی؛

ج. مدیریت تغییرات: حداقل شامل فرایندهای مرتبط با مدیریت تمامی تغییرات اعمال‌شده در تجهیزات پردازش، ذخیره‌سازی و انتقال اطلاعات و نیز ابزارهای امنیتی؛

د. مدیریت آسیب‌پذیری‌ها: حداقل شامل الزامات امنیتی مرتبط با پایش، شناسایی و برطرف سازی آسیب-پذیری‌های امنیتی تجهیزات پردازش، ذخیره‌سازی و انتقال اطلاعات و نیز ابزارهای امنیتی؛

ه. طبقه‌بندی اطلاعات: حداقل شامل الزاماتی جهت طبقه‌بندی و محافظت از اطلاعات معاملات صرافی با توجه به درجه اهمیت آن‌ها؛

و. مقابله با بدافزار: حداقل شامل الزاماتی جهت پیشگیری، شناسایی و مقابله با بدافزارها؛

ز. توسعه و نگهداری امن سامانه‌ها و برنامه کاربردی: حداقل شامل الزاماتی برای امن‌سازی چرخه توسعه سامانه‌های اطلاعاتی؛

ح. مدیریت دسترسی‌ها: حداقل شامل الزاماتی جهت محدود کردن دسترسی کاربران به سامانه‌ها و اطلاعات و نیز احراز هویت امن موجودیت‌های صرافی قبل از ارائه دسترسی؛

ط. مدیریت رمزنگاری: حداقل شامل الزاماتی جهت استفاده از الگوریتم‌های رمزنگاری امن و نیز مدیریت کلیدهای رمزنگاری؛

ی. مدیریت گذرواژه: حداقل شامل الزامات امنیتی برای انتخاب، توزیع و محافظت از گذرواژه‌ها؛

ک. امنیت فیزیکی: حداقل شامل الزاماتی جهت محدودیت و پایش دسترسی فیزیکی به تجهیزات شبکه، سامانه‌ها و اطلاعات موجود در صرافی

ل. مدیریت رویدادنگاری: حداقل شامل الزاماتی جهت پایش، ثبت و حفاظت از رویدادنگاشت‌های مرتبط با تجهیزات پردازش، ذخیره‌سازی و انتقال اطلاعات و نیز ابزارهای امنیتی؛

م. مدیریت مخاطرات دارایی‌های اطلاعاتی صرافی؛

ن. آگاهی‌رسانی و آموزش‌های امنیتی کارکنان و پیمانکاران؛ حداقل شامل الزاماتی در خصوص برنامه‌های آگاهی‌رسانی عمومی و نیز آموزش‌های تخصصی در حوزه امنیت اطلاعات؛

س. بهره‌برداری صحیح از تجهیزات و فناوری‌های کاربر نهایی.

ع. سند محدوده امنیت اطلاعات: حداقل مشخص‌کننده تمامی موجودیت‌های متصل به شبکه صرافی است.

۲-۱-۲- تمامی خط‌مشی‌ها و روش‌های اجرایی مرتبط، باید به ذینفعان داخلی و بیرونی (ازجمله پیمانکاران)، ابلاغ‌شده و از درک درست و آگاهی آن‌ها از الزامات امنیتی اطمینان حاصل شود.

۲-۱-۳- دوره‌های آگاهی‌رسانی عمومی در حوزه امنیت اطلاعات (حداقل شامل معرفی تهدیدات و آسیب‌پذیری‌های مرتبط با شرکت‌های صرافی و مسئولیت‌های افراد در حوزه امنیت اطلاعات) دست‌کم به‌صورت سالیانه، برای کارکنان صرافی برگزار شود.

۲-۱-٤- ضروری است آموزش‌های لازم به تمامی کارکنان در خصوص «آشنایی با روش‌های مهندسی اجتماعی» ارائه شود.

۲-۱-٥- نقش‌ها و مسئولیت‌های امنیت اطلاعات کارکنان/پیمانکاران باید شناسایی‌شده و ضمن ابلاغ رسمی به ایشان، از اینکه در این خصوص توجیه شده‌اند، اطمینان حاصل شود. این نقش‌ها و مسئولیت‌ها باید شامل و نه محدود به موارد زیر باشد:

أ. پیاده‌سازی و نگهداشت کنترل‌های امنیتی؛
ب. پیکربندی امن موجودیت‌های شبکه و بازبینی آن‌ها؛
ج. ارزیابی امنیتی تجهیزات پردازش، ذخیره‌سازی و انتقال اطلاعات و ابزارهای امنیتی؛
د. بازبینی روزانه رویدادنگاشت‌ها[1]؛
ه. رسیدگی به هشدارها و رخدادهای امنیت اطلاعات؛
و. مدیریت تغییرات؛ حداقل شامل مسئولیت‌های مرتبط با درخواست، اطلاع‌رسانی، بررسی و تائید نهایی تغییرات؛
ز. طبقه‌بندی و محافظت از اطلاعات؛
ح. پیاده‌سازی و نگهداشت کنترل‌های مرتبط با مقابله با بدافزار؛
ط. شناسایی الزامات امنیتی توسعه سامانه‌ها؛
ی. مدیریت دسترسی‌ها؛
ک. مدیریت رمزنگاری؛
ل. امنیت فیزیکی؛
م. مدیریت مخاطرات دارایی‌های اطلاعاتی صرافی؛
ن. آگاهی‌رسانی و آموزش‌های امنیتی کارکنان و پیمانکاران؛
س. محافظت از اطلاعات معاملات صرافی.

۲-۱-٦- باید محدوده اجرای الزامات سند حاضر در مستند «محدوده امنیت اطلاعات» به‌طور شفاف تعیین شود. محدوده اجرایی سند حاضر باید حداقل شامل تمامی موجودیت‌های متصل به شبکه صرافی باشد.

۲-۲- مدیریت تغییرات و پشتیبان‌گیری

۲-۲-۱- تمامی تغییرات اعمال‌شده در سامانه‌ها و تجهیزات شرکت صرافی، باید مطابق با روش اجرایی مصوب و مدون «مدیریت تغییرات» تحت کنترل قرار گرفته و به‌طور منظم مورد پایش و بازبینی قرار گیرد. این تغییرات شامل و نه محدود به موارد ذیل است:

أ. پیکربندی تجهیزات پردازش، ذخیره‌سازی و انتقال اطلاعات؛

[1] Log

ب. معماری شبکه ارتباطی؛
ج. پیکربندی ابزارهای امنیتی نظیر دیواره‌های آتش، سامانه پیشگیری و تشخص نفوذ IDS/IPS وWAF؛
د. تغییر در تاریخ و ساعت سیستم‌ها.

۲-۲-۲- در کنترل تغییرات باید حداقل موارد ذیل مورد توجه قرار گیرد:

أ. دلیل و شرح تغییر؛
ب. تأثیرات امنیتی تغییر؛
ج. تائید و مجازشماری تغییر؛
د. رسیدگی به وقفه و بازگشت به وضعیت پایدار.

۲-۲-۳- ضروری است روال اجرایی مناسب برای پشتیبان‌گیری از اطلاعات حساس شرکت صرافی، ایجاد و اجرایی شود. پشتیبان‌گیری از اطلاعات باید شامل و نه محدود به موارد ذیل باشد:

أ. پیکربندی تجهیزات ذخیره‌سازی، پردازش و انتقال اطلاعات؛
ب. پیکربندی ابزارهای امنیتی؛
ج. رویدادنگاشت‌های ثبت‌شده؛
د. اطلاعات حساس موجود در شرکت صرافی؛
ه. پایگاه‌های داده؛
و. زیرساخت مجازی‌سازی؛
ز. کدهای منبع برنامه (در صورت کاربردپذیر بودن).

۲-۲-٤- نسخ پشتیبان باید در بازه‌های زمانی منظم مورد ارزیابی قرار گیرند تا از صحت (یکپارچگی) آن‌ها اطمینان حاصل شود.

۲-۳- مدیریت آسیب‌پذیری

۲-۳-۱- پیاده‌سازی اثربخش خط‌مشی‌ها و روش‌های اجرایی باید هر ۶ ماه یک‌بار از طریق ممیزی داخلی ارزیابی‌شده و اقدامات اصلاحی برای برطرف‌سازی نقاط ضعف موجود تعریف و اجرا شود.

۲-۳-۲- تجهیزات پردازش، ذخیره‌سازی و انتقال اطلاعات و نیز ابزارهای امنیتی باید به‌صورت حداقل ماهانه (از طریق سامانه مدیریت آسیب‌پذیری خودکار مرکز کاشف بانک مرکزی ج.ا.ا) مورد ارزیابی امنیتی قرار گرفته و سوابق این ارزیابی‌ها به‌منظور پیگیری‌های بعدی نگهداری شود.

۲-۳-۳- در صورت توسعه سامانه‌های داخلی، ضروری است سامانه توسعه‌داده‌شده قبل از استفاده در محیط عملیاتی توسط آزمایشگاه مرجع بانک مرکزی ج.ا.ا مورد ارزیابی قرار گرفته و مجوزهای لازم را دریافت نماید.

۲-۳-٤- فهرست اقدامات صورت گرفته برای برطرف سازی آسیب‌پذیری‌های شناسایی‌شده باید ایجاد و سوابق آن‌ها به‌منظور پیگیری‌های بعدی نگهداری شود.

۲-۳-٥- اطلاعات جدیدترین رخدادهای امنیت اطلاعات و نیز آسیب‌پذیری‌های منتشرشده از مراجع معتبر و نیز بانک مرکزی ج.ا.ا احصاء شده و کنترل‌های امنیتی لازم در خصوص آن‌ها در نظر گرفته شود.

۲-۳-٦- فهرستی از دارایی‌ها (شامل و نه محدود به برنامه‌های کاربردی شخص ثالث، برنامه‌های کاربردی توسعه داده شده، سیستم‌عامل‌های مورد استفاده، میان‌افزارها، ابزارهای امنیتی و تجهیزات شبکه و زیرساخت) جهت مدیریت وصله‌ها و آسیب‌پذیری‌ها، ایجاد شده و وصله‌ها/به‌روزرسانی‌های کاربردپذیر، در پنجره‌های زمانی که از قبل تعیین شده است، نصب شود.

۲-۳-۷- وصله‌ها/به‌روزرسانی‌های با سطح حیاتی، حداکثر تا ۱۵ روز پس از انتشار، نصب شود.

۲-٤- امنیت فیزیکی

۲-٤-۱- باید فهرستی از اماکن حساس ایجاد و همواره به‌روز نگه‌داشته شود.

۲-٤-۲- اماکن حساس باید از طریق دوربین‌های نظارتی و با ملاحظات زیر پایش شوند:

أ. داده‌های گردآوری‌شده حداقل به مدت ۳ ماه نگهداری شوند؛
ب. تمامی ورودی/خروجی‌ها به اماکن حساس پوشش داده شود؛
ج. دوربین‌های نظارتی و تجهیزات مرتبط در مقابل دست‌کاری غیرمجاز محافظت شوند؛
د. داده‌های دوربین‌ها باید به‌صورت دوره‌ای بازبینی‌شده و موارد مشکوک رسیدگی شود.

۲-٤-۳- وضعیت امنیت اماکن حساس (نظیر محل نگهداری نسخ پشتیبان) باید حداقل هر ۱۲ ماه یک‌بار بازبینی شوند.

۲-٤-٤- تعمیرات و پشتیبانی سخت‌افزاری و نرم‌افزاری موجودیت‌های درگیر در پردازش، ذخیره‌سازی و انتقال اطلاعات، ابزارهای امنیتی، تجهیزات پشتیبانی‌کننده (نظیر UPS، دیزل ژنراتور، تهویه) و همچنین تجهیزات نظارتی مانند دوربین و دستگاه‌های کنترل تردد، صرفاً باید توسط اشخاص حقیقی یا حقوقی که با ایشان توافق‌نامه رازداری امضاء شده است و به تائید مدیر ارشد شرکت صرافی رسیده است، انجام شود.

۲-٤-٥- دسترسی فیزیکی به اماکن حساس (نظیر محل استقرار تجهیزات شبکه، سامانه‌ها، ایستگاه‌های‌کاری و محل‌های نگهداشت نسخ پشتیبان اطلاعات معاملات صرافی) باید صرفاً از طریق تجهیزات کنترل و پایش تردد، امکان‌پذیر باشد.

۲-٤-٦- اسناد و مدارک غیرالکترونیکی حاوی اطلاعات معاملات صرافی، در صورت عدم نیاز کسب‌وکاری، باید با استفاده از دستگاه خردکن امحاء شوند.

۲-٤-۷- هنگام مشاهده فعالیت‌های مشکوک، موضوع باید بلافاصله به مرکز حراست بانک مرکزی ج.ا.ا گزارش شود.

۲-٤-۸- سوابق ورود و خروج رسانه‌های حاوی اطلاعات حساس از/به صرافی باید ثبت و به مدت حداقل ۱۲ ماه نگهداری شود.

۲-٤-۹- سوابق ورود و خروج افراد به اماکن حساس باید ثبت و به مدت حداقل ۳ ماه نگهداری شود. این سوابق باید شامل و نه محدود به موارد ذیل باشد:

أ. مشخصات هویتی (مراجعین حقیقی) و نام شرکت مرتبط (مراجعین حقوقی)؛
ب. تاریخ و ساعت مراجعه؛
ج. نام پرسنلی که مجوز دهی فیزیکی را انجام داده است؛

۲-۵- امنیت شبکه و ارتباطات

۲-۵-۱- ارائه خدمات صرافی (انجام حواله ارزی- خریدوفروش ارز- خریدوفروش سکه- دریافت اطلاعات متقاضیان) به‌صورت غیرحضوری مجاز نیست. در مواردی که بنا به نیازمندی کسب‌وکاری نیاز به ارائه خدمات غیرحضوری وجود دارد، باید مجوزهای لازم از اداره امنیت اطلاعات بانک مرکزی ج.ا.ا دریافت شود.

۲-۵-۲- پورت‌های فیزیکی موجودیت‌های شبکه باید در برابر دسترسی غیرمجاز (فیزیکی و منطقی) محافظت شوند.

۲-۵-۳- ترافیک ورودی/خروجی شبکه صرافی باید به‌طور مستمر و از طریق ابزارهای امنیتی (حداقل شامل دیواره آتش، WAF، تجهیزات پیشگیری و تشخیص نفوذ IDS/IPS و سامانه ضدبدافزار) کنترل شده و از ورود/خروج ترافیک غیرضروری ممانعت شود.

۲-۵-٤- دسترسی به آدرس‌های IP داخلی و اطلاعات مسیریابی فقط به اشخاص مجاز محدود شود. فهرست این افراد باید مشخص و همواره به‌روز باشد.

۲-۵-۵- شبکه صرافی باید به‌صورت امن، ناحیه بندی شده و ارتباط بین نواحی مختلف، کاملاً محدود شود.

۲-۵-٦- اتصال «موجودیت‌های متصل به شبکه» صرافی، به اینترنت ممنوع است.

۲-۵-۷- کنترل‌های امنیتی لازم باید در تمامی تجهیزات پردازش، ذخیره‌سازی و انتقال اطلاعات متصل به شبکه صرافی شناسایی و به‌طور مستمر فعال باشند و کاربر امکان غیرفعال سازی آن را -مگر در موارد خاص و با اخذ مجوزهای لازم- نداشته باشد.

۲-۵-۸- با استفاده از سامانه ضد بدافزار از تمامی «موجودیت‌های متصل به شبکه صرافی» محافظت شود. سامانه ضد بدافزار باید قادر به شناسایی، حذف و مسدودسازی تمامی بدافزارهای شناخته‌شده باشد.

۲-۵-۹- سامانه ضد بدافزار باید به‌روز بوده و به‌طور خودکار به‌روزرسانی شود.

۲-۵-۱۰- کاربر نهایی نباید قادر به اعمال تغییر یا غیرفعال کردن سامانه ضد بدافزار باشد و در صورت لزوم هرگونه تغییر صرفاً به‌طور موقت، پس از دریافت مجوزهای لازم انجام‌شده و سوابق آن ثبت شود.

۲-۵-۱۱- اتصال گوشی تلفن همراه و انواع رسانه‌های ذخیره‌سازی قابل‌حمل (نظیر هارد اکسترنال، فلش مموری، دیسک نوری) به ایستگاه‌های کاری و سرورها ممنوع است و در صورت لزوم و پس از اخذ مجوزهای لازم، رسانه ذخیره‌ساز باید به یک رایانه جدا از شبکه عملیاتی صرافی متصل شده و توسط ابزار ضد بدافزار مورد پویش قرارگرفته و پس از ایجاد دسترسی موقت، به ایستگاه کاری یا سرورها متصل شود.

۲-۵-۱۲- دسترسی به «موجودیت‌های متصل به شبکه صرافی» از طریق تجهیزات بی‌سیم ممنوع است.

۲-۵-۱۳- هرگونه دسترسی راه دور به «موجودیت‌های متصل به شبکه» صرافی ممنوع است.

۲-۵-۱٤- ضروری است سازوکار[۲] Anti-spoofing برای شناسایی و مسدودسازی آدرس‌های IP با مبدأ جعلی برای دسترسی به شبکه‌های مورداستفاده در صرافی، پیاده‌سازی شود.

۲-۵-۱۵- تمام دسترسی‌های مدیریتی غیرکنسولی و نیز اطلاعات، باید با استفاده از سازوکارهای رمزنگاری قوی (مطابق با خط‌مشی رمزنگاری مدون) در مقابل افشای اطلاعات محافظت شود.

۲-۵-۱۶- در هنگام تبادل اطلاعات در شبکه صرافی ملاحظات ذیل باید در نظر گرفته شود:

أ. فقط از کلیدها و گواهینامه‌های مجاز و معتبر استفاده شود.
ب. از الگوریتم‌های رمزنگاری قوی استفاده شود.

۲-۵-۱۷- در زمان استفاده از هر نوع ابزار تبادل پیام نظیر رایانامه و پیام‌رسان‌های اجتماعی بومی، باید اطلاعات قبل از ارسال، به شیوه امن (مطابق با خط‌مشی رمزنگاری مدون) رمزنگاری شوند.

۲-۵-۱۸- فهرست مخاطرات امنیتی شرکت صرافی باید شناسایی و اقدامات لازم برای برطرف سازی آن‌ها تعریف‌شده و به تائید مدیر ارشد شرکت صرافی برسد.

۲-۵-۱۹- اطلاعات رسانه‌های ذخیره‌سازی درصورتی‌که دیگر نیازی به آن‌ها نباشد، باید به شیوه امن و به‌نحوی‌که قابل بازیابی نباشد، امحاء شود.

۲-۵-۲۰- در هنگام بروز رخدادهای امنیت اطلاعات (نظیر آلودگی به باج افزار)، باید از انجام اقداماتی که می‌تواند رویدادنگاشت‌های پشتیبانی‌کننده از تحلیل‌های بعدی را متأثر نماید (نظیر خاموش/ روشن کردن سیستم‌های آلوده)، اجتناب شده و مراتب در اسرع وقت به مرکز کاشف بانک مرکزی ج.ا.ا گزارش شود.

۲-۵-۲۱- شبکه اینترنت «موجودیت‌های متصل به شبکه» صرافی باید به صورت فیزیکی از سایر شبکه‌ها جداسازی شود.

تبصره: در صورتی که بنابه دلایل کسب‌وکاری امکان جداسازی فیزیکی شبکه اینترنت وجود نداشته باشد، باید ضمن اخذ مجوزهای لازم از بانک مرکزی ج.ا.ا، جداسازی به‌صورت منطقی صورت گرفته و از طریق به‌کارگیری سازوکارهای امنیتی لازم، انتقال اطلاعات بین شبکه‌ها، کاملاً محدود شده و تحت کنترل قرار گیرد.

۲-۶- مدیریت دارایی‌ها

۲-۶-۱- فهرست دارایی‌های اطلاعاتی شرکت صرافی باید تهیه و همواره به‌روزرسانی شود. این فهرست باید حداقل شامل و نه محدود به موارد زیر باشد:

أ. سامانه‌های اطلاعاتی به همراه دارایی‌های پشتیبانی‌کننده از آن‌ها؛
ب. کلیدهای رمزنگاری و گواهینامه‌ها؛
ج. اماکن حساس؛
د. زیرساخت فناوری اطلاعات (شبکه‌ها و تجهیزات شبکه)؛
ه. ابزارهای امنیتی (شامل و نه محدود به دیواره آتش، WAF، IDS/IPS، سامانه ضدبدافزار)؛
و. افراد (کاربران/راهبران)؛
ز. برنامه‌های کاربردی؛
ح. تجهیزات و رسانه‌های ذخیره‌ساز؛

[۲] تکنیکی برای شناسایی و رها کردن بسته‌هایی است که آدرس منبع نادرست دارند.

۲-٦-۲- فهرست تمامی فناوری‌هایی که طول عمر یا دوره پشتیبانی آن‌ها توسط تولیدکننده به اتمام رسیده است (فناوری منسوخ) باید شناسایی و احصاء شود.

۲-٦-۳- فهرست تمامی فناوری‌هایی که امکان پیاده‌سازی الزامات سند حاضر در آن‌ها وجود ندارد باید شناسایی و احصاء شود.

۲-٦-٤- معماری شبکه شرکت صرافی (شامل تمامی اتصالات شبکه داخلی و ارتباط با شبکه نورنتا، اینترنت و سایر شبکه‌ها) باید به‌صورت مستند و به‌روز ایجاد شود.

۲-٦-٥- نمودار جریان گردش داده‌های شبکه داخلی و تبادل اطلاعات با سامانه‌های خارج از شبکه صرافی، تدوین و به‌طور منظم به‌روزرسانی گردد. این نمودار باید حداقل شامل اطلاعات زیر باشد:

أ. تبادلات اطلاعات از طریق سرور ایمیل، سرور VPN، سرور دامین، تجهیزات ذخیره‌ساز و سایر موجودیت‌های پردازش، ذخیره‌سازی و انتقال اطلاعات؛
ب. تمامی اقلام اطلاعاتی محرمانه صرافی و محل انتقال، پردازش و ذخیره‌سازی آن‌ها؛
ج. ارتباط با تمامی نقاط خارج از شرکت صرافی؛
د. تمامی برنامه‌های کاربردی که پردازش اطلاعات را انجام می‌دهند؛
ه. تمامی تجهیزات و سامانه‌های متصل به شبکه صرافی؛
و. تمامی جداسازی‌های فیزیکی و منطقی شبکه.

۲-۷- رویدادنگاری و رسیدگی به رخداد

۲-۷-۱- وقایع موجودیت‌های متصل به شبکه صرافی، شامل و نه محدود به موارد ذیل باید رویدادنگاری شود:

أ. تجهیزات پردازش، ذخیره‌سازی و انتقال اطلاعات؛
ب. ابزارهای امنیتی (شامل و نه محدود به دیواره آتش، WAF، پیشگیری و تشخیص نفوذ IDS/IPS، سامانه ضدبدافزار)؛
ج. سامانه‌ها/سیستم‌های کلیدی (که وقفه در آن‌ها می‌تواند منجر به پیامدهای مهمی برای شرکت صرافی شود)؛

۲-۷-۲- برای شناسایی فعالیت‌های مشکوک، رویدادنگاشت‌ها باید به‌صورت روزانه بررسی‌شده و به فعالیت‌های مشکوک، رسیدگی شود. این حسابرسی‌ها باید شامل و نه محدود به موارد ذیل باشد:

أ. دسترسی کاربران به تجهیزات پردازش، ذخیره‌سازی و انتقال اطلاعات و نیز ابزارهای امنیتی؛
ب. تمامی فعالیت‌های کاربران با هر سطح دسترسی روی موجودیت‌های شبکه صرافی؛
ج. وقایع مرتبط با دسترسی به داده‌های رویدادنگاشت‌ها؛
د. تلاش‌های ناموفق جهت اخذ هر نوع دسترسی؛
ه. وقایع مرتبط با ایجاد، حذف و تغییر مؤلفه‌های احراز هویت (نظیر کلمات عبور و شناسه‌های کاربری)؛
و. وقایع مرتبط با ایجاد/حذف/تغییر حساب‌های کاربری و سطوح دسترسی.

۲-۷-۳- اقلام اطلاعاتی رویدادنگاشت‌ها باید شامل و نه محدود به موارد زیر باشد:

أ. شناسه کاربر؛
ب. نوع رویداد؛

ج. تاریخ و ساعت؛
د. موفقیت/شکست رویداد؛
ه. منشأ رویداد؛
و. نام یا شناسه داده، سیستم، منبع یا خدمت تحت تأثیر رویداد.

۲-۷-٤- توصیه می‌شود به‌منظور تحلیل رویدادنگاشت‌ها، از سازوکارهای خودکار (نظیر سامانه SIEM) استفاده شود.

۲-۷-٥- رویدادنگاشت‌ها باید به مدت حداقل ۱۲ ماه نگهداری شده و داده‌های ۳ ماه اخیر بلادرنگ[۳] در دسترس باشد.

۲-۷-٦- رویدادنگاشت‌ها باید در مقابل تخریب و تغییر غیرمجاز محافظت شوند.

۲-۷-۷- تمامی «موجودیت‌های متصل به شبکه صرافی» و نیز ابزارهای امنیتی معاملات صرافی باید هم‌زمان باشند.

۲-۷-۸- گزارش رخدادهای امنیت اطلاعات باید در اسرع وقت به اداره امنیت اطلاعات بانک مرکزی ج.ا.ا گزارش شود.

۲-۷-۹- ضرورت دارد تمهیدات لازم برای پاسخگویی ۷*۲۴ نماینده امنیت اطلاعات، در خصوص رخدادهای امنیت اطلاعات در نظر گرفته شود.

۲-۷-۱۰- شرکت صرافی موظف است برنامه‌ریزی‌های لازم را برای ارسال رویدادنگاشت‌های امنیتی به مرکز ارائه خدمات امنیتی مدیریت‌شده مرکز کاشف، انجام دهد.

۲-۸- مدیریت پیکربندی

۲-۸-۱- تمامی «موجودیت‌های متصل به شبکه صرافی» و نیز ابزارهای امنیتی باید به‌طور امن پیکربندی شوند. در پیکربندی این تجهیزات باید موارد ذیل موردنظر قرار گیرد:

أ. تمامی آسیب‌پذیری‌های شناخته‌شده برطرف شود؛
ب. با استانداردها و بهروش‌های مقاوم‌سازی و توصیه‌های تولیدکنندگان سازگار باشد؛
ج. به‌محض شناسایی آسیب‌پذیری‌های جدید، پیکربندی‌های دارایی‌های متأثر مورد بازنگری قرار گیرد؛
د. قبل یا به‌محض اتصال موجودیت جدید به شبکه صرافی، الزامات پیکربندی در موجودیت جدید اعمال گردد.

۲-۸-۲- چنانچه بنا بر نیازمندی‌های کسب‌وکاری نیاز به استفاده از خدمت[۴] یا پیکربندی غیر امنی باشد باید:

أ. توجیه کسب‌وکاری موردنظر مستند شده و مورد تائید مدیریت قرار گیرد؛
ب. کنترل‌های امنیتی تکمیلی جهت کاهش مخاطرات استفاده از خدمت یا پیکربندی غیر امن، شناسایی و پیاده‌سازی شود.

[۳] دسترسی به اطلاعات نیازمند صرف زمان جهت دسترسی به آرشیو و استخراج اطلاعات از رسانه‌های ذخیره‌سازی آفلاین مانندTape Drive نباشد.
[4] Service

۲-۸-۳- کارکردها، سرویس‌ها، پورت و پروتکل‌های ضروری هریک از «موجودیت‌های متصل به شبکه» شناسایی و فعال‌شده و سایر کارکردها، سرویس‌ها، پورت و پروتکل‌های غیرضروری مسدود شود.

۲-۸-٤- حداقل الزامات امنیتی موردنیاز برای تمامی خدمات، پروتکل‌ها و پورت‌هایی که در حال استفاده هستند، باید تدوین شود.

۲-۸-٥- هریک از موجودیت‌های ارائه‌دهنده خدمت (سرور) در شبکه صرافی باید یک کارکرد اصلی داشته باشند. به‌طور مثال یک سرور پایگاه داده باید فقط خدمات پایگاه داده ارائه کند و نباید هیچ خدمت دیگری (مانند سرویس میزبانی وب) ارائه نماید.

۲-۸-٦- پیکربندی سازوکارهای امنیتی (نظیر دیواره‌های آتش، سامانه ضد بدافزار، سامانه جلوگیری و تشخیص نفوذ) باید حداقل هر ۶ ماه یک‌بار بازبینی‌شده و سوابق این بازنگری‌ها نگهداری شود.

۲-۸-۷- فایل‌های پیکربندی[۵] سازوکارهای امنیتی (نظیر دیواره‌های آتش، سامانه ضد بدافزار، سامانه جلوگیری و تشخیص نفوذ) باید ضمن حصول اطمینان از سازگاری آن با تجهیزات فعال شبکه، از دسترسی غیرمجاز محافظت شود.

۲-۸-۸- تمامی حساب‌های کاربری پیش‌فرض تجهیزات و سامانه‌ها باید غیرفعال شود.

۲-۹- مدیریت گذرواژه و احراز هویت

۲-۹-۱- سامانه‌هایی که به شبکه صرافی متصل می‌شوند، باید دارای سازوکارهای احراز هویت چندعاملی (حداقل دوعاملی) باشند و هویت کاربران دارای دسترسی کاربری و راهبری، قبل از دسترسی به اطلاعات، به‌طور امن احراز شود.

۲-۹-۲- سازوکار احراز هویت چندعاملی نباید توسط کاربر عادی یا راهبر غیرفعال شود؛ مگر به طور موقت و در موارد خاص که شرایط آن مستند شده و به تائید مدیریت رسیده باشد.

۲-۹-۳- قبل از تغییر عوامل احراز هویت، هویت کاربر باید احراز شده باشد.

۲-۹-٤- تنظیم و بازنشانی کلمات عبور به‌عنوان عامل احراز هویت، باید با توجه به ملاحظات زیر انجام شود:

أ. در اولین تلاش برای ورود، کاربر ملزم به تغییر کلمه عبور پیش‌فرض شود؛
ب. طول کلمات عبور راهبران سامانه‌ها و تجهیزات نباید کمتر از ۱۲ و طول کلمات عبور کاربران نباید کمتر از ۸ کاراکتر نباشد؛
ج. کلمات عبور انتخاب‌شده باید دارای پیچیدگی کافی بوده و شامل حروف کوچک و بزرگ، اعداد و علائم باشد؛
د. چهار کلمه عبور قبلی نباید مجدد استفاده شود؛
ه. کلمات عبور باید حداکثر بعد از ۳۰ روز تغییر کند.

[۵] هر فایل یا تنظیماتی که برای پیکربندی یا همگام‌سازی «کنترل‌های امنیت شبکه» استفاده می‌شود. این شامل فایل‌ها، کنترل‌های خودکار و مبتنی بر سیستم، اسکریپت‌ها، تنظیمات، زیرساخت به‌عنوان کد یا سایر پارامترهایی است که از راه دور پشتیبان‌گیری، بایگانی یا ذخیره می‌شوند.

۲-۹-۵- استفاده از توکن به‌عنوان عامل احراز هویت به‌صورت مشترک، ممنوع است و هر کاربر باید توکن اختصاصی خود را داشته باشد.

۲-۹-٦- ذخیره کلمات عبور به هر شیوه‌ای در سامانه‌ها یا ایستگاه‌های‌کاری به‌صورت متن آشکار ممنوع است و باید از سازوکار مدیریت کلمه عبور و رمزنگاری جهت نگهداری کلمات عبور استفاده کرد.

۲-۱۰- مدیریت دسترسی‌ها

۲-۱۰-۱- دسترسی‌های اعطاء شده به سامانه‌ها و تجهیزات مورداستفاده در شبکه صرافی باید با رعایت ملاحظات زیر مدیریت شود:

أ. مجوزها و سطوح دسترسی با توجه به نیاز کسب‌وکار تعیین شود؛
ب. تعیین دسترسی باید بر اساس «حداقل نیاز به دانستن» و بر مبنای طبقه‌بندی شغلی و وظایف محول شده باشد؛
ج. اعطای دسترسی باید توسط افراد ذیصلاح (مالک سامانه‌ها، تجهیزات و اطلاعات) تائید شود.

۲-۱۰-۲- تمامی دسترسی‌های اعطاء شده (حساب‌های کاربری و سطوح دسترسی افراد) باید با توجه به ملاحظات زیر بازبینی شود:

أ. به‌صورت دوره‌ای و حداقل هر ۶ ماه یک‌بار بازبینی شود؛
ب. از مناسب بودن سطح دسترسی بر مبنای طبقه‌بندی شغلی و وظایف اطمینان حاصل شود؛
ج. دسترسی غیرضروری غیرفعال/حذف شود؛
د. سوابق مجازشماری دسترسی‌های تخصیص‌یافته از طرف نقش‌های ذیصلاح (مالک سامانه‌ها، تجهیزات و اطلاعات) ایجاد و نگهداری شود.

۲-۱۰-۳- قاعده پیش‌فرض اعطای دسترسی در تمامی سامانه‌ها و تجهیزات باید در وضعیت «عدم دسترسی به همه» تنظیم شده باشد.

۲-۱۰-٤- استفاده از حساب‌های کاربری اشتراکی برای دسترسی به سامانه‌ها و اطلاعات معاملات صرافی، برای کارکنان مجاز نیست.

۲-۱۰-۵- برای تمامی حساب‌های کاربری باید «چرخه عمر[٦]» تعریف شود و پس از اتمام طول عمر، نسبت به بازبینی دسترسی اعطاشده و در صورت نیاز غیرفعال سازی آن اقدام شود.

۲-۱۰-٦- تمامی حساب‌های کاربری مربوط به سامانه‌ها و اطلاعات معاملات صرافی که بیش از یک ماه بدون استفاده بوده‌اند باید مورد بررسی قرارگرفته و در صورت عدم نیاز غیرفعال/حذف شوند.

۲-۱۰-۷- اگر نشست کاربر حداکثر به مدت ۱۵ دقیقه آزاد باشد، کاربر باید با احراز هویت مجدد به نشست/ترمینال دسترسی پیدا کند.

[٦] چرخه عمر حساب کاربری فرآیند یکپارچه مدیریت حساب کاربری را تعریف می‌کند. این فرآیندها شامل ایجاد، بازبینی و به‌روزرسانی و غیرفعال حساب‌های کاربری است.

۲-۱۰-۸- حساب‌های کاربری بعد از حداکثر ۳ تلاش ناموفق برای ورود، باید تا زمان تائید راهبر غیرفعال شوند.

۲-۱۱- ملاحظات حراستی

۲-۱۱-۱- نماینده امنیت اطلاعات شرکت صرافی می‌بایست پیش از انتصاب به‌منظور تأیید صلاحیت به اداره حراست فناوری اطلاعات بانک مرکزی معرفی شود.