بانک مرکزی جمهوری اسلامی ایران

بسمه تعالی

وحدت ملت و همزمانی دولت

جناب آقای محمد ابراهیم مقدم نودهی ـ مدیرعامل محترم بانک تجارت
جناب آقای علی صدقی ـ مدیرعامل محترم بانک رفاه کارگران
جناب آقای محمدکاظم چقازردی ـ مدیرعامل محترم بانک سپه
جناب آقای اسماعیل للـه‌گانی ـ مدیرعامل محترم بانک صادرات ایران
جناب آقای مهندس علی‌اشرف افخمی ـ مدیرعامل محترم بانک صنعت و معدن
جناب آقای دکتر مرتضی شهیدزاده ـ مدیرعامل محترم بانک کشاورزی
جناب آقای دکتر محمد هاشم بت‌شکن ـ مدیرعامل محترم بانک مسکن
جناب آقای علی رستگار ـ مدیرعامل محترم بانک ملت
جناب آقای دکتر عبدالناصر همتی ـ مدیرعامل محترم بانک ملی ایران
جناب آقای دکتر جلال رسول‌اف ـ مدیرعامل محترم بانک آینده
جناب آقای حسن معتمدی ـ مدیرعامل محترم بانک اقتصاد نوین
جناب آقای آیت‌اله ابراهیمی ـ مدیرعامل محترم بانک انصار
جناب آقای سید محسن هاشمی ـ مدیرعامل محترم بانک ایران زمین
جناب آقای دکتر مجید قاسمی ـ مدیرعامل محترم بانک پاسارگاد
جناب آقای دکتر کورش پرویزیان ـ مدیرعامل محترم بانک پارسیان
جناب آقای دکتر محمد علی سهمانی‌اصل ـ مدیرعامل محترم بانک توسعه تعاون
جناب آقای دکتر علی صالح‌آبادی ـ مدیرعامل محترم بانک توسعه صادرات ایران
جناب آقای دکتر عباس عسکرزاده ـ مدیرعامل محترم بانک حکمت ایرانیان
جناب آقای دکتر پرویز عقیلی کرمانی ـ مدیرعامل محترم بانک خاورمیانه
جناب آقای دکتر احمد شفیع‌زاده ـ مدیرعامل محترم بانک دی
جناب آقای سید احمد طاهری‌بهبهانی ـ مدیرعامل محترم بانک سامان
مدیرعامل محترم بانک سرمایه
جناب آقای مهندس محمدرضا پیشرو ـ مدیرعامل محترم بانک سینا
جناب آقای دکتر حسین محمدپورزرندی ـ مدیرعامل محترم بانک شهر
مدیرعامل محترم بانک قوامین
مدیرعامل محترم بانک کارآفرین
جناب آقای علی اصغر سفری ـ مدیرعامل محترم بانک گردشگری
جناب آقای محمدحسین حسین‌زاده ـ مدیرعامل محترم بانک قرض‌الحسنه رسالت
مدیرعامل محترم بانک قرض‌الحسنه مهر ایران
جناب آقای داود بنایی ـ مدیرعامل محترم بانک مشترک ایران ـ ونزوئلا
مدیرعامل محترم شرکت دولتی پست بانک
مدیرعامل محترم مؤسسه اعتباری توسعه

باسلام؛

احتراماً، همان‌گونه که استحضار دارند یکی از مباحث مهم در راستای نیل به اهداف درنظر گرفته شده از پیاده‌سازی و اجرای سامانه‌های ملی پرداخت که همواره از اهمیت قابل توجهی برخوردار است؛ امنیت انکارناپذیری، جامعیت و مقابله با مخاطرات عملیاتی احتمالی ناشی از تغییر فرآیندها، اشتباهات انسانی و اتفاقات و خطاهای تکنیکی است.

در همین راستا و به منظور بهره‌مندی از سامانه چکاوک به عنوان سازو کاری توانمند و یکپارچه در عرصه پذیرش و پردازش چک که مهم‌ترین ابزار تعهد آور مالی است؛ بخشنامه حاضر با هدف تعریف و تبیین مخاطرات احتمالی ناشی از عملکرد در سامانه و ارائه راهکار جهت کاهش مخاطرات ذاتی و پیشگیری از تبدیل مخاطرات عملیاتی ناشی از عدم کفایت فرآیندها، روش‌های کنترلی و سیستم‌های داخلی به مخاطرات اعتباری و شهرت برای بانک‌ها و موسسات مالی و اعتباری تدوین گردیده، که در ذیل اهم مخاطرات احتمالی و راهکارهای جلوگیری از بروز آن تشریح می‌گردد:

<u>مخاطرات و راهکارها:</u>

۱- واگذاری چک جعلی و تخلف در ثبت اطلاعات چک واگذار شده

- تاکید بر لزوم رعایت دقت و کنترل اطلاعات توسط متصدیان شعب بانک‌های واگذارنده و عهده در زمان واگذاری و تعیین وضعیت چک‌ها
- پیاده‌سازی کنترل دو مرحله‌ای جهت اجرای فرآیندهای مربوط به واگذاری و تعیین وضعیت چک‌های پر اهمیت

۲- عدم واگذاری چک در چکاوک یا سیستم متمرکز بانکی و مغایرت فی مابین تعیین وضعیت صورت‌پذیرفته در سیستم‌های متمرکز و پاسخ ارائه شده به چکاوک

- تسریع در تهیه ایستگاه‌کاری مختص هر بانک به منظور برقراری اتصال سیستم‌های متمرکز بانکی به سامانه چکاوک
- پیاده‌سازی سازوکار تایید چند مرحله‌ای توسط کاربران در سطوح مختلف به منظور نظارت و کنترل بر عملیات صورت پذیرفته در سیستم‌های متمرکز بانکی و چکاوک

۳- سوء استفاده کاربران ارشد ازامکانات مختص دسترسی آنان در راستای ایجاد شعبه و نام کاربری موقت و حذف مشخصات پس از انجام عملیات غیر مجاز

- ایجاد ساختار سلسه مراتبی جهت تایید عملیات ثبت شده توسط کاربران ارشد
- رویدادنگاری از فعالیت‌های کاربران چکاوک
- استفاده از تصدیق هویت براساس دو فاکتور

۴- افشا نام کاربری و کلمه عبور کاربران و استفاده هم‌زمان از یک نام کاربری توسط متصدیان شعب و ستاد

- پیاده‌سازی فرآیندهای لازم جهت گزینش رمز عبور مناسب
- الزام کاربران به تغییر کلمه عبور در مقاطع زمانی کوتاه مدت
- آموزش صحیح کاربران به منظور پرهیز از انتخاب رمزهای ساده در سطوح مختلف کاربری اعم از ستاد و شعب
- الزام کاربران به استفاده شخصی از نام کاربری و رمز عبور مختص خود و حفاظت از آن‌ها
- استفاده از تصدیق هویت براساس دو فاکتور
- امن‌سازی رایانه‌های کاربران شعبه و پیشگیری از نصب بدافزار

۵- جعل و تحریف چک از طریق تحریف ترافیک شبکه داخلی بانک‌ها توسط حمله‌ی مرد میانی(MITM[1])

- پیکربندی امن تجهیزات شعبه اعم از رایانه‌ها و شبکه بانکی
- ارائه آموزش به کاربران در مورد شواهد حمله‌ی مرد میانی از طریق پیام خطای مربوط به گواهینامه‌ی الکترونیکی
- پایش شبکه جهت رصد حملات مرتبط با این تهدید و اطمینان از عدم تغییر پیکرندی‌های شبکه
- رمزنگاری کانال ارتباط درون بانکی
- تسریع در پیاده‌سازی ایستگاه کاری مختص هر بانک به منظور برقراری ارتباط سیستم‌های متمرکز بانکی و چکاوک

لیکن یکی از مهم‌ترین ساز وکارهای کنترلی، مجموعه تدابیری است که در قالب کنترل‌های داخلی با توجه به ساختار هر بانک تدوین شده و با هدف کسب اطمینان منطقی و معقول از دستیابی به اثربخشی و کارآیی عملیات، قابلیت اعتماد به گزارش‌های تولید شده و پایبندی به قوانین و مقررات جاری، اجرا می‌گردد. لذا انتظار می‌رود هر بانک با توجه به فرآیندهای موجود، اقدام مقتضی جهت اجرای موارد ذیل را صورت دهد:

- تدوین الزامات و خط‌مشی امنیتی در حوزه‌های مختلف از جمله فرآیندهای کاری، نیروی انسانی و شبکه‌های ارتباطی دخیل در سامانه چکاوک
- اطلاع‌رسانی به موقع و برگزاری دوره‌های آموزشی و نظارت بر حسن انجام کار

[1] Man – in – Middle Attack

علاوه بر این با عنایت به لزوم تهیه ایستگاه کاری مختص بانک/موسسه جهت برقراری ارتباط سیستم‌های متمرکز بانکی با سامانه چکاوک به منظور تسهیل در انجام فرآیندهای مربوط به واگذاری و تعیین وضعیت چک‌ها و پوشش برخی از مخاطرات ناشی از عدم تمرکز امور در سیستم‌های متمرکز بانکی و ایستگاه‌کاری، لازم است مقتضیات مکفی به منظور پیاده‌سازی راهکارهای ارائه شده جهت مقابله با رخداد های مخرب در ایستگاه کاری در دست تهیه و یا پیاده‌سازی شده، تعبیه گردد.

همچنین کلیه بانک‌ها و موسسات مالی و اعتباری عضو سامانه موظف خواهند بود برنامه‌ریزی‌های خود را به‌منظور تهیه و آماده‌سازی ایستگاه‌کاری و انجام آزمون‌های لازم به صورت موفق، به گونه‌ای انجام دهند که حداکثر تا تاریخ *۳۱ خرداد ماه سال ۱۳۹۵* ارتباط ایستگاه کاری مختص بانک/موسسه و سامانه چکاوک فراهم گردد. بدیهی است پس از تاریخ یادشده ارائه خدمات از طریق ایستگاه کاری بانک مرکزی ج.ا.ا میسر نخواهد بود.

تصدیق می‌فرمایند الزام به رعایت استانداردها و توصیه‌های امنیتی علاوه بر حفاظت از منافع مشتریان بانکی به حفاظت از حسن شهرت نظام بانکی نیز منتج خواهد شد. لذا خواهشمند است دستور فرمایند رهنمودهای اشاره شده به تمامی واحدهای ذیربط در آن بانک/موسسه ابلاغ و ضمن نظارت موثر برحسن اجرای آن، گزارش پیشرفت کار در زمینه مذکور به این بانک ارسال گردد./م‌ل(۲۶۶۳۹۰۱)

اداره نظام های پرداخت

داود محمدبیگی

۲۶۱۶

رونوشت:

- سرپرست محترم اداره معاملات ریالی ، جهت استحضار و صدور دستور اقدام مقتضی
- شرکت خدمات انفورماتیک ، جناب آقای عرفانیان دانشور، مدیر محترم پروژه‌های بانک مرکزی، جهت اطلاع