تعميم

السادة/ المحترمون

السلام عليكم ورحمة الله وبركاته،

الموضوع: الإجراءات الرقابية والتوعوية لموظفي الفروع وخدمة العملاء في البنوك والمصارف العاملة بالمملكة.

استناداً إلى الصلاحيات المنوطة بالبنك المركزي السعودي بموجب الأنظمة والتعليمات ذات العلاقة، وانطلاقاً من دور البنك المركزي الرقابي والإشرافي في السعي نحو تعزيز الحفاظ على خصوصية عملاء المؤسسات المالية الخاضعة لإشرافها والعاملين فيها، واستمرار تحسين وتعزيز الممارسات السليمة في البنوك والمصارف.

مرافق طيه الإجراءات الرقابية والتوعوية لموظفي الفروع وخدمة العملاء في البنوك والمصارف العاملة بالمملكة، التي تهدف إلى الحد من المخاطر التشغيلية المتعلقة بالتعامل مع الأنظمة البنكية، وضمان تنفيذ العمليات وفقاً للأنظمة والتعليمات والصلاحيات المعتمدة لحماية البنوك والعملاء من التعرض للخسائر.

للإحاطة، والعمل بموجبه قبل نهاية الربع الثالث لعام ٢٠٢١م.

وتقبلوا تحياتي،

فهد بن إبراهيم الشثري
وكيل المحافظ للرقابة

نطاق التوزيع:

- البنوك والمصارف العاملة بالمملكة.

المملكة العربية السعودية
مؤسسة النقد العربي السعودي
المركز الرئيسي - الرياض

تنبيه

تم ارسال مرفقات التعميم عن طريق الإيميل

الإجراءات الرقابية والتوعوية
لموظفي الفروع وخدمة العملاء في البنوك والمصارف
العاملة بالمملكة

أبريل ٢٠٢١م

البنك المركزي السعودي
SAMA
Saudi Central Bank

الفهرس

أولاً: المقدمة ٣

أ. الهدف ٣

ب. النطاق ٣

ثانياً: التعريفات ٣

ثالثاً: الإجراءات الرقابية ٣

رابعاً: الإجراءات التوعوية ٥

خامساً: أحكام عامة ٦

أولاً: المقدمة

أ. الهدف

تهدف هذه الإجراءات إلى وضع الحد الأدنى من الإجراءات الرقابية والتوعوية لموظفي الفروع وخدمة العملاء في البنوك والمصارف العاملة بالمملكة التي يجب الالتزام بها، للحد من المخاطر التشغيلية المتعلقة بالتعامل مع الأنظمة البنكية، وضمان تنفيذ العمليات وفقاً للأنظمة والتعليمات والصلاحيات المعتمدة لحماية البنوك والعملاء من التعرض للخسائر.

ب. النطاق

تُطبّق هذه الإجراءات على البنوك والمصارف العاملة بالمملكة، دون الإخلال بأي أنظمة أو تعليمات أخرى ذات علاقة، على سبيل المثال لا الحصر: الدليل التنظيمي لأمن المعلومات، والدليل التنظيمي لإدارة استمرارية الأعمال.

ثانياً: التعريفات

يُقصد بالألفاظ والعبارات الآتية –أينما وردت في هذه الإجراءات– المعاني الموضّحة أمام كل منها، ما لم يقتضِ السياق خلاف ذلك:

البنك المركزي: البنك المركزي السعودي.

البنوك: البنوك والمصارف العاملة بالمملكة.

الفروع: فروع البنوك والمصارف التجارية العاملة بالمملكة.

الموظفون: موظفو الفروع وخدمة العملاء.

العملاء: عملاء البنوك.

ثالثاً: الإجراءات الرقابية

على البنوك الالتزام بدرجة النضج المطلوبة للدليل التنظيمي لأمن المعلومات، والدليل التنظيمي لإدارة استمرارية الأعمال، مع الأخذ بالاعتبار الآتي:

١. أن تتضمّن السياسة الخاصة بأمن المعلومات الجوانب المتعلقة بأمن المعلومات لأعمال الموظفين، ومراجعتها بشكل دوري، وبحد أدنى الآتي:

أ. صلاحيات الدخول على الأنظمة البنكية، والتحقق من هوية من قام بعملية الدخول.

ب. ربط الصلاحيات على الأنظمة البنكية بالدرجات الوظيفية وتحديد مستوى الصلاحية لكل درجة وظيفية.

ج. إدارة كلمات المرور بما في ذلك الآتي:

١- أن تتكون كلمة المرور من أرقام وأحرف ورموز.

٢- وجوب تغيير كلمة المرور كل ثلاثة أشهر.

٣- في حال قيام الموظفين بإدخال بيانات الدخول الخاصة بالأنظمة البنكية بشكل خاطئ ثلاث مرات متتالية، فيتم تعليق اسم المستخدم ولا يتم استعادته إلا وفق إجراءات معينة حسب سياسة البنك الداخلية.

٤- التأكيد على الموظفين بالمحافظة على حسابات المستخدم أو بيانات الدخول وعدم الإفصاح عنها أو مشاركتها.

د. تقييد الوصول للأجهزة والأنظمة المستخدمة في البنوك وفقاً لأفضل الممارسات المعتمدة في أمن المعلومات، واحتياجات العمل بناءً على مبدأ "Need-to-Know"، على سبيل المثال لا الحصر: إخفاء رصيد العملاء عن الموظفين التي لا تتطلب مهام عملهم معرفة الرصيد.

هـ. تحديد الممارسات والسياسات الأمنية للمحافظة على سرية المعلومات.

و. تحديد الممارسات المصرفية غير الآمنة وغير السليمة.

ز. وضع سيناريوهات لكشف العمليات المشبوهة عند الدخول على الأنظمة.

ح. عدم السماح بنسخ أو مشاركة البيانات أو تثبيت البرامج دون موافقة صاحب الصلاحية.

ط. وضع إجراءات الدخول والإغلاق والحفظ والتأكيد على إغلاق شاشة البيانات في حالة عدم استخدامها.

ي. أن تكون المصادقة وضوابط الدخول مبنية على مخاطر وحساسية الأنظمة والبيانات المراد الوصول إليها.

٢. مراجعة الحد الأدنى من الصلاحيات للدخول على الأنظمة البنكية، وإجراء العمليات، والدخول إلى بيانات الحسابات البنكية، وبشكل دوري، وتوثيق ذلك في سجلات المراجعة الدورية.

٣. إخفاء تواقيع وأرصدة العملاء لجميع الحسابات التي تكون بحالة غير مطالب بها أو متروكة.

٤. مراقبة حسابات الموظفين المخصصة للدخول على الأنظمة البنكية، وحفظ كافة معلومات عمليات الدخول على معلومات الحسابات البنكية بشكل آلي للرجوع لها عند الحاجة ولمدة (٥) سنوات كحد أدنى، على أن تتضمن المعلومات المحفوظة بحد أدنى الآتي:

أ. اسم الموظف والرقم الوظيفي.

ب. عنوان بروتوكول الانترنت "IP Address".

ج. تاريخ ووقت الدخول.

د. الصلاحية.

هـ. المصادقة.

و. الإجراء الذي تم.

٥. وضع كافة الضوابط التقنية والأمنية اللازمة التي تُمكّن من تحديد هوية الموظف الذي يستخدم جهاز الحاسب الآلي أو أي من الأنظمة البنكية بدقة.

٦. تقييد السماح بالدخول على الأنظمة البنكية من خلال أجهزة الحاسب الآلي المتواجدة بالفروع بعد انتهاء ساعات العمل الرسمية، ووضع الضوابط الاحترازية اللازمة عند الحاجة للدخول على الأنظمة البنكية خارج أوقات العمل الرسمية.

٧. التأكد من توفير الخطط والحلول البديلة لضمان استمرارية الأعمال وتمكين الوصول الآمن للأنظمة البنكية.

٨. اتخاذ التدابير اللازمة في حال تبيّن الوصول إلى بيانات العملاء من قبل شخص غير مصرح له.

٩. التأكد من صلاحيات الدخول للموظفين ذوي الامتيازات الإدارية والموظفين الرئيسيين فقط، وقصر وصول الموظف المختص -مثل موظفي تقنية المعلومات والدعم الفني- إلى صيانة الشبكة، دون الوصول للمعلومات السرية للعملاء.

١٠. في حالة عمل صيانة لأنظمة الفرع، يجب التحقق من أن فريق الصيانة الخاصة بالفرع من ضمن الطاقم المدرجة أسمائهم لعمل الصيانة والمرسلة من الإدارة المختصة قبل المباشرة بالأعمال المطلوبة، مع وضع الإجراءات الرقابية الكافية.

رابعاً: الإجراءات التوعوية

على البنوك الالتزام بالآتي:

١. وضع سياسة خاصة بالاستخدام الآمن للأنظمة البنكية، وآلية التعامل مع اسم المستخدم وكلمة المرور للدخول على هذه الأنظمة، وأن يتم مراجعتها بشكل دوري.

٢. توعية الموظفين بضرورة التأكد من عدم مراقبة الغير لهم عند إدخالهم لاسم المستخدم أو كلمة المرور.

٣. تدريب وتأهيل الموظفين بالحد الأدنى من المعلومات المتعلقة بمجال أمن المعلومات.

٤. التوعية الدورية للموظفين بالتعليمات الصادرة عن البنك المركزي والسياسات التي لدى البنوك في شأنها، وخاصة ما يتعلق بسرية المعلومات والبيانات التي تخص حسابات العملاء، والعقوبات المترتبة على مخالفتها من خلال حملات ونشرات توعوية مستمرة وبحد أدنى مرة كل ثلاثة أشهر.

٥. التوعية الدورية للموظفين في مجال أمن المعلومات، ومكافحة الاحتيال المالي من خلال حملات ونشرات توعوية مستمرة وبحد أدنى مرة كل ثلاثة أشهر.
٦. إجراء اختبارات ودراسات استقصائية (Survey) بشكل دوري للموظفين وبحد أدنى مرة كل ستة أشهر للتحقق من كفاءة وفاعلية الإجراءات التوعوية المُشار إليها في البندين رقم (٤) و (٥) أعلاه.
٧. الحصول على إقرار من الموظفين عند مباشرتهم العمل، وبشكل سنوي (ورقياً أو إلكترونياً) بالاطلاع والالتزام بكافة السياسات المتعلقة بالاستخدام الآمن للأنظمة البنكية وآلية التعامل مع اسم المستخدم وكلمة المرور الخاصة بها.

خامساً: أحكام عامة

١. تُقرأ هذه الإجراءات جنباً إلى جنب مع كافة الأنظمة والتعليمات ذات العلاقة.
٢. تُعد هذه الإجراءات حداً أدنى لما يجب اتخاذه من البنوك تجاه تفعيل الجانب الرقابي والتوعوي للموظفين.
٣. يجب مراجعة السياسات والأدلة والإجراءات الحالية وتطويرها وبشكل دوري بما يضمن توافقها مع ما ورد في هذه الإجراءات، والتعليمات ذات العلاقة.
٤. تكليف أحد الإدارات الرقابية (إدارة المراجعة الداخلية أو إدارة الالتزام) بإجراء فحص أو مراجعة بشكل دوري (سنتين كحد أقصى) للتحقق من تطبيق المتطلبات الواردة في هذه الإجراءات.