البنك المركزي المصري
CENTRAL BANK OF EGYPT

القواعد المنظمة لخدمات منظومة الهوية المالية الرقمية للتعرف على عملاء البنوك والتحقق من هوياتهم الكترونيًا

داخل جمهورية مصر العربية

المحتويات:

مقدمة

تهدف هذه القواعد إلى وضع إطار عام لكافة البنوك العاملة في جمهورية مصر العربية والجهات المرخص لها والتي يُمكن أن تنضم إلى منظومة الهوية المالية الرقمية، وكذلك الوكلاء المصرفيون المعتمدون من قبل البنك المركزي المصري وكافة الأطراف المشاركة في تقديم خدمات الهوية المالية الرقمية، وذلك لإتاحة أقصى قدر من المرونة والأمان عند تقديم الخدمات والمنتجات الإلكترونية للأفراد الطبيعيين.

التعريفات

يكون لكل من الكلمات والعبارات التالية المعنى المبين لها أدناه أينما وردت في هذه القواعد وتقتصر التعريفات المذكورة فقط على هذه القواعد:

منظومة الهوية المالية الرقمية	المنصة المعتمدة من البنك المركزي المصري التي تتيح إنشاء هوية مالية رقمية والتعرف على العملاء من الافراد الطبيعيين والتحقق من هوياتهم إلكترونيًا، بهدف الحصول على الخدمات والمنتجات المصرفية المختلفة، واي خدمات اخري يقرها البنك المركزي المصري، بالإضافة إلى تحديث المستندات والبيانات والمعلومات التي تم الحصول عليها بشكل إلكتروني. **ويُشار إليها في هذه القواعد "بالمنظومة المعتمدة".**
الهوية المالية الرقمية	نسخة رقمية من بيانات هوية العميل بناءً على بيانات مستند تحقيق الشخصية والتي تم التحقق منها من خلال المنظومة المعتمدة.
شركة الهوية المالية الرقمية (هوية)	الشركة المسئولة عن إدارة وإتاحة منظومة الهوية المالية الرقمية.
التحقق الإلكتروني من هوية العملاء	التحقق الكترونياً من هوية العملاء وفقاً لمستندات الهوية التي تدعمها المنظومة المعتمدة والواردة ضمن إجراءات التعرف على عملاء البنوك والتحقق من هوياتهم الكترونياً الصادرة عن وحدة مكافحة غسل الأموال وتمويل الإرهاب (على سبيل المثال: بطاقة الرقم القومي/ جواز السفر) والتأكد من أن إنشاء الهوية المالية الرقمية من خلال المنظومة المعتمدة تم من قبل العميل ذاته.
البنك المشترك	البنك المصرح له من البنك المركزي المصري بتقديم خدمات مصرفية والتعرف على عملائه والتحقق من هوياتهم باستخدام المنظومة المعتمدة.
الوكيل المصرفى	كيان قانوني يتم التعاقد معه من قبل البنك وبعد حصول البنك على الموافقات اللازمة من البنك المركزي لتقديم خدمة أو أكثر من الخدمات المصرفية من خلال مركزه الرئيسي، أو أحد فروعه، أو منافذه الثابتة أو المتنقلة، وذلك بموجب عقود قانونية معتمدة من الإدارة القانونية بالبنك وملزمة لكلا الطرفين، على أن تتضمن تلك العقود المعايير المنصوص عليها بهذه التعليمات كحد أدنى. ويكون في نطاق تطبيق هذه التعليمات هو الوكيل المصرفي الذي يتم التعاقد معه للتعرف على العملاء والتحقق من هوياتهم الكترونياً نيابة عن البنوك.
شهادة الهوية المالية الرقمية Digital Financial Identity "DFI" Certificate	شهادة رقمية تصدرها المنظومة المعتمدة وتكون مرتبطة بتطبيق البنك والوكلاء المصرفيين وكذا جهاز الهاتف المحمول الخاص بالعميل والمستخدم في إتمام المعاملات المالية.

التطبيق الإلكتروني للتعرف على العملاء	التطبيقات الإلكترونية المعتمدة من البنك المركزي والمرتبطة بواجهات الربط الفنية مع منظومة الهوية المالية الرقمية، والتي تتيح من خلالها التعرف على العملاء والتحقق من هوياتهم والمصادقة الإلكترونية على المعاملات.
المصادقة الإلكترونية باستخدام منظومة الهوية المالية الرقمية	مجموعة من الوسائل التكنولوجية المستخدمة للتحقق من مصدر رسالة ما والتحقق من هوية أحد المشتركين عند اتصاله بالنظام، والتأكد من أن رسالة التحقق من الهوية لم يتم تعديلها أو استبدالها أثناء انتقالها، وتقوم مقام توقيع العميل.
الرقم التعريفي للهوية المالية الرقمية (Global PIN)	رقم سري مكون من ٦ أرقام يتم إنشائه من قبل العميل أثناء انشاء الهوية المالية الرقمية ويعد من أحد عوامل المصادقة الالكترونية للعميل.
المخاطر الكامنة (Inherent Risk)	مستوى المخاطر دون الأخذ في الاعتبار أي من الضوابط الرقابية أو إجراءات الحد من المخاطر المنفذة من قبل الجهات المرخص لها.
المخاطر المتبقية (Residual Risk)	مستوي المخاطر التي قد تتعرض لها الجهات المرخص لها بعد تنفيذها للضوابط الرقابية أو إجراءات الحد من المخاطر الكامنة.
القوائم السلبية	تشمل قوائم الكيانات الإرهابية والإرهابيين المنظمة بموجب القانون رقم ٨ لسنة ٢٠١٥ وتعديلاته، والقوائم الصادرة عن مجلس الأمن التابع للأمم المتحدة ذات الصلة بالإرهاب وتمويله وتمويل انتشار أسلحة الدمار الشامل.

١- نطاق التطبيق:

١-١ تسري هذه القواعد على كافة البنوك العاملة في جمهورية مصر العربية والجهات المرخص لها التي يمكن انضمامها إلى المنظومة المعتمدة بما في ذلك الوكلاء المصرفيين المصرح لهم من قبل البنك المركزي، وتُعتبر هذه القواعد هي الحد الأدنى اللازم لتقديم الخدمات المختلفة من خلال منظومة الهوية المالية الرقمية مثل: التعرف علي العملاء والتحقق من هوياتهم وتحديثها الكترونياً – المصادقة الإلكترونية على المعاملات البنكية وأوامر الدفع وأوامر التحويل، وقبول الشروط والأحكام الخاصة بها – مشاركة الهوية المالية الرقمية من خلال المنظومة المعتمدة، وعلى كافة البنوك والجهات المرخص لها ألا تكتفى بتطبيق هذه القواعد فقط وأن تتأكد من اتخاذ كافة ما يلزم نحو إدارة المخاطر المرتبطة بتقديم هذا النوع من الخدمات.

١-٢ تسري هذه القواعد -فيما يتعلق بتقديم خدمات الهوية المالية الرقمية- وذلك دون الإخلال بالتعليمات الرقابية الصادرة عن البنك المركزي المصري والمتعلقة بالضوابط الرقابية لمزاولة العمليات المصرفية الإلكترونية وإصدار وسائل دفع الكترونية، وكذلك التعليمات والقواعد الخاصة بمزاولة البنوك للأنشطة المصرفية، وتعليمات إدارة مخاطر التشغيل وفقاً لمقررات بازل، وتلك الخاصة بالحوكمة والرقابة الداخلية للبنوك، بالإضافة إلى الضوابط الرقابية للبنوك بشأن مكافحة غسل الأموال وتمويل الإرهاب، وإجراءات التعرف على عملاء البنوك والتحقق من هوياتهم الكترونياً الصادرة عن وحدة مكافحة غسل الأموال وتمويل الإرهاب، وأي تعليمات أخرى ذات صلة.

٢- إدارة الحوكمة للبنك المشترك

أولا: التزامات ومسئوليات مجلس الإدارة

يتعين أن يتوافر لدى البنك المشترك - بصفته المسئول عن التعرف على عملائه والتحقق من الهوية المالية الرقمية لهم من خلال المنظومة المعتمدة - سياسة معتمدة من مجلس إدارته تختص بإتاحة التعرف على هوية العملاء والتحقق منها الكترونياً باستخدام منظومة الهوية المالية الرقمية، على أن يتم مراجعتها على الأقل مرة سنوياً وتحديثها إذا لزم الأمر، ويجب أن تتضمن تلك السياسة ما يلي كحد أدنى:

١. آلية مناسبة لإدارة مخاطر التعرف على هوية العملاء والتحقق منها الكترونياً واتخاذ ما يلزم لتأمين ومتابعة تنفيذها بما يتفق مع مستوى المخاطر المقبولة والمعتمدة، وإجراءات واضحة للحد من تلك المخاطر، على أن تشمل ما يلي:

أ. الخطوات المتخذة لإنشاء الهوية المالية الرقمية والتصديق على إجراءات التعرف على العملاء والتحقق من هوياتهم الكترونياً.

ب. إجراءات اعتماد المستندات التي يتم الحصول عليها الكترونياً والوثائق الإضافية المطلوبة للتعرف على العملاء والتحقق من هوياتهم الكترونياً.

ج. إجراءات الكشف عن أي معاملات يشوبها الشك أو قد تبدو غير طبيعة مثل: محاولات الاحتيال (Fraud) بما يشمل أنظمة التتبع الخاصة بتلك المحاولات، والتصدي لها.

د. الإطار العام لحوكمة البيانات بما يشمل تصنيفها وفقًا لدرجة حساسيتها.

o. تقييم مخاطر غسل الأموال وتمويل الإرهاب والضوابط المطبقة في هذا الشأن.

و. تقييم مستوي أداء الخدمة وكفاءتها.

٢. المنهجية المتبعة لتحليل المخاطر من جانب البنك وكذا الإجراءات اللازمة للحد منها، مع الأخذ في الاعتبار المخاطر الكامنة (Inherent Risk) والمخاطر المتبقية (Residual Risk) التي تقع ضمن مستويات المخاطر المقبولة.

٣. الأسس اللازمة للتطوير والصيانة المستمرة للبنية التحتية وأنظمة التأمين الخاصة بها، وكذلك أدوات المراقبة والمتابعة المستمرة التي توفر الحماية المناسبة لنظم وبيانات العملاء الذين تم التعرف عليهم والتحقق من هوياتهم الكترونياً ضد أي تهديدات داخلية أو خارجية، وذلك للتأكد من ضمان كفاية وفعالية الإجراءات ذات الصلة، والحفاظ على سرية بيانات العملاء.

٤. تحديد صلاحيات الأشخاص المصرح لهم العمل على أنظمة البنية التحتية وذلك من خلال نظام تحكم مركزي.

٥. توفير الحماية اللازمة لكافة الأنظمة وخوادم النظام وقواعد البيانات والتطبيقات والاتصالات، وأنظمة التأمين الخاصة بالخدمة وبالأخص التأكد من أن جميع البرمجيات والتطبيقات المستخدمة في المعاملات المالية محدثة وتحتوي على أحدث تصحيحات الأمان.

٦. شروط الاستعانة بالوكلاء المصرفيين، بما يشمل معايير اختيارهم والمخاطر المرتبطة بهم والتأكد من وجود أنظمة رقابية عليهم.

٧. تحديد مسئوليات واضحة ومحددة للإشراف على سياسات وإجراءات وأساليب الأمن السيبراني الخاصة بالبنك والوكلاء المصرفيين، والتأكد من المراجعة الدورية لعمليات اختبار البنية التحتية وأنظمة الأمن السيبراني، ومراجعة نتائج تقارير عمليات تقييم مدى نضج وجاهزية الأمن السيبراني، واعداد التقييم الذاتي للأمن السيبراني وذلك بما يتوافق مع الإطار العام للأمن السيبراني الصادر عن البنك المركزي المصري، مع موافاة البنك المركزي بنتائج التقييم الذاتي، كما يتعين التحقق من تلك الإجراءات بواسطة جهة مستقلة، بالإضافة إلى المتابعة المستمرة وبصفة دورية لتطورات وتحديثات أنظمة البنية التحتية والتطبيقات، وأنظمة الأمن السيبراني في هذا المجال.

٨. تحديد الأدوار والمسئوليات لكافة الأطراف المعنية بتطبيق السياسة.

٩. خطة استمرارية الأعمال وتقييم مستوي أداء الخدمة وكفاءتها.

ثانياً: مسئوليات والتزامات الإدارة العليا بالبنك:

١. إعداد وتنفيذ السياسة المعتمدة من مجلس الإدارة والخاصة بإتاحة التعرف على هوية العملاء والتحقق منها الكترونياً باستخدام منظومة الهوية المالية الرقمية الواردة بالبند السابق.

٢. إعداد إجراءات عمل للعملاء الذين تم التعرف عليهم الكترونياً بما يشمل على سبيل المثال وليس الحصر:

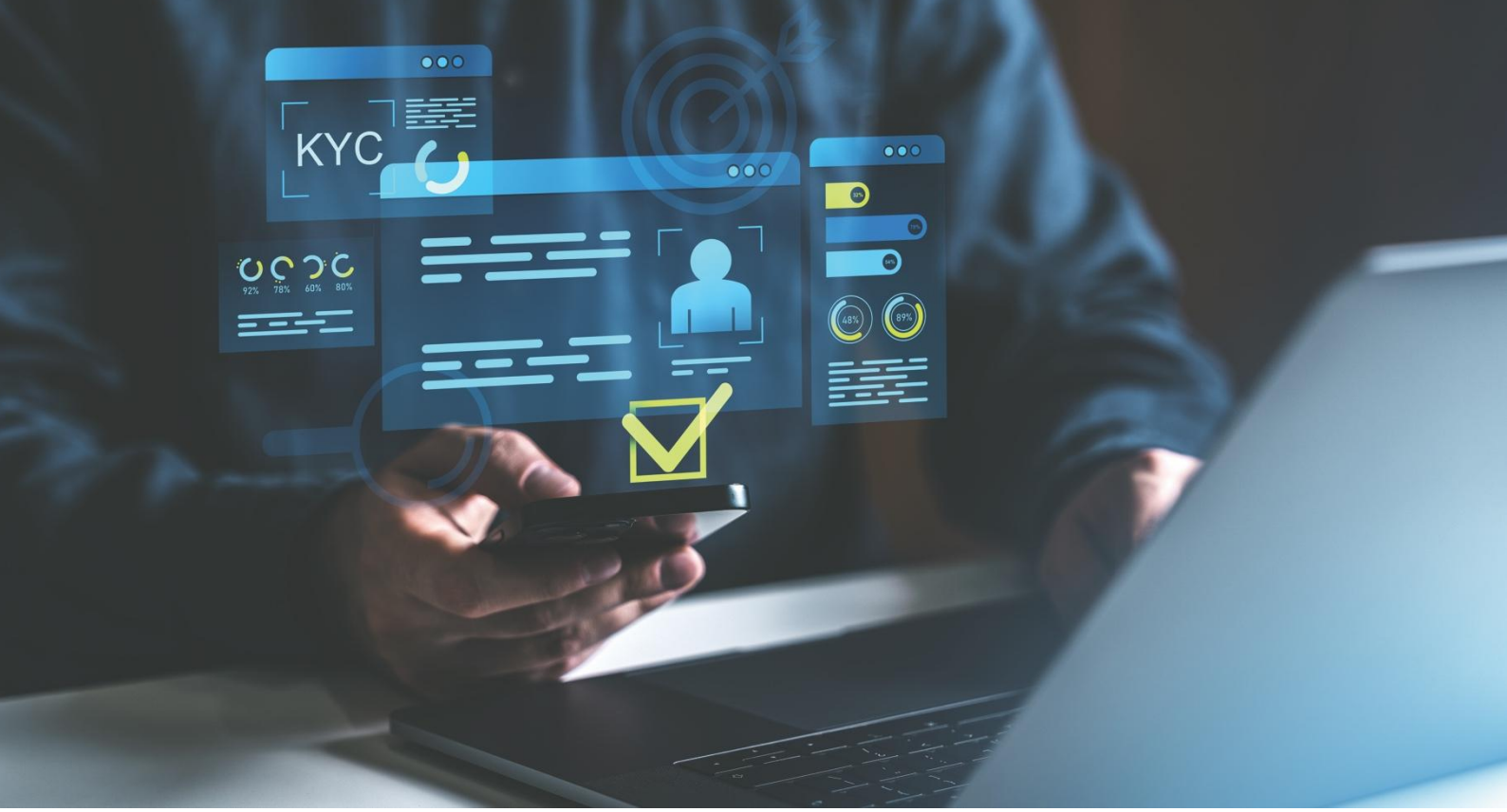
أ. اتاحة إمكانية الحصول على توقيع العميل المعتمد عند زيارته لأي من فروع البنك وفقاً ورغبة العميل.

ب. اتاحة كافة الخدمات للعميل بدون وجود أي تفضيلات او اختلافات بينه وبين العملاء الذين تم التعرف عليهم والتحقق من هوياتهم بشكل تقليدي.

٣. قيام قطاع المراجعة الداخلية بالبنك بالتحقق من كفاية نظم الرقابة الداخلية المتعلقة بالمنظومة المعتمدة ضمن خطة التفتيش وفقاً لدرجة المخاطر.

٤. توفير الموارد البشرية والتقنية اللازمة لاستيفاء متطلبات البنية التحتية التقنية.

٥. إدارة كافة المخاطر المتعلقة بالمنظومة المعتمدة، ورفع تقارير بصفة دورية لمجلس الإدارة.



٣-القواعد المنظمة والتشغيلية لإدارة خدمات الهوية المالية الرقمية:

يجب على جميع أطراف المنظومة المعتمدة الالتزام باعتبارات الأداء وضمان استمرارية العمل، ويتعين الالتزام بما يلي:

٣-١ توفير الخدمات المقدمة على مدار الساعة، مع ضمان أداء الخدمة للعملاء بالسرعة والكفاءة والدقة المناسبة مع إبلاغ العملاء مسبقاً في حال توقف أو تعطل الخدمة.

٣-٢ وضع معايير لتقييم ومتابعة مستوى أداء الخدمات المقدمة، واتخاذ التدابير اللازمة للتأكد من قدرة النظم الداخلية على تقديم الخدمات المختلفة.

٣-٣ التخطيط لضمان استمرارية العمل عند تطوير أي من الخدمات المقدمة، على أن يتم مراعاة ما يلي:

٣-٣-١ في حال حدوث عطل في الخدمة، يجب أن تحتوي خطة استمرارية العمل على خطوات محددة لكيفية استئناف أو استرجاع تلك الخدمات وتحدد هذه الخطوات بناء على أهداف وقت ونقطة الاسترجاع (RTO & RPO) المحددين مسبقاً مع ضرورة دورية المراجعة والتحديث بأي مستجدات أو مخاطر محتملة .

٣-٣-٢ وجود نسخ احتياطية مشفرة ومؤمنة للبيانات منفصلة عن الشبكة (Offline and offsite) لاستعادتها ووجود خطط عمل بديلة للطوارئ.

٣-٣-٣ تضمين خطة استمرارية العمل الخاصة بالخدمات المقدمة القدرة على التعامل مع أي من الحالات التي يتم فيها التعهيد لأطراف خارجية.

٣-٣-٤ القيام بتجارب اختبار خطط استمرارية الاعمال بشكل دوري على ان يتم الاختبار على الأقل مرة سنوياً وفي حالات التعهيد يجب الحصول على تقارير تجارب الاختبار لاستمرارية الاعمال من الجهات التي تم التعهيد اليها.

٣-٣-٥ وجود نسخة احتياطية بخاصية عدم التلاعب او التغير.

٤- مسئوليات والتزامات البنك المشترك

أولا: متطلبات عامة

١. يعتبر البنك هو المسئول الأول عن التحقق من هوية عملائه وذلك من خلال الالتزام بإجراءات التعرف على عملاء البنوك والتحقق من هوياتهم الكترونياً الصادرة عن وحده مكافحة غسل الأموال وتمويل الإرهاب.

٢. إمكانية استخدام البنك للمنظومة المعتمدة لتحديث بيانات العملاء بما يشمل العملاء الذين تم التعرف عليهم بطريقة تقليدية، وذلك وفقاً للضوابط والإجراءات الصادرة في هذا الشأن من قبل البنك المركزي ووحدة مكافحة غسل الأموال وتمويل الإرهاب.

٣. استيفاء موافقة العميل الالكترونية على كافة الشروط والأحكام الخاصة بإجراءات إنشاء الهوية المالية الرقمية الكترونياً أو على استخدامها في حالة إنشائها مسبقاً بمعرفة بنك آخر أو جهة أخرى.

٤. قدرة الأنظمة على التمييز بين العملاء الذي تم التعرف عليهم والتحقق من هوياتهم الكترونياً أو داخل فروع البنك (سواء الكترونياً أو بالصورة التقليدية)، وكذا العملاء الذي تم التعرف عليهم من خلال الوكلاء المصرفيين (سواء الكترونياً أو بالصورة التقليدية).

٥. اعتماد آليات وإجراءات واضحة لمعالجة حالات النزاع (Dispute Management Process) المتعلقة بالخدمة محل هذه القواعد، على أن تحدد هذه الآليات أدوار ومسؤوليات كافة الأطراف المشاركة، ومراحل التعامل مع النزاع، والجداول الزمنية اللازمة لمعالجته.

٦. التأكد من تزامن أنظمته من جانب مسارات التدقيق وسجلات المراجعة مع أنظمة شركة الهوية المالية الرقمية في حالات المصادقة والتأكد من أن كافة الشروط والأحكام التي يوافق عليها العميل تتضمن بند خاص بالتوقيتات الخاصة بالمصادقات من جانب شركة الهوية المالية الرقمية والبنك.

٧. إخطار العميل عند إتمام عملية انشاء الهوية المالية الرقمية - من خلال تطبيقاته الالكترونية - بأكثر من وسيلة.

٨. توفير أدوات الدعم الفني الكاملة للعملاء بما يتناسب مع مستوي أداء الخدمات المصرفية.

٩. تمكين العميل من الحصول على كافة الشروط والأحكام التي قام بالموافقة عليها الكترونياً وتلقيها من خلال البريد الالكتروني المسجل بالبنك أو أي من الوسائل الالكترونية الأخرى.

١٠. الحصول على موافقة مسبقة من البنك المركزي في حال الرغبة في ابرام اتفاقيات تتعلق بإسناد أي مهام تتعلق بالمنظومة المعتمدة أو بالربط الالكتروني معها، وفي حالة قيام البنك بإسناد بعض الخدمات لأطراف خارجية، فإن البنك يظل مسئولًا مسئولية كاملة تجاه مستخدمي النظام وتجاه التزام الأطراف الخارجية بهذه القواعد، والتأكد مما يأتي:

١-١٠ الاحتفاظ بسجل محدث يشتمل على جميع اتفاقات وتعاقدات الإسناد والاستعانة بالأطراف الخارجية.

٢-١٠ وضع حد أقصي لإسناد أكثر من وظيفة إلى مقدم خدمة واحد للحد من مخاطر التركز والتشغيل.

١١. تحديد كافة الاحكام والشروط للعملاء بدقة من خلال تطبيقات التعرف على العملاء والتحقق من هوياتهم الكترونياً مع مراعاة ما يلي كحد ادني:

١-١١ ألا يتم الاشتراك في الخدمة إلا بعد الحصول على موافقة العميل الكترونياً على الشروط والأحكام، بحيث تتضمن توضيح بشكل مُفصَّل الخطوات الواجب على مُستخدم النظام إتباعها لتفعيل الخدمة في حالة الاشتراك لأول مرة أو في حالة وقف الخدمة أو إعادة تشغيلها، موضحاً الوقت اللازم لإيقاف الخدمة من لحظة طلب العميل والطرق المختلفة لطلب إيقافها.

٢-١١ إيضاح كافة التكاليف والمصروفات والرسوم المتعلقة بالخدمة وأي تكلفة إضافية لاستخدام خدمات الإيقاف وإعادة التشغيل ودوريتها.

٣-١١ إيجاد آلية لدراسة الشكاوى ويُنص صراحة في بنود واحكام تقديم الخدمة على طريقة تقديم الشكوى إلى البنك والحد الأقصى للوقت المُستغرق للتحقيق في الشكوى من قِبل الأطراف المختلفة والرد على العميل والآلية المتبعة في حالة رغبة العميل في تصعيد شكواه.

٤-١١ التأكيد على التزام مُستخدم النظام بقراءة التحذيرات والإطارات التنبيهية (مثل التنبيهات الأمنية أو تنبيهات محاولات الاحتيال/الهندسة الاجتماعية Social Engineering.. إلخ) والتأكيد أيضًا على أن قبول مُستخدم النظام لأي تغيير في الشروط والأحكام الذي سيظهر من خلال النظام إلكترونياً والموافقة عليها الكترونياً للاستمرار في الحصول على الخدمة.

٥-١١ توضيح مسئوليات المُستخدم في الحفاظ على الجهاز المقترن بشهادة الهوية المالية الرقمية "DFI Certificate" وإبلاغ البنك في حال فقدانه او اشتباه العميل في ان بياناته السرية قد تم الاطلاع عليها من قبل الغير.

١٢. إجراء مراجعة دورية (على الأقل مرة سنوياً) لمعدلات ودقة عمليات التعرف على هوية العملاء المعهودة لشركة الهوية المالية الرقمية، بما يضمن التوافق مع الحدود الآمنة والمعايير المعتمدة.

١٣. وضع الإجراءات والقواعد المناسبة لإلغاء أو إيقاف شهادة الهوية المالية الرقمية "DFI Certificate" على الفور وفق طلب العميل أو في حال أي حدث آخر قد يعرض بيانات العميل للاستخدام غير المصرح به.

١٤. اتخاذ الإجراءات اللازمة حيال الموظفين لدى الأطراف الخارجية الذين تم إخلاء طرفهم أو تم تغيير مسئولياتهم وإلغاء صلاحياتهم على جميع الأنظمة والأنظمة الخارجية وأنظمة المساعدة (support portals) مع مراجعة الصلاحيات دورياً.

ثانياً: متطلبات التحقق الإلكتروني من الهوية

١. يلتزم البنك المشترك، عند إتمام إجراءات التعرف على هوية العملاء من خلال المنظومة المعتمدة، بالتحقق من هويه العميل إلكترونياً باستخدام وسائل التحقق المتاحة بالمنظومة المعتمدة مثل اختبار السمات البيومترية، ثم يتم استخدام وسائل المصادقة الإلكترونية الخاصة بمنظومة الهوية المالية الرقمية كبديل عن توقيع العميل لقبول الشروط والأحكام الخاصة بالخدمات، وذلك وفقاً للبند الخاص بالمصادقة الالكترونية الوارد لاحقاً.

٢. **<u>في حالة استخدام البنك لتطبيقاته الالكترونية للتعرف على هوية العملاء والتحقق منها الكترونياً، يجب مراعاة الآتي:</u>**

٢-١ التحقق من أن رقم الهاتف المحمول الخاص بالعميل بحوزته بالفعل، وذلك من خلال إرسال رسالة نصية تحتوي على الرقم السري المستخدم لمرة واحدة (OTP).

٢-٢ إنشاء شهادة الهوية المالية الرقمية "DFI Certificate" وربطها على جهاز الهاتف المحمول الخاص بالعميل والتطبيقات الالكترونية بعد إتمام إجراءات التحقق من هوية العميل.

٣. **<u>يلتزم البنك المشترك في حاله إتاحة التعرف على العملاء والتحقق من هوياتهم الكترونياً من خلال الوكلاء المصرفيين المعتمدين التأكد من التزام الوكلاء بما يلي:</u>**

٣-١ اقتصار تدخل الوكلاء المصرفيين على الحالات التي يتعذر على المنظومة المعتمدة معالجتها آلياً، كحالات التشابه الشديد في البيانات أو الملامح البيو مترية، مثل التوائم.

٣-٢ إنشاء الرقم التعريفي للهوية المالية الرقمية الخاص بالعميل من خلال تطبيق الهاتف المحمول الخاص بالبنك المشترك ولا يجوز استخدام الأجهزة الالكترونية الخاصة بالوكيل المصرفي لإنشاء الرقم التعريفي للهوية المالية الرقمية الخاص بالعملاء.

٣-٣ اتخاذ كافة الإجراءات التي تمنع أياً من موظفي الوكلاء المصرفيين أو المتعاملين معهم من استغلال موقعهم أو تعاملهم المباشر مع العملاء للحصول على بياناتهم أو مستنداتهم أو أي معلومات مالية تخصهم خارج نطاق الغرض المصرح به، ويجب أن يصاحب ما سبق تطبيق إجراءات للتوعية والتدريب الإلزامي لموظفي الوكيل المصرفي بشأن سرية البيانات والعقوبات المترتبة على مخالفة ذلك.

٣-٤ تطبيق ضوابط رقابية وتشغيلية على تعامل موظفي الوكلاء المصرفيين مع العملاء، على أن تشمل كحد أدنى ما يلي:

أ. تسجيل ومراقبة كافة المعاملات والإجراءات التي يقوم بها موظفو الوكيل عبر أنظمة معتمدة وقابلة للمراجعة.

ب. منع أي نسخ، أو تصوير، أو تخزين يدوي، أو إلكتروني لبيانات العملاء، أو مستنداتهم خارج المنظومة المعتمدة.

ج. تقييد الوصول إلى بيانات العملاء للموظفين المخولين فقط، وفقًا للصلاحيات المقررة.

د. إخطار البنك فورًا بأي واقعة أو شبهة استغلال أو تسريب لبيانات العملاء، مع اتخاذ الإجراءات التصحيحية اللازمة.

٣-٥ إتاحة إنشاء شهادة الهوية المالية الرقمية (DFI Certificate) وربطها بهاتف العميل وتطبيق البنك بعد التحقق من هوية العميل وذلك من خلال:

أ. مسح رمز الاستجابة السريع المؤمّن (QR Code) باستخدام الهاتف المحمول.
ب. قيام العميل بتعيين الرقم التعريفي للهوية المالية الرقمية (Global PIN) بعد التحقق من العميل الكترونياً.

٣-٦ إجراء عملية التحقق الإضافي من خلال بصمة الإصبع الخاصة بالعميل بما يضمن الفصل الدقيق بين العملاء واستكمال إجراءات التعرف عليهم وفقًا للضوابط المقررة وفي الحالات التي يحددها البنك المركزي.

٤. حال عدم التمكن من التعرف الكترونياً على العميل أو تعذر قراءة بيانات المستندات المدعومة من المنظومة المعتمدة والواردة بإجراءات التعرف على عملاء البنوك والتحقق من هوياتهم الكترونياً، يتم توجيهه إلى فروع البنك المشترك أو إلى الوكلاء المصرفيين لاتخاذ إجراءات إضافية للتحقق من هوية العميل وإنشاء الهوية المالية الرقمية له، وفي هذه الحالة يتعين على البنك استخدام كافة الوسائل المختلفة (مثل: موقع البنك أو مواقع التواصل الاجتماعي الرسمية للبنك) لتوضيح فروعه والوكلاء المتوفر لديهم أجهزة لوحية.

٥. ضرورة القيام بحملات التوعية والتدريب اللازمة لموظفي البنك ولموظفي الوكلاء المصرفيين والمسؤولين عن تشغيل ودعم خدمات التعرف على العملاء والتحقق من هوياتهم الكترونياً، بالإضافة إلى التوعية اللازمة للعملاء عن كيفية التعامل مع تلك الخدمة المقدمة مع ضرورة توضيح المخاطر المرتبطة باستخدام هذه الخدمة وكيفية التعامل معها من خلال المنظومة المعتمدة لرفع مستوى الوعي بالأمن السيبراني وحماية البيانات والخصوصية.

ثالثًا: المصادقة الإلكترونية

يُمكن للبنك الاعتماد على المنظومة المعتمدة في التصديق على المعاملات غير المالية كأحد بدائل التوقيع اليدوي للعميل، وفي حالة رغبة البنك في استخدام المنظومة في التصديق على المعاملات المالية يتم الحصول على موافقة إضافية من البنك المركزي، مع ضرورة الالتزام بكافة الضوابط الخاصة بالمصادقة الالكترونية ومستويات المصادقة المطلوبة والتي تصدر عن البنك المركزي المصري.

رابعًا: ضوابط الأمن السيبراني وحماية البيانات

١. يتعين على البنك المشترك الامتثال للإطار العام للأمن السيبراني الصادر عن البنك المركزي المصري الذي يستند على القواعد والمعايير العالمية المختصة في تأمين وحماية البنية التحتية والأنظمة والتطبيقات وكذلك المعلومات والبيانات الشخصية والحساسة وذلك للوصول الى اقصى قدر ممكن من التأمين ضد هجمات واختراقات الامن السيبراني وتعزيز القدرات البشرية.

٢. يجب أن يتضمن تطبيق الهاتف المحمول الخاص بالبنك المشترك آليات كشف كافية تضمن أن الهاتف المحمول ليس عرضه للمخاطر مثل: (Jailbroken/Rooted) على أن تتضمن إجراءات تأمين التطبيقات، على سبيل المثال لا الحصر:

أ. أن يطلب التطبيق الحد الأدنى من مجموعة الصلاحيات المطلوبة.
ب. حفظ مفاتيح تشفير التطبيق على الأجهزة الذكية بشكل آمن.
ج. أن تكون حزمة التطبيق موقعة رقمياً.

د. استخدام التطبيق لقناة اتصال آمنة مثل استخدام (Certificate/SSL pinning) مع التأكد من أن مفاتيح التشفير مدمجة داخل التطبيق.
ه. ألا يخزن التطبيق أي معلومات على الجهاز تتعلق بمعاملات الدفع أو بيانات العميل بخلاف البيانات اللازمة لعمل التطبيق.
و. ألا يقوم التطبيق بتخزين بيانات تسجيل الدخول وإعادة استخدامها (Back-end Authentication Required).
ز. عدم السماح بتثبيت التطبيقات على أنظمة تشغيل قديمة أو منتهية الصلاحية.

٣. يحظر اتصال أنظمة البنك المشاركة في خدمات المنظومة المعتمدة بالشبكة العالمية (الانترنت) أو أي من الشبكات غير المعتمدة إلا بعد الحصول على موافقة البنك المركزي المصري.

٤. تقع المسؤولية الكاملة لتقديم الخدمات على البنوك المشتركة بالخدمة والتي يجب عليها بذل العناية الواجبة لضمان تأمين كافة المعاملات، وكذا مراقبة كل من الأنظمة المتصلة بالنظام والبنية التحتية بصورة استباقية بشكل دائم على مدار الـ (٢٤) ساعة طوال أيام الأسبوع، وذلك لرصد وتسجيل أي مخالفات أمنية، أو أي اختراقات، أو نقاط ضعف مشتبه بها، وكذلك أي أنشطة غير طبيعية محل اشتباه قد تتم على الأنظمة، وذلك يجب ان يتم من خلال تفعيل مركز عمليات للأمن السيبراني (SOC).

٥. يجب أن يتم مراجعة كافة ما يتم إصداره من سجلات المراجعة (Audit Logs) وإنذارات التأمين اللحظية (Real Time Security Alerts) - مثل إنذارات أنظمة كشف ومنع الاختراق - بواسطة الموظفين أو فرق العمل المعنية وذلك بصفة دورية وفى الوقت المناسب.

٦. تطبيق معايير وإجراءات حصيفة فيما يخص إمكانية الدخول إلى أماكن عمل النظام (Physical Security) بما في ذلك البرامج والأجهزة المُشغِلة للنظام والخوادم والشبكات وأجهزة التشفير ومراكز المعلومات التي تقوم بتشغيل جزء أو أجزاء من النظام.

٧. تلتزم البنوك بتطبيق كافة التعليمات الرقابية الصادرة في شأن الاستجابة لحوادث أمن المعلومات والأمن السيبراني ووضع كافة الإجراءات لمواجهة أي اختراقات أمنية سواء كانت فعلية أو مشتبه فيها، وفي جميع الأحوال ويقع على عاتق البنك التأكد من اتباع الوكلاء المصرفيين تلك الإجراءات علي نحو ما يلي:

٧-١ سرعة اكتشاف مصدر الحدث، وتحديد ما إذا كان قد وقع نتيجة وجود نقاط ضعف في النظم التأمينية بالبنك من عدمه.
٧-٢ تقييم النطاق المحتمل للحدث ومدي تأثيره.
٧-٣ تصعيد الأمر إلى الإدارة العليا واللجان المختصة بالبنك بشكل فوري، إذا كان هذا الحدث قد يضر بسمعة البنك أو قد يؤدى إلى خسائر مالية.
٧-٤ إخطار العملاء المتضررين على الفور.
٧-٥ احتواء الخسائر المتعلقة بأصول البنوك وبياناتها ومدي تأثيرها علي سمعة البنوك، وبوجه خاص الخسائر المتعلقة بعملائها.
٧-٦ جمع كافة الأدلة الجنائية بما فيها الرقمية وحفظها بطريقة مناسبة وباسلوب يضمن الرقابة على تلك الأدلة وضمان عدم التلاعب بها لتغيير محتواها، لتسهيل التحقيقات اللاحقة وإقامة الدعاوى القضائية ضد مخترقي النظام والمشتبه فيهم إذا لزم الأمر، بالإضافة إلى تنفيذ عملية مراجعة لهذا الحدث.

٨. يجب على البنوك والوكلاء المصرفيين الالتزام بما يلي ، كما يقع على عاتق البنك التأكد من إتباع الوكلاء المصرفيين لتلك الإجراءات:

٨-١ استخدام الأساليب المناسبة للحفاظ علي سرية وسلامة المعلومات المتداولة عبر الشبكة الداخلية والخارجية للبنك، وذلك بما يتوافق مع قانون البنك المركزي والجهاز المصرفي وكذا التعليمات الصادرة من جانب البنك المركزي.

٨-٢ اختيار تكنولوجيا التشفير التي تتناسب مع حساسية وأهمية المعلومات وكذا درجة الحماية المطلوبة، وذلك باستخدام طرق التشفير المتعارف عليها دولياً، حيث تخضع نقاط القوة في هذه الطرق لاختبارات شاملة، وينبغي أن تطبق البنوك الممارسات السليمة لإدارة مفاتيح التشفير اللازمة لحماية هذه المفاتيح وكذا التعليمات الصادرة من البنك المركزي المصري.

٨-٣ القيام باختبارات الاختراق (Penetration Testing)، وذلك لإجراء تقييم مفصل ومتعمق للوضع الأمني للنظام من خلال محاكاة للهجمات الفعلية على البيئة الفعلية والاحتياطية، على أن يتم ذلك على الأقل مرة واحدة سنويا، أو عند حدوث تغيير في النظام، على أن تتم مراعاة ما يلي:

٨-٣-١ يجب أن يتم اختبار الاختراق من قبل أحد مقدمي الخدمة الخارجيين المستقلين، حيث يجب عليه أولًا التوقيع على اتفاقية السرية وعدم الإفصاح قبل مزاولة العمل Non-Disclosure Agreement.

٨-٣-٢ يجب أن يكون لدى البنوك والوكلاء المصرفيون تقرير مبدئي عن اختبار الاختراق وخطة المعالجة Penetration Test Report & Remediation Plan، التي تم اصدارها والموقعة من مقدم الخدمة الخارجي.

٨-٣-٣ يجب على البنوك والوكلاء المصرفيين التحقق من صحة معالجة الملاحظات الناتجة عن اختبار الاختراق سواء كان على الأنظمة الرئيسية أو الأنظمة البديلة المستخدمة لمواجهة الكوارث مع مراعاة إجراء اختبار الاختراق على الانظمة في مركز الطوارئ.

٨-٣-٤ يجب إجراء تمارين محاكاة هجوم سيبراني سنويًا بواسطة فريق خارجي (Red Team) لتقييم جاهزية الأنظمة.

٨-٣-٥ يجب على مقدم الخدمة الخارجي إصدار تقرير نهائي موقع منه عن اختبار الاختراق لكي يقوم البنك بتقديمه إلى البنك المركزي، بجانب التقرير المبدئي الأول.

٨-٣-٦ غير مسموح باختيار نفس مقدم الخدمة الخارجي لأداء أكثر من اختباري اختراق متتاليين.

٨-٤ التأكد من وجود مسارات التدقيق (Audit Trails) وسجلات المراقبة والمراجعة (Audit Logs) لكافة العمليات التي تتم عبر الأنظمة والتطبيقات الإلكترونية المختلفة وكذلك البنية التحتية الخاصة بهذه الخدمة، كما يجب ضمان حماية تلك المسارات والسجلات ضد أي تلاعب أو تغيير غير مُصرَّح به، وأن يتم الاحتفاظ بها لمدة زمنية تتوافق مع ما تحدده القوانين والتعليمات الرقابية الصادرة في هذا الشأن، وذلك بهدف تسهيل إجراءات التحقيق في أي عملية احتيال، وحل أي نزاع أو شكوى - إذا لزم الأمر - وعند تحديد ما سيتم الاحتفاظ به في مسارات التدقيق، يمكن الأخذ في الاعتبار الأنواع التالية من الأنشطة وذلك كحد أدنى:

٨-٤-١ عمليات فتح أو تعديل أو إغلاق حساب مستخدم على الأنظمة المختلفة الخاصة بالخدمة.

٨-٤-٢ أي عملية ذات تبعات مالية.

٨-٤-٣ أي تصريح يمنح مستخدم لتجاوز أي من الحدود أو الصلاحيات.

٨-٤-٤ أي تعديل، أو إضافة، أو إلغاء لصلاحيات المستخدمين، أو امتيازات خاصة بالدخول على الأنظمة.

٨-٥ إجراء تقييم دوري لنقاط الضعف (Vulnerability Assessment) كل ثلاثة أشهر على الأقل أو عند حدوث تغييراً جوهرياً في البيئة التشغيلية وبيئة الطوارئ للأنظمة المختلفة الخاصة بالخدمة لاكتشاف نقاط الضعف في بيئة تكنولوجيا المعلومات وتقييمها، ويمكن أن يتولى هذا التقييم جهة مستقلة وأن يكون مقدم خدمة تقييم نقاط الضعف مختلف عن مقدم الخدمة القائم باختبارات الاختراق، أو أن يتولى هذا التقييم إدارة أمن المعلومات بالبنك، وذلك على النحو الآتي:

٨-٥-١ يجب أن يحتوي نطاق تقييم نقاط الضعف على اختبار الثغرات الشائعة في النظام على سبيل المثال لا الحصر: (owasp testing guide) أو باستخدام (NIST Testing Guide).

٨-٥-٢ إعداد خطة لمعالجة المشاكل التي تظهر في تقييم نقاط الضعف، والتأكيد على غلق الثغرات بالخطة خلال وقت متناسب مع تصنيف نقاط الضعف، ثم التحقق من صحة هذه المعالجة عن طريق إعادة الاختبار لإثبات أنه قد تم التعامل بفعالية مع هذه المشاكل بأكملها وفي التوقيت المناسب.

خامسًا: مخاطر الاحتيال الرقمي

١. يتعين على البنوك وضع تدابير فعالة للرقابة المستمرة لضمان سرعة اكتشاف أي أنشطة يشوبها الشك أو قد تبدو غير طبيعية، ومنها على سبيل المثال لا الحصر: إجراء العميل لعدد من المحاولات الفاشلة للتسجيل على المنظومة المعتمدة أو التصديق على المعاملات بشكل خاطئ أكثر من مرة خلال فترة زمنية وجيزة، وخاصة إذا كانت تلك المعاملات تقترب من الحد الأقصى المسموح بالتعامل به، أو تسريب بيانات أو معلومات تحدث من خلال الخدمة يُشتبه في أن تؤدى إلى عمليات احتيال. ويجب على البنك في حالة رصد مثل تلك العمليات التواصل مع العملاء فوراً للتحقق من المعاملات أو الأنشطة على حساباتهم وإخطار الجهات المختصة.

٢. يجب على البنك المشترك تنفيذ نظام مراقبة فعال لتتبع وتسجيل جميع الأنشطة المتعلقة بالهوية المالية الرقمية، على ان يتضمن ذلك تسجيل الوصول ومراقبة العمليات المصرفية والمعاملات المالية للكشف عن أي أنشطة مشبوهة أو غير مشروعة.

٣. يجب أن تتمتع آلية الرقابة المتبعة بالبنك المشترك بالقدرة على سرعة إصدار تحذيرات إلى المختصين بالمتابعة والرصد للخدمات المقدمة عند حدوث أي عمليات محل شبهة احتيال، وكذلك أي أنشطة غير طبيعية، ويجب على البنوك في تلك الحالات أن تبذل العناية الواجبة للتصدي لحالات الاحتيال المحتملة فضلا عن التحقق من ذلك مع أصحاب هذه المعاملات أو الأنشطة في أسرع وقت ممكن واخطار الإدارة المركزية لمكافحة الاحتيال بالبنك المركزي.

٤. يتم الرجوع الى العملاء فور رصد أي معاملة غير طبيعية للتحقق من قيامهم بها.

٥. يجب على البنك تطبيق إجراءات محددة ومُعتمدة للتعامل مع المعاملات غير الطبيعية أو التي قد يشوبها الشك.

٦. يجب الإبلاغ عن حالات الاحتيال ذات الصلة بالخدمات المقدمة من خلال المنظومة المعتمدة على البريد الالكتروني بالعناوين التالية: fraudcombating@cbe.org.eg و eg-fincirt@cbe.org.eg.

٧. يجب على البنوك والوكلاء المصرفيين اجراء تقييم دوري وشامل لمخاطر الاحتيال على مستوي الأنشطة والخدمات التي تقدمها البنوك المشتركة، وذلك مرة واحدة سنوياً بحد أدنى أو عند إضافة خدمة جديدة أو اجراء تحديثات على الأنظمة - ويقع على عاتق البنك التأكد من اتباع الوكلاء المصرفيين لتلك الإجراءات-، على أن يتضمن ذلك ما يلي كحد أدني:

٧-١ تقييم فاعلية الضوابط المطبقة ومدي قدرتها على اكتشاف ومنع والاستجابة لحوادث الاحتيال مع تحديد أوجه القصور والإجراءات التصحيحية اللازمة.

٧-٢ تحليل سيناريوهات الاحتيال على مختلف الخدمات والعمليات وكذا على الوكلاء المصرفيين ومراجعة صلاحيات العاملين المختلفة على النظام.

٧-٣ مراجعة بيانات وخسائر الاحتيال وتحليل أنماطها.

٧-٤ اعداد تقرير ربع سنوي من مسئول مكافحة الاحتيال ورفعه إلى الإدارة المعنية بالبنك المركزي وفقاً للتعليمات الصادرة في هذا الخصوص.

سادسًا: مخاطر التشغيل وضمان استمرارية العمل

١. يجب على البنوك إجراء مراجعة دورية للعمليات والنظم المستخدمة في إدارة خدمات الهوية المالية الرقمية، بما يشمل تقييم الالتزام بالمعايير والسياسات المعمول بها وتحليل الثغرات وتوصيات لتحسين الأداء والأمان.

٢. في حاله خروج أحد البرامج أو الأنظمة من الخدمة يتم التخلص الآمن للبيانات المالية وتدميرها بحيث يستحيل استرجاعها مره اخرى من جميع الخوادم والأنظمة التكنولوجية.

٣. يجب على البنوك إعداد سجل بالأحداث العارضة المرتبطة بالخدمة المقدمة والتفاصيل الخاصة بها، بالإضافة إلى إعداد تقرير دوري يتم عرضه على الإدارة العليا ضمن تقرير مخاطر التشغيل لاتخاذ الإجراءات المناسبة لتلافي تكرارها.

٤. يتولى البنك مسئولية التأكد من إبلاغ البنك المركزي المصري بأي أحداث ومنها أحداث أمن المعلومات والأحداث السيبرانية بصورة صحيحة وبحد أقصى ٦ ساعات من اكتشاف الحادث وبكافة الحالات الواردة أدناه على سبيل المثال لا الحصر:

أ. أي هجمات احتيال لتسريب أو إفشاء هوية مُستخدم النظام أو وثائق اعتماد الشخصية (كالاحتيال Phishing)، وملفات التجسس (حصان طروادة Trojans)، والبرمجيات الخبيثة وبرمجيات الفدية Ransomware Malware.. إلخ).

ب. الدخول غير المصرح به إلى أنظمة تكنولوجيا المعلومات بالبنك لتسريب بيانات مُستخدم النظام المتعلقة بالخدمات المقدمة.

ج. أي عملية تخريبية للبيانات المتعلقة بأنظمة الخدمات المقدمة والتي لا يمكن استرجاعها.

د. الإيقاف التام المتعمد أو العارض للخدمات المقدمة لفترة تزيد عن الفترة المحددة كهدف لوقت الاسترجاع (RTO) المحدد من قبل البنك.

ه. أي حوادث امن معلومات أو هجمات سيبرانية بالبنية التحتية الرقمية الخاصة بالشركة او ذات الصلة بتلك الخدمات الرقمية المقدمة من الشركة على أن يتم إرسال هذه التقارير بالبريد الالكتروني على العناوين التالية: cbe.infosec@cbe.org.eg و eg-fincirt@cbe.org.eg.

و. يجب على البنك الالتزام بتنفيذ جميع التوصيات المرسلة دورياً في التحذيرات الأمنية الصادرة من مركز الاستجابة لطوارئ الحاسب الآلي للقطاع المالي وكذلك الالتزام بإرسال الردود وتحديثها بصورة شهرية (الأسبوع الأول من كل شهر) على البريد الإلكتروني التالي: csrat@cbe.org.eg

٥. يجب على البنك حال تعرض أي من الخدمات المقدمة الي أي من الاحداث التي قد تؤثر على اتاحة الخدمات للعملاء على سبيل المثال وليس الحصر "خطط البنك لتوقف الخدمة (الجزئي/ الكلى)" إبلاغ البنك المركزي - الإدارة المركزية للمنتجات الإلكترونية- على البريد الإلكتروني Digital.Services@cbe.org.eg وذلك قبل التوقف المشار اليه بـ ٤٨ ساعة على الأقل، على أن يشمل الإبلاغ ما يلي:

أ. تاريخ ووقت بدء الانقطاع وانتهائه.
ب. مقدار تأثر (العملاء-الخدمات) بهذا الانقطاع.
ج. الخطوات المتبعة لاستخدام مقر التعافي من الكوارث (DR) أثناء الانقطاع.

٦. ينبغي على البنك والوكلاء المصرفيين تطبيق سياسة الفصل بين المهام والرقابة الثنائية، وذلك للتأكد من عدم قيام أي من موظفيهما بأي عمل غير مصرح له، ويتضمن هذا على سبيل المثال لا الحصر: إدارة حساب المستخدم وتنفيذ المعاملات وحفظ وإدارة مفاتيح الشفرة الخاصة بالنظام وإدارة النظام (System Administration) وتشغيله (System Operations)، ويقع على عاتق البنك التأكد من اتباع الوكلاء المصرفيين لتلك الإجراءات.

سابعًا: السجلات

يتعين على البنك المشترك الاحتفاظ بما يلي - كحد ادني - على أنظمته الخاصة وفقاً للمدد المحددة قانوناً:

١. كافة البيانات الخاصة بالتعرف على العملاء والتحقق من هوياتهم من خلال المنظومة المعتمدة.
٢. المستندات الإضافية التي تم الحصول عليها من العميل الكترونياً.
٣. سجلات المعاملات التي تتم على حسابات العملاء.

ثامنًا: الشروط التعاقدية

١. **<u>يجب أن يتضمن العقد المبرم بين البنك المشترك وشركة الهوية المالية الرقمية بنود تتعلق بما يلي كحد أدنى:</u>**

١-١ تأمين سلامة وسرية وخصوصية وإتاحة بيانات العملاء التي تتم إتاحتها، أو معالجتها، أو تخزينها، أو نقلها بواسطة المنظومة المعتمدة وكذا إتباع الطرق الآمنة للتخلص منها حال انتفاء السبب.
١-٢ وضع آليات واضحة لإبلاغ العملاء بكيفية استخدام بياناتهم الشخصية وتخزينها ومعالجتها، وبيان الغرض من هذه المعالجة، والجهات المخوّل لها الوصول إلى تلك البيانات، بالإضافة إلى مدة الاحتفاظ بها.
١-٣ التزام شركة الهوية المالية الرقمية بكافة التعليمات الصادرة عن البنك المركزي، وكذا التعليمات الصادرة عن وحدة مكافحة غسل الأموال وتمويل الارهاب ذات الصلة بالمنظومة المعتمدة.
١-٤ آلية تسوية النزاعات.
١-٥ تحديد المسئوليات التعاقدية بوضوح ومنها على سبيل المثال لا الحصر:

أ. تحديد مسئوليات توفير المعلومات وتلقيها بشكل واضح وسليم.
ب. الرسوم والعمولات الخاصة باستخدام المنظومة المعتمدة.
ج. شروط وأحكام إنهاء التعاقد، وحقوق كل من البنك وشركة الهوية المالية الرقمية في هذه الحالة.
د. اتفاقية بعدم الإفصاح عن المعلومات لأطراف خارجية واتفاقية مستوى الخدمة (SLA)، والتي تشمل على سبيل المثال لا الحصر: تحديد الأدوار والمسئوليات والوقت المطلوب لتنفيذ الخدمة وإجراءات وبيانات

التصعيد والعقوبات في حال عدم الالتزام بها، بالإضافة إلى البنود التي تحفظ حق البنك في مراجعة الخدمات أو الاعتماد على تقارير المراجعة المعتمدة.

ه. إجراءات الإبلاغ في حالة حدوث أي خرق للبيانات (Breach Reporting SLA Data).

و. خضوع كافة النظم والعمليات لنظام إدارة المخاطر وسياسات الخصوصية وأمن المعلومات التي تتفق مع المعايير الخاصة بالبنك.

ز. توفير كافة تقارير المراجعة والتقييم لقطاعي الرقابة المكتبية والميدانية بالبنك المركزي المصري.

ح. النص صراحة على أن للبنك المركزي المصري حق الاطلاع والرقابة والتفتيش على النظم الداخلية لشركة الهوية المالية الرقمية سواء بشكل مخطط أو غير مخطط.

٢. **<u>يجب أن يتضمن العقد المبرم بين البنك المشترك والوكيل المصرفي البنود التالية كحد أدنى:</u>**

٢-١ دور كل من البنك والوكيل المصرفي في التعاقد، وحقوق والتزامات كل منهما.

٢-٢ النص على أن للبنك صاحب عقد الوكالة حق الاطلاع والرقابة والتفتيش على النظم الداخلية لوكلائه للتأكد من توافق قواعد العمل المتبعة مع تلك الصادرة عن البنك المركزي المصري.

٢-٣ التزام الوكيل المصرفي بإبلاغ البنك بأسماء الموظفين المخولين باستخدام النظام وصلاحياتهم وأي تغيير قد يطرأ عليهم.

٢-٤ توافر نظم وإجراءات لدى الوكيل المصرفي تضمن مستويات مرتفعة من الكفاءة والنزاهة لدى تعيين العاملين لديه وتدريبهم بصفة مستمرة.

٢-٥ المقرات التي سيتم من خلالها تقديم خدمات الوكالة المصرفية، واقتصار تقديم الخدمات من خلالها دون غيرها.

٢-٦ أن للبنك المركزي الحق في الاطلاع والرقابة والتفتيش على النظم الداخلية للوكيل المصرفي سواء بشكل مخطط أو غير مخطط بما يشمل مقاره.

٢-٧ تعهد الوكيل المصرفي بأن كافة البيانات والوثائق الخاصة بالعملاء ملك خاص للبنك صاحب عقد الوكالة ولا يحق للوكيل استعمالها بأي شكل من الأشكال أو مشاركتها مع أي طرف آخر، والتعهد بالحفاظ على سرية بيانات العملاء وعدم الإفصاح عنها (خلال وبعد انتهاء عقد الوكالة المصرفية).

٢-٨ وجود لاصقات أو لافتات تتضمن آلية واضحة لاستقبال شكاوى العملاء في مقرات الوكلاء المصرفيون المعتمدة بحيث يتم إحالتها للبنك للتعامل معها وذلك بالتوافق مع تعليمات حماية حقوق عملاء البنوك.

٢-٩ على الوكيل المصرفي إخطار البنك بإغلاق أي منفذ لتقديم الخدمة بصورة دائمة أو مؤقتة بمجرد أخذ قرار الغلق.

٢-١٠ شروط وأحكام إنهاء عقد الوكالة المصرفية.

٢-١١ التزام الوكلاء المصرفيون بإبلاغ البنوك بجميع تقارير الحوادث السيبرانية وحوادث امن المعلومات وفق إطار زمني محدد.

٥- مسئوليات والتزامات شركة الهوية المالية الرقمية "هوية"

١. إنشاء وإدارة المنظومة المعتمدة من داخل جمهورية مصر العربية.

٢. إصدار القواعد الخاصة بالربط الفني وتحديثاتها وتوفير البيئة اللازمة لتقديم خدمات المنظومة المعتمدة، وذلك بعد استيفاء موافقة البنك المركزي المصري.

٣. تحديد اللوائح والارشادات متضمنة أدوار ومسؤوليات والتزامات المشاركين بالمنظومة المعتمدة.

٤. الالتزام بالربط المؤمن مع أي من الجهات الموثوقة للحصول على البيانات اللازمة لإنشاء الهوية المالية الرقمية الخاصة بالمواطنين داخل جمهورية مصر العربية على سبيل المثال وليس الحصر: "مصلحة الأحوال المدنية"، وذلك بعد استيفاء موافقة البنك المركزي.

٥. التأكد من إنشاء هوية مالية رقمية برقم مميز واحد فقط لكل عميل ولا يتم تكراره مع مراعاة إمكانية تقدم العميل بمستندات مختلفة للتحقق من هويته، على سبيل المثال لا الحصر: التسجيل باستخدام بطاقة الرقم القومي وجواز السفر.

٦. الالتزام بإجراء مراجعة دورية لمعدلات ودقة عمليات التعرف على هوية العملاء، بما يضمن التوافق مع الحدود الآمنة والمعايير المعتمدة وذلك بعد التنسيق مع البنوك المشتركة.

٧. إتاحة الخدمات التالية للبنوك المشتركة بالمنظومة المعتمدة:

٧-١ التعرف على العملاء والتحقق من هوياتهم الكترونياً من خلال التسجيل الإلكتروني عبر التطبيقات الإلكترونية المعتمدة أو الأجهزة اللوحية ومنافذ الوكلاء المصرفيين.

٧-٢ إتاحة وسائل المصادقة الإلكترونية من خلال المنظومة المعتمدة بهدف التحقق من هوية العميل والتصديق على المعاملات وقبول الشروط والأحكام الخاصة بها المقدمة عبر الوسائط الإلكترونية والاحتفاظ بالسجلات الخاصة

بذلك وفقاً للمدد المحددة قانوناً، شريطة الحصول على موافقة العميل، وعلى الشركة أن تتيح الآليات التالية للتحقق من هوية العملاء:

أ. شهادة الهوية المالية الرقمية "DFI Certificate"، وذلك لمراعاة التحقق من أن المعاملات تتم من خلال ذات التطبيق والهاتف الذي تم من خلاله انشاء تلك الهوية.
ب. الرقم السري المستخدم لمرة واحدة (OTP).
ج. الرقم التعريفي للهوية المالية الرقمية "Global PIN"
د. صفات بيومترية خاصة بالعميل مثل (صورة الوجه - بصمة الإصبع- ...)

٧-٣ مشاركة الهوية المالية الرقمية مع البنوك المشاركة والوكلاء المصرفيين بالمنظومة المعتمدة شريطة الحصول على الموافقة المسبقة من العملاء والاحتفاظ بها.

٧-٤ تحديث بيانات الهوية المالية الرقمية الكترونياً.

٧-٥ خدمات الكشف عن العملاء على القوائم السلبية وإتاحة ما أسفرت عنه نتيجة الكشف للبنك المشترك لاتخاذ القرار النهائي بشأن التعامل مع العميل من عدمه.

٨. الالتزام بتوفير الدعم الفني للبنوك والوكلاء المصرفيين المشتركين بالمنظومة المعتمدة.

٩. توفير إمكانية الحصول على موافقة العميل الالكترونية على كافة الشروط والأحكام الخاصة بإجراءات انشاء الهوية المالية الرقمية الكترونياً وحصولها على بيانات العميل وصورته وتسجيلها ضمن سجلاتها على ان يتم مشاركتها مع البنك.

١٠. الالتزام بالتأكد من أن المنظومة المعتمدة تدعم قراءة البيانات الكترونياً على سبيل المثال لا الحصر:

١٠-١ قراءة بيانات بطاقة الرقم القومي بالتكامل مع أنظمة مصلحة الأحوال المدنية وأي مصادر أخرى موثوق بها.

١٠-٢ إمكانية الوصول إلى البيانات المسجلة على الرقاقة الإلكترونية المؤمنة القابلة للقراءة عن بعد وأي من المستندات الرسمية السارية لتحقيق الشخصية التي تدعمها المنظومة المعتمدة والواردة ضمن إجراءات التعرف على عملاء البنوك والتحقق من هوياتهم الكترونياً الصادرة عن وحدة مكافحة غسل الأموال وتمويل الإرهاب.

١٠-٣ الحصول على صورة حية للعميل (liveness detection) أثناء تقديم الطلب والتأكد من تطابقها مع المالك الأصلي لمستندات التحقق من هوية العميل المستخدمة في تقديم الطلب.

١١. التأكد من أن المنظومة المعتمدة قادرة على التفرقة بين كافة المعاملات الواردة لكل تطبيق الكتروني على حده سواء للبنك المشترك أو الوكلاء المصرفيين أو الجهات المرخص لها من البنك المركزي.

١٢. إتاحة المنظومة المعتمدة إمكانية اصدار اخطارات بنجاح أو فشل عملية انشاء الهوية المالية الرقمية مع الأسباب المتعلقة بذلك لكل من البنك والوكيل المصرفي المشترك بالمنظومة المعتمدة.

١٣. الالتزام بالاحتفاظ بسجلات الكترونية لكافة المعاملات التي تتم من خلال المنظومة المعتمدة وفقاً للمدد المدرجة بقانون مكافحة غسل الأموال ولائحته التنفيذية وضوابط مكافحة غسل الأموال وتمويل الإرهاب الصادرة من البنك المركزي في ذات الشأن، على أن تتضمن كحد أدنى بيان المعاملة، تاريخ المعاملة، التطبيق المستخدم، وسائل التصديق المستخدمة.

١٤. الالتزام بتوفير كافة التقارير والبيانات والاحصائيات بما يشمل تقارير المراجعة والتقييم للبنك المركزي ويحق لمفتشيه القيام بالرقابة الميدانية على الشركة.

١٥. الالتزام بتشكيل لجنة لأمن المعلومات وتشمل اختصاصاتها المهام والأنشطة التي تهدف إلى تعزيز أمن المعلومات وحماية البيانات، ومن أهمها وضع آلية لحوكمة الأمن السيبراني، وسبل تعزيزها من سياسات وإجراءات ومراجعتها وتحديثها بصفة دورية، بالإضافة الي وضع نظم رقابة وإدارة المخاطر المتعلقة بها، وإعداد تقارير دورية عن حالة أمن المعلومات والأمن السيبراني في الشركة، وتقوم اللجنة برفع توصياتها إلى مجلس إدارة الشركة و/ أو لجنة المخاطر لاتخاذ الإجراءات التصحيحية- إن وجدت.

١٦. قيام لجنة أمن المعلومات بالشركة بإبلاغ مجلس إدارتها و/ أو لجنة المخاطر بأي مخاطر جوهرية ذات الصلة، ووضع الضوابط الأمنية المتبعة للتحكم في الدخول المصرح على أنظمة البيئة الفعلية وكذلك البنية التحتية الخاصة بهذه الخدمة أو أي أنظمة أخرى مرتبطة بهذه المنظومة المعتمدة قد تؤدي إلى اختراق الأنظمة.

١٧. القيام بالربط بصورة مؤمنة بما يُراعى من خلالها سرية وسلامة وإتاحة وخصوصية البيانات والمعلومات التي يتم تبادلها بين كلًا من البنوك المشتركة والوكلاء المصرفيين داخل جمهورية مصر العربية مع الأخذ بعين الاعتبار ما يلي:

١-١٧ تأمين اتصالات بيانات المنظومة المعتمدة الكاملة (Eco-system) والنظام البيئي التشغيلي للأنظمة المتصلة بالأطراف الخارجية، ووضع خطط البرامج التدريبية الهادفة لزيادة الوعي الأمني لدي جميع موظفي الشركة وبالأخص القائمين على توفير هذه الخدمة للحد من مخاطر هجمات الهندسة الاجتماعية (Social Engineering).

٢-١٧ استخدام أنظمة متقدمة للكشف عن محاولات الاحتيال مع تحديد الأنماط غير الطبيعية، ويتم اخطار الإدارة المركزية لمكافحة الاحتيال بالبنك المركزي المصري ومركز الاستجابة لطوارئ الحاسب الالي للقطاع المالي فور اكتشاف أي محاولات احتيالية، بالإضافة إلى وضع كافة التدابير اللازمة لمكافحة الاحتيال الالكتروني (على سبيل المثال، تقنيات مكافحة التزييف العميق (Anti Deep Fake)

٣-١٧ وضع وتطبيق معايير للكشف عن محاولات التزوير في البيانات البيومترية (مثل الصور أو الفيديوهات المُعدلة).

٤-١٧ ضمان مراقبة ومتابعة حوادث أمن المعلومات والأمن السيبراني على مدار الساعة مع وضع الآليات والإجراءات التي سيتم اتباعها في هذا الشأن واستخدام تقنيات التشفير عالية المستوى للحماية من الهجمات السيبرانية، وضمان تنفيذ سياسات الاستجابة لتلك الحوادث بما يشمل إجراءات اكتشاف هذه الحوادث وطرق الاستجابة السريعة والتعافي للحد من المخاطر الناتجة عنها، وفي حالة حدوث أي اختراقات او تسريبات لمعلومات تتعلق بالأمن السيبراني يتم ابلاغ مركز الاستجابة لطوارئ الحاسب الالي للقطاع المالي خلال ٦ ساعات من اكتشاف الحالة بحد أقصى

٥-١٧ آليات التشفير المستخدمة لحماية الشبكات والبيانات أثناء نقلها أو تخزينها (At-Rest/In-Transit) طبقاً لأفضل الممارسات العالمية.

٦-١٧ تقييم مخاطر الأمن السيبراني بصورة دورية لأي طرف ثالث (موردين، وكلاء، شركاء تقنيين) يتعامل مع بيانات الهوية المالية الرقمية واشتراط حصولهم على شهادات أمنية وفقاً لمتطلبات البنك المركزي المصري، مع القيام بالمراجعة الدورية لهذا التقييم وفقاً لما تم اكتشافه.

٧-١٧ القيام باختبارات اختراق للأنظمة والبنية التحتية التكنولوجية للشركة (Infrastructure Penetration Test) وإجراء تقييم نقاط الضعف (Credentialed vulnerability Assessment) وإجراء تقييم مخاطر الطرف الثالث بصفة دورية للتأكد من تأمين شبكات الربط وأنظمة البنية التحتية ضد أي محاولات اختراق، على أن تتم هذه الاختبارات بصورة شاملة تتيح اكتشاف جميع الثغرات والمشاكل الفنية في التطبيقات وأنظمة البنية التحتية المستخدمة وأي أنظمة وسيطة، واعداد تقارير عنها وعرضها علي مجلس الإدارة من خلال لجنة أمن المعلومات أو المخاطر الخاصة بالشركة واخطار البنك المركزي بمخرجات هذه التقارير.

١٨. المراقبة والمراجعة المستمرة باستخدام تقنيات حديثة لتحديد أي نشاط غير طبيعيٍ أو تهديدات تقنية محتملة بشكل استباقي وعلى مدار ٢٤ ساعة.

١٩. الالتزام بإنشاء نظام مركزي يتم من خلاله تسجيل عدد محاولات التسجيل الخاطئة وبياناتها بالكامل.
٢٠. الالتزام بإجراء مراجعة دورية للعمليات والنظم المستخدمة في إدارة خدمات الهوية المالية الرقمية، بما يشمل ذلك تقييم الالتزام بالمعايير والسياسات المعمول بها وتحليل الثغرات وتوصيات لتحسين الأداء والأمان.

٢١. في حاله خروج أحد البرامج أو الأنظمة من الخدمة يتم التخلص الامن للبيانات المالية وتدميرها بحيث يستحيل استرجاعها مره اخرى من جميع الخوادم والأنظمة التكنولوجية.

٢٢. يجب على المنظومة المعتمدة الاحتفاظ بسجلات دقيقة (سجلات المراجعة والمراقبة ومسارات التدقيق) لجميع المعاملات والأنشطة المتعلقة بالهوية المالية الرقمية وفقاً لما تم التطرق له من التزامات، كما يجب توفير آليات لإدارة وحفظ هذه السجلات لفترة زمنية محددة وفقًا لمتطلبات القوانين والقواعد المعمول بها.

٦- توعية العملاء

يجب على البنوك القيام بما يلي:

٦-١ إيلاء اهتماماً خاصاً لتوعية العملاء عن طريق تقديم حملات توعية مختلفة وكذا نصائح سهلة الفهم وواضحة تتعلق بالاحتياطات الأمنية الواجب اتخاذها عند التعامل مع تلك الخدمات والتزامهم حيال ذلك، وذلك نظراً لأن الأجهزة التي يستخدمها العملاء تقع خارج نطاق سيطرة البنك، لذا فإن احتمال ظهور مخاطر أمنية تزداد في حالة عدم معرفة مُستخدم النظام بالاحتياطات الأمنية الضرورية لاستخدام الخدمة أو سوء فهمها.

٦-٢ توعيه العملاء والتأكيد عليهم أن موظفي البنك أو وكلائه المصرفيون لا يجوز لهم مطالبة مُستخدم النظام الإفصاح عن البيانات السرية عن طريق البريد الإلكتروني أو غيره وفي حالة حدوث ذلك يجب على مُستخدم النظام الاتصال بالبنك في أسرع وقت ممكن.

٦-٣ توعية العملاء بالطرق التي يمكنهم من خلالها التأكد من صحة التطبيق الرسمي والتزام البنك بإطلاق حملات دعائية تخص زيادة وعي العملاء فيما يخص الخدمات المشار اليها.

٦-٤ فيما يتعلق بالاحتياطات الأمنية الواجب إتباعها فانه يتعين توعية العملاء وفقا لطبيعتهم، وطبيعة الخدمات المقدمة، وذلك على النحو التالي كحد أدنى:

أ. اختيار وحماية وسائل التحقق الخاصة بالعميل.

ب. ضرورة عدم الإفصاح عن أي معلومات شخصية - كبطاقة الهوية أو جواز السفر أو العناوين أو أرقام حسابات البنك الخاصة بهم - لأي شخص لم يتأكد من هويته أو استخدام تطبيقات هواتف محمولة موضع شك. كما يجب التأكيد على العملاء بعدم الإفصاح عن كلمات السر لأي شخص بما في ذلك موظفي البنك أو وكلائه، وذلك بهدف الحماية ضد تقنيات الهندسة الاجتماعية (Social Engineering Techniques).

ج. مراجعة النصائح والإرشادات الخاصة بالاحتياطات التأمينية التي يتم تقديمها للعملاء للتأكد من كفايتها وملائمتها للتغيرات التي تستجد على البيئة التكنولوجية والخدمات المقدمة.

د. إخطار مستخدم النظام بالإجراءات الواجب اتباعها في حالة اكتشاف أي شخص آخر لوسائل التحقق الخاصة بمُستخدم النظام.

ه. توعية العميل بضرورة إبلاغ البنك فوراً في حالة فقدان الهاتف المحمول المرتبط بالمنظومة.

٧- إجراءات الحصول على التراخيص

إجراءات الحصول على موافقة البنك المركزي على استخدام منظومة التعرف على هوية العملاء الكترونياً باستخدام الهوية المالية الرقمية

٧-١ يجب على البنوك أو أي من الجهات الراغبة في الاشتراك في المنظومة المعتمدة أن تتقدم بطلب للحصول على موافقة البنك المركزي المصري وذلك باستيفاء المستندات التالية كحد أدنى:

٧-١-١ دورة العمل التفصيلية.

٧-١-٢ بيانات البنية التحتية لمنظومة الجهة الراغبة في الحصول على الترخيص والتي سيتم استخدامها.

٧-١-٣ التكنولوجيا اللازمة وضوابط أمن المعلومات والأمن السيبراني لتأمين البنية التحتية والأنظمة والتطبيقات وكافة المعلومات والبيانات في حالاتها المختلفة من نقل ومعالجة وتخزين وحفظ في نسخ احتياطية بما يضمن سرية وسلامة وإتاحة البيانات والتوافق مع الإطار العام للأمن السيبراني.

٧-١-٤ خطة العمل الخاصة بالربط الفني مع شركة الهوية المالية الرقمية.

٧-١-٥ البيانات المتعلقة بالتطبيق الخاص بالتحقق من هوية العملاء الكترونيا.

٧-١-٦ تقديم خطة عمل لمدة ثلاث سنوات تتضمن التالي:

أ. عدد العملاء المستهدف تقديم الخدمة لهم.

ب. المنتجات والخدمات التي سيتم تطبيقها.

ج. خطة تسويقية شاملة للتعريف بالخدمة وتفعيل استخدامها.

٧-١-٧ قيام البنك بعمل الاختبارات اللازمة للتأكد من التوافق مع القواعد الخاصة بالبنك المركزي المصري ونظم العمل الخاصة بشركة الهوية المالية الرقمية.

٧-٢ يجب على البنوك موافاة البنك المركزي المصري بما يلي قبل الإطلاق الفعلي للخدمة:

٧-٢-١ تقرير اختبارات الاختراق (Penetration Test Report)، وتقارير تقييم نقاط الضعف (Credential vulnerability assessment) على بيئة العمل الفعلية والطوارئ بما يشمل جميع الأنظمة و التطبيقات و البنية التحتية و أساليب التأمين المتبعة،على ان تتم هذه الاختبارات بصورة شاملة تتيح اكتشاف جميع الثغرات و المشاكل الفنية وذلك للتأكد من عدم وجود أي نقاط ضعف عالية أو متوسطة الخطورة، ويتم تقديم التقرير المشار اليه إلى البنك المركزي المصري في مدة لا تتجاوز ثلاثة أشهر من تاريخ إصداره من مقدم

خدمة خارجي مستقل والخاصة بكافة الخدمات المذكورة أعلاه، ومن ثم الحصول على موافقة البنك المركزي المصري بتفعيل الخدمة.

٧-٢-٢ تقييم المخاطر الذي قام البنك بإجرائه على الخدمة والذي يوضح أن الضوابط التي سيتم تطبيقها تصل بمستوى المخاطر للمستوى المقبول وتوضح إجراءات إدارة ورصد أية مخاطر بصورة فعالة.

٧-٢-٣ يجب على البنوك إجراء تقييم مخاطر الأمن السيبراني .(cybersecurity risk assessment) علي ان يتم اعتمادها من السلطة المختصة.

٧-٢-٤ استيفاء تقييم مخاطر من قبل ادارة الالتزام.

٧-٢-٥ موافاة البنك المركزي بتقرير (SOC 2 Type1) من جهة معتمدة قبل الإطلاق وموافاة البنك المركزي بتقرير (SOC 2 Type 2) من جهة معتمدة خلال ٦ أشهر من الإطلاق.

٧-٢-٦ إجراء تقييم أثر الخصوصية (Privacy Impact Assessment) قبل إطلاق الخدمة وذلك بما يضمن تحديد ومعالجة المخاطر التي قد تؤدي إلى انتهاك الخصوصية أو إساءة استخدام الهوية او أي مخاطر احتيال مرتبطة بها ويعد هذا التقييم جزءا في منظومة إدارة مخاطر الاحتيال ويقدم للإدارة المركزية لمكافحة الاحتيال وذلك للوقوف على:

- تقييم المخاطر المحتملة على خصوصية العملاء، على سبيل المثال (مخاطر تسريب البيانات – سوء الاستخدام – الوصول غير المصرح به)
- تحديد الضوابط اللازمة للحد من تلك المخاطر
- الوقوف على البيانات الشخصية التي سوف يتم جمعها أو معالجتها وتحليل أسلوب استخدام تلك البيانات وما يمكن الوصول إليها

البنك المركزي المصري
CENTRAL BANK OF EGYPT

القواعد المنظمة لخدمات منظـــــومة الهوية المالية الرقمية للتعرف على عملاء البنوك والتحقق من هويـــــاتهم الكترونياً

داخل جمهورية مصر العربية