



سلطة النقد الفلسطينية
PALESTINE MONETARY AUTHORITY

تعليمات رقم (11) لسنة 2022 بشأن الإطار التنظيمي للأمن السيبراني

استناداً لأحكام القرار بقانون رقم (9) لسنة 2010 بشأن المصارف، لا سيما المادتين (43) و (72) منه،
ووفقاً للصلاحيات المخولة لنا،
وتحقيقاً للمصلحة العامة،
فقد أصدرنا التعليمات التالية:

مادة (1) الهدف ونطاق التطبيق

1. تهدف أحكام هذه التعليمات إلى وضع إطار عام لإدارة المخاطر السيبرانية وفق أفضل الممارسات والمعايير المعمول بها، والحد من تأثيرها على الاصول المعلوماتية والتقنية.
2. تطبق أحكام هذه التعليمات على كافة المصارف المرخص لها من سلطة النقد بمزاولة العمل المصرفي في فلسطين.

مادة (2) وظيفة الأمن السيبراني

يجب على المصرف الإلتزام بالآتي:

1. إنشاء وظيفة لإدارة مخاطر الأمن السيبراني في دائرة المخاطر.
2. تعيين كادر وظيفي يمتلك الخبرة العلمية والعملية والشهادات المهنية المتخصصة الكافية لإدارة مخاطر الأمن السيبراني والحاقهم بدورات وورشات تدريبية بشكل مستمر، للقيام بالمهام الآتية:
 - أ. إعداد سياسة خاصة بالمصرف وخطط عمل لإدارة مخاطر الأمن السيبراني وفق أحكام هذه التعليمات وتحديثها سنوياً أو عند إجراء أي تعديلات جوهرية على الأنظمة.
 - ب. إجراء تقييم دوري لمدى كفاية وكفاءة سياسة الأمن السيبراني ومراجعة منتظمة للإعدادات والضوابط الأمنية والفنية المطبقة وتطوير البنية التحتية الخاصة بالأمن السيبراني.
 - ت. تحديد نقاط الضعف والمخاطر السيبرانية المحتملة والفجوات التي تحتاج للمتابعة والتصويب، وتوفير الحلول والضوابط المناسبة للتخفيف والحد من تأثيرها.





سلطة النقد الفلسطينية
PALESTINE MONETARY AUTHORITY

- ث. الاشراف وتقديم الدعم لمسؤولي الأنظمة بشأن تطوير وإقتناء وتطبيق التحديثات على الأنظمة بما يتوافق مع سياسة وضوابط الأمن السيبراني لدى المصرف.
- ج. التنسيق مع المسؤولين عن إدارة الأجهزة وأنظمة البنية التحتية في دائرة تكنولوجيا المعلومات بهدف تطبيق ضوابط الأمن السيبراني بفعالية.
- ح. اعداد برامج توعوية لموظفي المصرف بشأن مفاهيم ومتطلبات الأمن السيبراني بما يتوافق مع سياسة المصرف.
- خ. إعداد تقارير بشأن الأمن السيبراني ضمن تقارير إدارة المخاطر.

مادة (3) مركز عمليات أمن المعلومات

- يجب على المصرف تشكيل فريق متخصص أو التعاقد مع طرف ثالث وفقاً لتعليمات الإسناد الخارجي النافذة لإدارة مركز عمليات أمن المعلومات، وتوفير الأنظمة والبرامج اللازمة مثل Security Information and Event Management (SIEM) للقيام بالمهام المناطة بهم، ومنها:
1. الكشف عن التهديدات الأمنية من خلال المراقبة المستمرة (24/7).
 2. مراقبة وكشف التعديلات التي تتم على الأنظمة والملفات لضمان سلامتها.
 3. مراقبة الأنظمة من أي هجوم أو تطفل خارجي أو داخلي.
 4. مراقبة وتحليل السجلات والأحداث الأمنية (Logs & Events).
 5. تفعيل خطة الاستجابة للأحداث ضمن الإجراءات المعتمدة.
 6. تقييم الثغرات والتهديدات بشكل استباقي للحد من تأثيرها.
 7. التوثيق الكافي للأحداث والتهديدات والحفاظ على الأدلة، ورفع تقارير رقابية بشكل دوري وفقاً لتقدير سلطة النقد.

مادة (4) الإبلاغ عن الحوادث وتبادل المعلومات

في حال تعرض المصرف لأي حدث سيبراني ذو تأثير على استمرارية تقديم الخدمات أو بيانات العملاء أو الأنظمة والشبكات، يجب على المصرف إبلاغ سلطة النقد فوراً بذلك، شريطة أن يعزز الإبلاغ خطياً بشكل تفصيلي عن الآثار المترتبة وإجراءات الاستجابة والإجراءات الوقائية التي تم اتخاذها.





سلطة النقد الفلسطينية
PALESTINE MONETARY AUTHORITY

مادة (5) حماية البيانات والخصوصية

مع مراعاة ما ورد في التعليمات النافذة بشأن سرية البيانات، يجب على المصرف تضمين سياسة حماية البيانات وخصوصيتها الضوابط والإجراءات المناسبة للحفاظ على السرية والنزاهة والتوافرية وحماية البيانات الشخصية وصلاحيات الوصول إليها وإستخدامها وتخزينها والإحتفاظ بها واثناء عمليات الربط والتكامل والتشغيل البيئي (Interoperability) بإستخدام الوسائل التقنية المختلفة مثل API بين الأنظمة المختلفة.

مادة (6) أحكام عامة

1. يعتبر الإطار التنظيمي للأمن السيبراني المرفق ملحق رقم (1) جزءاً لا يتجزأ من هذه التعليمات.
2. لا يعتبر الملحق رقم (1) بديلاً عن قيام المصرف بتطوير موانيق داخلية للأمن السيبراني تحدد فيها آليات وإجراءات التزامه بمتطلبات الإطار او أية معايير إضافية يرى المصرف اهمية تطبيقها وبما لا يتعارض مع التشريعات النافذة.
3. يجوز للمصرف التعاقد مع طرف آخر وفقاً لتعليمات الإسناد الخارجي النافذة، لغاية تقييم المخاطر السيبرانية لديه.

مادة (7) العقوبات

يُعاقب كل من يخالف أحكام هذه التعليمات وفق أحكام القرار بقانون رقم (9) لسنة 2010 بشأن المصارف.

مادة (8) التنفيذ والنفاذ

يجب على كافة الجهات المختصة، كل فيما يخصه، تنفيذ أحكام هذه التعليمات، وتطبيق من تاريخ صدورها.
صدرت في مدينة رام الله بتاريخ 22 / 11 / 2022.

د. فراس ملح

المحافظ

رام

ملحق رقم (1)

الإطار التنظيمي للأمن السيبراني

Cyber Security Framework

مقدمة

تسعى سلطة النقد بشكل دائم ضمن استراتيجيتها اتخاذ التدابير اللازمة وضمان قدرتها وجاهزيتها والمصارف الخاضعة لرقابتها على تقديم الخدمات باستمرار وفي جميع الظروف، ونظرا للاستخدام المتزايد للتكنولوجيا، وإلى دورها في تحسين فعالية وكفاءة الأعمال والخدمات التي يتم تقديمها، إلا أن هناك مخاطر ونقاط ضعف إضافة إلى تأثير الحوادث/الهجمات السيبرانية على جودة الأعمال مما يؤكد الحاجة لضرورة التأهب الكافي لمخاطر الأمن السيبراني بشكل مستمر في المصارف والمؤسسات المالية. وبعد الاطلاع على أفضل الممارسات والتجارب في مجال الأمن السيبراني والاستفادة منها، فإنه كان لا بد من وضع ضوابط ومتطلبات بهدف تأمين الفضاء السيبراني في المصارف، وحماية الأصول المعلوماتية والتقنية والتركيز على الأهداف الأساسية لحماية البيانات والمعلومات والحفاظ على مرونة الخدمات واستمرارية تقديمها، وهي:

1. سرية المعلومة (Confidentiality): ضمان عدم إتاحة الوصول للمعلومات والأنظمة الحساسة من قبل أفراد أو كيانات أو عمليات غير مصرح بها.
2. سلامة المعلومة (Integrity): ضمان عدم تعديل أو حذف البيانات والمعلومات الحساسة بطريقة غير مصرح بها ولا يمكن اكتشافها.
3. توافر المعلومة (Availability): ضمان الوصول المصرح به في الوقت المناسب إلى المعلومات واستخدامها.

1. حوكمة الأمن السيبراني (Cybersecurity Governance)	
1.1	استراتيجية الأمن السيبراني Cybersecurity Strategy
1.2	إدارة الأمن السيبراني Cybersecurity Management
1.3	سياسات وإجراءات الأمن السيبراني Cybersecurity Policies and Procedures
1.4	أدوار ومسؤوليات الأمن السيبراني Cybersecurity Roles and Responsibilities
1.5	إدارة مخاطر الأمن السيبراني Cybersecurity Risk Management
1.6	الأمن السيبراني ضمن إدارة مشاريع Cybersecurity in Projects Management
1.7	الامتثال لمتطلبات سلطة النقد ومعايير الأمن السيبراني Cybersecurity Regulatory Compliance
1.8	المراجعة والتدقيق الدوري للأمن السيبراني Cybersecurity Periodical Assessment and Audit
1.9	الأمن السيبراني المتعلق بالموارد البشرية Cybersecurity in Human Resources
1.10	التوعية والتدريب بالأمن السيبراني Cybersecurity Awareness and Training
2. ضوابط تعزيز الأمن السيبراني (Cybersecurity Defense Controls)	
2.1	إدارة الأصول Asset Management
2.2	إدارة هويات الدخول والصلاحيات Identity and Access Management
2.3	حماية الأنظمة وأجهزة معالجة المعلومات Information Systems and Processing Facilities Protection
2.4	اقتناء وتطوير البرمجيات Software Development and Acquisition
2.5	حماية البريد الإلكتروني E-mail Protection
2.6	إدارة أمن البنية التحتية والشبكات Infrastructure and Networks Security Management
2.7	ضوابط الاتصال عن بُعد Remote Connection Controls
2.8	أمن الأجهزة المحمولة Portable Devices Security
2.9	أمن البيانات والمعلومات Data and Information Protection
2.10	التشفير Cryptography
2.11	إدارة النسخ الاحتياطية والاسترجاع Backup and Recovery Management
2.12	إدارة الثغرات Vulnerabilities Management

إدارة سجلات الاحداث ومراقبة الأمن السيبراني Cybersecurity Event Logs and Monitoring Management	2.13
إدارة حوادث وتهديدات الأمن السيبراني Cybersecurity Incident and Threat Management	2.14
الأمن المادي Physical Security	2.15
حماية التطبيقات الداخلية والخارجية Internal and Web Applications Security	2.16
3. صمود الأمن السيبراني وإدارة استمرارية العمل Cybersecurity Resilience and Business Continuity Management (BCM)	
4. الأمن السيبراني المتعلق بالأطراف الخارجية والحوسبة السحابية Third-Party and Cloud Computing Cybersecurity	
الأمن السيبراني المتعلق بالأطراف الخارجية Third-Party Cybersecurity	4.1
الأمن السيبراني المتعلق بالحوسبة السحابية Cloud Computing Cybersecurity	4.2

ضوابط الأمن السيبراني

1. حوكمة الامن السيبراني Cybersecurity Governance

تتطلب الحوكمة السيبرانية الفعالة اعداد إطار واضح وشامل للمرونة السيبرانية (كتوجيهات إرشادية) داخل البيئة التشغيلية للمصرف، والذي يشمل السياسات والإجراءات والضوابط الواجب اتخاذها لضمان السيطرة على التهديدات والمخاطر السيبرانية المتوقعة، والحفاظ على بيئة مرنة تضمن استمرارية عمل الأنظمة والعمليات بشكل آمن وفعال. يجب على المصرف الالتزام بتطبيق ضوابط التعليمات والمعايير ذات العلاقة بمتطلبات الحوكمة ومراجعتها بشكل دوري من خلال لجنة توجيهية، وتوفير استراتيجية وإطار عمل للأمن السيبراني.

متطلبات الحوكمة السيبرانية:

1. ان يضم مجلس الإدارة والإدارة العليا أو من يتم تفويضه، أشخاصاً يتمتعون بالمعرفة والمهارات اللازمة لفهم وإدارة المخاطر السيبرانية.
2. توفير اجراءات استباقية لإدارة التهديدات والمخاطر السيبرانية الحالية والناشئة وغير المتوقعة التي قد يواجهها المصرف.
3. توفير الدعم لإدارة المخاطر السيبرانية وعلى كافة المستويات داخل بيئة العمل.
4. تخصيص الموارد والخبرات الكافية لإدارة المخاطر والتهديدات السيبرانية.

1.1 استراتيجية الامن السيبراني Cybersecurity Strategy

الهدف: ضمان إسهام خطط العمل والأهداف والمشاريع الخاصة بالأمن السيبراني داخل المصرف، في تحقيق متطلبات سلطة النقد ذات العلاقة.

الضوابط: يجب على المصرف الالتزام بالآتي:

- 1.1.1 اعداد واعتماد استراتيجية الامن السيبراني للمصرف من قبل مجلس الإدارة.
- 1.1.2 ان تضع استراتيجية الأمن السيبراني للمصرف أولوية حماية أصول وأنظمة المصرف.
- 1.1.3 أن تشمل استراتيجية المصرف على السياسات والإجراءات والكادر البشري إضافة لأصول تكنولوجيا المعلومات وإدارة المخاطر السيبرانية.
- 1.1.4 ان تشمل استراتيجية الامن السيبراني ما يلي:
 - أ. الأهداف الاستراتيجية للمصرف والتي ترتبط بالأمن السيبراني.
 - ب. الاطراف والجهات الرئيسة الفاعلة والمسؤولة عن تنفيذ الاستراتيجية.
 - ت. الموارد الداخلية والخارجية لتنفيذ التوجيهات والعمليات وسير عملها بشكل سليم.
 - ث. الأشخاص والعمليات والموارد التكنولوجية اللازمة لإدارة المخاطر السيبرانية.
 - ج. آليات التواصل والتعاون مع أصحاب المصلحة ومتخذي القرار للاستجابة بشكل سريع وفعال للتعافي من الهجمات السيبرانية.
 - ح. اعتماد خطة عمل لتطبيق استراتيجية الامن السيبراني الخاصة بالمصرف.
- 1.1.5 مراجعة استراتيجية الأمن السيبراني مرة واحدة سنوياً على الأقل او عند حدوث تغييرات تتطلب ذلك.

1.2 إدارة الأمن السيبراني Cybersecurity Management

الهدف: ضمان التزام ودعم مجلس إدارة المصرف والإدارة العليا بشأن إدارة وتطبيق سياسات وإجراءات الامن السيبراني في المصرف وفقاً لمتطلبات سلطة النقد ذات العلاقة.

الضوابط: يجب على المصرف الالتزام بالآتي:

1.2.1. اجراء توعية وتقييم دوري لمستوى وعي أعضاء مجلس الإدارة والإدارة العليا لأدوارهم ومسؤولياتهم بشأن إدارة الأمن السيبراني، بما في ذلك معرفتهم بالمخاطر والتهديدات السيبرانية.

1.2.2. ان يكون مسؤول/ ضابط الأمن السيبراني مستقل ادارياً عن إدارة تكنولوجيا المعلومات في المصرف ويتمتع بالخبرة العلمية والعملية العالية.

1.2.3. ان تقوم الجهة المسؤولة عن الامن السيبراني برفع تقارير دورية او كلما اقتضت الضرورة، للإدارة العليا ومجلس الإدارة فيما يخص الامن السيبراني في المصرف، على ان يتضمن التقرير ما يلي:

أ. أهم التحديات والمعوقات وكشف تحليل الفجوات المتعلقة بتطبيق سياسة الأمن السيبراني.

ب. نتائج تقييم المخاطر السيبرانية.

ت. نتائج تقييم مدى كفاية وكفاءة السياسات والإجراءات والضوابط الخاصة بالأمن السيبراني.

ث. التوصيات والإجراءات الواجب تنفيذها.

ج. ملخص يستعرض أهم الاحداث والتهديدات المتعلقة بالأمن السيبراني التي تعرض لها المصرف خلال فترة التقرير.

1.2.4. إنشاء لجنة توجيهية داخلية (steering Committee) مكونة من أعضاء من الإدارة العليا من عدة دوائر مثل التمويل،

المخاطر، العمليات، أمن المعلومات/السيبراني، تكنولوجيا المعلومات، القانونية، الموارد البشرية، وقد يتم الاستعانة بجهات خارجية إذا اقتضت الضرورة، بحيث تهدف لتطوير وتنفيذ استراتيجية الأمن السيبراني والإشراف على تطبيقها وأن يكون ارتباطها مباشرة بمجلس الإدارة او الإدارة العليا ويتم إطلاع مجلس الإدارة بالأمور الجوهرية، على أن تكون أبرز مهامها:

أ. تحديد وتقييم أولويات واحتياجات أصحاب المصلحة الداخليين والخارجيين في المصرف.

ب. تقديم التوجيه للإدارة العليا بشأن ما يجب أن تحققة استراتيجية الأمن السيبراني.

ت. اتخاذ القرارات المتعلقة بالأمن السيبراني والآلية التي يجب ان تتم لاتخاذ هذه القرارات.

ث. يجب الاخذ بعين الاعتبار طبيعة مخاطر المصرف وتحمله لشهية المخاطر عند تحديد كيفية معالجة المخاطر السيبرانية.

ج. تقييم الآلية التي قد تتأثر بها الدوائر المختلفة داخل المصرف، وكيفية التعامل والتنسيق فيما بينها لتحقيق النتائج المرجوة من

استراتيجية الامن السيبراني على مستوى المصرف.

ح. تقييم آلية مراقبة أداء ونتائج المرونة السيبرانية، والتدخل عند الحاجة لضمان تطبيق إطار عمل الامن السيبراني بشكل سليم.

خ. ضمان وجود تنسيق وتبادل في المعلومات والخبرات بما يخص الأمن السيبراني بين المصرف والأطراف الخارجية ذات

العلاقة، والمشاركة في الورشات والندوات والمؤتمرات المتعلقة بالأمن السيبراني.

د. تحديد الإجراءات اللازمة لتصميم المرونة السيبرانية وتنفيذها وتحديثها ومتابعتها.

ذ. تحديد الآلية المستخدمة في إدارة المشاريع الخاصة بالمرونة السيبرانية، بما في ذلك تحديد الإجراءات والموازنة التقديرية.

1.2.5. مسؤوليات مجلس الإدارة أو من يفوض عنه:

أ. اعتماد استراتيجية الأمن السيبراني، والتأكد من مراجعتها وتحديثها بانتظام مرة واحدة سنوياً على الأقل، وفقاً للمتغيرات والتهديدات المصاحبة والمخاطر السيبرانية.

ب. متابعة التقارير بصورة مستمرة بكافة المخاطر والتهديدات السيبرانية، وضمان توافقها مع تحمل المصرف للمخاطر وشهيته، حتى تتمكن من تحقيق أهداف المصرف واستراتيجيته.

ت. نشر وتعزيز أهمية دور الموظفين في تحمل المسؤولية لضمان "المرونة السيبرانية" وقدرة المصرف على التعامل مع التهديدات والمخاطر السيبرانية.

ث. اعداد واعتماد نظام فعال لإدارة مخاطر الأنظمة والعمليات المصرفية وضمان تحديثه، على أن يشمل إجراءات المساءلة والضوابط الواجب تطبيقها للحد من آثار هذه المخاطر.

وعليه، يجب على مجلس الإدارة أو من يفوض الالتزام بالآتي:

أ. وجود عضو أو أكثر في المجلس أو من يفوض، ممن يمتلكون المعرفة والخبرة والمهارات اللازمة لفهم وتقييم المخاطر والتهديدات السيبرانية التي قد تؤثر على المصرف، والقدرة على فهم وتقييم توصيات الإدارة العليا الخاصة بالأمن السيبراني. أو الاستعانة بموظفين من خارج أعضاء المجلس أو جهة خارجية مستقلة لتقديم المشورة والدعم اللازم لرفع تقاريرها الخاصة بالأمن السيبراني للمجلس.

ب. التأكد من إدراج المخاطر السيبرانية وتنفيذ إطار المرونة السيبرانية، بانتظام في جدول أعمال اجتماع المجلس.

ت. العمل على تعزيز ونشر وتنمية الوعي بضرورة الالتزام بسياسة الأمن السيبراني في المصرف.

ث. الإشراف على تنفيذ الإدارة العليا لحملة التوعية اللازمة للموظفين بالمخاطر والتهديدات المرتبطة بالأمن السيبراني.

ج. التأكد أن الإدارة العليا تقوم بانتظام باختبارات التقييم الذاتي للمرونة السيبرانية، ومراجعة التقييم الذاتي واتخاذ القرارات المناسبة لزيادة فعالية الضوابط الخاصة بالأمن السيبراني وضمان تكاملها مع استراتيجية المصرف.

ح. مراجعة واعتماد أولويات الإدارة العليا والخطط التنفيذية وتخصيص الموارد اللازمة للأمن السيبراني، بناءً على مؤشرات الأداء الرئيسية (KPIs) ونتائج التقييم الذاتي.

1.2.6. يجب على الإدارة العليا الالتزام بالآتي:

أ. تقديم تقرير منتظم لمجلس الإدارة حول الحالة العامة لبرنامج المرونة السيبرانية، متضمنة أهم المخاطر والقضايا الرئيسية مثل الموازنة التقديرية والاحتياجات من الموارد الحالية والمستقبلية، لضمان تحقيق أهداف المرونة السيبرانية بالتنسيق مع إدارة تكنولوجيا المعلومات ومخاطر أمن المعلومات/ السيبراني.

ب. اعداد برنامج خاص للتدريب وتنمية المهارات حول مفاهيم ومخاطر الأمن السيبراني والمرونة السيبرانية، على أن يشمل التدريب أعضاء مجلس الإدارة والإدارة العليا وكافة موظفي المصرف، على أن يكون مرة واحدة سنوياً على الأقل، بحيث تشمل البرامج على مواضيع ذات علاقة مثل (الاستجابة للحوادث، التهديدات السيبرانية الحالية، نقاط الضعف، الخ)، والهجمات والتقنيات المستخدمة في التهديدات.

ت. توفير تدريب متخصص بالأمن السيبراني للموظفين الذين يمتلكون صلاحيات وصول واسعة إلى المعلومات والأصول الحساسة.

ث. اعتماد مصفوفة الصلاحيات وفصل المهام بين الموظفين في المواقع ذات المخاطر العالية وتفعيل التدوير الوظيفي لتجنب مخاطر التركيز.

ج. المراجعة الدورية للمهارات والكفاءات ومتطلبات التدريب لضمان انسجامها مع تطور التقنيات والمخاطر السيبرانية.

ح. توفير برنامج حوافز للموظفين، لتعزيز الانتماء وضمان الالتزام التام بالضوابط والتعليمات الخاصة بالمخاطر السيبرانية.

خ. قياس مدى فعالية أنشطة المرونة السيبرانية واتساقها مع أنشطة الأعمال في المصرف، ورفع التقارير لمجلس الإدارة بالخصوص.

د. ضمان امتثال الموظفين لسياسات ومعايير المرونة والأمن السيبراني المعتمدة في المصرف، ومحاسبة الموظفين على عدم الامتثال لها.

1.3. سياسات وإجراءات الامن السيبراني Cybersecurity Policies and Procedures

الهدف: ضمان توثيق متطلبات الامن السيبراني والتزام المصرف بها، وذلك وفقاً لاحتياجات العمل والمخاطر التنظيمية فيها ومتطلبات سلطة النقد ذات العلاقة.

الضوابط: يجب على المصرف الالتزام بالآتي:

- 1.3.1. تحديد سياسات وإجراءات الامن السيبراني والتأكد من انها تتناسب واحتياجاتها والمخاطر المحيطة بها وان تتوافق ومتطلبات سلطة النقد، وتوثيقها واعتمادها من قبل مجلس الإدارة أو من يفوضه، وتعميمها على ذوي العلاقة من الاطراف المعنية بها خاصة الموظفين.
- 1.3.2. ان تحتوي السياسة على المقدمة، الهدف، النطاق، المهام والمسؤوليات، متطلبات السياسة، المراجعة، التحديث والموافقة.
- 1.3.3. توزيع السياسات وإجراءات الامن السيبراني ضمن المهام والمسؤوليات للموظفين كل حسب مهامه.
- 1.3.4. ضمان تطبيق سياسات وإجراءات الامن السيبراني.
- 1.3.5. أن تستند سياسات وإجراءات الامن السيبراني على معايير تقنية.
- 1.3.6. مراجعة سياسات وإجراءات ومعايير الامن السيبراني بناء على النهج القائم على المخاطر وتحديثها على الأقل مرة واحدة سنوياً أو في حالة حدوث تغييرات في متطلبات سلطة النقد والمعايير ذات العلاقة، وتوثيق هذه التغييرات والتحديثات بما يشمل قائمة المراجعين واعتمادها حسب الأصول.

1.4. أدوار ومسؤوليات الأمن السيبراني Cybersecurity Roles and Responsibilities

الهدف: ضمان تحديد أدوار ومسؤوليات واضحة لجميع الأطراف المعنية في تطبيق ضوابط الامن السيبراني في المصرف.

الضوابط: يجب على المصرف الالتزام بالآتي:

- 1.4.1. تحديد واعتماد الهيكل التنظيمي لحوكمة الأمن السيبراني، وتوضيح الادوار والمسؤوليات الخاصة بالأمن السيبراني، وتكليف الاشخاص المعنيين بها، وتوفير الدعم اللازم لإنفاذ ذلك، مع الأخذ بعين الاعتبار عدم تعارض المصالح ومبدأ الفصل في الصلاحيات.
- 1.4.2. مراجعة أدوار ومسؤوليات الامن السيبراني في المصرف وتحديثها مرة واحدة سنوياً (أو في حالة حدوث تغييرات في متطلبات سلطة النقد ذات العلاقة).
- 1.4.3. التأكد من وضوح المهام وتوفير فصل ما بين مهام موظف امن المعلومات في دائرة المخاطر وموظف امن المعلومات في دائرة تكنولوجيا المعلومات بما يشمل رفع التقارير الرقابية.

1.5. إدارة مخاطر الأمن السيبراني Cybersecurity Risk Management

الهدف: ضمان إدارة مخاطر الامن السيبراني وفق منهجية تهدف إلى حماية أصول المصرف المعلوماتية والتقنية، وذلك وفقاً للسياسات والاجراءات التنظيمية للمصرف ومتطلبات سلطة النقد ذات العلاقة.

الضوابط: يجب على المصرف الالتزام بالآتي:

- 1.5.1. تحديد وتوثيق واعتماد وتطبيق منهجية وإجراءات إدارة مخاطر الامن السيبراني وفقاً لاعتبارات السرية وتوافر وسلامة الاصول المعلوماتية والتقنية.
- 1.5.2. تنفيذ إجراءات تقييم مخاطر الامن السيبراني بحد أدنى في الحالات التالية:
 - أ. في مرحلة مبكرة من المشاريع التقنية.
 - ب. قبل إجراء تغيير جوهري في البنية التقنية.
 - ت. عند التخطيط للحصول على خدمات إسناد خارجي.

ث. عند التخطيط وقبل إطلاق منتجات وخدمات تقنية جديدة.

1.5.3. التأكد من شمول برنامج تقييم مخاطر الأمن السيبراني في المصرف بالحد الأدنى على:

- أ. تحديد وتوثيق نقاط الضعف في أصول البيئة التكنولوجية.
- ب. تحديد وتوثيق التهديدات الداخلية والخارجية الناتجة عن نقاط الضعف المحددة.
- ت. تحديد وتوثيق التأثيرات المحتملة على العمليات والخدمات في المصرف.
- ث. تحديد المخاطر بناء على ما تم تحديده من نقاط ضعف وتهديدات واحتمالات والتأثيرات.
- ج. تحديد وتوثيق طرق الاستجابة للمخاطر وتحديد أولوياتها.

1.5.4. إجراءات وآلية تقييم المخاطر:

يجب على المصرف الالتزام بالآتي:

- أ. تقييم مخاطر الأمن السيبراني من خلال تحديد أصول المصرف من معلومات وأنظمة، وتحديد العمليات والإجراءات والوظائف ونظم المعلومات الحرجة والتي قد تؤثر على هذه الأصول وسبل الوصول إليها بما في ذلك الأنظمة الداخلية والخارجية بشكل دوري أو عند إجراء أي تغيير جوهري.
- ب. إعداد وتطبيق الضوابط الإدارية لتقييم المخاطر لكل أصل من أصول المصرف، لتحديد الثغرات التي يمكن استغلالها في تهديدات محتملة قد تؤثر على سرية أو سلامة أو توافر هذا الأصل.
- ت. إجراء تحليل فجوات وتقييم للمخاطر السيبرانية Gap Analysis and Risk Assessments بشكل سنوي أو عند إجراء أي تغييرات جوهريّة، لتحديد مدى كفاية الضوابط المطبقة، وفعالية خطط الاستجابة والاسترجاع. بالإضافة إلى ذلك، على المصرف وضع خطة لمعالجة أي ثغرات يتم اكتشافها على الفور.
- ث. على الإدارة العليا تحديد مسؤولية إدارة مخاطر الأمن السيبراني (فريق، لجنة، إلخ) في المصرف، ووفقاً لذلك، يجب أن تقوم الجهة المعنية بإدارة مخاطر الأمن السيبراني في دائرة المخاطر بتحديد مخاطر تكنولوجيا المعلومات وعملية قبول المخاطر، ومراجعة وتقييم الحوادث التي تتعلق بعدم الامتثال لسياسات إدارة بيئة تكنولوجيا المعلومات، بحيث تتضمن العملية بالحد الأدنى ما يلي:

1. تقييم المخاطر ووصفها واعتمادها من مالك المخاطر Risk Owner والإدارة العليا.
 2. تحديد ضوابط تخفيف أثر المخاطر Mitigating Controls.
 3. إعداد خطة تصحيحية لتقليل أثر تلك المخاطر Remedial Plan.
- ج. تحديد المخاطر من خلال (مصفوفة مخاطر) وتحديد الأثر (مالي/ تشغيلي) على أصول المصرف المترتب عن كل تهديد، ومن ثم عمل التحليل النوعي والكمي للأثر، بحيث يعتمد مدى تأثير المخاطر على احتمالية حدوث الترابط بين التهديدات والثغرات القادرة على التسبب بالحاق ضرر على أصول المصرف عند وقوع الحدث.
- ح. تطوير مصفوفة تهديدات ونقاط ضعف (Threat and Vulnerability Matrix) بهدف تقييم تأثير التهديد على بيئة تكنولوجيا المعلومات وتحديد أولويات الاستجابة والتعامل معها.
- خ. إن تتضمن عملية تقييم المخاطر السيبرانية تحديد الأحداث والأنشطة التي يمكن أن تتسبب في تعطيل العمليات الحرجة في المصرف، أو تشكل مخاطر مرتبطة بالسمعة أو الأرباح، وتقييم الامتثال للمتطلبات التنظيمية الخاصة بتقييم المخاطر.
- د. إجراء تقييم التهديدات Threat Assessment التي قد تنشأ من داخل أو خارج المصرف، بما يغطي التهديدات المحتملة مثل: الطبيعية، الحروب، الحوادث، التهديدات والبرمجيات الخبيثة.

ذ. إجراء تقييم الثغرات Vulnerability Assessment بحيث يتم تحديد كل ثغرة واحتمالية استغلالها، بالإضافة لتقييم السياسات والإجراءات والمعايير والضوابط المادية والتقنية وما إلى ذلك.

1.5.5. مراجعة منهجية وإجراءات إدارة مخاطر الامن السيبراني وتحديثها مرة واحدة على الأقل سنويا (أو في حالة حدوث تغييرات في متطلبات سلطة النقد والمعايير ذات العلاقة)، كما يجب توثيق التغييرات واعتمادها.

1.5.6. إنشاء سجل مخاطر الامن السيبراني الخاص بالأنظمة الحرجة، ومتابعته بشكل دوري.

1.6. الامن السيبراني ضمن إدارة المشاريع Cybersecurity in Projects Management

الهدف: التأكد من تطبيق متطلبات الامن السيبراني ضمن سياسة وإجراءات إدارة مشاريع المصرف لحماية السرية وسلامة الاصول المعلوماتية والتقنية للمصرف ودقتها وتوافرها، وذلك وفقا للسياسات والإجراءات التنظيمية للمصرف ومتطلبات سلطة النقد ذات العلاقة.

الضوابط: يجب على المصرف الالتزام بالآتي:

1.6.1. تضمين متطلبات الامن السيبراني في منهجية وإجراءات إدارة المشاريع وإدارة التغيير على الاصول المعلوماتية والتقنية في المصرف لضمان تحديد مخاطر الامن السيبراني ومعالجتها كجزء من دورة حياة المشروع.

1.6.2. أن تغطي متطلبات الامن السيبراني لإدارة المشاريع والتغييرات على الاصول المعلوماتية والتقنية للمصرف بالحد الأدنى ما يلي:

أ. تقييم الثغرات ومعالجتها.

ب. اجراء فحص الاختراق وتقييم أمني (Penetration Testing and Security Assessment) للبنية التحتية وتطبيقات الويب وواجهة برمجة التطبيقات (APIs) وتطبيقات الهاتف المحمول.

ت. اجراء مراجعة للإعدادات والتدعيم (Hardening and Configuration Secure) وحزم التحديثات قبل إطلاق المشاريع والتغييرات.

ث. تنفيذ اختبارات التحمل (Stress Testing) للتأكد من سعة وكفاية مكونات البنية التكنولوجية المختلفة.

ج. التأكد من تطبيق متطلبات استمرارية العمل ذات العلاقة.

1.6.3. أن تغطي متطلبات الامن السيبراني لمشاريع تطوير التطبيقات والبرمجيات الخاصة للمصرف بحد أدنى ما يلي:

أ. استخدام معايير التطوير الآمن للتطبيقات (Secure Coding Standards) بما يشمل تأمين الوصول، والتخزين، والتوثيق لكود البرامج واصداراتها، واجراء مراجعة أمنية لكود البرامج والأنظمة قبل اطلاقها (Security Source Code Review).

ب. استخدام مصادر مرخصة وموثوقة لأدوات تطوير التطبيقات (Applications Libraries).

ت. اجراء اختبار للتحقق من مدى استيفاء التطبيقات للمتطلبات الامنية السيبرانية للمصرف.

ث. التأكد من مدى أمن التكامل بين التطبيقات (Integration).

ج. تطبيق الضوابط الأمنية اللازمة لتأمين واجهة برمجة التطبيقات (Authenticated API).

ح. تطبيق الضوابط التي تضمن النقل الآمن والموثوق للتطبيقات من بيئات الاختبار (Testing Environment) الى بيئات الإنتاج (Production Environment) مع حذف أي بيانات او هويات او كلمات مرور متعلقة ببيئات الاختبار، قبل النقل.

1.6.4. مراجعة متطلبات الامن السيبراني في إدارة المشاريع في المصرف من جهة مستقلة داخلية/ او خارجية متخصصة وقبل إطلاق المشروع في البيئة الحية.

1.7. المراجعة والتدقيق الدوري للأمن السيبراني Cybersecurity Periodical Assessment and Audit

الهدف: التأكد من أن ضوابط الامن السيبراني لدى المصرف مطبقة وفقا للسياسات والاجراءات التنظيمية للمصرف، ومتطلبات سلطة النقد ذات العلاقة.

الضوابط: يجب على المصرف الالتزام بالآتي:

- 1.7.1. متابعة تطبيق ضوابط الامن السيبراني.
- 1.7.2. مراجعة وتدقيق تطبيق ضوابط الامن السيبراني في المصرف، من قبل أطراف مستقلة عن الادارة المعنية بالأمن السيبراني (مثل دائرة التدقيق الداخلي في المصرف).
- 1.7.3. توثيق نتائج مراجعة وتدقيق الامن السيبراني ووضع خطط عمل تصحيحية ووقائية واضحة لمعالجة المشاكل والمخاطر مع الاخذ بعين الاعتبار مخاطر وأولوية الثغرات، وعرضها على اللجنة الاشرافية للأمن السيبراني والإدارة العليا.

1.8. الامن السيبراني المتعلق بالموارد البشرية Cybersecurity in Human Resources

الهدف: ضمان المعالجة الفعالة لمخاطر ومتطلبات الامن السيبراني المرتبطة بالموظفين (موظفين ومتقاعدين) في المصرف قبل وأثناء وعند انتهاء/إنهاء عملهم، وذلك وفقا للسياسات والاجراءات التنظيمية للمصرف، ومتطلبات سلطة النقد ذات العلاقة.

الضوابط: يجب على المصرف الالتزام بالآتي:

- 1.8.1. تحديد واعتماد وتطبيق متطلبات الامن السيبراني المتعلقة بالموظفين قبل توظيفهم وأثناء عملهم وعند انتهاء/إنهاء عملهم.
- 1.8.2. أن تغطي متطلبات الامن السيبراني قبل بداية عمل الموظفين بالمصرف بالحد الأدنى ما يلي:
 - أ. تضمين مسؤوليات الامن السيبراني ومتطلبات المحافظة على سرية المعلومات (Clauses Non-Disclosure) في عقود الموظفين في المصرف (لتشمل خلال وبعد انتهاء/إنهاء العلاقة الوظيفية مع المصرف).
 - ب. إجراء المسح الأمني (Vetting or Screening) للموظفين والمتقاعدين في وظائف الامن السيبراني والوظائف التقنية ذات الصلاحيات الهامة والحساسة.
 - ت. ان تكون متطلبات الامن السيبراني المتعلقة بالموظفين والمتقاعدين واضحة ومتاحة للجميع ضمن سياسة الامن السيبراني للمصرف، والتأكد من وعي الموظفين وإدراكهم وامتثالهم لما تتضمنه السياسة.
 - ث. تحديد الاجراءات التأديبية في حالة مخالفة السياسات والاجراءات المرتبطة بالأمن السيبراني كجزء من سياسة الموارد البشرية.
 - ج. الاخذ بعين الاعتبار تقييم مخاطر المستخدمين الداخليين بما يشمل مخاطر تغيير/اتلاف/حذف البيانات والنسخ الاحتياطية، تعطيل الأنظمة، إساءة استخدام الأنظمة لتحقيق مكاسب شخصية، احتجاز/ سرقة بيانات المصرف الاستراتيجية أو بيانات العميل الخاصة من خلال التجسس أو الاحتيال.
 - ح. ان يشغل وظائف الدعم، والتطوير التقني، والإدارة المعنية بالأمن السيبراني موظفون ذوو كفاءة عالية.
- 1.8.3. أن تغطي متطلبات الامن السيبراني خلال عمل الموظفين بالمصرف بحد أدنى ما يلي:
 - أ. التوعية بالأمن السيبراني.
 - ب. تطبيق متطلبات الامن السيبراني والالتزام بها وفقا لسياسات واجراءات وعمليات الامن السيبراني للمصرف.
- 1.8.4. مراجعة وإلغاء الصلاحيات للموظفين مباشرة بعد انتهاء/إنهاء الخدمة لهم بالمصرف.
- 1.8.5. مراجعة متطلبات الامن السيبراني المتعلقة بالموظفين في المصرف دورياً.

1.9.1. التوعية والتدريب بالأمن السيبراني Cybersecurity Awareness and Training

الهدف: التأكد من حصول الموظفين والأطراف الخارجية على التدريب والتوعية اللازمة بواجباتهم ومسؤولياتهم في مجال الامن السيبراني بما يتوافق مع السياسات والإجراءات ذات الصلة، والتأكد من تزويد الموظفين بالمهارات والمؤهلات والدورات التدريبية اللازمة لحماية الأصول المعلوماتية والتقنية للمصرف والقيام بمسؤولياتهم تجاه الامن السيبراني.

الضوابط: يجب على المصرف الالتزام بالآتي:

- 1.9.1. تطوير واعتماد وتطبيق برنامج للتوعية بالأمن السيبراني في المصرف من خلال كافة الوسائل المتاحة دورياً، لتعزيز الوعي بالأمن السيبراني وتهديداته ومخاطره.
- 1.9.2. أن يغطي برنامج التوعية بالأمن السيبراني كيفية حماية المصرف من أهم المخاطر والتهديدات السيبرانية وما يستجد منها مثل: (رسائل التصيد الإلكتروني، هجمات التصيد، Anti-Phishing، كذلك التعامل الآمن مع (الأجهزة المحمولة ووسائل التخزين، خدمات تصفح الانترنت، وسائل التواصل الاجتماعي).
- 1.9.3. توعية عملائه عبر برامج ونشرات توعية للتواصل معهم فيما يتعلق برسائل البريد الإلكتروني المخادعة والمشبوهة (phishing and suspicious emails)، وذلك من خلال كافة وسائل الاتصال المتاحة.
- 1.9.4. توفير المهارات المتخصصة والتدريب اللازم للموظفين في المجالات الوظيفية ذات العلاقة بالأمن السيبراني في المصرف، بما يشمل (مطورو البرامج والتطبيقات ومشغلو الأنظمة، الوظائف الاشرافية والتنفيذية).
- 1.9.5. مراجعة تطبيق برنامج التوعية بالأمن السيبراني في المصرف دورياً.

2. ضوابط تعزيز الامن السيبراني Cybersecurity Defense Controls

2.1. إدارة الأصول Asset Management

الهدف: ضمان تصنيف وإدارة أصول المعلومات للمصرف بشكل آمن وفعال، بما يشمل (الأجهزة والأنظمة والتطبيقات وقواعد البيانات وخطوط الاتصال، ... الخ)، من اجل دعم العمليات التشغيلية ومتطلبات الامن السيبراني فيه، بما يحقق سرية وسلامة الأصول المعلوماتية والتقنية للمصرف ودقتها وتوافرها.

الضوابط: يجب على المصرف الالتزام بالآتي:

- 2.1.1. تحديد واعتماد اجراءات تصنيف وإدارة أصول المعلومات في المصرف وتنفيذها ومراقبتها ومراجعتها وتحديثها دورياً لتأمين الأصول خلال دورة حياتها.
- 2.1.2. أن تحدد عملية إدارة الأصول دور مالك الأصول Asset Owner والمستخدمين المستهدفين، ويجب أن تتضمن ضوابط لتحديد وحماية ومراقبة أصول المعلومات.
- 2.1.3. تحديد واعتماد سياسة الاستخدام المقبول لأصول المعلومات Policy for Acceptable Use وتنفيذها ومراجعتها بشكل دوري.
- 2.1.4. تحديد جميع أصول المعلومات في المصرف والاحتفاظ بقائمة جرد في سجل الأصول، على أن يحتوي سجل الأصول بالحد الأدنى على اسم الأصل والوصف والمالك والتصنيف.
- 2.1.5. وجود آلية فعالة للكشف عن الأصول (الأنظمة والتطبيقات) وتفصيلها Asset detection and inventory من خلال برامج مخصصة ومرخصة لذلك، قادرة على اكتشاف أي أنظمة أو تطبيقات غير مصرح بها.
- 2.1.6. تصنيف أصول المعلومات بالاستناد لنهج قائم على المخاطر وفقاً لقيمتها وأهميتها ومدى حساسيتها والمتطلبات القانونية.
- 2.1.7. فصل التطبيقات عالية الخطورة مادياً (Physically) أو منطقياً (Logically).

2.1.8. أن تكون إجراءات اقتناء أصول المعلومات متوافقة مع إجراءات الشراء المعتمدة في المصرف وبما يتوافق مع سياسة أمن المعلومات المعتمدة.

2.1.9. تحديد واعتماد إجراءات اتلاف أصول المعلومات وتنفيذها ومراجعتها بانتظام.

2.1.10. التخلص من المعلومات الحساسة الموجودة في أصول المعلومات (اتلافها) عن طريق تقنيات مناسبة تجعل المعلومات غير قابلة للاسترداد مثل (secure erase, secure wiping, double crosscut, shredding).

2.1.11. تحديد عملية إدارة وتصنيف الأصول وتطبيقها بما يضمن الكشف المبكر عن استخدام الأصول غير المصرح بها ومنع استخدامها.

2.1.12. اعتماد آلية لتدريب وتوعية الموظفين والمتعاقدين بالضوابط الخاصة بالاستخدام المسموح لأصول المصرف من أنظمة وأجهزة وبيانات ... الخ.

2.2. إدارة هويات الدخول والصلاحيات Identity and Access Management

الهدف: ضمان اقتصار الوصول الى أصول المصرف المعلوماتية والتقنية على المستخدمين والعمليات والأجهزة المصرح لهم، وأن يتم تقييد صلاحيات الوصول بالحد الأدنى المطلوب لإنجاز الاعمال المتعلقة بالمصرف.

الضوابط: يجب على المصرف الالتزام بالآتي:

2.2.1. تحديد وتوثيق واعتماد وتطبيق متطلبات الامن السيبراني لإدارة هويات الدخول والصلاحيات في المصرف ضمن سياسة إدارة الوصول وتنفيذها ومراجعتها بشكل دوري، وأن تستند السياسة على متطلبات العمل والممارسات الفضلى الخاصة بأمن المعلومات لإدارة صلاحيات الوصول.

2.2.2. أن تغطي متطلبات الامن السيبراني المتعلقة بإدارة هويات الدخول والصلاحيات في المصرف بحد أدنى ما يلي:

أ. التحقق من هوية المستخدم (User Authentication) بناء على إدارة تسجيل المستخدم، وإدارة كلمة المرور.

ب. تطبيق مبدأ التحقق من الهوية متعدد العناصر (Multi-Factor Authentication) لعمليات الدخول عن بُعد لجميع المستخدمين وذوي الصلاحيات العالية والحساسة منهم، وعلى الأنظمة المستخدمة لإدارة الأنظمة الحساسة ومتابعتها.

ت. إدارة صلاحيات المستخدمين (Authorization) بالاستناد الى مبادئ التحكم بالدخول والصلاحيات (مبدأ الحاجة إلى المعرفة والاستخدام "Need-to-know and Need-to-use"، ومبدأ الحد الأدنى من الصلاحيات والامتيازات "Privilege

Least"، ومبدأ فصل المهام "Segregation of Duties").

ث. مراجعة واتباع منهجية بنية الوصول الأمن Zero Trust للهوية.

ج. التأكد من تعريف جميع الموظفين، بأسماء مستخدمين واضحة تدل على أصحابها وتجنب الأسماء العامة و (Shared accounts)، لضمان المتابعة الفعالة والمساءلة على ما يتم تنفيذه من أنشطة.

ح. أن تستند عملية منح صلاحيات الوصول لبيانات وأنظمة المصرف إلى المصفوفة المعتمدة للتحكم في الوصول (Access Control Matrix).

خ. إيقاف أو تغيير أسماء المستخدمين الرئيسية والعامة ذات الصلاحيات الواسعة (administrator) على الأنظمة وكلمات المرور الخاصة بها وتوفير آلية لتوثيقها ومراقبة وتسجيل استخدامها على الأنظمة من خلال موافقات إدارية.

د. إدارة صلاحيات الوصول الهامة والحساسة (Privileged Access Management) من خلال اعتماد آلية لتسجيل ومتابعة الأعمال والتغييرات التي يتم تنفيذها على الأنظمة والبيانات الحساسة باستخدام هذه الصلاحيات.

ذ. القيام بمراجعة دورية لهويات الدخول والصلاحيات الممنوحة على أنظمة المصرف بشكل دوري.

ر. الإدارة الآمنة لحسابات الخدمات (Service Account) ما بين التطبيقات والأنظمة، وتعطيل الاستخدام البشري لهذه الحسابات (Interactive login).

ز. منع الوصول أو التعامل المباشر لأي مستخدم مع قواعد البيانات بما يشمل مشرفي قواعد البيانات (DBA) أو المستخدمين المخولين بذلك إلا من خلال نظام إدارة صلاحيات الدخول Privilege Access Managment، وبخلاف ذلك يتم من خلال التطبيقات فقط، وبناء على الصلاحيات المخول بها، مع مراعاة تطبيق معايير أمنية تحد أو تمنع من إطلاع مشرفي قواعد البيانات على البيانات المصنفة (Classified Data).

س. توزيع الصلاحيات والمسؤوليات على الأنظمة والبيانات، المتعلقة بتنفيذ المهام الحرجة والحساسة، باستخدام مبادئ الفصل في الصلاحيات لتجنب مخاطر تركّز الصلاحيات على العمليات الحرجة للمصرف.

ش. تطبيق ضوابط آمنة على تخزين معلومات المصادقة للمستخدمين (Users Authentication Information) وأثناء إرسالها.

ص. مراقبة تسجيلات الدخول المتزامنة (Concurrent logins) لنفس المستخدم ومنعها على الأنظمة والتطبيقات الحساسة.

ض. توفير التوثيق والمراقبة المناسبة لسجلات التدقيق (Audit records) لجميع أنشطة إدارة الوصول ووصول المستخدمين.

2.2.3. إدارة كلمة المرور Password Management

أ. توثيق واعتماد سياسة شاملة لإدارة كلمات المرور (Password Management Policy) بما يتوافق مع أحد المعايير العالمية وتطبيقها ومراجعتها بشكل دوري.

ب. أن تتضمن سياسة إدارة كلمات المرور متطلبات التعقيد (complexity) وسجل كلمة المرور password history ، وقفل الحساب account lockout، والحد الأقصى لعمر كلمة المرور maximum password age، والحد الأدنى لطول كلمة المرور minimum password length، وإجراءات تسجيل الدخول الآمن.

ت. ألا يقل طول كلمة المرور عن ثمانية أحرف، وأن تتضمن حروف وأرقام ورموز خاصة special characters.

ث. تغيير جميع كلمات مرور الحسابات الافتراضية والمعروفة للعامة systems default, vendor supplied and publicly documented accounts passwords (بما في ذلك حسابات الخدمة service accounts).

ج. اعتماد إجراءات إبلاغ/ تسليم كلمات المرور للمستخدم بطريقة آمنة لضمان وصولها للمستخدم المقصود.

ح. استخدام المصادقة متعددة العوامل multi-factor authentication (مثل كلمة المرور لمرة واحدة OTP أو المصادقة باستخدام Token) للمستخدمين الذين لديهم صلاحيات وامتيازات وصول عالية privileged or administrative or elevated access على الأنظمة والبيانات.

خ. اعتماد وتطبيق سياسة آمنة خاصة بمعايير أمن وحماية كلمات المرور والاستناد للممارسات الفضلى المعمول بها بالخصوص.

د. استخدام الطرق والخوارزميات الآمنة لحفظ ومعالجة كلمات المرور مثل استخدام (Hashing Functions).

2.2.4. القيام بمراجعة دورية لمدى تطبيق متطلبات الامن السيبراني لإدارة هويات الدخول وصلاحيات المستخدمين.

2.3. حماية الأنظمة وأجهزة معالجة المعلومات Information System and Processing Facilities Protection

الهدف: ضمان حماية الأنظمة وأجهزة معالجة المعلومات بما في ذلك أجهزة المستخدمين والبنى التحتية للمصرف من المخاطر السيبرانية.

الضوابط: يجب على المصرف الالتزام بالآتي:

2.3.1. تحديد وتوثيق واعتماد وتطبيق متطلبات الامن السيبراني لحماية الأنظمة وأجهزة معالجة المعلومات فيه.

2.3.2. أن تغطي متطلبات الامن السيبراني لحماية الأنظمة وأجهزة معالجة المعلومات للمصرف بالحد الأدنى ما يلي:

أ. الحماية من الفيروسات والبرامج والأنشطة المشبوهة والبرمجيات الضارة (Malware) على أجهزة المستخدمين والخوادم باستخدام تقنيات وآليات الحماية الحديثة والمتقدمة، وإدارتها بشكل آمن، على أن تشمل بالحد الأدنى ما يلي:

1. APT Protection.
2. Endpoint Detection and Response EDR.
3. Micro segmentation.
4. Threat hunting.
5. Hardening and Compliance.
6. Resource monitoring.

ب. التقييد الحازم لاستخدام أجهزة وسائط التخزين الخارجية وضمان الاستخدام الآمن لها.

ت. إدارة حزم التحديثات والصلاحيات على الأنظمة والتطبيقات والأجهزة (Patch Management).

ث. السماح فقط بقائمة محددة من ملفات التشغيل (whitelisting) للتطبيقات والبرامج، للعمل على الخوادم الخاصة بالأنظمة الحساسة.

ج. حماية الخوادم الخاصة بالأنظمة بتقنيات حماية الأجهزة الطرفية (End-Point Protection) المعتمدة لدى المصرف.

ح. تطبيق حزم التحديثات والإصلاحات الأمنية على الأنظمة بشكل مستمر مع اتباع آليات إدارة التغييرات المعتمدة لدى المصرف.

خ. تخصيص أجهزة حاسوب (Workstations) للعاملين في الوظائف التقنية ذات الصلاحيات الهامة والحساسية على الشبكة والأنظمة، على أن تكون معزولة في شبكة خاصة بإدارة الأنظمة والشبكة (Network Management).

د. تشفير عملية الوصول الإشرافي عبر الشبكة (Non-console Administrator Access) لأي من المكونات التقنية للأنظمة والشبكة، باستخدام خوارزميات وبروتوكولات التشفير الآمنة.

ذ. مراجعة إعدادات الأنظمة وتحسينها (Secure configuration and Hardening) كل ستة أشهر على الأقل.

ر. مراجعة الإعدادات المصنعية (Default configuration) وتعديلها والتأكد من عدم وجود كلمات مرور ثابتة، وخلفية، واقتراضية (Hard-Coded, Backdoor and Default Passwords).

ز. حماية السجلات والملفات الحساسة للأنظمة من الوصول غير المصرح به، أو العبث، أو التغيير، أو الحذف غير المشروع.

س. مزامنة التوقيت (Clock Synchronization) مركزياً وضمان اتصال أجهزة الشبكة والبنية التحتية بخادم مزامنة التوقيت.

2.4. اقتناء وتطوير البرمجيات Software Development and Acquisition

الهدف: ضمان أمن ومرونة وسلامة كافة الأنظمة والتطبيقات والبرامج التي تم تطويرها أو تم الاستعانة بمصادر خارجية أو شراؤها.

أمن البرمجيات Software Security

يجب على المصرف الالتزام بالآتي:

2.4.1. إعداد واعتماد والمراجعة الدورية لمتطلبات الأمن السيبراني وإجراءات تطوير التطبيقات وخدمات الويب الآمنة وفقاً للمعايير العالمية.

2.4.2. التأكد من عزل بيانات الاختبار والتطوير عن أنظمة المصرف الحية Production Systems، وأن يتم منح الوصول إلى هذه البيانات والأنظمة للمستخدمين المصرح لهم بناءً على موافقات معززة بمتطلبات العمل.

2.4.3. توضيح وتصنيف التطبيقات التي يتم تطويرها داخل المصرف وما يتم شراؤه من الخارج وفقاً لسياسة التصنيف.

2.4.4. مراجعة النصوص البرمجية Source code review للبرامج المطورة داخلياً أو الحصول على شهادة فحص للبرامج المطورة خارجياً للتأكد من عدم وجود كود خبيث يسمح بإنشاء أي اتصالات خارجية، وللعثور على الثغرات الأمنية الناشئة عن coding issues أو poor coding practices أو المحاولات الخبيثة malicious attempts.

2.4.5. أن يحصل المصرف على نسخة من الكود البرمجي source code للتطبيقات الحرجة المطورة والاحتفاظ بها في مكان امن ضمن ضوابط، وإذا لم يكن ذلك ممكناً على المصرف القيام بإجراءات تعاقدية لضمان توفر نسخة من الكود البرمجي لدى طرف ثالث arranging an escrow for the source code.

2.4.6. إجراء فحوصات سلامة البيانات Integrity checks على البرامج والأنظمة.

2.4.7. استضافة الخوادم والأنظمة عالية المخاطر والتي تتصل بالشبكات العامة في منطقة منعزلة DMZ ووضع الإجراءات اللازمة لتطبيق متطلبات (Zero trust, Segmentation and micro segmentation).

2.5. حماية البريد الإلكتروني E-mail Protection

الهدف: ضمان حماية البريد الإلكتروني للمصرف من المخاطر السيبرانية.

الضوابط: يجب على المصرف الالتزام بالآتي:

2.5.1. تحديد وتوثيق واعتماد وتطبيق متطلبات الامن السيبراني لحماية البريد الإلكتروني.

2.5.2. أن تغطي متطلبات الامن السيبراني لحماية البريد الإلكتروني بحد أدنى ما يلي:

أ. اتخاذ الإجراءات والضوابط اللازمة لعدم استخدام البريد الإلكتروني العام (Public Email Accounts) ضمن شبكة وأنظمة المصرف مثل (Gmail, Hotmail, ..etc.).

ب. توعية المستخدمين بالمبادئ الأساسية للاستخدام الآمن للبريد الإلكتروني مثل (عدم فتح الرسائل مجهولة المصدر، وعدم تحميل المرفقات غير الموثوقة وغير معلومة المصدر، عدم الاحتفاظ برسائل البريد المؤذي Spam Mails، ضرورة إبلاغ فريق أمن المعلومات عن الرسائل غير موثوقة المصدر).

ت. توعية المستخدمين بمفهوم الهندسة الاجتماعية (Social Engineering) وعدم الكشف عن معلوماتهم الشخصية والمالية لمصادر غير موثوق بها سواء عبر البريد الإلكتروني أو مواقع التواصل الاجتماعي.

ث. تحليل وتصفية رسائل البريد الإلكتروني (Filtering) (وخصوصاً رسائل التصيد الإلكتروني "Emails Phishing" والرسائل العشوائية "Spam Emails") باستخدام تقنيات وآليات الحماية الحديثة والمتقدمة للبريد الإلكتروني. ج. تعزيز ضوابط وإعدادات خوادم البريد الإلكتروني ونظام أسماء النطاقات DNS، وفقاً لأفضل الممارسات المتبعة بالخصوص مثل Sender Policy Framework (SPF)، و Domain Keys Identified Mail (DKIM)، والتوقيع الرقمي digital signing لمنع التصيد الاحتيالي.

ح. التحقق من الهوية متعدد العناصر (Multi-Factor Authentication) للدخول عن بُعد والدخول عن طريق صفحة موقع البريد الإلكتروني (Webmail).

خ. النسخ الاحتياطي وأرشفة البريد الإلكتروني.

د. الحماية من الهجمات الإلكترونية المتقدمة مثل (APT Protection)، التي تستخدم عادة الفيروسات والبرمجيات الضارة غير المعروفة مسبقاً (Malware Zero-Day)، وإدارتها بشكل آمن.

2.5.3. مراجعة تطبيق متطلبات الامن السيبراني الخاصة بحماية البريد الإلكتروني للمصرف دورياً، على أن تشمل الآتي:

أ. ضوابط حماية البريد الإلكتروني و APT Sandbox.

ب. تصنيف رسائل البريد الإلكتروني.

ت. حماية البريد الإلكتروني من فقدان والتسرب من خلال DLP.

ث. حماية سرية البريد الإلكتروني من خلال تشفير البيانات بين الطرفين المرسل والمستقبل حسب سياسة تصنيف البيانات المعتمدة في المصرف.

2.6. إدارة أمن البنية التحتية والشبكات Infrastructure and Networks Security Management

الهدف: ضمان تصميم بنية البيئة التكنولوجية والشبكات للمصرف بشكل آمن ومتناسق يراعي الممارسات الفضلى المطبقة لمبادئ الأمن السيبراني.

الضوابط: يجب على المصرف الالتزام بالآتي:

- 2.6.1. تحديد وتوثيق واعتماد وتطبيق متطلبات الامن السيبراني لإدارة أمن البنية التحتية وشبكات المصرف.
- 2.6.2. أن تغطي متطلبات الامن السيبراني لإدارة أمن البنية التحتية وشبكات المصرف بحد أدنى ما يلي:
 1. أن يضمن تصميم البنية التحتية والشبكات حماية سرية معلومات المصرف وسلامتها وتوافرها وأن يتم تصميمها لتجنب تعطل الخدمة وتقليل المساحة المعرضة للهجوم وتقليل التأثير على عمليات وخدمات المصرف واكتشاف التهديدات بسهولة.
 2. العزل والتقسيم المادي (Physically using for example: Routers, Switches, Firewalls)، والمنطقي (Logically using for example: VLAN, DMZ) لمكونات شبكات المصرف بشكل آمن، والالتزام بما يضمن السيطرة على مخاطر الامن السيبراني ذات العلاقة باستخدام مبدأ الدفاع الامني متعدد المراحل (Defense-in-Depth)، وبالاتناد الى الضوابط والتوصيات المعمول بها في المعايير العالمية بالخصوص.
 3. عزل بيئات التطوير والاختبار عن شبكة بيئة الإنتاج (Production Environment).
 4. تطبيق أنظمة الحماية المتقدمة لاكتشاف ومنع الاختراقات (IPS/IDS) على الشبكة الحرجة الداخلية والخارجية لحماية شبكة المصرف من الاختراق.
 5. تجنب وجود نقاط فشل أحادية في تصميم وتطبيق شبكة الإنتاج الخاصة بالمصرف (Single point of failer) بما يضمن استمرارية العمل.
 6. توفير كشف محدث بمكونات شبكة المصرف (Detailed Inventory) يشمل الأجهزة والخوادم والأنظمة المستخدمة في إدارة الشبكة.
 7. اعتماد وتوثيق اعدادات أجهزة الشبكة وتحديثها بعد كل تغيير، والقيام بمراجعة دورية لهذه الاعدادات ومقارنتها بالإعدادات المطبقة على أجهزة الشبكة الفعالة لضمان تكاملتها وتحديد أي تغييرات غير مصرح بها.
 8. تطبيق المراقبة الفعالة (24/7) لأنظمة وأجهزة الشبكة والبنية التحتية.
 9. توفير ضوابط لإدارة وحماية السجلات الخاصة بأجهزة الشبكة والبنية التحتية (Logs) بما يضمن منع تعديل/ حذف هذه السجلات، وتوفير المراجعة والنسخ الاحتياطي لها.
 10. اتخاذ التدابير الفنية اللازمة لاتصال أجهزة الضيوف Guest Devices بشبكة منفصلة عن شبكة المصرف.
 11. توفير قنوات اتصال آمنة لإدارة أجهزة الشبكة والبنية التحتية باستخدام بروتوكولات تضمن أمن البيانات أثناء النقل مثل SSH, IPSEC، وكذلك توفير رقابة ثنائية في إدارة هذه الأجهزة.
 12. توفير الحلول التقنية لإدارة الوصول لأجهزة الشبكة والبنية التحتية الحرجة، كتطبيق المصادقة (Authentication)، وتحديد الصلاحيات (Authorization)، وتسجيل الحركات والاحداث التي ينفذها المستخدم (Accounting).
 13. تفعيل خاصية (Audit Trail) على أجهزة الشبكة والبنية التحتية الحرجة لتسجيل النشاطات اليومية على هذه الأجهزة ومراجعتها عند الحاجة.
 14. اتخاذ الإجراءات والضوابط الكفيلة بمنع وصول المستخدمين للمواقع غير المصرح بها أو تحميل برامج غير موثوقة على أجهزة المصرف، وتوفير المراقبة والحماية لاستخدام شبكة الانترنت من خلال (Proxies and filtering gateways).

15. اتخاذ الإجراءات اللازمة لضمان أمن الشبكات اللاسلكية وحمايتها باستخدام وسائل أمانة كالتشفير والتحقق من الهوية، وعدم ربط الشبكات اللاسلكية بالشبكة الداخلية والأنظمة الحساسة للمصرف إلا بناءً على دراسة متكاملة للمخاطر المترتبة على ذلك والتعامل معها بما يضمن حماية الأصول، وتوفير السياسات والإجراءات اللازمة لإدارة أنظمة الشبكة اللاسلكية الخاصة بالمصرف بما يضمن أمن بياناته وتوفير المراقبة الفعالة لاستخدامها والمراجعة الدورية.
16. توفير الضوابط الأمنية لنظام أسماء النطاقات (DNS).
17. حماية قناة تصفح الإنترنت من الهجمات الإلكترونية المتقدمة مثل (APT Protection)، التي تستخدم عادة الفيروسات والبرمجيات الضارة غير المعروفة مسبقاً (Zero-Day Malware)، وإدارتها بشكل آمن.
18. مراجعة إعدادات جدار الحماية (Firewall Rules) وقوائمها، كل ستة أشهر على الأقل.
19. منع التوصيل المباشر لأي جهاز من الشبكة المحلية للأنظمة الحساسة إلا بعد الفحص والتأكد من تطبيق عناصر وضوابط الحماية اللازمة، للمستويات المقبولة للأنظمة الحساسة.
20. عدم إتاحة اتصال الأنظمة الحساسة بالإنترنت في حال كانت تقدم خدمة داخلية للمصرف، وعدم وجود حاجة مرتبطة بمصلحة العمل للوصول للخدمة من خارج شبكة المصرف.
21. السماح بقائمة محدودة (Whitelisting) فقط، لقوائم جدار الحماية الخاصة بالأنظمة الحساسة.
22. تطبيق مبادئ الأمن متعدد المستويات (multi-layer security) والفصل في الصلاحيات ومنح الحد الأدنى من الصلاحيات بناءً على حاجة العمل (least privilege and segregation of duties).
23. توفير القدرة على المراقبة وتسجيل الأحداث وإنشاء التقارير.
24. توفر خطط استمرارية الأعمال وترتيبات التعافي من الكوارث.
25. أن تستند معايير وضوابط الإعدادات الأمنية على أفضل الممارسات العالمية (مثل NIST ومعايير مركز أمان الإنترنت (CIS)) والإرشادات الصادرة عن الشركات المزودة للمعدات الأصلية (OEMs) والسياسات والإجراءات الداخلية المعتمدة والممارسات الفضلى المتبعة.
26. اقتناء وتثبيت إصدارات مرخصة ومحدثة من البرامج.
27. حماية البيانات بما يتماشى مع متطلبات إدارة الأصول وتصنيف المعلومات.
28. تعطيل أو تقييد الوصول إلى الخدمات والمنافذ الضعيفة أو غير الضرورية weak or unnecessary services and ports.
29. تغيير كلمات المرور الافتراضية (Default passwords)، وإزالة أو تعطيل الحسابات/ أسماء الدخول غير الضرورية.
30. تطبيق إجراءات الأمان الخاصة بقتل أو إنهاء الـ sessions (application page logout or logoff or close) بعد فترة محددة مسبقاً من عدم النشاط.
31. مزامنة ساعات النظام مع الساعة المركزية (Synchronizing System Clocks with Central-Clock).

2.6.3. أمن البيئة الافتراضية Virtualization Environment security

يجب على المصرف الالتزام بالآتي:

- أ. تحديد المخاطر المرتبطة بأنظمة وتقنيات البيئة الافتراضية، وإجراء تقييم المخاطر لفهم تأثيرها على البنية التحتية للمصرف.
- ب. تعزيز وتقوية البيئة الافتراضية، وتوفير أنظمة إدارة ومراقبة الأجهزة الافتراضية والأنظمة الأخرى المتصلة بها، مع مراعاة تطبيق الممارسات الفضلى المعمول بها لتأمينها مثل:

1. التأكد من وضع وتطبيق قيود على استخدام موارد البيئة الافتراضية مثل المعالجات والذاكرة ومساحة التخزين وواجهات الشبكة الافتراضية على كل جهاز افتراضي ضمن البيئة الافتراضية Virtual Machine.
2. تكوين إعدادات الأجهزة الافتراضية (VMs) بشكل افتراضي بناءً على احتياجات العمل (Default Configuration) بما يراعي مبدأ منح الحد الأدنى من الامتيازات والصلاحيات.
3. عدم السماح بمشاركة الملفات (File sharing) بين الجهاز المضيف (Host) والجهاز الافتراضي (VM) إلا إذا تم إجراء تقييم مناسب للمخاطر لمنع الهجمات مثل (VM hyper jacking and VM escape).
4. تعطيل البرامج والخدمات والإعدادات غير الضرورية على الأجهزة الافتراضية (VMs) بشكل افتراضي (Default Configuration).
5. استخدام أسماء مستخدمين وكلمات مرور خاصة (separate credentials) لإدارة البيئة الافتراضية وأنظمة التشغيل الخاصة بها.
6. حماية البيئة الافتراضية وأجهزة VMs بواسطة جدار حماية خاص (local firewall) وتفعيل جدار حماية على نظام التشغيل المضيف (host OS)، وتكوين إعدادات جدران الحماية وفقاً لممارسات أمن المعلومات المعتمدة في المصرف.
7. تطبيق ضوابط الأمان المادية والمنطقية (Physical and Logical Security Controls) لمنع الوصول غير المصرح به إلى البيئة الافتراضية.
8. الالتزام بسياسة إدارة التغيير المعتمدة (Change Management Policy) قبل إجراء أي تغييرات في البيئة الافتراضية، والالتزام بتنصيب التصحيحات على الأجهزة الافتراضية (VMs) وتحديثها (shall be patched and updated وفقاً لسياسة إدارة التصحيح المعتمدة (Patch Management Policy).
9. تفعيل خاصية تسجيل الأحداث (Logging) على الأجهزة الافتراضية (VMs) والاحتفاظ بالسجلات ومراقبتها وفقاً لإرشادات مراقبة النظام logging and system monitoring guidelines.

2.6.4. ضوابط حماية مركز البيانات Data Center Protection Controls

الضوابط: يجب على المصرف الالتزام بالآتي:

- أ. التأكد من أن مركز/ مراكز البيانات والمرافق التابعة تتمتع بالمرونة والحماية المادية Physically Secured من التهديدات الداخلية والخارجية.
- ب. القيام بمراجعة للبيئة المحيطة بمراكز البيانات والمباني والمرافق التابعة لها، ضمن نطاق تقييم المخاطر بما يشمل الثغرات والتهديدات.
- ت. إجراء تقييم للتوافرية الدائمة Redundancy and Fault Tolerance لتجهيزات الطاقة الكهربائية والتكييف ونظام إخماد الحريق، وخطوط الاتصالات بشكل دوري.
- ث. توفير الضوابط والأنظمة اللازمة لاكتشاف أي أحداث/خلل يمكن أن تؤثر على تشغيل مركز البيانات والمرافق التابعة (مثل الدخان ودرجة الحرارة والمياه والغبار وإنذارات الوصول access alarms وتنبيهات توفر الخدمة service availability alerts وإمدادات الطاقة والاتصالات والخوادم).
- ج. حماية المعدات والمنشآت في المصرف من انقطاع وعدم انتظام التيار الكهربائي، من خلال توفير مصدر طاقة غير منقطع (UPS) ومولد كهربائي (Generator) ومراعاة التوافرية العالية في الأجهزة الحرجة High Availability.
- ح. اتخاذ الإجراءات الكفيلة بتقييد الوصول إلى مركز البيانات والمرافق التابعة لتكون للموظفين المخولين فقط بناءً على موافقات إدارية موثقة.

خ. ضبط صلاحية وصول الزائرين والأفراد من غير موظفي المصرف أو مسؤولي الانظمة الذين يحتاجون إلى الوصول المؤقت إلى مركز البيانات والمرافق التابعة لأداء أعمال محددة مثل الصيانة، من خلال حصولهم على الموافقات الإدارية الموثقة للزيارات.

د. التأكد من أن مركز البيانات ومحيطه والمرافق التابعة له خاضعة للمراقبة والحماية من خلال أنظمة التحكم والمراقبة وتسجيل وتوثيق الأنشطة التي تتم داخل مرافق المصرف.

ذ. وضع تدابير أمنية مادية (Physical Access Controls) لمنع الوصول غير المصرح به إلى مركز البيانات والمرافق التابعة.

2.6.5. مراجعة تطبيق متطلبات الامن السيبراني الخاصة بإدارة أمن البنية التحتية وشبكات المصرف دورياً.

2.7. ضوابط الاتصال عن بُعد Remote Connection Controls

الهدف: ضمان الوصول الآمن عن بعد الى أصول المصرف مع توفر المراقبة الفعالة.

يجب على المصرف الالتزام بالآتي:

- 2.7.1. توفير السياسات والإجراءات اللازمة لإدارة الوصول عن بُعد لشبكة المصرف.
- 2.7.2. ضبط صلاحية الوصول عن بُعد لشبكة المصرف باستخدام أدوات خاصة آمنة ومرخصة مثل (VPN Tools)، وتطبيق آليات للكشف عن عمليات الوصول عن بعد غير المسموح بها الى أصول المصرف.
- 2.7.3. تطبيق إجراءات إدارة الصلاحيات Privilege access management عن بعد والتحكم بها ومراقبتها وتأمينها ومراجعتها.
- 2.7.4. تطبيق منهجية Zero Trust Architecture.
- 2.7.5. توفير أنظمة الحماية والتشفير المرخصة والأمانة لعملية الاتصال والدخول عن بُعد (Encryption from End to End)، لضمان أمن البيانات أثناء انتقالها خلال فترة الاتصال.
- 2.7.6. اقتصار منح صلاحية الوصول عن بُعد على الأشخاص المخولين بناءً على حاجة العمل وبعد الحصول على الموافقات الإدارية اللازمة، على ان يتم مراجعتها بشكل دوري.
- 2.7.7. عدم السماح بالوصول عن بُعد إلا من خلال قائمة الأجهزة أو العناوين (IPs) المعتمدة، على ان يتم تعريف كل جهاز او عنوان IP بمستخدم محدد بناءً على حاجة العمل.
- 2.7.8. عدم السماح بالوصول المباشر عن بُعد إلى الأنظمة الداخلية للمصرف (Internal Production Systems).
- 2.7.9. حماية الاتصال عن بُعد لشبكة المصرف بواسطة أجهزة مناسبة Firewall, IPS، وعزل التطبيقات المتاحة عن بُعد عن الأنظمة الحساسة للمصرف من خلال إعدادات خاصة مثل (DMZ) بحيث توفر التحكم الآمن في قناة الاتصال VPN.
- 2.7.10. تطبيق تقنيات المراقبة وتسجيل الاحداث لخدمة الوصول عن بُعد (VPN logging, monitoring and recording of access) بما يضمن توثيق عمليات الوصول والأنشطة التي تتم من خلال الوصول عن بُعد.
- 2.7.11. تفعيل أدوات المصادقة مثل (Two Factor Authentication) قبل إنشاء وتمكين قناة الاتصال VPN، مثل استخدام رمز الوصول للأجهزة أو البرامج كمصادقة أساسية متبوعة بمصادقة Radius أو LDAP أو AD أو TACACS+.
- 2.7.12. إجراء التقييم الفني اللازم للأجهزة المستخدمة في الوصول عن بُعد، والتأكد من انها مجهزة ببرامج أمان محدثة، وتحديثات الأمان latest security patches، وبرامج مكافحة الفيروسات والبرامج الضارة anti-malware.
- 2.7.13. التأكد من تطبيق خاصية قطع الاتصال غير النشط بعد فترة زمنية محددة VPN inactivity timeouts.

2.7.14. تطبيق القيود والضوابط الفنية على المنافذ وبروتوكولات وخدمات الشبكة والتي تضمن منع الوصول عن بُعد من غير المصرح بهم وتعزيز أمن أجهزة الشبكة وتعطيل منافذ الشبكة غير المستخدمة، مثل (MAC filtering configuration on routers, wireless controllers).

2.7.15. توفير المراقبة والمراجعة اللازمة لصلاحيات الوصول عن بُعد الممنوحة لمسؤولي أنظمة الشبكة والبنية التحتية الخاصة بالمصرف (Administrators).

2.8. أمن الأجهزة المحمولة Portable Devices Security

الهدف: ضمان حماية الأجهزة المحمولة الخاصة بالمصرف بما في ذلك أجهزة الحاسوب المحمولة والهواتف الذكية والأجهزة اللوحية من المخاطر السيبرانية، وضمان التعامل الآمن مع المعلومات الحساسة وحمايتها أثناء النقل والتخزين.

الضوابط: يجب على المصرف الالتزام بالآتي:

2.8.1. تحديد وتوثيق واعتماد وتطبيق متطلبات الامن السيبراني الخاصة بأمن الاجهزة المحمولة في حال تم استخدام الأجهزة الشخصية والسماح للموظفين المعنيين بالوصول الى الأنظمة والمعلومات من خلالها (Bring your own device BYOD) عند ربطها بشبكة المصرف يجب أن تغطي متطلبات الامن السيبراني الخاصة بأمن الاجهزة المحمولة وأجهزة (BYOD) بالحد الأدنى ما يلي:

أ. تطبيق نظام خاص بإدارة الأجهزة المحمولة (Mobile Device Management Solution) يضمن تشفير بيانات المصرف المخزنة على هذه الأجهزة وليس بالضرورة تشفير الجهاز بالكامل، وأن يتم استخدام هذه الأجهزة فقط بناءً على مصلحة العمل. ب. اعتماد وتطبيق سياسات وإجراءات تتضمن ضوابط لاستعمال الأجهزة المحمولة والأجهزة الشخصية (BYOD) ضمن البيئة التكنولوجية للمصرف بما يضمن أمن وخصوصية وسرية بيانات المصرف.

ت. منع الوصول من الأجهزة المحمولة للأنظمة الحساسة الا لفترة مؤقتة فقط، وذلك بعد اجراء تقييم المخاطر، والحصول على الموافقات اللازمة من الإدارة المعنية بالأمن السيبراني في المصرف.

ث. فصل وتشفير البيانات والمعلومات الخاصة بالمصرف والمخزنة على الأجهزة المحمولة والشخصية التي يمكن من خلالها الوصول لأنظمة المصرف الحساسة، وان تكون محمية بكلمة مرور قوية، ولا يسمح بالدخول من خلال الأجهزة الشخصية إلى بيانات او أنظمة عالية المخاطر دون موافقة مسبقة.

ج. عدم السماح للأجهزة المحمولة والشخصية التي لا تلتزم بسياسة وضوابط BYOD بالاتصال بشبكة المصرف، وأن تخضع هذه الأجهزة للضوابط المعمول بها في إدارة الأجهزة المملوكة للمصرف.

ح. اتخاذ التدابير الأمنية الكافية من أنظمة مراقبة وجدران الحماية Firewalls و IPS لضمان حماية ومراقبة العمليات التي تتم من خلال الأجهزة المحمولة والشخصية باعتبار انه يتم استخدام هذه الأجهزة خارج شبكة المصرف.

خ. في حالة فقدان أو سرقة الأجهزة المحمولة او الشخصية، يجب اتباع إجراءات إدارة الحوادث وفقاً لسياسات المصرف بالخصوص، والتأكد من تمكين خاصية الوصول عن بُعد أو قفل الطوارئ Emergency Lock Features للأجهزة الشخصية والمحمولة، وحذف البيانات والمعلومات الخاصة بالمصرف والموجودة على هذه الاجهزة.

د. التوعية الامنية للمستخدمين بالمخاطر والتهديدات المصاحبة لاستخدام الأجهزة المحمولة في أعمال المصرف.

2.8.2. مراجعة تطبيق متطلبات الامن السيبراني الخاصة بأمن الاجهزة المحمولة والأجهزة الشخصية (BYOD) للمصرف دورياً.

2.9. أمن البيانات والمعلومات Data and Information Security

الهدف: ضمان حماية سرية وسلامة وتوافر بيانات ومعلومات المصرف وفقاً للسياسات والإجراءات واستراتيجية المخاطر الخاصة بالمصرف ومتطلبات سلطة النقد ذات العلاقة.

الضوابط: يجب على المصرف الالتزام بالآتي:

2.9.1. تحديد وتوثيق واعتماد وتطبيق متطلبات الامن السيبراني لحماية بيانات ومعلومات المصرف، والتعامل معها وفقاً للتعليمات النافذة.

2.9.2. أن تغطي متطلبات الامن السيبراني لحماية البيانات والمعلومات بالحد الأدنى ما يلي:

أ. ملكية البيانات والمعلومات.

ب. تصنيف البيانات والمعلومات، وآلية ترميزها (Mechanisms Labeling and Classification).

ت. خصوصية البيانات والمعلومات.

ث. توفير ضوابط واجراءات الحماية اللازمة للبيانات في جميع حالاتها (Data at-rest, Data at-transit) وكذلك اجراءات تغيير وحذف البيانات.

ج. توفر إجراءات إدارة التخزين Data Capacity Management لضمان توافر البيانات Availability.

ح. عدم استخدام بيانات الأنظمة الحساسة في غير البيئة الحية (Production Environment) إلا بعد استخدام ضوابط مشددة لحماية تلك البيانات مثل: تقنيات اخفاء البيانات (Data Masking) او تقنيات مزج البيانات (Data Scrambling).

خ. حماية البيانات المصنفة بالأنظمة الحساسة من خلال تقنيات منع تسريب البيانات (Data Leakage Prevention).

د. اعتماد وتطبيق سياسة تصنيف المعلومات بناءً على المعايير العالمية المعتمدة بالخصوص، مثل ISO، NIST. بحيث يتم تصنيف البيانات على أساس الحساسية والتأثير.

ذ. توعية مستخدمي المعلومات من موظفين وشركاء بوضع العلامات الخاصة بتصنيف البيانات، وتوضيح ضرورة معرفة التصنيف وتأثيرها على أمن المعلومات.

ر. التأكد من التخزين الآمن وتطبيق التشفير اللازم لأي معلومات أو بيانات تتعلق بتفاصيل الشبكات الداخلية وتكوينات الانظمة وبيانات التعريف الشخصية والمعلومات الحساسة الأخرى.

ز. إتاحة الوصول الى المعلومات بناءً على متطلبات محددة وعلى أساس الحاجة للمعرفة، وبناءً على الطلب وبعد الحصول على الموافقات الإدارية اللازمة.

2.9.3. أمن قواعد البيانات Database Security

يجب على المصرف الالتزام بالآتي:

أ. تعزيز وتأمين قواعد البيانات وأنظمتها الفرعية Databases and its subsystems وفقاً لإرشادات الشركة الخاصة hardening guidelines، ويجب تغيير الثوابت Parameters مثل أسماء المستخدمين وكلمات المرور الافتراضية، أو سلاسل الاتصال connection strings أو أي إعدادات غير آمنة في وقت التثبيت any insecure configuration shall be changed at the time of installation.

ب. ان تخضع صلاحيات الوصول إلى المعلومات في قاعدة البيانات لمبدأ منح الحد الأدنى من الصلاحيات والامتيازات Least Privilege، ويجب تصنيف المعلومات المخزنة في قاعدة البيانات وفقاً لسياسة التصنيف Classification Policy.

ت. تطبيق الضوابط اللازمة لعدم تجاوز صلاحيات الوصول المعتمدة لقاعدة البيانات بما يضمن عدم إتاحة الوصول غير المصرح.

ث. أن تكون حسابات نظام التشغيل (OS Accounts) التي يستخدمها موظفو إدارة قواعد البيانات DBAs لتسجيل الدخول إلى خادم قاعدة البيانات لتنفيذ أعمال مرتبطة بإدارة قواعد البيانات، حسابات فردية وتجنب مشاركة الحسابات Shared Accounts، ويكون استخدام حساب مشترك فقط لأغراض تشغيل وظائف إدارة قواعد البيانات من صيانة ومراقبة، والنسخ الاحتياطي بعد تطبيق ضوابط الرقابة الثنائية.

ج. أن تخضع صلاحيات الوصول لقواعد البيانات Access to databases للمراقبة وتسجيل الأحداث والمراجعة الدورية من قبل إدارة قواعد البيانات DBAs وكذلك فريق أمن المعلومات في المصرف، ويجب أرشفة السجلات (Logs) على خادم خاص بناءً على السياسة المعتمدة للاحتفاظ بالسجلات.

ح. تشفير قاعدة البيانات التي تحتوي على معلومات هامة وسرية critical and confidential information، وتوثيق إجراءات إدارة المفاتيح الآمنة secure keys وفقاً لسياسة التشفير المعتمدة في المصرف.

خ. تطبيق تصحيحات قاعدة البيانات Database shall be patched، وفقاً لسياسة إدارة التصحيح المعتمدة patch management policy، واتخاذ الإجراءات اللازمة للحفاظ على مستويات تصحيح أمان maintain security patch levels للرجوع إليها في الوقت المناسب.

2.9.4. منع تسرب البيانات Data loss prevention

يجب على المصرف الالتزام بالآتي:

أ. يجب تحديد وتطبيق إجراءات شاملة لمعالجة الحوادث وإعداد التقارير incident handling and reporting procedures بما يتماشى مع إرشادات إدارة الحوادث الأمنية security incident management المعتمدة وأفضل المعايير والممارسات بالخصوص.

ب. تشفير البيانات الحساسة التي يتم إرسالها إلى أطراف خارجية باستخدام تقنيات تشفير قوية، مثل RSA، SHA لضمان حماية البيانات المخزنة data at rest أو أثناء النقل أو الاستخدام وفقاً لسياسة التشفير المعتمدة.

ت. وضع ضوابط للكشف عن الأنشطة المشبوهة فيما يتعلق بالوصول إلى البيانات أو تعديلها أو نقلها.

ث. تعطيل منافذ وسائط التخزين المحمولة لأجهزة الحاسوب portable storage media ports، إلا في حالات الضرورة التي تستلزم ذلك وبعد الحصول على الموافقات اللازمة.

ج. تطبيق تدابير مثل Endpoint DLP solutions لمعالجة مخاطر النسخ غير المصرح به unauthorized downloading لبيانات العملاء إلى وسائط التخزين المحمولة portable storage media واحتمال فقدان هذه الوسائط التي تحتوي على معلومات حساسة.

ح. الطلب من مشغلي ومقدمي خدمات الاستعانة الخارجية الذين يتطلب عملهم التعامل مع بيانات عملاء المصرف أو نقلها أو الوصول إليها، الامتنال لضوابط أمن بيانات المصرف وسياسات وإجراءات منع تسرب البيانات، بما في ذلك الضوابط الواردة في هذه التعليمات، وتوقيع اتفاقية عدم إفشاء (Non-Disclosure Agreement NDA)، ويجب على المصرف تطبيق ضوابط فعالة للمراقبة والتحقق من امتثال مقدم الخدمة للضوابط المذكورة، ويجب تحديد هذه المتطلبات بوضوح في الاتفاقيات.

2.10. التشفير Cryptography

الهدف: ضمان حماية الاصول المعلوماتية الالكترونية للمصرف من خلال الاستخدام السليم والفعال للتشفير، وفقاً للسياسات والإجراءات التنظيمية، ومتطلبات سلطة النقد ذات العلاقة.

الضوابط: يجب على المصرف الالتزام بالآتي:

2.10.1. تحديد وتوثيق واعتماد وتطبيق متطلبات الامن السيبراني للتشفير في المصرف.

2.10.2. أن تغطي متطلبات الامن السيبراني للتشفير بالحد الأدنى ما يلي:

أ. اعتماد سياسة تشفير خاصة بالمصرف تستند لأفضل المعايير والتقنيات بالخصوص.
ب. تطبيق أفضل وأحدث المعايير الخاصة بتقنيات التشفير وإدارة مفاتيح التشفير، مثل ISO 11770، للتحكم في دورة حياة مفاتيح التشفير وإدارتها.

ت. ان تضمن تقنيات تشفير البيانات الحساسة للمصرف، سلامة المعلومات المشفرة وحمايتها من الكشف غير المصرح به من خلال تطبيق أفضل الضوابط والممارسات لتأمين سرية البيانات أثناء نقلها (Data-In-Transit) أو تخزينها (Data-At-Rest) أو استخدامها على مستوى الملفات أو قاعدة البيانات أو على مستوى أعمدة محددة داخل قاعدة البيانات.

ث. تأمين كلمات المرور وحمايتها من الكشف غير المصرح به أثناء حفظها أو نقلها أو استخدامها، ويجب تشفير كلمات المرور ذات الصلاحيات الواسعة privileged passwords وتخزينها خارج الموقع off-site مع ملفات النسخ الاحتياطي في كل مرة يتم فيها تغيير كلمة المرور، لضمان الاسترداد الكامل complete recovery.

2.10.3. مراجعة تطبيق متطلبات الامن السيبراني للتشفير في المصرف دورياً.

2.11. إدارة النسخ الاحتياطية والاسترجاع Backup and Recovery Management

الهدف: ضمان حماية وحفظ بيانات ومعلومات المصرف والاعدادات التقنية للأنظمة والتطبيقات الخاصة بالمصرف من الاضرار الناجمة عن المخاطر السيبرانية، وفقاً للسياسات والاجراءات التنظيمية للمصرف، ومتطلبات سلطة النقد ذات العلاقة.

الضوابط: يجب على المصرف الالتزام بالآتي:

2.11.1. تحديد وتوثيق واعتماد وتطبيق متطلبات الامن السيبراني لإدارة النسخ الاحتياطية للمصرف.

2.11.2. أن تغطي متطلبات الامن السيبراني لإدارة النسخ الاحتياطية بالحد الأدنى ما يلي:

أ. اعداد واعتماد السياسات والإجراءات اللازمة لإدارة عمليات النسخ الاحتياطي والاسترجاع لبيانات وأنظمة المصرف بما يوضح فترات التخزين، وأماكن حفظ النسخ، والفحص الدوري للنسخ، وآلية الاسترجاع، وصلاحيات الوصول وما الى ذلك من ضوابط.

ب. شمول عملية النسخ الاحتياطية لكافة الأصول المعلوماتية والتقنية في المصرف.

ت. القدرة على استعادة البيانات والأنظمة بعد التعرض لأي حدث طارئ ضمن الفترة الزمنية المعتمدة والمقبولة.

ث. إجراء فحص دوري لمدى فعالية استعادة النسخ الاحتياطية.

ج. توفير نسخة احتياطية يومية لبيانات وأنظمة المصرف والاحتفاظ بها خارج مركز بيانات المصرف على أن يتم تشفيرها وتطبيق ضوابط تضمن عدم السماح بالوصول أو التعديل عليها من قبل أشخاص غير مخولين.

ح. عمل النسخ الاحتياطي على فترات زمنية مخطط لها، بناءً على تقييم المخاطر للمصرف، على ان يتم عمل النسخ الاحتياطي للأنظمة الحساسة بشكل يومي.

خ. تأمين الوصول، والتخزين، والنقل لمحتوى النسخ الاحتياطية للأنظمة الحساسة ووسائطها، وحمايتها من الاتلاف، أو التعديل، أو الاطلاع غير المصرح به.

2.11.3. مراجعة تطبيق متطلبات الامن السيبراني لإدارة النسخ الاحتياطية للمصرف دورياً.

2.12. إدارة الثغرات Vulnerabilities Management

الهدف: ضمان اكتشاف الثغرات في الوقت المناسب ومعالجتها بشكل فعال، لمنع أو تقليل احتمالية استغلال هذه الثغرات من خلال الهجمات السيبرانية، وتقليل الآثار السلبية الناجمة عنها على أعمال المصرف.

الضوابط: يجب على المصرف الالتزام بالآتي:

2.12.1. تحديد وتوثيق واعتماد وتطبيق متطلبات الامن السيبراني لإدارة الثغرات للمصرف.

2.12.2. أن تغطي متطلبات الامن السيبراني لإدارة الثغرات بالحد الأدنى ما يلي:

- أ. القدرة على فحص واكتشاف الثغرات دورياً بشكل ربع سنوي، على ان يتم فحص الثغرات واكتشافها على المكونات التقنية للأنظمة الحساسة مرة واحدة شهرياً على الأقل.
- ب. تصنيف الثغرات حسب خطورتها.
- ت. معالجة الثغرات بناءً على تصنيفها والمخاطر السيبرانية المترتبة عليها.
- ث. إدارة حزم التحديثات والإصلاحات الأمنية لمعالجة الثغرات.
- ج. التواصل والاشتراك مع مصادر موثوقة فيما يتعلق بالتنبيهات المتعلقة بالثغرات الجديدة والمحدثة.
- ح. استخدام وسائل وأدوات موثوقة لاكتشاف الثغرات.
- خ. تقييم الثغرات ومعالجتها (بتنصيب حزم التحديثات والإصلاحات) على المكونات التقنية للأنظمة الحساسة الخارجية والمتصلة بالإنترنت مرة واحدة شهرياً على الأقل، وبشكل دوري للأنظمة الحساسة الداخلية.
- د. إجراء اختبارات تقييم شامل للثغرات (Vulnerability Assessment (VA) exercises) على الأقل مرتين سنوياً أو حسب الحاجة، والاستناد لأفضل الممارسات والمعايير المتبعة لإجراء هذه الاختبارات، مثل OWASP و OSSTMM و SANS، ومقارنة نتائج عمليات فحص الثغرات السابقة للتحقق من معالجة هذه الثغرات والتخفيف من أثرها.
- ذ. إعداد خطة عمل لمعالجة نقاط الضعف المحددة ومشاركتها مع الإدارة العليا.
- ر. إجراء مراجعة لمدى قبول مخاطر الثغرات الموجودة Risks Acceptance بشكل نصف سنوي لتحديد ما إذا كانت الضوابط أو التصحيحات المتوفرة يمكن أن تعالج الثغرات التي تم قبولها سابقاً، أو إذا تغيرت الظروف بشكل يزيد من أثر هذه المخاطر.
- ز. معالجة فورية للثغرات ذات المخاطر المرتفعة (Critical, High and medium, Vulnerabilities) خاصة للتطبيقات والخدمات الإلكترونية الخاصة بالعملاء، إضافة للمعالجة الفورية للثغرات الداخلية الحرجة ومرتفعة المخاطر مع الأخذ في الاعتبار الثغرات الأمنية المستخدمة حالياً لاختراق المؤسسات (active exploit)، مع اتباع آليات إدارة التغيير المعتمدة.

2.12.3. إجراءات الأمان ضد البرامج الضارة Security measures against malware

يجب على المصرف الالتزام بالآتي:

- أ. توفير أنظمة مرخصة ومحدثة لمكافحة البرامج الضارة Malware وتطبيق ضوابط للكشف عنها والحد من تأثيرها على كافة المستويات (الخوادم، الشبكة والمستخدم)، مثل (Next generation Anti-Malware/ Endpoint Detection and Response EDR).
- ب. تعطيل وظيفة التشغيل التلقائي Auto run على أجهزة الحاسوب المكتبية والمحمولة والخوادم، وإجراء فحص تلقائي لمكافحة البرامج الضارة لوسائط التخزين.
- ت. توفير آلية لتصفية المرفقات في بوابة البريد الإلكتروني filter attachments at the email gateway.
- ث. توفير آلية لمراقبة السجلات Logs على أجهزة Firewalls و IPS / IDS و DNS, Proxy وخوادم بشكل دائم للكشف المبكر عن الهجمات السيبرانية.

2.12.4. الحماية ضد هجمات تعطيل الخدمة DOS و DDOS

يجب على المصرف الالتزام بالآتي:

أ. تحديد نقاط الاختناقات المحتملة potential bottlenecks ونقاط الفشل single points of failure التي يمكن أن تكون عرضة لهجمات تعطيل الخدمة DOS / DDoS، من خلال إجراء تحليل وتقييم لتصميم الشبكة واختبار الإعدادات network design analysis and configuration testing.

ب. التأكد من تطبيق مزود خدمة الإنترنت للبرامج والإعدادات الخاصة بمكافحة هجمات تعطيل الخدمة.

ت. إعداد استراتيجيات واضحة بخصوص الحماية من هجمات تعطيل الخدمة وإعداد إجراءات استجابة للحوادث incident response procedures يتم التحقق منها بشكل دوري لضمان الاستجابة السريعة والفعالة ضد هجمات DOS / DDoS.

2.12.5 إدارة التهديدات السيبرانية Cyber Threat Management

يجب على المصرف الالتزام بالآتي:

أ. توثيق واعتماد آلية تحديد التهديدات السيبرانية وإدارتها وضمان تنفيذها ومراجعتها بشكل دوري، على أن تتماشى مع السياسات والإجراءات الخاصة بتبادل المعلومات حول التهديدات السيبرانية.

ب. جمع ومعالجة المعلومات والبيانات المنشورة من قبل مصادر داخلية وخارجية محددة بشكل متسق.

ت. إبلاغ الإدارة عن التهديدات والمخاطر السيبرانية بناءً على الحاجة وأهمية وأثر التهديد.

ث. تحديد التهديدات والمخاطر واتخاذ الإجراءات اللازمة لحماية أصول البيئة التكنولوجية الخاصة بها وفقاً لإجراءات إدارة الحوادث.

ج. تعزيز وتوفير مصادر متنوعة للمعلومات عن التهديدات السيبرانية للجهة المختصة في المصرف بشكل مستمر.

ح. العمل بشكل مستمر مع سلطة النقد لتبادل المعلومات الخاصة بالمصرف حول التهديدات (الداخلية والخارجية) والهجمات السيبرانية التي يتعرض لها وآلية معالجتها والتعامل معها.

2.12.6 الكشف المبكر عن الهجمات السيبرانية Early detection of cyber intrusions and- Attacks

يجب على المصرف الالتزام بالآتي:

أ. توفير آليات وتقنيات المراقبة الدائمة لبيئة العمل مثل (أجهزة وأنظمة البيئة التكنولوجية، الشبكات) للكشف المبكر عن أحداث الأمن السيبراني المحتملة.

ب. تطبيق نظام منع الاختراق IPS - intrusion prevention system على المستويين الداخلي والخارجي.

ت. توفير آلية لمراقبة الأنشطة المشبوهة suspicious activities على الخوادم والشبكات والأجهزة endpoint devices بما يضمن الكشف والإشعار وحجب الأنشطة المشبوهة على الأجهزة المستهدفة.

ث. توفير آلية لتحليل تدفق البيانات عبر الشبكة network traffic analysis، وإعطاء أولوية للتعامل مع أي انحرافات أو حالات مشبوهة.

ج. إعداد إطار استجابة للحوادث incident response framework يشمل خطة استجابة للاختراق السيبراني cyber-breach

response plan بحيث توفر الخطة إمكانية قياس التفاصيل المتعلقة بمكافحة الهجمات السيبرانية cyber intrusions and attacks.

ح. إجراء تحقيق شامل لتحديد مدى وتأثير الاختراق في حالة التسلل لشبكة المصرف عبر الإنترنت، بالإضافة إلى لاكتشاف نقاط الضعف التي يتم استغلالها من قبل المهاجمين.

2.12.7 اختبار الاختراق Penetration Testing

الضوابط: يجب على المصرف الالتزام بالآتي:

- أ. تحديد وتوثيق واعتماد وتنفيذ متطلبات الامن السيبراني الخاصة باختبار الاختراق في المصرف.
- ب. أن تغطي متطلبات الامن السيبراني لاختبار الاختراق بالحد الأدنى ما يلي:
 1. نطاق عمل اختبار الاختراق، ليشمل جميع الأنظمة والخدمات المتاحة من خلال الانترنت ومكوناتها التقنية، ومنها: البنية التحتية، المواقع الالكترونية، تطبيقات الويب، تطبيقات الهواتف الذكية، البريد الالكتروني والدخول عن بُعد.
 2. عمل اختبار الاختراق بشكل دوري، على ان يتم تنفيذ اختبار الاختراق بشكل سنوي مرة واحدة على الأقل من قبل جهة أو فريق مؤهل او عند حدوث أي تغييرات جوهرية.
 - ت. تصحيح الثغرات التي تم العثور عليها وإعادة الاختبار للتأكد من معالجة كافة الثغرات.
- 2.12.8. مراجعة تطبيق متطلبات الامن السيبراني لعمليات اختبار الاختراق وإدارة الثغرات التقنية للمصرف دورياً.

2.13. إدارة سجلات الاحداث ومراقبة الأمن السيبراني Cybersecurity Event Logs and Monitoring Management

- الهدف: ضمان تجميع وتحليل ومراقبة سجلات أحداث الامن السيبراني في الوقت المناسب بهدف الكشف المبكر عن الهجمات السيبرانية وإدارة مخاطرها بفعالية لمنع أو تقليل الآثار المترتبة على أعمال المصرف.
- الضوابط: يجب على المصرف الالتزام بالآتي:
- 2.13.1. تحديد وتوثيق واعتماد وتطبيق متطلبات إدارة سجلات الاحداث ومراقبة الأمن السيبراني للمصرف.
 - 2.13.2. أن تغطي متطلبات إدارة سجلات الاحداث ومراقبة الأمن السيبراني بالحد الأدنى ما يلي:
 - أ. تفعيل سجلات الاحداث (Logs Event) الخاصة بالأمن السيبراني على الاصول المعلوماتية لدى المصرف.
 - ب. تفعيل سجلات الاحداث لتسجيل العمليات التي تتم من خلال أسماء المستخدمين ذات الصلاحيات الواسعة على الأصول المعلوماتية، وتسجيل وتوثيق عمليات الدخول عن بُعد لشبكة وأنظمة المصرف.
 - ت. استخدام التقنيات اللازمة (SIEM) لجمع سجلات الاحداث الخاصة بالأمن السيبراني.
 - ث. المراقبة المستمرة لسجلات الاحداث الخاصة بالأنظمة الحساسة على مدار الساعة 24/7 من خلال مركز إدارة عمليات امن المعلومات SOC – Security Operation Center وان يكون فريق المراقبة مدرب ومؤهل.
 - ج. الاحتفاظ بسجلات الاحداث الخاصة بالأمن السيبراني المتعلقة بالأنظمة وحمايتها لمدة عام على الأقل، على ان تكون شاملة.
 - ح. تفعيل التنبيهات وسجلات الاحداث المتعلقة بإدارة تغييرات الملفات (File Integrity Management) ومراقبتها.
 - خ. مراقبة وتحليل سلوك المستخدم (UBA “User Behavior Analytics”).
 - د. رفع تقارير أسبوعية وشهرية للجهات المعنية في الإدارة عن الثغرات والتهديدات المهمة.
 - 2.13.3. مراجعة تطبيق متطلبات إدارة سجلات الاحداث ومراقبة الامن السيبراني في المصرف دورياً.

2.14. إدارة حوادث وتهديدات الامن السيبراني Cybersecurity Incident and Threat Management

- الهدف: ضمان تحديد واكتشاف حوادث الامن السيبراني في الوقت المناسب وإدارتها بشكل فعال والتعامل مع تهديدات الامن السيبراني استباقياً لمنع أو التخفيف من الآثار المترتبة على أعمال المصرف.
- الضوابط: يجب على المصرف الالتزام بالآتي:
- 2.14.1. تحديد وتوثيق واعتماد وتطبيق متطلبات إدارة حوادث وتهديدات الامن السيبراني في المصرف.
 - 2.14.2. أن تغطي متطلبات إدارة حوادث وتهديدات الامن السيبراني بالحد الأدنى ما يلي:
 - أ. وضع خطط الاستجابة للحوادث الامنية وآليات التصعيد.

ب. تصنيف حوادث الامن السيبراني.

ت. ابلاغ سلطة النقد عن الحوادث المتعلقة بالامن السيبراني لديه.

ث. مشاركة التنبيهات والمعلومات الاستباقية ومؤشرات الاختراق وتقارير حوادث الامن السيبراني مع سلطة النقد.

ج. الحصول على المعلومات الاستباقية (Intelligence Threat) والتعامل معها.

2.14.3. مراجعة تطبيق متطلبات إدارة حوادث وتهديدات الامن السيبراني في المصرف دورياً.

2.15. الأمن المادي Physical Security

الهدف: ضمان حماية الاصول المعلوماتية والتقنية للمصرف من الوصول المادي (Physical Access) غير المصرح به والفقدان والسرقة والتخريب.

الضوابط: يجب على المصرف الالتزام بالآتي:

2.15.1. تحديد وتوثيق واعتماد وتطبيق متطلبات الامن السيبراني لحماية الاصول المعلوماتية والتقنية للمصرف من الوصول المادي غير المصرح به والفقدان والسرقة والتخريب.

2.15.2. أن تتضمن متطلبات الامن السيبراني لحماية الاصول المعلوماتية والتقنية للمصرف من الوصول المادي غير المصرح به، بالحد الأدنى الضوابط التالية:

أ. اعتماد سياسة لضبط صلاحيات الوصول المادي للأماكن الحساسة في المصرف (مثل: مركز البيانات الرئيسي، مركز التعافي من الكوارث، مركز المراقبة والتحكم، وغيرها)، لتقتصر على الأشخاص المصرح لهم بناء على حاجة العمل وبعد الحصول على الموافقات الإدارية.

ب. التأكد من التزام مقدمي خدمات الصيانة أو الضيوف الذين يزورون مباني المصرف بسياسة وضوابط الوصول المادية المعتمدة.

ت. تقسيم المساحات Physical spaces الى مناطق منفصلة Zones بناءً على حساسيتها واستخدامها ومتطلبات الأمن الخاصة بها، من خلال تحديد وتطبيق المتطلبات والضوابط المادية لكل منطقة منفصلة.

ث. أن يقتصر الوصول إلى هذه المناطق على الموظفين المصرح لهم بناءً على موافقات إدارية موثقة.

ج. مراجعة حقوق وصلاحيات الوصول المادي وتحديثها بشكل دوري والإيقاف الفوري للصلاحيات غير المستخدمة.

ح. توفير سجلات الدخول وأنظمة مراقبة CCTV لتوثيق الاعمال التي تتم وحماية هذه السجلات.

خ. الاتلاف والأمن وإعادة استخدام الاصول المادية التي قد تحتوي على معلومات مصنفة مثل: الوثائق الورقية ووسائط الحفظ والتخزين.

د. توفير عناصر التحكم في الدخول Security barriers and entry controls لحماية المرافق الحساسة مثل مراكز البيانات ومرافق إصدار البطاقات والأرقام السرية card and pin generation facilities.

ذ. عدم وجود علامات واضحة تحدد أماكن وجود المرافق الحساسة الخاصة بمعالجة المعلومات.

ر. إعداد واعتماد اجراءات لإدارة أمن المواقع الحساسة في المصرف، على أن تغطي ما يلي:

1. إدارة وتشغيل وصيانة نظام التحكم بالوصول ونظام الإنذار.

2. إدارة المفاتيح Key management، وتسجيل وإزالة مستخدمي الأنظمة، وإصدار البطاقات الشخصية التعريفية.

3. التوعية الأمنية والتدريب، والمراجعة الدورية.

4. فحص ومراجعة السجلات Audit Trails and Logs.

5. الإبلاغ عن حوادث وانتهاكات أمن تكنولوجيا المعلومات والاتصالات.

2.15.3. توفير المراجعة الدورية لمتطلبات وضوابط الامن السيبراني الخاصة بحماية الاصول المعلوماتية والتقنية للمصرف من الوصول المادي غير المصرح به والفقدان والسرقة والتخريب.

2.16. حماية التطبيقات الداخلية والخارجية Internal and External Web Applications Security

الهدف: ضمان حماية تطبيقات المصرف الداخلية والمتاحة للوصول الخارجي من خلال الانترنت (Internet-Facing Web Application Security)، من المخاطر السيبرانية.

الضوابط: يجب على المصرف الالتزام بالآتي:

2.16.1. تحديد وتوثيق واعتماد وتطبيق متطلبات الامن السيبراني لحماية تطبيقات المصرف الداخلية والمتاحة من خلال الانترنت (تطبيقات الويب) من المخاطر السيبرانية.

2.16.2. أن تغطي متطلبات الامن السيبراني لحماية التطبيقات بالحد الأدنى ما يلي:

أ. إعداد واعتماد سياسة وإجراءات عمل واضحة لإدارة تطبيقات المصرف بما يضمن سرية وسلامة وتوافرية البيانات والأنظمة (Confidentiality, Integrity, Availability).

ب. استخدام جدار الحماية لتطبيقات الويب (Web Application Firewall) لحماية التطبيقات الموجودة ضمن البنية التحتية لشبكة المصرف والمتاحة عبر شبكة الانترنت.

ت. إجراء تقييمات الثغرات Vulnerability Assessments ومراجعات الكود Code Reviews واختبار الاختراق بشكل دوري أو عند الحاجة أو إجراء تغييرات جوهرية.

ث. إجراء اختبارات أمان للتطبيقات المتاحة عبر الانترنت أو الهواتف الذكية (ما قبل التنفيذ، وبعد التنفيذ وبعد أي تغييرات رئيسية)، ويجب مشاركة التقارير مع الادارة ومتابعتها وتصويب الملاحظات.

ج. إعداد إرشادات التطوير الآمن للتطبيقات وفقاً لمعايير عالمية بالخصوص مثل Open Web Application Security Project (OWASP).

ح. تأمين البيانات والمعلومات المستخدمة في التطبيقات الداخلية والمتاحة عبر الانترنت في جميع مراحل استخدامها (أثناء التخزين، والانتقال والاستخدام) وفقاً للإرشادات الموضحة في ضوابط التشفير.

خ. تطبيق ضوابط الحماية اللازمة ضمن المستويات المتعددة (Multi-Tier Architecture)، بالحد الأدنى (3-Tier Architecture) على مستوى المستخدم ومستوى التطبيق ومستوى قاعدة البيانات.

د. استخدام بروتوكولات آمنة (مثل SSH, HTTPS).

ذ. التوعية بسياسة وضوابط الاستخدام الآمن للمستخدمين.

ر. التحقق من الهوية متعدد العناصر (Multi-Factor Authentication) لعمليات دخول المستخدمين واستخدام الأنظمة.

ز. الإدارة الآمنة للجلسات (Secure Session Management)، ويشمل موثوقية الجلسات (Authenticity)، وإقفالها (lockout)، وانتهاء مهلتها (Timeout).

س. تطبيق الحد الأدنى من معايير أمن وحماية التطبيقات (OWASP Top Ten).

ش. اعتماد إجراءات آمنة لتزويد عملاء ومستخدمي خدمات الانترنت بمعلومات تسجيل الدخول عبر الانترنت.

ص. تطبيق نظام مراقبة للتنبيه عن أي أنشطة غير طبيعية ومشبوهة قد تحدث على الأنظمة المتاحة عبر الانترنت، أو أخطاء الإرسال، أو المعاملات غير المعتادة، بحيث يعتمد المصرف إجراءات عمل للتحقق من هذه التنبيهات أو الأخطاء ومتابعتها وإغلاقها.

ض. الحفاظ على مرونة عالية وتوافرية دائمة لأنظمتها المتاحة عبر الإنترنت وأنظمة الدعم والمساندة، ووضع تدابير للتخطيط ومتابعة استخدام السعة التخزينية وتوفير الحماية من الهجمات المحتملة عبر الإنترنت.

2.16.3 الإدارة الآمنة لدورة حياة البرامج Secure Software Lifecycle Management

الضوابط: يجب على المصرف الالتزام بالآتي:

- أ. إعداد واعتماد إجراءات آمنة لإدارة دورة حياة البرامج والتطبيقات وضمان تنفيذها ومراقبتها ومراجعتها وتحديثها بشكل دوري.
- ب. الأخذ بعين الاعتبار مبادئ الأمن والخصوصية ومتطلبات التصنيف أثناء تصميم البرامج الجديدة وتوضيحها في الاتفاقية مع الشركات المزودة، وأن تخضع جميع التحسينات للتطبيقات الداخلية أو الخارجية الجاهزة لنفس العملية.
- ت. أن يشارك فريق أمن المعلومات بمراحل تقييم ومعالجة متطلبات الأمان خلال كافة مراحل إدارة دورة حياة البرنامج (التصميم والتطوير والاختبار والتنفيذ والصيانة والاتلاف وما إلى ذلك).
- ث. اعتماد ممارسات كود البرمجة الآمنة (Secure Coding Practices) وفقاً للمتطلبات التنظيمية وأفضل الممارسات العالمية (مثل (Open Web Application Security Project (OWASP) لضمان معالجة نقاط الضعف الشائعة في الكود أثناء التطوير وتنفيذ ضوابط الحماية والكشف والتصحيح والتحكم المناسبة.
- ج. تطبيق مبدأ فصل الصلاحيات من خلال تقييد الوصول إلى بيانات الإنتاج والاختبار والتطوير.
- ح. تقييد صلاحية الوصول إلى الكود البرمجي (Source Code) للبرنامج وتسجيل الأحداث التي تتم عليه (Logging).
- خ. اعتماد ضوابط إدارة صلاحية الوصول إلى الكود البرمجي (Source Code) من خلال ضوابط التخزين الآمن للكود سواء لدى المصرف أو عند جهة ضامنة (Escrow arrangement) ووضع شروط تعاقدية صارمة مع مزود التطبيق/الخدمة.
- د. الحصول على شهادة تقييم الأمان (Security assessment certificate) أو ما يعادلها من الأدلة للبرامج الجاهزة للتأكد من اختبار مزود الخدمة للتطبيقات ومعالجة الثغرات.

2.16.4 الاحتيال الداخلي Internal fraud

يجب على المصرف الالتزام بالآتي:

- أ. أن يكون لدى المصرف سياسات وإجراءات وضوابط تحد من قدرة الموظفين على ارتكاب جرائم الاحتيال.
- ب. اعتماد إطار عمل لمنع الاحتيال ضمن الرقابة الداخلية وإدارة المخاطر بالتعاون مع دوائر الأعمال المختلفة، وتنفيذ المراجعات الدورية لمختلف الأنظمة والضوابط المطبقة عليها، وتقييم ومعالجة الثغرات ان وجدت.
- ت. توفير الآليات والأنظمة اللازمة لمراقبة الاحتيال والحالات المشبوهة.
- ث. لمنع جرائم الاحتيال التي تتم من خلال معلومات بطاقات الائتمان، يجب تطبيق الضوابط الأمنية على الوسائط التي تحتوي على معلومات حساب فعالة، وأرقام حسابات، وأرقام PIN، وأرصدة الحسابات، بحيث يتم حفظها في مكان أو منطقة خاضعة لضوابط وصول.
- ج. ضمان الفصل في الصلاحيات في الوظائف والمهام ووضع إجراءات وضوابط وصول لمنع الاطلاع على أي بيانات ومعلومات قد يتم استغلالها في عمليات الاحتيال الداخلي.

2.16.5 الاحتيال الخارجي External fraud

يجب على المصرف الالتزام بالآتي:

- أ. مراقبة الحركات والعمليات التي تتم عبر التطبيقات المتاحة عبر الإنترنت (Online)، للكشف المبكر ومنع أي نشاط احتيالي محتمل، ويجب توفير آلية أو نظام لمراقبة الاحتيال (Real-Time Fraud Monitoring System) للكشف عن محاولات الاحتيال والأنشطة المشبوهة.
- ب. إعداد واعتماد السياسات والإجراءات والتدابير الخاصة بمكافحة محاولات الاحتيال من خلال أنظمة مراقبة وكشف الاحتيال والأنشطة المشبوهة.
- ت. إبلاغ سلطة النقد عن أي محاولة احتيال بناء على التعليمات النافذة، ومنها على سبيل المثال محاولة الاختلاس باستخدام وسائل وتقنيات إلكترونية، أو الاحتيال من خلال مواقع مزيفة أو بطاقات انتمان مزورة.

2.16.6. إدارة مخاطر الاحتيال Fraud risk management

يجب على المصرف الالتزام بالآتي:

- أ. تشكيل فريق لإدارة مخاطر الاحتيال لتقييم نقاط الضعف الخاصة بالاحتيال Fraud vulnerability assessments، مثل الإنترنت، وأجهزة الصراف الآلي، الخدمات المتاحة عبر الإنترنت Online.
- ب. أن يخضع فريق إدارة مخاطر الاحتيال للتدريب المستمر لتعزيز مهاراته وكفاءاته.
- ت. تنفيذ تحليل وتقييم للمنتجات والأنظمة والعمليات الجديدة بحثاً عن نقاط الضعف المرتبطة بالاحتيال fraud vulnerabilities قبل إدخالها وتطبيقها في المصرف.
- ث. أن تحتوي الأنظمة المتاحة عبر الإنترنت على ضوابط وميزات أمان عالية، مثل كلمات مرور قوية، والمصادقة الثنائية two-factor authentication، وتعريف حد أعلى لقيمة المعاملات والحركات، وتوفير تنبيهات الرسائل القصيرة للعملاء.
- ج. وضع الإجراءات وضوابط الوصول المناسبة للتأكد من أن الموظفين المخولين فقط هم من يملكون صلاحية الوصول للمعلومات مع إمكانية التحقق.
- ح. تطبيق إجراءات اعرف عميلك (KYC) واعرف موظفك للتأكد من منع الاحتيال، ويجب تنفيذ إجراءات العناية الواجبة للعملاء والموظفين والبائعين قبل تسجيلهم.
- خ. بذل العناية الواجبة في توعية الموظفين والعملاء حول سياسات وإجراءات ومخاطر الاحتيال بشكل منتظم.
- د. تخصيص بريد إلكتروني ورقم هاتف للموظفين والعملاء للإبلاغ عن أي أنشطة احتيالية مشبوهة، وإنشاء فريق متخصص للرد على استفسارات العملاء ومخاوفهم، وتدريب مسؤولي الخدمات المصرفية عبر الهاتف وموظفي الفروع على الردود على استفسارات العملاء ومخاوفهم بشأن الاحتيال.

2.16.7. أمن الأنظمة المتاحة عبر الهواتف الذكية ووسائل الدفع Mobile online services and payment security

الضوابط: يجب على المصرف الالتزام بالآتي:

- أ. اعتماد وتطبيق الإجراءات اللازمة لضمان أمان الخدمات المتاحة عبر الهواتف الذكية ووسائل الدفع.
- ب. إجراء تقييم للمخاطر لتحديد سيناريوهات الاحتيال المحتملة ووضع التدابير المناسبة لمواجهة هجمات الاحتيال باستخدام وسائل الدفع أو الهواتف الذكية.
- ت. تطبيق أعلى معايير الأمن والحماية للمعلومات الحساسة أو السرية المستخدمة في خدمات الهواتف الذكية ووسائل الدفع (Online Mobile Services and Payments)، مثل:

1. Code Obfuscation.
2. Code Protection.
3. Tamper Detection.
4. Code Signing.
5. Certificate Pinning.

ث. توعية العملاء بشأن التدابير الأمنية الخاصة بحماية أجهزتهم المحمولة من الفيروسات والبرامج الضارة الأخرى.

ج. زيادة أمن وسلامة المعاملات التي تتم من خلال بطاقات الدفع كتطبيق تقنية 3D Secure، من قبل جهات إصدار البطاقة لمصادقة حامل البطاقة، ويجب إبلاغ العملاء بإجراء المصادقة والتسجيل من خلال عملية مخصصة مع المصرف.

ح. تطبيق ضوابط لتقييد تثبيت واستخدام تطبيقات الهاتف المحمول على أجهزة المحمول (jailbreak) والتي تسمح لمالك الهاتف بالوصول الكامل إلى الـ (Root) الخاص بنظام التشغيل والوصول إلى جميع ميزات النظام والتطبيقات دون أي قيود.

خ. التأكد من أن تطبيق الهاتف المحمول يوفر التشفير للبيانات المخزنة على جهاز العميل من خلال التطبيق إن وجدت.

د. التأكد من تطبيق الهاتف المحمول لضوابط التحقق من رقم الجوال ورقم IMEI لجهاز العميل (الهوية الدولية للأجهزة المحمولة) عند استخدام التطبيقات لأول مرة.

ذ. السماح للعميل بالوصول إلى تطبيق الهاتف المحمول الخاص بالمصرف من ثلاثة أجهزة معتمدة كحد أقصى.

2.16.8. أمن بطاقات الدفع Payment card security

الضوابط: يجب على المصرف الالتزام بالآتي:

- أ. تطبيق السياسات والإجراءات المعتمدة والامتثال لمعايير الأمان الدولية والممارسات الفضلى الخاصة بأمن وسلامة بيانات بطاقات الدفع، مثل PCI-DSS Payment Card Industry Data Security Standard.
- ب. التأكد من تطبيق الضوابط الأمنية على أنظمة بطاقات الدفع payment card systems and networks والشبكات المستخدمة في نقل بيانات البطاقة لتنفيذ العمليات.
- ت. تطبيق مبدأ المصادقة الثنائية (Two Factor Authentication) مثل كلمة المرور لمرة واحدة (OTP) أو الرقم السري PIN على المعاملات التي تتم من خلال بطاقات الدفع لتقليل مخاطر الاحتيال.
- ث. استخدام رقائق/ شرائح آمنة (متوافقة مع EMV Standards) لتخزين البيانات الحساسة على بطاقة الدفع، وتطبيق تقنيات قوية للمصادقة على البطاقة مثل dynamic data authentication (DDA) أو combined data authentication ("CDA") لمعاملات البطاقة (Online and Offline).
- ج. ألا يكون رقم البطاقة الكامل جزءاً من أي بيانات اتصال مع العملاء.
- ح. تطبيق الضوابط اللازمة على عملية إنشاء رقم التعريف الشخصي للبطاقة (PIN) لتقييد الوصول إلى رقم التعريف الشخصي للعميل على أن يكون فقط للمستلم المقصود.
- خ. تطبيق نظام التنبيهات الفورية Transaction Alerts لإخطار حامل البطاقة عن تنفيذ أي عمليات السحب/إيداع تتم من قبل بطاقة الدفع الخاصة به، على أن يتضمن التنبيه معلومات عن العملية مثل نوع العملية التي تمت ومقدارها ومكان تنفيذها.
- د. تطبيق أنظمة قوية للكشف عن الاحتيال والتزوير تضمن الحد من الأنشطة الاحتيالية المشبوهة.
- ذ. تطبيق آليات لاكتشاف أي سلوك يخالف بشكل كبير عن نمط الاستخدام المعتاد لحامل البطاقة، ويجب إجراء تحقيق في هذه العمليات والتأكد من توفر موافقة حامل البطاقة قبل إتمام العملية.

2.16.9. حماية أنظمة الدفع الإلكترونية Protection of Electronic Payment Systems

يجب على المصرف إعداد واعتماد سياسة تأمين أنظمة الدفع الإلكترونية وتنفيذها ومراجعتها وتحديثها بشكل دوري على أن تشمل بالحد الأدنى ما يلي:

- أ. آليات حماية السجلات الهامة ضد الإقضاء غير المصرح به وإساءة الاستخدام والتلف والتدمير والسرقة والتلاعب.
- ب. ضوابط لرصد ومتابعة الأطراف الخارجية المشاركة في تشغيل أنظمة الدفع والتسوية.

- ت. تحديد ثلاث محاولات فاشلة كحد أقصى لتسجيل الدخول أو المصادقة، بعدها يتم حظر الوصول إلى أنظمة المدفوعات الإلكترونية بشكل مؤقت أو دائم. ويجب على المصرف اعتماد الإجراءات اللازمة لإعادة تنشيط الوصول المحظور. وضمان تطبيقها، على أن تتم عملية إعادة التنشيط بعد بذل إجراءات العناية الواجبة لضمان التحقق من هوية المستخدم.
- ث. اعتماد إجراءات تضمن التسليم الآمن لبيانات اعتماد العملاء (اسم المستخدم وكلمة المرور ورقم التعريف الشخصي) وإجراء مصادقة لأجهزة العملاء وضمان أمن بيانات الاعتماد وبرامج الدفع (تطبيقات الويب والهواتف الذكية وما إلى ذلك).
- ج. ضمان تطبيق ضوابط وإجراءات فعالة لتقليل مخاطر التحويل غير المصرح به للأموال بناءً على مخاطر تكنولوجيا المعلومات المستخدمة أو مخاطر الملف الشخصي للعميل.
- ح. الالتزام بإجراء تدقيق مستقل لأمن أنظمة الدفع الإلكترونية سنوياً وفقاً لإجراءات التقييم المعتمدة الخاصة بإدارة الثغرات الأمنية، والممارسات الفضلى المتبعة بالخصوص (مثل PCI-DSS و EMV).
- خ. أن تحتوي جميع عمليات المدفوعات الإلكترونية على أرقام مرجعية فريدة للمعاملات لتمكين التتبع والمساءلة.
- د. ألا تكشف رسائل التحقق من المعاملات تفاصيل أو بيانات حساسة عن أنظمة الدفع المستخدمة مثل (البنية التحتية أو التطبيقات).
- ذ. تطبيق تدابير فعالة لإخطار وتنبيه العملاء بالتغييرات المهمة على الملف الشخصي للدفع (payment profile)، بما يشمل (التغييرات في القيم المحددة مسبقاً مثل كلمة المرور وحدود التحويل، تسجيل مستفيدين جدد، التحويلات الإلكترونية للمستفيدين).
- ر. اعتماد تقنيات وخوارزميات تشفير قوية ومعتمدة دولياً لحماية المعلومات الحساسة أثناء التخزين أو النقل.
- ز. التأكد من أن إجراءات التحقق من الهوية الشخصية مثل الأسئلة الشخصية التي تستخدمها مراكز خدمة العملاء للتحقق من هوية العميل، ليست عامة ولا يسهل الحصول عليها أو تكرارها (مثل العلاقات المصرفية والرصيد الحالي والمعلومات غير المتاحة على البطاقة والأسئلة الشخصية والمعاملات الأخيرة).
- س. عدم إتاحة إجراء التغييرات على المعلومات الحساسة للعملاء (مثل رقم الهاتف المحمول وعنوان البريد الإلكتروني) من خلال ماكينة الصراف الآلي وتطبيقات الهاتف المحمول وخدمة الاستجابة الصوتية التفاعلية (IVR) والخدمات المصرفية عبر الإنترنت، إلا بعد التأكد من هوية العميل باستخدام العوامل المتعددة للمصادقة، وفي حالة تغيير رقم الهاتف الخليوي يتم إرسال العامل الثاني للمصادقة إلى الرقم القديم.
- ش. التأكد من تطبيق ضوابط فعالة للتحقق من سلامة المعلومات التي تتم معالجتها بواسطة أنظمة الدفع الإلكترونية مثل التوفيق بين أرصدة الحسابات بعد تحديثات المعاملات بين الأنظمة المختلفة.
- ص. التأكد من تطبيق ضوابط فعالة لضمان التخفيف من المخاطر والتهديدات المتعلقة بالربط الشبكي (مثل man-in-the-authentication bypass, network sniffing, middle attack، وما إلى ذلك).

2.16.10 مراقبة معاملات الدفع الإلكتروني Electronic Payment Transaction Monitoring

الضوابط: يجب على المصرف الالتزام بالآتي:

- أ. إعداد واعتماد آلية فعالة لمراقبة معاملات الدفع الإلكترونية وضمان تنفيذها ومراجعتها بشكل دوري على أن تكون متوافقة مع التعليمات النافذة وحسب المخاطر والضوابط المطبقة.
- ب. أن تراعي عملية مراقبة معاملات الدفع الإلكترونية عوامل الخطر التالية بالحد الأدنى (حدود المعاملات، سيناريوهات الاحتيال الشائعة، أنماط دفع غير طبيعية فيما يتعلق بسجل معاملات الدفع، تفضيل معاملة العميل، مخاطر موقع الدافع والمدفوع له في وقت تنفيذ معاملة الدفع، محاولات الدخول الفاشلة، التغييرات في المعلومات الحساسة للعملاء).

- ت. التحقيق من المعاملات غير العادية وإبلاغ العملاء إذا لزم الأمر.
- ث. على المصرف إخطار العملاء من خلال قنوات الاتصال الفعالة عن جميع المعاملات التي تتم على حساباتهم بما في ذلك المعاملات المرفوضة.

2.16.11. أمن أجهزة الخدمة الذاتية للعملاء (ATMs, POSs, ...etc) Customer Self Service Machines

الضوابط: يجب على المصرف الالتزام بالآتي:

- أ. تطبيق ضوابط وتدابير الأمن المادي اللازمة لحماية أجهزة الخدمة الذاتية للعملاء من السرقة والتلف، والالتزام بتعليمات سلطة النقد بشأن متطلبات الأمن والسلامة لأجهزة الصراف الآلي.
- ب. تطبيق ضوابط الفصل في الصلاحيات بين معالجة البطاقة، وإنشاء رقم التعريف الشخصي (PIN)، وتسليم البطاقة ورقم التعريف الشخصي (PIN) للعميل، والتأكد من أن البطاقة الصادرة غير فعالة (Inactive) والبداة بإجراءات عملية تفعيلها.
- ت. تطبيق ضوابط إيقاف/ حجب البطاقة (Block) بعد ثلاث محاولات فاشلة لإدخال رقم PIN وإخطار العميل بشكل فعال لمنع سوء الاستخدام المحتمل، وأن تتم عملية إعادة تفعيلها من خلال إجراءات تضمن اتخاذ العناية الواجبة للتأكد من هوية ومعلومات العميل.
- ث. إجراء فحوصات أمنية لمواقع أجهزة الخدمة الذاتية للعملاء بشكل دوري للتحقق من فعالية الضوابط والتدابير الأمنية المطبقة.
- ج. ضمان تشفير أرقام PIN الخاصة بالعميل أثناء الإرسال.
- ح. توفير آليات المتابعة والمراقبة اللازمة لأنشطة مزودي الخدمات من الأطراف الخارجية الذين يمتلكون صلاحية الوصول إلى جهاز الصراف الآلي، وعدم منحهم صلاحية الدخول إلا برفقة موظفي المصرف المصرح لهم، وتوفير اتفاقيات إسناد مناسبة توضح الأدوار والمسؤوليات.
- خ. أن تقوم الأجهزة الذاتية للخدمة الذاتية للعملاء بمصادقة معاملات العملاء (authenticate customer transactions) باستخدام البطاقة (مثل بطاقة الخصم، وبطاقة الائتمان، وبطاقة مدنية)، وأرقام PIN (ثابتة أو لمرة واحدة).
- د. توعية العملاء من خلال رسائل التوعية والتنبيه بشكل منتظم توضح الاستخدام الآمن لأجهزة الصراف الآلي مثل:
 1. كفاءة تحقق العميل من عدم تثبيت جهاز أو شيء غير طبيعي على جهاز الصراف الآلي.
 2. كفاءة تحقق العميل من فتحة البطاقة قبل إدخال بطاقة الدفع للتأكد من عدم تثبيت قارئ بطاقة خارجي غير طبيعي.
- ذ. أن تلتزم أجهزة نقاط البيع (POS) بتطبيق أفضل الممارسات والمعايير مثل: متطلبات PCI PED / PTS ومتطلبات أمن PIN، وكذلك:

1. توفير الخصوصية والحماية للعملاء أثناء استخدام POS وأثناء إدخال رمز PIN على الأجهزة الطرفية لـ POS.
2. توفير التشفير اللازم لبيانات العملاء والعملية المنفذة أثناء جميع مراحل انتقالها وعدم تمرير بيانات البطاقة وحفظها بشكل واضح (Clear Text) لتجنب سرقة البيانات.
3. توفير تقنيات منع التلاعب بشكل واضح وسريع الاستجابة في حالة اكتشاف محاولات تلاعب.
4. يجب أن يدعم النظام الخاص بأجهزة نقاط البيع (POS) أفضل تقنيات التشفير.
5. يجب ألا تحتوي إيصالات البيع أو الدفع على تفاصيل وبيانات حساسة خاصة بالعميل أو بطاقة الائتمان.

2.16.12. تكنولوجيا اللاتلامسية Contactless Technology

- أ. إجراء تقييم للمخاطر لتحديد المخاطر الناجمة عن استخدام تقنية NFC و QR code وتطبيق الضوابط للحد من تلك المخاطر.
- ب. تطبيق الحدود المناسبة على عدد وقيمة معاملات NFC، وأن يتم فرض مصادقة إضافية على المعاملات اللاحقة.

ت. إخطار العملاء من خلال إرسال تنبيهات لقنوات الاتصال الفعالة للمعاملات التي تتم باستخدام تقنيات اللاتلامسية.

2.16.13. الأنظمة المصرفية الرئيسية Core banking systems

الضوابط: يجب على المصرف الالتزام بالآتي:

- أ. إعداد واعتماد سياسات وإجراءات عمل خاصة بإدارة ومستخدمي الأنظمة المصرفية الرئيسية بما يراعي ضوابط الرقابة الثنائية والفصل في الصلاحيات.
- ب. إعداد واعتماد مصفوفة صلاحيات مالية ووظيفية (Authority Matrix) شاملة لكافة مستخدمي الأنظمة المصرفية ولكافة المسميات الوظيفية ومنح الحد الأدنى من الصلاحيات المالية والوظيفية اللازمة لإنجاز مهام العمل.
- ت. استخدام آليات المصادقة (authentication mechanisms) التي تضمن وصول الموظفين المخولين بشكل واضح إلى المعلومات الحساسة، وأن تكون الصلاحيات المالية والوظيفية الممنوحة مستندة لمصفوفة الصلاحيات المعتمدة بالخصوص.
- ث. استخدام نسخ معتمدة ومرخصة للبرامج والأنظمة الخاصة بتشغيل الأنظمة المصرفية مع ضرورة توفر عقود صيانة من المورد لضمان استمرارية عملها.
- ج. إن تنسم الأنظمة المصرفية بالمرونة من خلال ضمان استمرارية عملها والتوافرية العالية على مستوى الأعمال والمستويات الفنية.
- ح. توفير الآليات والتقنيات اللازمة لتأمين التطبيقات وقواعد البيانات الخاصة بالأنظمة المصرفية، وفقاً للسياسات والإجراءات المعتمدة بالخصوص مثل التشفير وإدارة المفاتيح.
- خ. تنفيذ تقييم نقاط الضعف VA واختبارات الأمان اللازمة بشكل دوري للتطبيقات المرتبطة بالأنظمة المصرفية وقواعد البيانات.
- د. توفير سياسة للامتثال، ومتطلبات الأمان، والأحداث الأمنية، وتوثيق وأرشفة الأحداث التي تتم على الأنظمة المصرفية بهدف الرجوع إليها عند الحاجة أو تحليلها والتأكد من الامتثال للمتطلبات القانونية للاحتفاظ بالبيانات.
- ذ. تطبيق إجراءات مراقبة النزاهة (Integrity control processes) على البيانات الموجودة في قاعدة البيانات، بالإضافة إلى توفير آلية لتوثيق إصدارات النظام ضمن إجراءات تطبيق التغييرات (versioning system for the application changes).
- ر. أن تكون المعلومات والبيانات الحساسة مخفية عن الوصول غير المصرح به من خلال تطبيق الإجراءات الأمنية مثل تقنيات التشفير والعزل بمناطق آمنة، ويجب حماية المعلومات الحساسة لقاعدة بيانات التطبيقات والأنظمة المصرفية باستخدام أحدث معايير التشفير.
- ز. تطبيق ضوابط أمان خاصة بالأنظمة والتطبيقات المصرفية المتاحة عبر الإنترنت مثل (قطع اتصال المستخدم بعد خمس دقائق من عدم استخدام الخدمة، عدم السماح بالدخول المتزامن لأكثر من خدمة بنفس الوقت باستخدام نفس اسم المستخدم، وتقتصر صلاحية كلمات المرور لمرة واحدة (OTP) على خمس دقائق كحد أقصى).
- س. أن تتضمن التطبيقات المصرفية المتاحة عبر الإنترنت (بخلاف تطبيقات الهاتف المحمول) عناصر تحكم إضافية مثل صورة الوصول الآمن (secure access image) و/أو رسالة آمنة عند تسجيل الدخول للمساعدة في الكشف عن مواقع التصيد المشبوهة phishing sites.
- ش. اعتماد تدابير موثوقة وفعالة للمصادقة (Authentication Measures) من خلال تطبيق ضوابط مصادقة قوية متعددة العوامل (multi factor authentication) مثل: استخدام عامل تحقق إضافي (تنشيط الحساب، والمعاملات المالية مثل تحويل الأموال، ودفع الفواتير وإضافة المستفيدين) باستخدام طرق تحقق إضافية منها (إنشاء كلمة سر لمرة واحدة (OTP) بواسطة الجهاز، إرسال كلمة السر OTP إلى العميل عبر الرسائل القصيرة، الشهادات الرقمية المخزنة في البطاقات الذكية

(digital certificates stored in smart cards)، استخدام الأجهزة الأخرى التي في حوزة العميل لترخيص المعاملات كعامل إضافي).

ص. تنفيذ ضوابط للكشف عن محاولات التصيد الاحتيالي لتحديد المستخدم (مثل اسم المستخدم)، وتحديد التطبيق (أسئلة تسجيل الدخول المسبق pre logon challenge questions، ومفتاح الموقع، والمصادقة متعددة الشاشات، وما إلى ذلك) ومصادقة المستخدم بكلمة مرور كجزء من عملية المصادقة.

ض. التأكد من اتخاذ الإجراءات المناسبة وتطبيق ضوابط الأمن المعتمدة للتحقق من هوية المستخدمين المتاح لهم الوصول عن بُعد لأنظمة وخدمات المصرف.

2.16.14. توفير المراجعة الدورية لمتطلبات وضوابط حماية التطبيقات الداخلية والمتاحة عبر الانترنت من المخاطر السيبرانية.

3. صمود الامن السيبراني وإدارة استمرارية العمل

Cybersecurity Resilience and Business Continuity Management -BCM

الهدف: ضمان توافر الأنظمة والبيانات والخدمات الالكترونية للمصرف خلال الأحداث الطارئة والكوارث وتقليل الآثار الناتجة عن الاضطرابات والحوادث السيبرانية على الأنظمة الحرجة، من خلال تطبيق متطلبات صمود الأمن السيبراني وإعداد واعتماد برنامج مناسب لاستمرارية الأعمال والتعافي من الكوارث.

الضوابط: يجب على المصرف الالتزام بالآتي:

- 3.1. تحديد وتوثيق واعتماد وتطبيق متطلبات الامن السيبراني ضمن إدارة استمرارية اعمال المصرف.
- 3.2. اعتماد السياسات والإجراءات والخطط المتعلقة بإدارة استمرارية العمل وصمود الأمن السيبراني.
- 3.3. وضع خطط الاستجابة لحوادث الامن السيبراني التي قد تؤثر على استمرارية أعمال المصرف.
- 3.4. أن يخضع الموقع البديل لاستعادة النظم والعمليات والخدمات الحرجة (DRS) لضوابط الأمن وإجراءات الوصول وفقاً لتقييم مخاطر المواقع الحساسة في المصرف.
- 3.5. أن يكون الموقع البديل (AS) يحاكي بتجهيزاته الموقع الأصلي.
- 3.6. إعداد واعتماد استراتيجية النسخ الاحتياطي وتطبيقها ومراجعتها بشكل دوري، على أن تتضمن (دورية النسخ الاحتياطي backup periodicity؛ وآليات التخزين والاتلاف storage and disposal mechanisms، والتدابير الأمنية لحماية المعلومات ووسائل التخزين).
- 3.7. عمل نسخة احتياطية من المعلومات والاحتفاظ بها وتخزينها وفقاً لاستراتيجية النسخ الاحتياطي، وإجراء اختبارات الاستعادة الدورية Periodic restoration tests على المعلومات المخزنة بالنسخ الاحتياطي.
- 3.8. توفير المراجعة الدورية لمتطلبات وضوابط الامن السيبراني الخاصة بإدارة استمرارية أعمال المصرف.

4. الامن السيبراني المتعلق بالأطراف الخارجية والحوسبة السحابية

Third-Party and Cloud Computing Cybersecurity

4.1. الامن السيبراني المتعلق بالأطراف الخارجية Third-Party Cybersecurity

الهدف: ضمان حماية أصول المصرف من مخاطر الامن السيبراني المتعلقة بالأطراف الخارجية، وفقاً للسياسات والاجراءات التنظيمية للمصرف والتعليمات النافذة.

الضوابط: يجب على المصرف الالتزام بالآتي:

- 4.1.1. تحديد واعتماد وتطبيق متطلبات الأمن السيبراني ضمن سياسة الاستعانة بمصادر خارجية وتعميمها على الجهات ذات العلاقة، ومراجعة السياسة دورياً من قبل إدارة المخاطر وأمن المعلومات والدوائر ذات العلاقة.
- 4.1.2. أن يكون مجلس الإدارة والإدارة العليا للمصرف مسؤولاً عن الحوكمة والامتثال وإدارة المخاطر المتعلقة بالإسناد الخارجي، وضمان جودة الخدمات المقدمة.
- 4.1.3. الحصول على الموافقة المسبقة من سلطة النقد قبل البدء بإجراءات التعاقد للحصول على خدمات الإسناد الخارجي، بما يتضمن توضيح نطاق تقديم الخدمة والإجراءات والضوابط الوقائية المتخذة بالخصوص.
- 4.1.4. إجراء تقييم شامل للمخاطر المرتبطة بالإسناد الخارجي، وتطبيق العناية الواجبة لإعداد ضوابط مناسبة لمقدمي الخدمات.
- 4.1.5. إبرام اتفاقيات تتبّع عمليات الإسناد الخارجي مثل SLA, NDA.
- 4.1.6. أن تتضمن إجراءات الاستعانة بمصادر خارجية شرط موافقة المصرف على أي تعاقد من الباطن بين مقدم الخدمة وأطراف أخرى.
- 4.1.7. أن لا تتضمن اتفاقيات الاستعانة بمصادر خارجية ما يعيق قدرة المصرف أو سلطة النقد على إجراء عمليات التدقيق والتفتيش.
- 4.1.8. أن تتم مراقبة ومراجعة التقارير المقدمة من مقدم خدمة الإسناد الخارجي بشكل مستمر، وإجراء عمليات التدقيق لضمان الالتزام باتفاقيات مستوى الخدمة SLAs.
- 4.1.9. في حالة تقديم خدمات الإسناد الخارجي من خلال الوصول عن بُعد، يجب على المصرف التأكد من تشفير قنوات الاتصال وحمايتها باستخدام أحدث التقنيات، وتوفير الآليات اللازمة لمراقبة وتوثيق العمليات التي تتم على أصول المصرف خلال عملية الاتصال.
- 4.1.10. التأكد من التزام مقدمي خدمات الإسناد الخارجي بضوابط إدارة التغييرات والتحديثات المعتمدة في المصرف، عند تطبيق أية تغييرات أو تحديثات للأنظمة أو البرامج أو Source Code، والتأكد من أن مطوري مقدم الخدمة يعملون فقط ضمن البيانات الخاصة بالتطوير والاختبار.
- 4.1.11. تطوير المهارات التكنولوجية للموظفين الذين يتواصلون بشكل مستمر مع مقدمي خدمات الإسناد الخارجي الخاصة بالبيئة التكنولوجية للمصرف كإجراء للطوارئ.
- 4.1.12. أن تتضمن اتفاقية الاستعانة بمصادر خارجية من عدم وجود أي عوائق قانونية عند الحاجة للوصول أو الحصول على الكود application source code الذي طوره مقدم خدمة الإسناد الخارجي.
- 4.1.13. على مقدم خدمة الإسناد الخارجي تزويد المصرف بتقارير منتظمة عن أي أحداث أمنية ذات علاقة بالخدمة.
- 4.1.14. التأكد من تطبيق مقدم خدمة الإسناد للإجراءات الخاصة بالتوافرية الدائمة واستمرارية العمل (High Availability and Business Continuity) لضمان عدم انقطاع الخدمة في حالات الطوارئ والأحداث الاستثنائية.
- 4.1.15. التأكد من تطبيق مقدم الخدمة للحد الأدنى من السياسات والإجراءات والضوابط الأمنية لضمان أمن أنظمة وعمليات المصرف.
- 4.1.16. تحديد وإدراج الحد الأدنى من متطلبات وضوابط الأمن السيبراني في جميع اتفاقيات الاستعانة بمصادر خارجية تتعلق بتكنولوجيا المعلومات.
- 4.1.17. بذل العناية الواجبة أثناء اختيار المصرف للأطراف الخارجية التي سيتم التعاقد معها ويجب أن تشمل دراسة إمكانيات الأطراف الخارجية بما يخص:
 - أ. التعرف الجيد على مقدم الخدمة من خلال دراسة المؤهلات والخبرات الخاصة بالطاقت المختص بتقديم الخدمة والتأكد من ان لدى مقدم الخدمة الخبرة والكفاءة الكافية لتنفيذ النشاط المقترح على مدى الفترة المتعاقد عليها والتأكد من حسن سمعة مقدم

الخدمة وأنظمة الالتزام والشكاوى والتظلمات لديه.

ب. التأكد من القدرة المالية لمقدم الخدمة والقدرة على إتمام التعاقد حتى في ظل الظروف المعاكسة، وقدرته على الالتزامات ببنود التعاقد.

ت. التأكد من وجود ضوابط داخلية وسياسة معتمدة للأمن السيبراني لدى مقدم الخدمة.

ث. ضوابط وممارسات الأمن السيبراني.

ج. ترتيبات وخطط استمرارية العمل والتعافي من الكوارث BCP وDR لديه.

ح. الامتثال للقوانين واللوائح المعمول بها.

4.1.18. أن تتضمن اتفاقية الاستعانة بمصادر خارجية بالحد الأدنى ما يلي:

أ. نطاق الخدمات ومتطلبات مستويات الخدمة.

ب. الأدوار والمسؤوليات فيما يتعلق بتنفيذ متطلبات الأمن السيبراني.

ت. سرية وأمن المعلومات المشتركة.

ث. متطلبات إدارة العمليات والمخاطر.

ج. متطلبات استمرارية الأعمال وإدارة الأزمات.

ح. الحق في التدقيق والتفتيش.

خ. شروط إنهاء التعاقد.

د. المتطلبات المتعلقة بالإخطارات والكشف عن أحداث خرق البيانات.

4.1.19. الاحتفاظ بقائمة محدثة لجميع اتفاقيات الاستعانة بمصادر خارجية.

4.1.20. إجراء تقييم دوري لمقدمي خدمات الاسناد لضمان كفاية الضوابط المنفذة والتي سيتم تنفيذها لتلبية متطلبات الأمان اللازمة وفقا لاتفاقية الاستعانة.

4.1.21. تنفيذ عمليات متابعة لأنشطة مزودي خدمة الاسناد الخارجيين، على ان تغطي عملية المتابعة بالحد الأدنى:

أ. الامتثال المستمر لمتطلبات الأمن.

ب. الامتثال لمتطلبات سرية وأمن المعلومات.

ت. الامتثال لمتطلبات استمرارية الأعمال والتعافي من الكوارث.

4.1.22. توثيق وتسجيل المخاطر والتهديدات التي تم رصدها أثناء عملية المراقبة ومتابعتها لتصويبها وإغلاقها.

4.1.23. مراجعة متطلبات الأمان للاتفاقية وتحديثها بشكل دوري أو عند إجراء تغييرات كبيرة في الخدمات التي يقدمها مقدمو الطرف الثالث.

4.1.24. ضمان التخلص الآمن من أصول المعلومات التي تم تبادلها خلال اتفاقية الاستعانة بمصادر خارجية.

4.2. الامن السيبراني المتعلق بالحوسبة السحابية Cloud Computing Cybersecurity

الهدف: ضمان معالجة المخاطر السيبرانية وتنفيذ متطلبات الامن السيبراني للحوسبة السحابية بشكل ملائم وفعال، وفقا للسياسات والاجراءات التنظيمية للمصرف، والتعليمات النافذة، وضمان حماية الاصول المعلوماتية والتقنية للمصرف على خدمات الحوسبة السحابية التي تتم استضافتها أو معالجتها أو إدارتها بواسطة أطراف خارجية.

الضوابط: يجب على المصرف الالتزام بالآتي:

4.2.1. تحديد وتوثيق واعتماد وتطبيق متطلبات الامن السيبراني الخاصة باستخدام خدمات الحوسبة السحابية.

4.2.2. إعداد واعتماد سياسة تلي الجوانب الأمنية للخدمات السحابية وتنفيذها وتعميمها ومراجعتها وتحديثها بشكل دوري، على أن

- تتضمن سياسة أمن الحوسبة السحابية بالحد الأدنى ما يلي:
- أ. العمليات والضوابط التكنولوجية لكل نوع من أنواع الخدمات السحابية.
 - ب. الرقابة والمسؤولية التشغيلية اليومية وفصل الأدوار.
 - ت. مراعاة مخاطر مشاركة الخدمة مع أكثر من عميل واختلاط البيانات ومعالجة وتخزين البيانات في مواقع متعددة.
 - ث. الامتثال للمتطلبات القانونية الخاصة بمكان حفظ البيانات.
- 4.2.3 قبل البدء بإجراءات إتمام التعاقد مع مزودي الخدمات السحابية، على المصرف تحديد ما إذا كان استخدام الخدمات السحابية يتوافق مع شهية المخاطر واستراتيجية المصرف والسياسات والإجراءات المعتمدة، ويجب أن يجري تصنيف المعلومات الخاصة بالوظيفة أو الخدمة المسندة على الحوسبة السحابية وتحديد البيانات الحساسة المعرضة للمخاطر.
- 4.2.4 أن تغطي متطلبات الأمن السيبراني الخاصة باستخدام خدمات الحوسبة السحابية بحد أدنى ما يلي:
- أ. تصنيف البيانات قبل استضافتها لدى مقدمي خدمات الحوسبة السحابية، وإعادتها للمصرف عند انتهاء الخدمة.
 - ب. فصل بيئة تكنولوجيا المعلومات الخاصة بالمصرف (وخصوصا الخوادم الافتراضية) عن غيرها من البيئات التابعة لجهات أخرى في خدمات الحوسبة السحابية.
- 4.2.5 إجراء تقييم للمخاطر يأخذ في الاعتبار فوائد وإيجابيات استخدام الخدمات السحابية والمخاطر المرتبطة بها ويضع تدابير التخفيف، على أن يأخذ التقييم بعين الاعتبار بالحد الأدنى:
- أ. التأثير المحتمل لأي انقطاع في الخدمة السحابية بما في ذلك التأثير على توفر البيانات والخدمات.
 - ب. إدارة صلاحيات الوصول وفصل المسؤوليات فيما يتعلق بالخدمات السحابية.
 - ت. موقع تخزين البيانات على السحابة.
 - ث. إدارة المنافذ والتحكم والسمعة والخبرة واستراتيجيات الخروج.
 - ج. المتعاقدون من الباطن الذين يستخدمهم مقدمو الخدمات السحابية.
 - ح. مخاطر احتكار الخدمة السحابية لدى مزود واحد.
- 4.2.6 إجراء مراجعة وتقييم لامتثال مزود الخدمة السحابية للضوابط والممارسات الأمنية الفضلى ذات العلاقة بالخدمات المقدمة وإدارة وحفظ البيانات وآلية التخلص منها، والتدقيق الخارجي.
- 4.2.7 بذل العناية الواجبة للإشراف والمتابعة على أعمال مقدم الخدمات السحابية من أجل إدارة المخاطر الأمنية المرتبطة بالخدمة السحابية بشكل فعال، كجزء من إجراءات الحوكمة وإدارة المخاطر الشاملة.
- 4.2.8 الامتثال التنظيمي والقانوني للأمن السيبراني والتعليمات النافذة.
- 4.2.9 ضمان وجود اتفاقية مكتوبة مع مزود الخدمات السحابية بحيث تشمل المتطلبات التالية:
- أ. تحديد نطاق الخدمة واتفاقيات المستوى التشغيلي للخدمة والأدوار والمسؤوليات.
 - ب. مواقع تخزين البيانات واستمرارية الأعمال واستعادة البيانات بعد الكوارث بعد الحصول على موافقة سلطة النقد المسبقة وخصوصية البيانات والسرية وتقاسم المعلومات والوصول إلى البيانات والتشفير وإمكانية نقل والاحتفاظ بالبيانات.
 - ت. مدونة السلوك وإدارة المنافذ.
 - ث. إدارة الحوادث وإدارة الأزمات واستراتيجيات الإبلاغ عن الحوادث.
 - ج. إجراءات الإنهاء الآمن للتعاقد.
- 4.2.10 توفير المراجعة الدورية لمتطلبات وضوابط الأمن السيبراني الخاصة بخدمات الحوسبة السحابية.