



CBY

## منشور دوري رقم (1) لسنة 1445هـ / 2024م بشأن تعليمات الأمان السيبراني والتكيف مع المخاطر السيبرانية

### المقدمة:

تهدف تعليمات هذا المنشور لحماية المعلومات وتوفير الحد الأدنى من المطلبات الأساسية في الأمان السيبراني لتقليل المخاطر على الأصول المعلوماتية والتقنية للمؤسسة المالية من التهديدات الداخلية والخارجية إضافة إلى تعزيز سلامة وسمعة ومهنية القطاع المالي والمصرفي في الجمهورية اليمنية، وما يكفل حماية عملياته والحفاظ على عملائه وتعزيز الثقة فيما بينهم من خلال تعزيز سرية وسلامة وتوافر البيانات وفقاً لأفضل الممارسات والمعايير المتبعة في مجال الأمان السيبراني.



Date: 18/02/2024

NO: .....

CBY

قطاع الرقابة على البنوك  
مكتب الوكيل

البنك المركزي اليمني  
المركز الرئيسي  
صنعاء  
التاريخ: 1445 / 08 / 1445 هـ  
الرقم: ق. د. 338

## الفهرس

3	الفصل الأول
3	التسمية والتعرifات
7	الأهداف ونطاق السريان:
8	الفصل الثاني
8	الأدوار والمسؤوليات
8	أولاً : حوكمة الأمن السيبراني:
8	ثانياً: سياسة وبرنامج الأمن السيبراني:
11	الفصل الثالث
11	إدارة المخاطر السيبرانية
11	أولاً: تحديد العمليات الحرجة وأصول المعلومات الداعمة في المؤسسة المالية:
11	ثانياً: تقييم المخاطر السيبرانية:
12	ثالثاً: سجل المخاطر السيبرانية:
14	الفصل الرابع
14	ضوابط الحماية
14	أولاً: حماية الأنظمة والبرمجيات والشبكات والأجهزة الشبكية:
18	ثانياً: ضوابط الحماية الخاصة بالبريد الإلكتروني:
19	ثالثاً: السجلات:
20	الفصل الخامس
20	الكشف عن الحوادث السيبرانية
21	الفصل السادس
21	الاستجابة للحوادث السيبرانية الطارئة والتعافي منها
23	الفصل السابع
23	الاختبارات
24	الفصل الثامن
24	الإسناد الخارجي
26	الفصل التاسع
26	التنوعية الأمنية
26	أولاً: التدريب وزيادة الوعي:
27	ثانياً: تبادل معلومات الحوادث السيبرانية..
28	الفصل العاشر
28	الأمن السيبراني لوسائل التواصل الاجتماعي
29	الفصل الحادي عشر
29	أحكام عامة وختامية





Date: 18/02/2024

NO: .....

CBY

قطاع الرقابة على البنوك  
مكتب الوكيل

البنك المركزي اليمني  
المركز الرئيسي  
صنعاء  
التاريخ: 08/08/1445 هـ  
الرقم: ق. د. 338

## الفصل الأول

### التسمية والتعريفات والأهداف ونطاق السريان

#### المادة (1) : التسمية :

يسعى هذا المنشور (تعليمات الأمان السيبراني والتكيف مع المخاطر السيبرانية).

#### المادة (2) : التعريفات :

يكون للألفاظ والعبارات التالية حينما وردت في هذا المنشور المعاني المحددة أمام كل منها ما لم

تدل القرينة على خلاف ذلك:

الجمهورية اليمنية.	الجمهورية
البنك المركزي اليمني.	البنك المركزي
البنك أو المصرف أو أي شخص آخر مرخص له من البنك المركزي بمزاولة الأعمال والأنشطة المالية بما فيه الشركات والمؤسسة المتخصصة بالتمويل أو أعمال التأمين أو الصرافة أو تحويل الأموال أو استثمارها وتوظيفها أو شركات الخدمات المالية وغير ذلك من الأعمال والأنشطة المالية المشابهة أو التي يحددها البنك المركزي.	المؤسسة المالية (Financial institution)
مجلس إدارة المؤسسة المالية ومن في حكمه في المستوى التنظيمي.	مجلس الإدارة
المدير العام أو نائب المدير العام أو المدير التنفيذي أو مدير التدقيق أو المدير المالي أو مدير المخاطر أو مدير الامتثال، أو أي موظف له سلطة تنفيذية موازية لسلطات أي من المذكورين، أو من في حكمهم.	الإدارة التنفيذية
الحفظ على سرية وتكاملية وتوافرها المعلومات وأصول المعلومات التابعة للمؤسسة المالية ضمن الفضاء السيبراني من أي تهديد سيبراني، عن طريق مجموعة من الوسائل والسياسات والتعليمات وأفضل الممارسات بهذا الخصوص.	الأمن السيبراني (Cyber Security)
الشبكات الداخلية والأجهزة الطرفية والخوادم الرئيسية والبرمجيات العاملة عليها وجميع الأجهزة المساعدة لها في مراكز البيانات الرئيسية أو الاحتياطية الخاصة بالمؤسسة المالية.	بيئة تكنولوجيا المعلومات والاتصالات
الأجهزة والمعدات الشبكية وأجهزة الحماية وخطوط الهاتف والخطوط المبنية وخطوط الفايبر وخطوط خدمات الإنترنت بجميع أنواعها المستخدمة في بيئة تكنولوجيا معلومات المؤسسة المالية.	أنظمة الاتصالات
الأنظمة المرتبطة بنشاط المؤسسة المالية بصورة مباشرة ويؤدي توقيفها أو اختراقها إلى توقف نشاط/عمل المؤسسة المالية بشكل كلي أو جزئي.	الأنظمة الحرجة
أي بيانات شفوية أو مكتوبة أو سجلات أو إحصاءات أو وثائق مكتوبة أو مصورة أو مسجلة أو مخزنة إلكترونيًا أو بأي طريقة أخرى تعد ذات قيمة للمؤسسة المالية.	المعلومات (Information)



Date: 18/02/2024

NO: .....

C BY

## قطاع الرقابة على البنوك

### مكتب الوكيل

**البنك المركزي اليمني**  
**المركز الرئيسي**  
**صنعاء**  
**التاريخ: 08/08/1445 هـ**  
**الرقم: ق. د. 338**

الحقائق الخام يمكن توضيحها بالحروف والرموز والأرقام المخزنة ضمن بيئه تكنولوجيا المؤسسة المالية.	البيانات (Data)
أي ملفات إلكترونية، أو غير إلكترونية، أو أجهزة، أو وسائل تخزين، أو برامج، أو أي من مكونات بيئه تكنولوجيا المعلومات والاتصالات المتعلقة بأعمال المؤسسة المالية.	أصول المعلومات (Information Assets)
مجال افتراضي ضمن بيئه المعلومات يتكون من شبكة متراقبة من البنية التحتية لأنظمة المعلومات بما في ذلك الإنترن特 وشبكات الاتصالات وأنظمة الكمبيوتر وأجهزة الموبايل والأجهزة اللوحية الذكية.	الفضاء السيبراني (Cyberspace)
محاولة لسرقة المعلومات أو كشفها أو تغييرها أو تعطيلها أو إتلافها من خلال الوصول غير المصرح به إلى بيئه تكنولوجيا المعلومات والاتصالات أو من خلال هجوم إلكتروني يشنه مجرمو الإنترن特 على شبكات وأنظمة الكمبيوتر.	الهجوم السيبراني / الاختراق (Cyber Attack)
قدرة المؤسسة المالية على توقع، وتحمل، واحتواء الهجوم السيبراني ثم التعافي منه سريعاً.	التكيف السيبراني (Cyber Resilience)
طرف أو حدث يتحمل أن يستغل (عن قصد أو غير قصد) بسبب ثغرة أو مجموعة من الثغرات أو نقاط الضعف التي قد تكون موجودة في بيئه تكنولوجيا المعلومات والاتصالات للمؤسسة المالية مما قد يؤثر على الأمن السيبراني فيها.	التهديد السيبراني (Cyber Threat)
أي حدث في نظام أو شبكة معلومات المؤسسة المالية ينتج عنه هجوم سيبراني.	الحدث السيبراني (Cyber Event)
حدث سيبراني قد يهدد سرية أو سلامة أو توفر نظام أو شبكة المعلومات أو البيانات.	الحادث السيبراني (Cyber Incident)
احتمال كامن للتعرض للخسارة أو الضرر في بيئه تكنولوجيا المعلومات أو أنظمة اتصالات المؤسسة المالية.	المخاطر السيبرانية (Cyber Risk)
المخاطر التي تهدد سرية أو سلامة أو توافر المعلومات والبيانات، وتشمل على سبيل المثال لا الحصر مخاطر أمن المعلومات والمخاطر السيبرانية، بالإضافة إلى الثغرات والعيوب البرمجية، أو تعطل الخدمات من خلال انقطاع الكهرباء، أو الحرائق أو تسرب المياه لمركز البيانات نتيجة أسباب طبيعية أو بشرية، أو مخاطر التعديل أو الاطلاع على البيانات من قبل أشخاص غير مخولين، أو أي مخاطر أمنية أخرى في بيئه تكنولوجيا المعلومات تؤثر سلباً على عمليات ونشاط المؤسسة المالية.	مخاطر تكنولوجيا المعلومات (IT Risk)
ترتيبات المؤسسة المالية لوضع نظرة استراتيجية لكيفية سيطرتها على أمثلها السيبراني، بما في ذلك تحديد المخاطر وإدارتها، وبناء إطار للمسؤوليات لاتخاذ القرارات.	الحكومة السيبرانية (Cyber Governance)
مجموعة من القواعد والإجراءات الموثقة التي تحدد كيفية حماية المؤسسة المالية من التهديدات والهجمات الإلكترونية وضمان أمن وسلامة أصولها ومعلوماتها الرقمية.	سياسة الأمان السيبراني Cyber Security Policy



Date: 18/02/2024

NO: .....

CBY

قطاع الرقابة على البنوك  
مكتب الوكيل

البنك المركزي اليمني  
المركز الرئيسي  
صنعاء  
التاريخ: 1445 / 08 / 18 هـ  
الرقم: ق. ر. 338

الخطوات والإجراءات التي يتم تنفيذها لتطبيق سياسة الأمن السيبراني.	برنامج الأمن السيبراني (Cyber Security Program)
عملية إدارة توافرية، وأمن، وسهولة استخدام، وسلامة البيانات في المؤسسة المالية.	حوكمة البيانات (Data Governance)
برمجيات أو ملفات ضارة تتضمن وظائف ذات قدرات تؤثر سلبياً سواءً بشكل مباشر أو غير مباشر على بيئة تكنولوجيا معلومات واتصالات المؤسسة المالية.	الشيفرات الخبيثة (Malicious Code)
توظيف الإجراءات والضوابط والتدابير الملائمة لتقديم خدمات وأعمال المؤسسة المالية بصورة موثوقة.	الحماية (Protection)
توظيف الضوابط والإجراءات الملائمة بغض النظر بوقوع الحدث السيبراني فوراً.	الكشف (Detection)
توظيف الضوابط والإجراءات المناسبة لاحتواء الحدث السيبراني عند كشفه.	الاستجابة (Response)
عملية استرجاع المعلومات المخزنة على وسائل النسخ الاحتياطية عند تلف أو فقدان المعلومات الأصلية أو الحاجة إليها بعد مدة من الزمن لإعادة سير عمل المؤسسة المالية.	الاستعادة (Restore)
إعادة الأعمال والوظائف والخدمات في المؤسسة المالية إلى وضعها الطبيعي وإعادة تشغيل موارد التكنولوجيا المعتمد عليها في تشغيل عمليات المؤسسة المالية إلى ما كانت عليه قبل وقوع الحدث.	التعافي (Recovery)
خلل أو نقص في ضوابط الحماية المستخدمة في أي من مكونات بيئة تكنولوجيا المعلومات واتصالات المؤسسة المالية والتي يمكن استغلالها في عمليات الاختراق والهجوم السيبراني.	نقاط الضعف (Vulnerabilities)
القواعد والآليات المتبعة للسماح باستخدام الأشخاص المخولين فقط لأصول المعلومات فيما يتوافق مع طبيعة مسؤولياتهم في المؤسسة المالية.	ضوابط الوصول/النفاذ (Access Control)
مستوى الصلاحيات المنوحة للمستخدمين للوصول إلى أي من مكونات بيئة تكنولوجيا المعلومات واتصالات المؤسسة المالية.	الامتيازات (Privileges)
ضبط وتوثيق أي تغيير يتم إجراؤه على أي من مكونات بيئة تكنولوجيا المعلومات واتصالات المؤسسة المالية، أو أي تغيير في الإجراءات المعمول بها لديها من قبل الأطراف المخولة بالموافقة على إجراء التغيير.	إدارة التغيير (Change Management)
تحديد مستوى الحساسية المناسب للمعلومات التي يتم إنشاؤها، أو تغييرها، أو نقلها، أو تعديلها، أو حفظها على أية وسائل وبأية تقنيات ممكنة، اعتماداً على المخاطر المرتبطة نتيجة الإطلاع أو الاستخدام غير المشروع لتلك المعلومات.	تصنيف المعلومات (Information Classification)
حماية البيانات والمعلومات من الإطلاع والنشر والإفصاح والاستخدام غير المشروع من غير المخولين.	السرية (Confidentiality)





Date: 18/02/2024

NO: .....

CBY

قطاع الرقابة على البنوك  
مكتب الوكيل

البنك المركزي اليمني  
المركز الرئيسي  
صنعاء  
التاريخ: 1445 / 08 / 1445 هـ  
الرقم: ق. د. 338

دقة وموثوقية وسلامة المعلومات والبيانات واتساقها على مدار دورة حياتها بالكامل لأي نظام يخزن البيانات أو يعالجها أو يسترجعها.	تكامل (سلامة) البيانات (Data Integrity)
توفر الوصول إلى البيانات واستخدامها في الوقت المناسب وبالشكل الصحيح من قبل الأشخاص المصرح لهم عند الحاجة إليها.	توافرية البيانات (Data Availability)
عملية تحديد وتوثيق العمليات والأنشطة ذات الأولوية العالية للمؤسسة المالية، وتحديد الموارد والإجراءات الضرورية لضمان استمرارية تشغيل تلك العمليات والأنشطة خلال فترات الانقطاع أو الكوارث. كما يحدد (BIA) الوقت المستهدف لاستئناف العمليات بعد وقوع حدث ما، بالإضافة إلى مستوى الخسائر المقبولة نتيجة توقف تلك العمليات.	تحليل أثر الأعمال (Business Impact Analysis)
الوقت الفعلي الذي يتعين على المؤسسة المالية خلاله استعادة عملياتها وخدماتها ووظائفها عند مستوى خدمة مقبولة بعد انقطاع الخدمة.	زمن التعافي المستهدف (Recovery Time Objective - RTO)
حجم البيانات المسموح بفقدانها عند الاستعادة بعد وقوع كارثة أو هجوم سيبراني.	نقطة الاسترجاع المستهدفة (Recovery Point Objective RPO)
عمليات تحديد وقياس وضبط ومراقبة المخاطر السيبرانية.	إدارة المخاطر السيبرانية (Management Cyber Risk)
العمليات الهامة التي لا يمكن تحمل توقفها لفترات زمنية طويلة بحسب دراسات تحليل الأثر على أعمال المؤسسة المالية.	العمليات الحرجة (Critical Operations)
الوسيلة التي يتم من خلالها تخزين وتبادل الرسائل والملفات الإلكترونية بين الأشخاص أو المؤسسة المالية.	البريد الإلكتروني (E-mail)
تحويل البيانات والمعلومات إلى شكل غير مقرء أو غير مفهوم.	التشغير (Encryption)
الجهة التي تعهد إليها المؤسسة المالية توقي الأعمال الفنية والتقنية فيها بشكل كلي أو جزئي لمساعدتها على القيام بالأعمال المرخصة.	الطرف الثالث (Third Party)
نظام أمني يتحقق من هوية المستخدم، يتطلب استخدام عدة عناصر مستقلة من آليات التتحقق من الهوية.	التحقق من الهوية متعدد العناصر (Multi-Factor Authentication-MFA)
الاستعانة بطرف ثالث أو توظيف موارده لتسهيل أعمال المؤسسة المالية أو جزء من أعمالها التي تقع ضمن مسؤوليته.	الإسناد الخارجي (Outsourcing)
معايير وإجراءات الحماية التي تراقب أو تحدد الدخول إلى أي من مراافق أو موارد أو معلومات المؤسسة المالية أو منع الوصول إلى مصادر المعلومات والأنظمة مثل المباني وخزائن الملفات والأجهزة المكتبية، والمحمولة، والهواتف، والمعدات.	الأمن النادي (Physical Security)
المساهمين أو الموظفين أو الدائنين أو العملاء أو المزودين الخارجيين أو الجهات الرقابية المعنية.	أصحاب المصالح (Stakeholders)





Date: 18/02/2024

NO: .....

قطاع الرقابة على البنوك  
مكتب الوكيل

CBY

البنك المركزي اليمني  
المركز الرئيسي  
صنعاء  
التاريخ: 1445 / 08 / 2024 هـ  
الرقم: ق. د. 338

ملفات تحتوي على معلومات حول نظام التشغيل أو التطبيق أو أنشطة المستخدم التي تنتج عن مكونات النظام لفهم نشاط النظام وتشخيص المشاكل التي قد يتعرض لها.	سجلات الأحداث (Event log)
ملفات تحتوي على سلسلة من البيانات تقدم أدلة مستندية على تسلسل العمليات التي تحدث على الأنظمة.	سجلات التدقيق (Audit Trail)
قياس وتحديد احتمالية حدوث المخاطر وشدةها وتوقع مستوى تأثيراتها على المؤسسة المالية.	تقييم المخاطر (Risk Assessment)
تجربة تتم من قبل المختصين ويتم من خلالها البحث عن الثغرات الأمنية لأنظمة المعلومات واستغلالها لمحاولة اختراق تلك الأنظمة من خارج أو داخل المؤسسة المالية لمعرفة مدى فعالية الضوابط الأمنية المستخدمة من قبل المؤسسة المالية لحماية أنظمتها.	اختبارات الاختراق (Penetration Testing)
إمكانية الاتصال بأنظمة المؤسسة المالية من خارج الشبكة الداخلية الخاصة بها سواءً كان ذلك لغايات عمل موظفيها عن بعد أو لتأمين الاتصال مع شركاء العمل أو من قبل طرف ثالث.	الوصول عن بعد (Remote Access)

المادة (3) - الأهداف:

يهدف هذا المنشور إلى ما يلي:

- توفير الحد الأدنى من المتطلبات الأساسية للأمن السيبراني لتقليل المخاطر السيبرانية على الأصول المعلوماتية والتقنية للمؤسسة المالية من التهديدات الداخلية والخارجية.
- تعزيز سلامة وسمعة ومهنية القطاع المالي والمصرفي في الجمهورية، بما يكفل حماية عملياته والحفاظ على عملائه وتعزيز الثقة فيما بينهم.
- تعزيز سرية المعلومات (Data Confidentiality)
- تعزيز سلامة المعلومات (Data Integrity)
- تعزيز توافر المعلومات (Data Availability)

المادة (4) - نطاق السيطرة:

يسري هذا المنشور على كافة المؤسسة المالية الخاضعة لإشراف ورقابة البنك المركزي.





Date: 18/02/2024

NO: .....

قطاع الرقابة على البنوك  
مكتب الوكيل

البنك المركزي اليمني  
المركز الرئيسي  
صنعاء  
التاريخ: 08/08/1445 هـ  
الرقم: ق. د. 338

CBY

## الفصل الثاني الأدوار والمسؤوليات

### أولاً : حوكمة الأمان السيبراني:

المادة (5): يجب أن تضم إدارة المؤسسة المالية أشخاصاً يتمتعون بمهارات و المعارف المناسبة لفهم وإدارة المخاطر السيبرانية.

المادة (6): يتولى مجلس الإدارة المسؤوليات والمهام التالية:

1. اعتماد سياسة وإجراءات الأمان السيبراني (Cyber Security Policy).

2. اعتماد برنامج الأمان السيبراني (Cyber Security Program).

ويجوز لمجلس الإدارة أن يشكل لجأناً لفحص الامتثال لسياسة وبرنامج الأمان السيبراني.

المادة (7): تتولى إدارة المؤسسة المالية المسؤوليات والمهام التالية كل بحسب موقعه:

1. متابعة تطبيق وتحديث سياسة وإجراءات الأمان السيبراني.

2. متابعة تطبيق برنامج الأمان السيبراني بحيث يكون متكاملاً مع الإطار العام لإدارة مخاطر تكنولوجيا المعلومات، والاستمرار بتحديثه وتطويره.

3. التأكد من وجود سجل شامل خاص بالمخاطر السيبرانية (Cyber Risk Register) وتحديثه بشكل مستمر، وبحيث يكون متواافقاً مع ملف مخاطر تكنولوجيا المعلومات (IT Risk Profile).

4. متابعة مستوى المخاطر السيبرانية بشكل مستمر.

5. اعتماد قوائم الصالحيات المتعلقة بإدارة الأمان والمخاطر السيبرانية من حيث تحديد الجهات أو الأشخاص أو الأطراف المسؤولة بشكل أولي (Responsible)، وتلك المسؤولة بشكل نهائى (Accountable)، وتلك المستشار (Consulted)، وتلك التي يتم اطلاعها (Informed)، على كافة العمليات كما وإدارة وضبط تلك القوائم والرقابة والتدقيق عليها.

### ثانياً: سياسة وبرنامج الأمان السيبراني:

المادة (8): يجب أن تكون سياسة وإجراءات الأمان السيبراني عبارة عن وثيقة مخصصة للأمان السيبراني في المؤسسة المالية، ويراعى عند إعدادها وتحديثها مساهمة كافة الأطراف المعنية بالأمان السيبراني وأمن المعلومات واعتماد أفضل الممارسات الدولية والمراجع والدروس وال عبر المستفادة من حوادث الأمان السيبراني، ويمكن للمؤسسة المالية تضمين سياسة الأمان السيبراني بسياسة أمن المعلومات تحت مسمى "سياسة أمن المعلومات والأمان السيبراني" وكذلك تضمين برنامج الأمان السيبراني ضمن برنامج أمن المعلومات تحت مسمى "برنامج أمن المعلومات والأمان السيبراني" شريطة تحقيق جميع ما ورد في هذا المنشور.





Date: 18/02/2024

NO: .....

CBY

قطاع الرقابة على البنوك  
مكتب الوكيل

البنك المركزي اليمني  
المركز الرئيسي  
صنعاء  
التاريخ: 08/08/1445 هـ  
الرقم: ق. د. 338

**المادة (9):** يجب أن تتضمن سياسة الأمان السيبراني في المؤسسة المالية المحاورة التالية كحد أدنى:

1. تحديد الأدوار والمسؤوليات بما في ذلك مسؤولية اتخاذ القرار داخل المؤسسة المالية فيما يتعلق بإدارة المخاطر السيبرانية وبما يشمل حالات الطوارئ والأزمات.
2. حوكمة البيانات وتصنيفها.
3. أمن وإدارة المعلومات وبيئة تكنولوجيا المعلومات والاتصالات.
4. خصوصية بيانات العملاء.
5. إدارة المخاطر السيبرانية.
6. ضوابط الحماية للحد من السيطرة على المخاطر السيبرانية.
7. خطط استمرارية الأعمال والتعافي من الكوارث.
8. التعاون مع الأطراف المعنية بالأمن السيبراني وأمن المعلومات للاستجابة الفعالة لمواجهة الهجمات السيبرانية والتعافي منها.
9. مراقبة الأنظمة والشبكات والتطبيقات وتطويرها.
10. ضوابط الأمان المادي والبيئي.
11. إدارة العمليات المسندة للطرف الثالث.
12. توعية وتدريب الموظفين داخل المؤسسة المالية بخصوص الأمان السيبراني لضمان تطبيقهم لبنود سياسة إجراءات الأمان السيبراني.
13. تحديد آلية الإفصاح للأطراف المعنية عن بنود سياسة الأمان السيبراني.

**المادة (10):** على المؤسسة المالية تطبيق برنامج الأمان السيبراني (Cyber Security Program) والاستمرار بتحديثه لضمان تحقيق متطلبات السرية (Confidentiality) والتكاملية (Integrity) وتوافر البيانات (Availability) في بيئة تكنولوجيا المعلومات والاتصالات، على أن يكون للبرنامج القدرة على ما يلي:

1. تحديد التهديدات الداخلية والخارجية التي تحدث نتيجة للمخاطر السيبرانية.
2. تحديد وتصنيف مخاطر وحساسية المعلومات في بيئة تكنولوجيا المعلومات والاتصالات.
3. تحديد الجهات ذات الصلاحية للوصول/النفاذ واستخدام المعلومات وبيئة تكنولوجيا المعلومات والاتصالات.
4. تطبيق سياسة الأمان السيبراني وتشغيل بيئة تكنولوجيا المعلومات والاتصالات الازمة لضمان حماية أصول المعلومات والمعلومات الحساسة في المؤسسة المالية من الاختراق غير المشروع.
5. كشف الهجمات السيبرانية الناجحة والفاشلة فور حدوثها ما أمكن.
6. اتخاذ الإجراءات التصحيحية الازمة للسيطرة على/والحد من الآثار السلبية للمخاطر السيبرانية.
7. إجراءات إعادة تشغيل عمليات المؤسسة المالية بعد توقفها بما في ذلك المتعلقة بالخدمات والمتطلبات القانونية والرقابية خلال الفترة الزمنية المقبولة والمحددة ضمن خطة استمرارية العمل وبما يتواافق مع ما ورد في المادة (33) من هذا المنشور.





Date: 18/02/2024

NO: .....

قطاع الرقابة على البنوك  
مكتب الوكيل

CBY

البنك المركزي اليمني  
المركز الرئيسي  
صنعاء  
التاريخ: 08/08/1445هـ  
الرقم: ق. ر. 338

المادة (11): يجب على المؤسسة المالية إدارة أمن المعلومات بما فيها الأمن السيبراني من خلال مدير أمن معلومات متخصص بحيث لا يتبع إدارياً لإدارة تقنية المعلومات ويتمتع بالاستقلالية وبما يضمن عدم تضارب المصالح وأن يكون لديه الخبرة العملية والمعرفة المهنية الازمة ليكون مسؤولاً عن المهام التالية كحد أدنى:

1. الإشراف بشكل مباشر على وضع سياسة وبرنامج الأمن السيبراني وضمان تنفيذهما والعمل على مراجعتهما وتحديثهما باستمرار.
2. تقييم مدى كفاية وكفاءة سياسة وإجراءات وبرنامج الأمن السيبراني.
3. مراجعة فعالية ضوابط الحماية المعتمدة في سياسة الأمن السيبراني لدى المؤسسة المالية بشكل مستمر.
4. رفع تقارير نصف سنوية على الأقل أو كلما دعت الحاجة لمجلس الإدارة وإدارة المؤسسة المالية فيما يخص الأمن السيبراني، على أن تتضمن التقارير النقاط التالية بالحد الأدنى:
  - 4.1. الانحرافات المتعلقة بتطبيق سياسة الأمن السيبراني وإجراءاتها.
  - 4.2. نتائج تقييم المخاطر السيبرانية.
  - 4.3. نتائج تقييم مدى كفاية وكفاءة سياسة وبرنامج الأمن السيبراني.
  - 4.4. التوصيات والإجراءات والمتطلبات الواجب تنفيذها.
- 4.5. ملخص لأهم أحداث التهديدات والهجمات السيبرانية التي تعرضت لها المؤسسة المالية خلال فترة التقرير.
5. تحديد وتقييم المخاطر السيبرانية.

المادة (12): بالرغم مما ورد في المادة (11) أعلاه يحق للمؤسسة المالية إسناد مهام إدارة أمن المعلومات أو جزء منها لطرف ثالث على أن يتلزم بما يلي:

1. الطلب من الطرف الثالث الالتزام بما يلي المطالبات الواردة في هذا المنشور فيما يخص إدارة أمن المعلومات.
2. فحص امتناع الطرف الثالث لمطالبات التعليمات فيما يخص إدارة أمن المعلومات.
3. توقيع الطرف الثالث لإتفاقية عدم الإفشاء (NDA Agreement) وسرية البيانات والمعلومات.

المادة (13): على المؤسسة المالية قبل إجراء تغيير في بيئتها تكنولوجيا المعلومات والاتصالات أو بعد وقوع أي حدث يؤثر على أمن المعلومات التأكد ما إذا كانت هناك حاجة إلى إدخال تغييرات أو تحسينات على سياسة وبرنامج الأمن السيبراني.



Date: 18/02/2024

NO: .....

قطاع الرقابة على البنوك  
مكتب الوكيل

البنك المركزي اليمني  
المركز الرئيسي  
صنعاء  
التاريخ: 1445 / 08 / 1445 هـ  
الرقم: ق. د. 338

CBY

## الفصل الثالث

### إدارة المخاطر السيبرانية

#### أولاً: تحديد العمليات الحرجية وأصول المعلومات الداعمة في المؤسسة المالية:

المادة (14): لغرض تقييم المخاطر السيبرانية التي قد تواجه المؤسسة المالية، يجب علّها تحديد ما يلي:

1. الوظائف والعمليات الحرجية.
2. أصول المعلومات وفهم عملياته وإجراءاته وأنظمته وما يتعلّق بها من موارد ونظم المعلومات وسبل الوصول إليها، بما في ذلك النظم الداخلية والخارجية المرتبطة بها.

يتم تحديد الأصول من خلال إجراء تحليل (Business Impact Analysis) أو ما يطلق عليه (BIA) وهو عملية تحديد وتوثيق العمليات والأنشطة ذات الأولوية العالية للمؤسسة المالية، وتحديد الموارد والإجراءات الضرورية لضمان استمرارية تشغيل تلك العمليات والأنشطة خلال فترات الانقطاع أو الكوارث. كما يحدد (BIA) الوقت المستهدف لاستئناف العمليات بعد وقوع حدث ما، بالإضافة إلى مستوى الخسائر المقبولة نتيجة توقف تلك العمليات.

يتم أيضًا خلال الإتفاق مع جميع الإدارات المعنية والإدارة التنفيذية على نقاط الاسترجاع المستهدفة (Recovery Time Objective - RTO) ومقدار زمن التعافي المستهدف (Recovery Point Objective - RPO) لكل خدمة تكنولوجيا المعلومات وتوثيقها واستخدامها كمتطلبات لتصميم الخدمة وخطط استمرارية تكنولوجيا المعلومات.

المادة (15): على المؤسسة المالية مراجعة التحليل والتصنيف للوظائف والعمليات الحرجية وأصول المعلومات وتحديث التصنيفات بشكل مستمر.

#### ثانياً: تقييم المخاطر السيبرانية:

المادة (16): على المؤسسة المالية تحليل عوامل المخاطر السيبرانية (Cyber Risk Factor Analysis) بشكل مستمر

من حيث تحديد ما يلي:

1. التهديدات الداخلية.
2. الهديدات الخارجية.
3. مواطن الضعف في إدارة موارد بيئة تكنولوجيا المعلومات والاتصالات.
4. مواطن الضعف في قدرة بيئة تكنولوجيا المعلومات والاتصالات على تمكين عمليات المؤسسة المالية.
5. مواطن الضعف في إدارة مخاطر بيئة تكنولوجيا المعلومات والاتصالات.



Date: 18 / 02 / 2024

NO: .....

CBY

قطاع الرقابة على البنوك  
مكتب الوكيل

المادة (17) : على المؤسسة المالية تحليل سيناريوهات المخاطر السيبرانية (Cyber Risk Scenario Analysis) بشكل

مستمر من حيث تحديد ما يلي كحد أدنى:

1. مصدر التهديد السيبراني (داخلي أو خارجي).
2. نوع التهديد السيبراني (طبيعي أو مفتعل أو تكنولوجي).
3. الحدث السيبراني.
4. الأصول أو الموارد المتأثرة بالمخاطر السيبرانية (Assets or Resources Affected) مثل موارد بشرية أو هيكل تنظيمية أو عمليات أو بيئة تكنولوجيا المعلومات والاتصالات أو معلومات.
5. الوقت (وقت الحدث، ومرة الحدث، وعمر الحدث عند اكتشافه).

المادة (18) : يحق للمؤسسة المالية الاستعانة بطرف ثالث لغایات تقييم المخاطر السيبرانية مع مراعاة الطرف الثالث لاتفاقية عدم الإفشاء (NDA).

ثالثاً: سجل المخاطر السيبرانية:

المادة (19) : على المؤسسة المالية إنشاء والاستمرار بتحديث السجل الشامل الخاص بالمخاطر السيبرانية Register (Cyber Risk) على أن يتضمن كحد أدنى ما يلي:

1. مالك الأصل وفريق التقييم، تاريخ التقييم اللاحق، ملخص تقييم المخاطر السيبرانية وخيارات إدارتها.
2. تقييم المخاطر السيبرانية من حيث احتساب محوري المخاطر متمثلة باحتمالية الحدث (Probability) وحجم الأثر (Impact or Severity)، ويفضل استخدام مقياس معياري زوجي لمحاري التقييم، وإظهار حجم الأثر اعتماداً على أهداف وعمليات المؤسسة المالية المتضمنة تكنولوجيا المعلومات باستخدام محاور التقييم لأحد النماذج العالمية التالية على سبيل المثال:

COBIT Information Criteria .2.1

Balanced Scorecard (BSC) .2.2

Extended BSC .2.3

Wester man .2.4

COSO ERM .2.5

Factor Analysis of Information Risk (FAIR) .2.6

NIST Cybersecurity Framework .2.7

.3. مستوى المخاطر المقبول (Risk Appetite).

.4. خيارات إدارة المخاطر:

- 4.1 قبول المخاطر: أن تقبل المؤسسة المالية المخاطر المعينة دون اتخاذ أي إجراءات للتخفيف أو للتجنب لأن العواقب والتأثيرات المحتملة للمخاطر يمكن التغاضي عنها ويتم اتخاذ القرار في بعض الحالات عندما يكون مستوى المخاطر ضمن درجة المخاطر التي تقبلها المؤسسة المالية أو



Date: 18/02/2024

NO: .....

CBY

قطاع الرقابة على البنوك  
مكتب الوكيل

البنك المركزي اليمني  
المركز الرئيسي  
صنعاء  
التاريخ: 08/08/1445 هـ  
الرقم: ق. د. 338

عندما تكون الخسارة المحتملة المرتبطة بالمخاطر أقل من تكلفة تجنبها أو تخفيفها (يتطلب اتخاذ هذا القرار موافقة رسمية من مجلس الإدارة والإدارة التنفيذية للمؤسسة المالية).

4.2. تخفيف المخاطر: إجراء تتخذه المؤسسة المالية لتقليل المخاطر، حيث يمكن التخفيف من حدة المخاطر من خلال وضع ضوابط تقلل من احتمالية تأثيرها، وقد لا يؤدي تخفيف المخاطر إلى القضاء على المخاطر ولكنه يقلل من التأثير على الأصول أو احتمالية حدوثه.

4.3. تجنب المخاطر: القضاء على جميع الاحتمالات التي قد تسبب مخاطر معينة، وعادةً ما يتم اتخاذ هذا الخيار عندما تكون المخاطر غير مقبولة من قبل المؤسسة المالية أو لا يمكن تحويلها.

4.4. تحويل المخاطر: الحد من تأثير المخاطر عن طريق نقل المسئولية إلى كيانات أخرى، المثال الأكثر شيوعاً هو التأمين ضد المخاطر.

5. بنود خطة إدارة المخاطر ومتابعتها (نفذت أو قيد التنفيذ بحسب الخطة).

6. معايير أداء رئيسية لمراقبة مستوى المخاطر (Key Risk Indicators) والتتأكد من عدم تجاوز المخاطر المقبولة ودرجة تحمل المخاطر (نسبة الإنحراف المضافة للمخاطر المقبولة).

7. معايير لتقدير سرية، نزاهة، أمن، وتتوفر الأنظمة والمعلومات الحساسة.

8. تحديد مسؤوليات موظفي المؤسسة المالية تجاه المخاطر.



Date: 18/02/2024

NO: .....

قطاع الرقابة على البنوك  
مكتب الوكيل

CBY

البنك المركزي اليمني  
المركز الرئيسي  
صنعاء  
التاريخ: 08/08/1445 هـ  
الرقم: ق. ر. 338

## الفصل الرابع

### ضوابط الحماية

#### أولاً: حماية الأنظمة والبرمجيات والشبكات والأجهزة الشبكية:

المادة (20): على المؤسسة المالية توفير ضوابط الحماية لجميع مكونات بيئه تكنولوجيا المعلومات والاتصالات وأنظمة والبرمجيات والشبكات والأجهزة الشبكية من أي حدث سبيراني، وعلى سبيل المثال لا الحصر توفر ما يلي:

1. العزل والتقطيع المادي أو المنطقي لأجزاء الشبكات بشكل آمن، بما يضمن عزل تأثير الأنظمة المعرضة للهجوم السبيراني عن غيرها في حال حدوثه، وبما يمكن من تسهيل استعادة الخدمات بكفاءة وفعالية وبحسب تقييم المؤسسة المالية للمخاطر السبيرانية اعتماداً على مبدأ الدفاع الأممي متعدد المستويات (Defense-in-Depth).
2. تطبيق مبدأ الثقة الصفرية (Zero Trust) بحيث عدم السماح بأي وصول إلى الشبكة أو الموارد إلا بعد التأكيد والتحقق من هوية الطرف المتصل وصلاحياته بشكل كامل في كل مرة يتم فيها محاولة الوصول.
3. تأمين الشبكات اللاسلكية وحمايتها باستخدام وسائل آمنة للتحقق من الهوية والتشفير، وعدم ربط الشبكات اللاسلكية بشبكة المؤسسة المالية الداخلية إلا بناءً على دراسة متكاملة للمخاطر المرتبطة على ذلك والتعامل معها بما يضمن حماية بيئه تكنولوجيا المعلومات والاتصالات للمؤسسة المالية.
4. تقييم مدى كفاءة تصميم الربط الشبكي والأجهزة الشبكية بما فيها أجهزة وبرمجيات الحماية باستمرار لتلبية احتياجات العمل، والاحتفاظ بتصميم محدث للربط الشبكي بالإضافة إلى الاحتفاظ بقائمة محدثة للأجهزة المتصلة بشبكة المؤسسة المالية ومخططات مركز المعلومات والموقع الرئيسية والموقع الاحتياطي للمؤسسة المالية بمكان آمن يمكن المعينين فقط من الوصول إليه.
5. توفير ضوابط وقائية لمنع ربط الأجهزة غير المرخصة أو المملوكة من قبل الموظفين بشبكات وخوادم وأنظمة المؤسسة المالية بما في ذلك أجهزة الحاسوب وأي أجهزة أخرى دون الحصول على الموافقات اللازمة، وتطبيق سياسات وقواعد أمن المعلومات والأمن السبيراني عليها في حال الموافقة على الربط، والعمل على توفير ضوابط رقابية للكشف عن أي أجهزة مرتبطة بشبكات وأنظمة المؤسسة المالية بطرق غير مشروعة.
6. توفير الأجهزة والبرمجيات اللازمة لمراقبة وتحذير وكشف الهجوم السبيراني والوصول غير المشروع مثل أجهزة كشف النفاذ (Intrusion Detection Systems) والتتأكد من تحديثها بشكل مستمر وتوظيفها بشكل فعال في عمليات المراقبة وكشف الهجمات.



Date: 18/02/2024

NO: .....

CBY

قطاع الرقابة على البنوك  
مكتب الوكيل

البنك المركزي اليمني  
المركز الرئيسي  
صنعاء  
التاريخ: 08/08/1445 هـ  
الرقم: ق. د. 338

7. تثبيت وتفعيل برامج الحماية من الفيروسات على جميع الخوادم والأجهزة المرتبطة بشبكة المؤسسة المالية، والتأكد من تحديثها بشكل مستمر وتوظيفها بشكل فعال في عمليات المراقبة وكشف الهجمات.
8. فصل موقع البنية التحتية (الموقع الرئيسية وموقع التعافي من الكوارث) الخاصة بالأنظمة الحرجية بمنطقة آمنة محدودة الدخول وتوثيق سجلات الدخول لها والخروج منها بالإضافة إلى توفير أنظمة مراقبة مناسبة.
9. فصل بيئه التجربة وبيئة التطوير للأنظمة الحرجية عن البيئة الحية (Live Environment)، كما وتقييد وصول المطوريين للبيئة الحية.
10. التقييد الحازم لاستخدام أجهزة وسائل التخزين الخارجية والأمن المتعلق بها.
11. تحديث أنظمة التشغيل والبرمجيات المثبتة على جميع الأجهزة والخوادم الخاصة بالمؤسسة المالية بأخر التحديثات الموصى بها من قبل المزودين لتلك الأنظمة وخصوصاً التحديثات المتعلقة بإغلاق الثغرات الأمنية لتفادي مخاطر الأنظمة غير المحدثة، وبما يتناسب مع سياسة Patch Management (Policy Management) المؤسسة المالية مع الحرص على تطبيق سياسات وإجراءات التغيير بالسرعة الممكنة، واتخاذ قرارات مبنية على مخاطر تكنولوجيا المعلومات والمخاطر السيبرانية وتوفير ضوابط بديلة وفعالة في حال تعذر ذلك مع ضرورة إجراء الفحوصات اللاحقة قبل تنفيذ هذه التحديثات على الأنظمة.
12. حذف أي برمجيات أو ملفات مخزنة على خوادم الأنظمة الحرجية والتي ليس لها علاقة بالأنظمة المعامل بها لدى المؤسسة المالية.
13. تقييد وصول الموظفين للإنترنت للموقع والخدمات الموثوقة فقط، ويشمل ذلك التقييد الحازم للموقع الإلكترونية المشبوهة، وموقع مشاركة وتخزين الملفات، وموقع الدخول عن بعد.
14. فصل عمليات وصول الموظفين للأنظمة الحرجية عند وصولهم للإنترنت، وإذا دعت الحاجة إلى غير ذلك يجب أخذ الموافقة اللاحقة وتوثيقها.
15. وضع معايير أمنية لإعدادات بيئه تكنولوجيا المعلومات والاتصالات حسب أفضل الممارسات وتوثيق ذلك.
16. وضع إجراءات ومبادئ توجيهية مصممة لضمان أمان عمليات تطوير البرامج والتطبيقات داخل بيئه المؤسسة المالية.
17. مراجعة وتحديث جميع الإجراءات والمبادئ التوجيهية المصممة لضمان أمان عمليات تطوير البرامج والتطبيقات بشكل دوري ومن قبل أشخاص مؤهلين وبحسب المعايير الدولية المعتمدة بهذاخصوص.
18. وضع إجراءات تقييم أو اختبار أمن للبرامج والتطبيقات التي تم تطويرها خارج بيئه المؤسسة المالية. تحديد الأنشطة التي قد تشكل خطراً على أنظمة المؤسسة المالية وبالأخص الأنظمة المالية وعميمها على الموظفين لمنع الانحراف فيها.





Date: 18/02/2024

NO: .....

CBY

قطاع الرقابة على البنوك  
مكتب الوكيل

البنك المركزي اليمني  
المركز الرئيسي  
صنعاء  
التاريخ: 08/08/1445 هـ  
الرقم: ق. ر. 338

19. العمل بنظم تشفير ذات اعتمادية عالية للملفات الحساسة المخزنة في الأجهزة أو التي يتم تناقلها عبر الشبكات.

**المادة (21):** على المؤسسة المالية استخدام أنظمة حماية من مصادر متنوعة ضمن مستويات مختلفة (Different Security Tiers) على جميع أنظمتها الحرجية.

**المادة (22):** على المؤسسة المالية توفير ضوابط الحماية للأنظمة والبيانات الحساسة وخاصةً ضوابط التحقق من هوية مستخدم تلك الأنظمة والبيانات على أن تتضمن بالحد الأدنى ما يلي:

- استخدام ضوابط نفاذ قوية (Strong Authentication) وفعالة من خلال التتحقق من الهوية متعددة العناصر (Multi Factor Authentication) وبحسب مستوى المخاطر، مع ضمان فصلها بشكل مناسب وبطريقة تقلل من احتمالية معرفة الغير لإحدى عناصرها من خلال العنصر الآخر واستخدام الوسائل والتكنولوجيات الازمة بما يضمن تحديد المسؤوليات.
- في حال الحاجة الماسة للوصول عن بعد إلى بيئة تكنولوجيا المعلومات (Remote Access) فيجب أن يتم استخدامها بأضيق الحدود، مع توفير ضوابط النفاذ من خلال وسائل التتحقق متعدد العناصر (MFA) واستخدام تقنيات تشفير ذات اعتمادية عالية والضوابط الأخرى المصاحبة للحد من مخاطر الهجمات السيبرانية غير المصرح بها.
- تطبيق المعايير الأمنية الدولية وأفضل الممارسات العالمية عند اختيار مواصفات كلمات المرور.

**المادة (23):** على المؤسسة المالية توفير ضوابط الحماية الخاصة بالمعلومات المتعلقة بأعمالها وعلى وجه الخصوص ما يلي:

- التخلص من المعلومات الحساسة التي لم تعد ضرورية لتشغيل العمليات الحرجية وبما يتواافق مع القوانين واللوائح والأنظمة والتعليمات الصادرة بهذا الخصوص.
- ضمان توافرية المعلومات الخاصة بعمل المؤسسة المالية من خلال أخذ النسخ الاحتياطية لها بشكل دوري وبموقع آمنة داخل وخارج أماكن عمل المؤسسة المالية مع تجنب حفظ النسخ خارج نطاق الجمهورية اليمنية إضافةً إلى عمل مزامنة للبيانات مع الموقع الاحتياطي.
- الالتزام بسياسة تصنيف البيانات عند إرسال رسائل ذات محتوى سري وتشفيه تلك الرسائل حسب مستوى حساسيتها.
- تفعيل الضوابط الازمة لحماية سرية المعلومات الحساسة التي يتم الاحتفاظ بها أو تناقلها عبر الشبكات الخارجية بما في ذلك تشفيه تلك المعلومات.
- إذا تعذر على المؤسسة المالية تشفيه المعلومات الحساسة المخزنة المستخدمة في التراسل، فعلمها حمايتها بطرق بديلة وفعالة بحيث يتم مراجعتها ومصادقتها من قبل مدير أمن المعلومات.





Date: 18/02/2024

NO: .....

CBY

قطاع الرقابة على البنوك  
مكتب الوكيل

البنك المركزي اليمني  
المركز الرئيسي  
صنعاء  
التاريخ: 08/08/1445 هـ  
الرقم: ق. ر. 338

المادة (24): على المؤسسة المالية توفير ضوابط الحماية الخاصة بضوابط الوصول/النفاذ (Access Controls)

إلى أنظمتها، وعلى وجه الخصوص ما يلي:

1. المراقبة المستمرة لنشاط المستخدمين المصرح لهم بالاستخدام والوصول/النفاذ إلى أنظمة وشبكات المؤسسة المالية، واكتشاف الوصول لمنع الاستخدام غير المصرح به أو العبث بالمعلومات الحساسة.
2. إغلاق الحساب بعد عدد معين من المحاولات الفاشلة لتسجيل الدخول.
3. مراجعة صلاحيات الاستخدام والنفاذ المنوحة على تلك الأنظمة بشكل دوري وعند حدوث أي تغيير على الأنظمة أو المسميات الوظيفية، والتأكد من ملاءمتها لطبيعة العمل واستخدامها بشكل مشروع وحذف الصلاحيات ورموز التعريف غير المستخدمة وبشكل فوري.
4. توظيف ضوابط الحماية الازمة للتحكم بالنفاذ لأنظمة وخوادم وبرمجيات المؤسسة المالية، وذلك من خلال توفير مصفوفة دليل الصلاحيات (Authority Matrix) للأنظمة، وتكون معتمدة من إدارة المؤسسة المالية بحيث تبين الصلاحيات التي تمنع على مستوى الوظيفة لكافة الأنظمة، على أن تراعي مصفوفة الصلاحيات المبادئ التالية:

- 4.1. الفصل في المهام (Segregation of Duties).
- 4.2. الرقابة الثنائية على العمليات الحساسة (Dual Control).
- 4.3. منح الصلاحيات بحسب الحاجة.
5. الامتثال ومراقبة الامتثال لسياسة كلمة المرور، مع التركيز على ضرورة تغيير كلمات المرور الافتراضية المصاحبة لأنظمة والأجهزة الجديدة وبشكل فوري عند البدء باستخدامها.
6. تطبيق قاعدة منح الصلاحيات بالحد الأدنى وحسب حاجة العمل (Least privileges and on a need basis to know) على أن تتم مراجعة هذه الصلاحيات باستمرار.
7. الأخذ بقاعدة الوصول التي تفيد بأن "الوصول بشكل عام ممنوع باستثناء ما هو مسموح".
8. عدم استخدام الحسابات المشتركة (Shared / Generic Accounts).
9. إدارة ضوابط وصول خاصة للصلاحيات الهامة والحساسة على الأنظمة الحرجة (Privileged Access Management).

المادة (25): على المؤسسة المالية توفير ضوابط الحماية الخاصة بمخاطر التهديد السيبراني الداخلي، وعلى وجه الخصوص ما يلي:

1. مراقبة وتحليل أنشطة الأشخاص غير المصرح لهم بالنفاذ/الوصول لبيئة تكنولوجيا المعلومات والاتصالات في حال محاولتهم النفاذ/الوصول غير المصرح به إليها.
2. وضع أسس وضوابط التعيين المناسبة للموظفين الجدد خاصةً المرتبطة بأعمالهم بالأنظمة الحرجة للتأكد من سجلهم الوظيفي إن وجد.
3. إجراء مراجعة شاملة لأعمال الموظفين الجدد ومثليها على جميع الموظفين على فترات منتظمة طوال فترة عملهم، بما يتاسب مع صلاحيات النفاذ واستخدامهم لأنظمة الحرجة.





Date: 18/02/2024

قطاع الرقابة على البنوك  
مكتب الوكيل

التاريخ: 08/08/1445 هـ  
الرقم: ق. د. 338

NO: .....

CBY

4. تفعيل الضوابط الالزامية لإدارة المخاطر المتعلقة بالموظفين الذين تنتهي علاقتهم الوظيفية مع المؤسسة المالية أو ينقطعون عن العمل بشكل مؤقت لفترات طويلة خاصةً بسبب سلوك مشبوه.

5. يجب أن تتضمن العقود التي يتم توقيعها مع الموظفين بنوداً قانونيةً واضحةً تمنعهم من تسريب المعلومات أو اختراق الأنظمة أو النفاذ بشكل غير مصرح به، وعلى سبيل المثال توقيع نموذج تعهد بهذا الخصوص وفقاً لما يتناسب مع أنظمة وبيانات المؤسسة المالية.

**ثانياً: ضوابط الحماية الخاصة بالبريد الإلكتروني:**

المادة (26):

1. على المؤسسة المالية تطبيق سياسة إدارة وتعريف تطبيقات وبروتوكولات ونطاق البريد الإلكتروني الذي يحمل اسم المؤسسة المالية على الإنترنت متضمناً تطبيق الضوابط والمعايير الآمنة لنظام البريد الإلكتروني، وكحد أدنى ما يلي:

1.1. السماح لمستخدم البريد الإلكتروني بالنفذ لحسابه فقط بعد التأكد من هويته ومن خلال اتباع طريقة التحقق من هوية المستخدم التي يصعب على الغير اخراها، أو استخدام طريقة التحقق المتعدد من الهوية (Multi Factor Authentication) خاصةً للمستخدمين الذين تعتبر طبيعة عملهم حساسة وذات أثر ومخاطر على عمليات المؤسسة المالية وسمعتها.

1.2. استخدام تقنيات تشفير ذات اعتمادية عالية للمعلومات المصنفة لضمان حماية عمليات الاتصال بالبريد الإلكتروني.

1.3. تفعيل خاصية "Reverse DNS Check" للتحقق من مطابقة العنوان الرقمي (IP) المرسل للبريد الإلكتروني (الوارد) مع اسم النطاق والجهاز الصادر عنهما.

1.4. تفعيل خاصية (Real-time Blocking List - RBL Check) لحجب الرسائل الواردة من مصادر مشبوهة اعتماداً على قوائم بيانات دولية موثوقة ومحدثة، لهذا الشأن بالإضافة لقوائم داخلية تبني وتحدث لتحقيق ذات الغرض.

1.5. تفعيل خاصية "Sender Policy Framework - SPF Check" ما أمكن وبما يساهم في تقليل احتمالية استلام رسائل بريد إلكتروني من غير مصادرها الأصلية.

1.6. النظر في إمكانية تفعيل خاصية "DNSSEC" ضمن مكونات البيئة التقنية لدى المؤسسة المالية.

1.7. حجب المرفقات والروابط المشبوهة ضمن رسائل البريد الإلكتروني من خلال فحصها بواسطة برامجيات معتمدة، لهذا الخصوص، وحظر الملفات ذات الإمدادات التنفيذية (Executable Files) وتحديد سقف مسموح به لحجم الم��ق، مع ضرورة تفعيل سياسة مناسبة على نظام البريد الإلكتروني للتعامل مع تلك الرسائل بناءً على درجة مخاطرها.

1.8. النظر في إمكانية تعين سقوف لعدد الاتصالات بخادم البريد الإلكتروني من المصدر الواحد وبما يتناسب مع مواصفات خادم البريد الإلكتروني ومتطلبات العمل حيثما لزم.

1.9. توظيف خصائص التوافقية وخطط استمرارية العمل لخدمات البريد الإلكتروني حسب تحليل (Business Impact Analysis) (BIA).



Date: 18/02/2024

NO: .....

CBY

قطاع الرقابة على البنوك  
مكتب الوكيل

البنك المركزي اليمني  
المركز الرئيسي  
صنعاء  
التاريخ: 08/08/1445 هـ  
الرقم: ق. د. 338

1.10. التأكد من متابعة تنزيل التحديثات لنظام الإيميل ونظام التشغيل للخادم المستضيف لنظام الإيميل لضمان سد الثغرات الأمنية و/أو الأبواب الخلفية (Back Door) في حال كان نظام الإيميلات مسكن محلياً.

1.11. الاحتفاظ بسجلات التتبع لأنظمة البريد الإلكتروني العاملة في المؤسسة المالية لفترة زمنية تحدد ضمن سياسة الاحتفاظ بالبيانات بحيث لا تقل عن ثلاثة أشهر.

2. العمل على تطوير برنامج توعوي يُحدث باستمرار ويوجه لمستخدمي البريد الإلكتروني بشأن آلية التعامل مع رسائل البريد الإلكتروني الاحتيالية والمشكوك فيها وطرق اكتشافها، وتتضمن الآلية على وجه الخصوص إمكانية التواصل مع مرسل البريد الإلكتروني في حال الشك بهويته وذلك من خلال وسائل الاتصالات الأخرى.

ثالثاً: السجلات:

المادة (27): على المؤسسة المالية الالتزام بما يلي:

1. توفير سجلات الأحداث وسجلات التدقيق لبيئة تكنولوجيا المعلومات والاتصالات وأنظمة العاملة عليها.
2. إيجاد آلية لإدارة وتحليل ومراقبة وتوثيق سجلات الأحداث والتدقيق بشكل مستمر حسب تصنيف أهمية الأنظمة العاملة على بيئة تكنولوجيا المعلومات والاتصالات.
3. تحديد أنواع السجلات التي يتعين الاحتفاظ بها ومدة الاحتفاظ وصلاحيات الإطلاع عليها.
4. توفير الحماية اللازمة لسجلات الأحداث والتدقيق لضمان توافرها وتكاملها.
5. إيجاد آلية مناسبة للتحقق من مراجعة سجلات الأحداث لبيئة تكنولوجيا المعلومات والاتصالات من قبل جهة مستقلة داخل أو خارج المؤسسة المالية.



Date: 18/02/2024

NO: .....

CBY

قطاع الرقابة على البنوك  
مكتب الوكيل

البنك المركزي اليمني  
المركز الرئيسي  
صنعاء  
التاريخ: 08/08/1445 هـ  
الرقم: ق. د. 338

## الفصل الخامس

### الكشف عن الحوادث السيبرانية

**المادة (28):** يجب على المؤسسة المالية وضع الإجراءات المناسبة للكشف عن حوادث الأمن السيبراني بناءً على مصادر البيانات، حيث يمكن اعتبار سجلات الأنظمة الحالية بمثابة المصدر الذي يمكن من خلاله استخراج البيانات وجمعها وتحليلها لاكتشاف تهديدات أو حوادث الأمن السيبراني، وعلى سبيل المثال، تُظهر سجلات أحداث الأمن السيبراني أن مستخدماً أو عملية غير مصرح بها قد حصلت على حق الوصول إلى موارد معالجة المعلومات، وقد تعرض السجلات أيضًا بعض السلوكيات الضارة التي يقوم بها المهاجمون على موارد معالجة المعلومات، في حالة وقوع حادث للأمن السيبراني، وتتوفر السجلات المعلومات الالزمة لجهود التحقيق لتحديد أسباب الحادث والمساعدة في التخفيف من الحوادث المستقبلية.

**المادة (29):** تعتبر سجلات الأحداث أحد مصادر البيانات التي يمكن استخدامها للكشف عن حوادث الأمن السيبراني والتحقيق فيها، وعلى المؤسسة المالية تتبع سجلات الأحداث بصورة مستمرة بحيث تتضمن كحد أدنى ما يلي:

1. سجلات أحداث النطاق (Domain Name).
2. سجلات أحداث خادم البريد الإلكتروني.
3. سجلات أحداث جدران الحماية (Firewalls) والبوابة (Gateway).
4. سجلات أحداث أنظمة التشغيل على الخوادم.
5. سجلات أحداث التطبيقات والأنظمة الحساسة.
6. سجلات أحداث الوصول عن بعد Remote Access.

**المادة (30):** يجب أن تكون تدابير الكشف لدى المؤسسة المالية قادرة على دعم عملية الاستجابة للحوادث وجمع المعلومات والأدلة الالزمة لعمليات التحقيق (Forensic IT Audit) كلما اقتضت الحاجة إليها من خلال اتباع ممارسات الاحتفاظ بسجلات الأحداث فترة كافية.

**المادة (31):** على المؤسسة المالية توفير الآليات والأنظمة الالزمة لضمان مراقبة مستمرة وإيجاد ترابطات سببية (Correlations) للكشف عن الأنشطة والأحداث غير الاعتيادية التي قد تؤثر على أعمال المؤسسة المالية أو تسبب في خسارة مالية لها.

**المادة (32):** يجب اتخاذ تدابير للكشف عن مواطن التسريبات المحتملة للمعلومات والشيفرات الخبيثة والتهديدات الأمنية ونقط الضعف والثغرات الأمنية، وضرورة متابعة آخر التحديثات الأمنية والتحقق من تطبيق هذه التحديثات أولاً بأول.

Date: 18 / 02 / 2024

NO: .....



قطاع الرقابة على البنوك  
مكتب الوكيل

CBY

البنك المركزي اليمني  
المركز الرئيسي  
صنعاء  
التاريخ: 08 / 08 / 1445 هـ  
الرقم : ق. د. 338

## الفصل السادس

### الاستجابة للحوادث السيبرانية الطارئة والتعافي منها

المادة (33): على المؤسسة المالية توفير ضوابط الاستجابة للحوادث السيبرانية الطارئة وفقاً لما يلي:

1. تحليل (Business Impact Analysis) الذي تم الإتفاق عليه مع جميع الإدارات المعنية والإدارة التنفيذية كما هو موضح في مادة رقم (14) أعلاه.
2. وضع خطة للاستجابة للحوادث السيبرانية بحيث تكون مصممة للاستجابة الفورية والتعافي من أي حدث طارئ يتعلق بالأمن السيبراني للمؤسسة المالية.
3. عمل فحص لخطة الاستجابة للحوادث السيبرانية وتحديثها باستمرار بالاستناد إلى المعلومات الحالية عن التهديدات السيبرانية والدورات المستفادة من الأحداث السابقة التي تعرضت لها المؤسسة المالية أو أي كيان آخر داخل أو خارج الجمهورية.
4. يجب أن تتضمن خطة الاستجابة للحوادث السيبرانية على ما يلي كحد أدنى:
  - 4.1. تعريف الأدوار والمسؤوليات لاتخاذ القرار بشكل واضح.
  - 4.2. العمليات الداخلية المعنية بالاستجابة للحوادث السيبرانية.
  - 4.3. أهداف خطة الاستجابة للحوادث السيبرانية.
  - 4.4. تحديد الاحتياجات الالزامية لمعالجة مواطن الضعف في أي من مكونات بيئه تكنولوجيا المعلومات والاتصالات وما يرتبط بها من ضوابط.
  - 4.5. مخاطر الحوادث السيبرانية.
  - 4.6. التوثيق والإبلاغ بشأن حوادث الأمن السيبراني وأنشطة الاستجابة للحوادث ذات الصلة.
  - 4.7. تقييم ومراجعة خطة الاستجابة للحوادث السيبرانية حسب الحاجة في أعقاب الحدث السيبراني.
  - 4.8. أماكن حفظ الخطة (Hard copy, Soft copy) والإجراءات الخاصة بها.
5. التعاون والتنسيق مع الجهات المعنية المرتبطة بالمؤسسة المالية لمساعدة في الاستجابة للحوادث السيبرانية بغض احتواء تلك الأحداث غير المتوقعة والتقليل من آثارها خاصةً إذا كانت أنظمة تلك الجهات مرتبطة بأنظمة المؤسسة المالية، كما والتعاون مع تلك الجهات عند وضع خطة الاستجابة للحوادث السيبرانية.
6. إجراء تحقيق وتقييم شامل عند الكشف عن أي هجوم سيبراني أو محاولة لهجوم سيبراني، لتحديد طبيعته ومداه والأضرار التي لحقت بالمؤسسة المالية، كما يجب أن تتخذ المؤسسة المالية إجراءات فورية لاحتواء الحدث السيبراني لمنع المزيد من الأضرار ولاستعادة عملياتها استناداً إلى خطة الاستجابة للحوادث السيبرانية.





Date: 18 / 02 / 2024

NO: .....

CBY

قطاع الرقابة على البنوك  
مكتب الوكيل

البنك المركزي اليمني  
المركز الرئيسي  
صنعاء  
التاريخ: 08 / 08 / 1445 هـ  
الرقم: ق. د. 338

7. تصميم واختبار جميع أنظمة المؤسسة المالية وعملياتها بحيث يكون زمن التعافي المستهدف (Recovery Time Objective -RTO) للعمليات الحرجية من الكوارث متوافق مع خطط استمرارية تكنولوجيا المعلومات، وينبغي أيضًا وضع سيناريوهات الاستجابة في حال فشل القدرة على الاستئناف خلال هذه الفترة.

8. تصميم واختبار أنظمة المؤسسة المالية وعملياتها لتمكين استعادة البيانات الحساسة بعد حدوث الهجوم السيبراني، وينبغي وضع ضوابط صارمة لكشف وحماية تلك البيانات.

9. اتخاذ إجراءات تمكن المؤسسة المالية من تحديد مواطن الضعف التي تبيّنت نتيجة تحقيق في حدث سيبراني طارئ لمنع المزيد من الأضرار واحتواء الحدث وإصلاح الأضرار والจบولة دون تكرار الحدث مستقبلاً.

**المادة (34): على المؤسسة المالية اتخاذ إجراءات التعافي الازمة من الحوادث السيبرانية وعلى أن تتضمن هذه الإجراءات ما يلي:**

1. القضاء على آثار الحوادث الضارة.
2. التأكد من عودة الأنظمة والبيانات لوضعها الطبيعي.
3. تحديد وتحفييف ومعالجة نقاط الضعف التي تم استغلالها لمنع وقوع حوادث مماثلة.
4. التواصل بشكل مناسب مع جميع الجهات الداخلية والخارجية ذات العلاقة مع المؤسسة المالية فيما يخص التعافي من الحدث السيبراني.



Date: 18 / 02 / 2024

NO: .....

CBY

قطاع الرقابة على البنوك  
مكتب الوكيل

البنك المركزي اليمني  
المركز الرئيسي  
صنعاء  
التاريخ: 08 / 08 / 1445 هـ  
الرقم : ق. د. 338

## الفصل السابع

### الاختبارات

المادة (35): على المؤسسة المالية العمل على اختبار مكونات بيئه تكنولوجيا المعلومات والاتصالات بعد وقوع الحدث السيبراني وبالتنسيق مع الجهات المرتبطة بها.

المادة (36): على المؤسسة المالية الالتزام بما يلي:

- تنفيذ اختبارات الاختراق لأنظمة الحرجة وفحص الثغرات الأمنية لبيئة تكنولوجيا المعلومات والاتصالات المساندة لهذه الأنظمة على الأقل مرة واحدة سنويًا، أو بعد إجراء تعديل جذري على الأنظمة أو البيئة مع مراعاة ما يلي:
  - أن يتم بناء نطاق الفحص استناداً إلى درجة حساسية الأنظمة وما يرتبط بها من أنظمة مساندة وداعمة.
  - أن يتم تنفيذ الاختبارات على مستوى التطبيقات والشبكات الداخلية والخارجية في المؤسسة المالية.
  - تنفيذ تقييم نقاط الضعف والثغرات الأمنية لأنظمة الحرجة والأنظمة المساندة الداعمة لها والشبكات الداخلية والخارجية بشكل دوري واتخاذ الإجراءات الكفيلة بمعالجة الثغرات المكتشفة.
  - مراقبة أنظمة المؤسسة المالية بشكل مستمر وفعال للكشف عن أي خلل في أي من مكونات بيئه تكنولوجيا المعلومات والاتصالات والذي قد يشير إلى وجود ثغرات جديدة.

المادة (37): على المؤسسة المالية وضع برنامج اختبار شامل للتحقق من فاعلية سياسة وبرنامج الأمان السيبراني على أساس منتظم ومتكرر وعلى أن يتم إطلاع مجلس الإدارة والإدارة على النحو المناسب بنتائج هذا الاختبار.



Date: 18 / 02 / 2024

NO: .....

CBY

قطاع الرقابة على البنوك  
مكتب الوكيل

البنك المركزي اليمني  
المركز الرئيسي  
صنعاء  
التاريخ: 08 / 08 / 1445 هـ  
الرقم : ق. د. 338

## الفصل الثامن الإسناد الخارجي

**المادة (38):** على المؤسسة المالية تقييم الحاجة لإسناد العمليات الحرجة لطرف ثالث بالاعتماد على تقييم شامل للمخاطر السيبرانية مع مراعاة الضوابط التي وردت في هذا المنشور أو أي تشريعات نافذة بهذا الخصوص.

**المادة (39):** في حال إسناد المؤسسة المالية جزءاً من عملياتها إلى طرف ثالث يجب عليها الالتزام بما يلي:

- التأكد من توفير ضوابط الحماية الازمة للسيطرة على المخاطر السيبرانية المتعلقة بالأنظمة والبيانات الحساسة المستضافة لدى الطرف الثالث للمؤسسة المالية وعملائها وعمل اختبارات دورية ومنتظمة لتقييم تلك الضوابط من قبل جهات مستقلة والحصول على تطمئنات مؤثقة بحسب المعايير الدولية المقبولة بهذا الخصوص وبما يتفق وهذا المنشور و/أو الإشراف والرقابة المستمرة على الخدمات المقدمة من قبل الطرف الثالث.
- على مجلس الإدارة والإدارة التنفيذية إنشاء نظام وآلية لإدارة الخدمات المقدمة من الطرف الثالث بغرض دعم عملية تقديم خدمات المؤسسة المالية وتضمين ذلك بسياسة الإسناد الخارجي لديها.
- توقيع اتفاقية عدم الإفصاح (Non-disclosure Agreement) وحماية وسرية البيانات والمعلومات بينها والطرف الثالث.
- الالتزام بأية شروط أو متطلبات يحددها البنك المركزي بهذا الخصوص، مع تأهيل قائمة لشركات الإسناد.

**المادة (40):** يجب على المؤسسة المالية تضمين البنود التالية بسياسة الإسناد الخارجي فيما يخص المخاطر السيبرانية:

- إجراءات ضبط وصول/نفاذ الطرف الثالث عن بعد بما في ذلك ضرورة النفاذ عبر وسائل توثيق / تحقق الهوية متعدد العناصر (Multi-factor Authentication) للحد من وصوله إلى الأنظمة والمعلومات الحساسة.
- الضوابط الواجب الالتزام بها من قبل الطرف الثالث المتعلقة بالتشمير لحماية المعلومات الحساسة الخاصة بالمؤسسة المالية أثناء تناقلها أو تخزينها من قبل الطرف الثالث.
- الإشعار الواجب تقديمها للمؤسسة المالية في حالة وقوع حادث للأمن السيبراني يؤثر بشكل مباشر أو غير مباشر على أنظمتها أو معلوماتها الحساسة التي يحتفظ بها الطرف الثالث.

**المادة (41):** على المؤسسة المالية عند توقيع اتفاقيات إسناد (Outsourcing) مع الطرف الثالث التأكد من أن تتضمن العقود المبرمة بينها وبين الطرف الثالث متطلبات هذه التعليمات وعلى وجه الخصوص ما يلي:

- الالتزام الطرف الثالث بتطبيق بنود هذه التعليمات بالقدر الذي يتاسب مع أهمية وطبيعة عمليات المؤسسة المالية والخدمات والبرامج والبنية التحتية المقدمة لها قبل وأثناء فترة التعاقد، وبما لا يعي



Date: 18/02/2024

NO: .....

CBY

قطاع الرقابة على البنوك  
مكتب الوكيل

البنك المركزي اليمني  
المركز الرئيسي  
صنعاء  
التاريخ: 08/08/1445 هـ  
الرقم: ق. د. 338

مجلس الإدارة والإدارة التنفيذية للمؤسسة المالية من المسئولية عن تحقيق متطلبات هذا المنشور، على أن يتم تحديث الاتفاقيات مع الشركات المتعاقد معها حالياً بتاريخ نفاذ هذا المنشور أو خلال فترة التعاقد أيهما أسبق وبما يتفق مع متطلبات المنشور.

2. حق التدقيق (Audit Right) للمؤسسة المالية لتقدير المخاطر السيبرانية الناشئة عن ممارسات الطرف الثالث والتي تؤثر على المؤسسة المالية، وذلك من قبل طرف آخر محايده وموثوق يتضمن تقديم رسائل تطمئن تقدم رأيه بخصوص فحص الضوابط ومدى كفيتها، وذلك بحسب المعايير الدولية المتبعة بهذا الخصوص.
3. الحد الأدنى من ممارسات الأمن السيبراني المطلوب تلبيتها من قبل الطرف الثالث بما في ذلك الإجراءات الأمنية اللاحمة فيما يتعلق بمستوى الخدمة (Service Level).
4. التزام الطرف الثالث بسياسة الأمن السيبراني المعهود بها لدى المؤسسة المالية وبما يتفق مع التعليمات الواردة في هذا المنشور.
5. قيام الطرف الثالث بتزويد المؤسسة المالية بتقارير فورية حول أي محاولة اختراق سيبراني أو أحداث طارئة قد تتعرض لها بيانات وخدمات المؤسسة المالية لديهم.





Date: 18 /02 /2024

NO: .....

CBY

قطاع الرقابة على البنوك  
مكتب الوكيل

البنك المركزي اليمني  
المركز الرئيسي  
صنعاء  
التاريخ: 08 / 08 / 1445 هـ  
الرقم: ق. د. 338

## الفصل التاسع الوعية الأمنية

### أولاً: التدريب وزيادة الوعي:

المادة (42): على المؤسسة المالية نشر ثقافة أن الأمان السيبراني مسؤولية مشتركة بين جميع موظفيها بحيث يكون كل موظف على دراية بمسؤوليته وواجباته تجاه الأمان السيبراني وذلك من خلال القيام بعمليات توعية وتدريب منتظمة لجميع الموظفين فيها بجميع مستوياتهم بهدف تعزيز الثقافة بأهمية الأمان السيبراني داخل المؤسسة المالية على أن يتم تحديها لتعكس المخاطر التي تحددها المؤسسة المالية في تقييمها للمخاطر وأن تتضمن عملية التوعية كحد أدنى ما يلي:

1. التوعية بالأمان السيبراني وأنواع التهديدات السيبرانية.
2. كيفية الكشف عن المخاطر السيبرانية وطرق تجنبيها والحماية منها.
3. كيفية الإبلاغ عن أي نشاط وحوادث غير عادلة.
4. آخر التهديدات الجديدة وطرق تجنبيها والحماية منها.
5. آلية تطبيق التعليمات والتوعية بالمهام والمسؤوليات وتأثيرات المسائلة في حالات عدم الامتثال.
6. تقييم برنامج التوعية بالأمان السيبراني بحيث يتضمن قياس النجاح إجراء تقييمات ومراجعات دورية للبرنامج.
7. قياس ما إذا كان سلوك الموظفين ومعارفهم ومهاراتهم في التعامل مع المعلومات وأجهزة الكمبيوتر قد تحسن، وعلى سبيل المثال قد تجري المؤسسة المالية اختبارات الهندسة الاجتماعية للموظفين من خلال هجمات التصيد المحاكية والمنظمة على أن تستخدم النتائج في تحديث البرنامج وتحسينه.
8. تزويد الموظفين وإطلاعهم على سياسات أمن المعلومات وسياسة الأمان السيبراني وتوقيعهم على الإقرار بفهمها والالتزام بمحتواها.

المادة (43): على المؤسسة المالية توفير تدريب خاص ومكثف للعاملين في مجال تكنولوجيا المعلومات وأمن المعلومات والأمان السيبراني والموظفين الذين لديهم صلاحيات الوصول إلى الأنظمة الحرجية والمعلومات الحساسة كل حسب اختصاصه.

المادة (44): على المؤسسة المالية توفير برامج التوعية مرة واحدة في السنة على الأقل لأعضاء مجلس الإدارة والإدارة حول مخاطر تكنولوجيا المعلومات والأمان السيبراني وأفضل الممارسات الدولية في هذا الصدد.

### المادة (45):

1. على المؤسسة المالية توعية عملائها لتفادي مخاطر الهجوم السيبراني وضرورة اتباع الضوابط المقررة لحفظ بياناتهم المالية والمصرفية وأخذ الحيطة والحذر، ومنها:



Date: 18 / 02 / 2024

NO: .....

CBY

قطاع الرقابة على البنوك  
مكتب الوكيل

البنك المركزي اليمني  
المركز الرئيسي  
صنعاء

التاريخ: 08 / 08 / 1445 هـ  
الرقم: ق. د. 338

1.1. تعلم وفهم سياسة الأمان السيبراني والخصوصية لموقع الويب والتطبيقات الخاصة بالمؤسسة المالية.

1.2. حماية الهوية الشخصية وبيانات التعريف بالهوية من خلال استخدام معرفات مختلفة لتطبيقات الويب المختلفة والتقليل من مشاركة المعلومات الشخصية على موقع الويب أو التطبيقات التي تطلب هذه المعلومات.

1.3. إبلاغ الأطراف ذات العلاقة بالمؤسسة المالية عن الأحداث المشبوهة التي تواجههم.

1.4. عدم مشاركة المعلومات المصرفية على موقع الويب أو التطبيقات غير المؤوثة التي تطلب هذه المعلومات.

1.5. ضرورة توعية العملاء بشكل مستمر عن كيفية التأكد من هوية المؤسسة المالية على الإنترنت وعبر تطبيقات الهاتف أثناء استخدام خدماتها.

2. على المؤسسة المالية توضيح الطرق المعتمدة والأمنة لتبلغ الجهات ذات العلاقة عن أي حدث سيبراني أو سرقة للبيانات.

### ثانياً: تبادل معلومات الحوادث السيبرانية

المادة (46): على المؤسسة المالية تبادل معلومات الحوادث السيبرانية في الوقت المناسب مع الجهات ذات العلاقة والجهات المؤوثة والمتخصصة بمواضيع المخاطر السيبرانية السائدة حالياً والتهديدات ونقاط الضعف والحوادث والاستجابات، لتعزيز الضوابط المفعة في المؤسسة المالية والحد من الأضرار وزيادة الوعي فيما يتواافق مع أي تعاميم أو تعليمات صادرة عن البنك المركزي بهذا الخصوص.

المادة (47): على المؤسسة المالية الاعتماد على بيانات الحوادث السيبرانية الداخلية والخارجية في تقييم المخاطر السيبرانية.



Date: 18 / 02 / 2024

NO: .....

CBY

قطاع الرقابة على البنوك  
مكتب الوكيل

البنك المركزي اليمني  
المركز الرئيسي  
صنعاء

التاريخ: 08 / 08 / 1445 هـ

الرقم: ق. د. 338

## الفصل العاشر

### الأمن السيبراني لوسائل التواصل الاجتماعي

المادة (48): على المؤسسة المالية اتخاذ التدابير المناسبة لحماية حساباتها في وسائل التواصل الاجتماعي بحيث

تتضمن كحد أدنى ما يلي:

1. تكليف موظف / موظفين بمسؤولية إدارة كل حساب تابع للمؤسسة المالية على وسائل التواصل الاجتماعي.
2. حماية الحسابات باستخدام كلمات مرور آمنة باتباع أفضل ممارسات إدارة كلمات المرور الموصى بها.
3. ربط حسابات المؤسسة المالية في وسائل التواصل الاجتماعي باستخدام البريد الإلكتروني ورقم الهاتف المسروق بهما من قبل المؤسسة المالية.

المادة (49): يجب أن تحتوي حسابات المؤسسة المالية في وسائل التواصل الاجتماعي على شارات تحقق ظهر أن

الحسابات أصلية وتساعد في بناء الثقة بين المؤسسة المالية وعملائها، وبالتالي يضمن المستخدمون التفاعل مع الحسابات التي تم التحقق منها.



Date: 18/02/2024

NO: .....

CBY

قطاع الرقابة على البنوك  
مكتب الوكيل

البنك المركزي اليمني  
المركز الرئيسي  
صنعاء

التاريخ: 08/08/1445 هـ  
الرقم: ق.د. 338

## الفصل الحادي عشر أحكام عامة وختامية

**المادة (50):** على المؤسسة المالية إيقاف العمل بالخدمات والأنظمة والأجهزة غير المستخدمة بسبب عدم الحاجة لها بشكل نهائى وفق سياستها المعتمدة بهذا الخصوص وبطريقة تضمن عدم تأثير الخدمات أو الأنظمة أو العمليات الأخرى، مع مراعاة متطلبات الاحتفاظ بالسجلات والبيانات التاريخية بحسب القوانين النافذة.

**المادة (51):**

- على المؤسسة المالية إخطار وحدة جمع المعلومات المالية في البنك المركزي في حال اكتشاف تعرضها لأى حادث سبيراني أو أى محاولة هجوم سبيراني تتسم بدرجة خطورة عالية على أنظمتها أو شبكاتها في موعد أقصاه (72) ساعة من لحظة اكتشاف الحادث أو الهجوم السبيراني.
- على المؤسسة المالية تزويذ البنك المركزي بتفاصيل الأحداث السبيرانية وأثارها وإجراءات الاستجابة والإجراءات الوقائية التي تم اتخاذها بشكل دوري وبحسب الآلية التي يحددها البنك المركزي.

**المادة (52):** على المؤسسة المالية الإفصاح عن سياسة الأمن السبيراني الخاصة بها مع أصحاب المصالح.

**المادة (53):** على المؤسسة المالية إعلام العميل عن أية تحديات في الإجراءات الأمنية الواجب اتباعها من قبله وحسب الآلية المنقولة مع العميل.

**المادة (54):** يجب أن تشتمل برامج المدقق الداخلي والمدقق الخارجي على آليات تضمن الرقابة والمتابعة المستمرة لبنود هذا المنشور.

**المادة (55):** على المؤسسة المالية التأكد من أن كافة الأنظمة والتجهيزات المستخدمة لديها متوافقة مع المعايير العالمية والمحلية.

**المادة (56):** يُعمل بهذا المنشور من تاريخ صدوره، ويتم تزويذ البنك المركزي قطاع الرقابة على البنوك بالسياسة والإجراءات التي تم اعتمادها من قبلكم في موعد أقصاه 30 سبتمبر 2024م وبأي تقارير أو بيانات يراها مناسبة التزاماً بالمنشور.

صدر بالبنك المركزي - المركز الرئيسي - صنعاء

بتاريخ: 08/شaban/1445هـ

الموافق: 18/FEB/2024م

فواز قاسم البنا

وكيل قطاع الرقابة على البنوك

