الرقـــم: ١/١/٢٦/ ١٩٨٤

التاريـخ: ٢٠١٨/٢/٦

الموافق: ٢٠/ جمادى الاولى/ ١٤٣٩

البنك المركزي الأردني

تعليمات التكيف مع المخاطـر السيبرانية

جدول المحتويات

الفصل الأول

الإسناد ونطاق التطبيق والتعريفات

المادة (١):

صدرت هذه التعليمات سنداً لأحكام المادة (٤/ب/٣و٤) والمواد (٥٠/ج، ٦٥/ب) من قانون البنك المركزي الأردني رقم (٢٣) لسنة ١٩٧١ وتعديلاته، والمادة (٩٩/ ب) من قانون البنوك رقم ٢٨ لسنة ٢٠٠٠ وتعديلاته، والمادة (٢٢/ب) من قانون المعاملات الإلكترونية رقم (١٥) لسنة ٢٠١٥ وتعديلاته، وتعتبر نافذة بعد اثني عشر شهراً من تاريخها، ما لم ينص على خلاف ذلك.

المادة (٢):

تسمى هذه التعليمات " تعليمات التكيف مع المخاطـر السيبرانية ".

المادة (٣):

أ. تسري هذه التعليمات على جميع البنوك المرخصة والمؤسسات المالية وشركات المعلومات الائتمانية وشركات التمويل الأصغر الخاضعة لإشراف ورقابة البنك المركزي الأردني.

ب. على فروع البنوك الأجنبية العاملة في المملكة الالتزام بهذه التعليمات بالقدر الذي ينطبق عليها أو بدليل وسياسات الحاكمية والإدارة للمعلومات والتكنولوجيا المصاحبة لها الصادرة عن البنك الأم أو السلطة الرقابية في الدولة الأم أيهما أكثر تحقيقاً لأهداف هذه التعليمات، وفي حال كانت التعليمات الصادرة عن البنك الأم أو السلطة الرقابية في الدولة الأم أكثر تحقيقاً لأهداف التعليمات على الفرع تقديم ما يؤيد ذلك للبنك المركزي، فإن على هذا الفرع تقديم ما يؤيد ذلك إلى البنك المركزي، مع مراعاة عدم التعارض مع التشريعات النافذة في المملكة، وفي حال وجود تعارض فعلى الفرع إعلام البنك المركزي والشركة الأم بذلك وتقديم التوضيح اللازم لهذا التعارض والحصول على موافقة البنك المركزي على أسلوب معالجة هذا التعارض.

المادة (٤):

يراعي البنك عند تطبيق التعليمات كل ما ورد في تعليمات حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها رقم (٢٠١٦/٦٥) تاريخ ٢٠١٦/١٠/٢٥ وعلى وجه الخصوص ما يتعلق بإدارة أمن ومخاطر تكنولوجيا

المعلومات وتقرأ معها بشكل متكامل، وتراعي المؤسسة المالية وشركة المعلومات الائتمانية وشركة التمويل الأصغر تطبيق التعليمات المشار إليها بالقدر الذي يتوافق ويلبي هذه التعليمات.

المادة (٥):

أ. يكون للكلمات والعبارات التالية حيثما وردت في هذه التعليمات المعاني المخصصة لها أدناه ما لم تدل القرينة على خلاف ذلك:

المؤسسة المالية	:	**أي من الشركات المساهمة العامة أو المساهمة الخاصة المرخص لها بمزاولة خدمات الدفع أو إدارة وتشغيل أنظمة الدفع الالكتروني.**
شركة المعلومات الائتمانية	:	الشركة المرخصة وفقاً لأحكام قانون المعلومات الائتمانية رقم (١٥) لسنة ٢٠١٠ والنظام الصادر بمقتضاه.
شركة التمويل الأصغر	:	الشركة المالية التي تمارس نشاط التمويل الأصغر والمرخصة وفقا لأحكام نظام شركات التمويل الأصغر رقم (٥) لسنة ٢٠١٥.
الشركة	:	البنك أو البنك الإسلامي أو المؤسسة المالية أو شركة المعلومات الائتمانية أو شركة التمويل الأصغر.
المجلس	:	مجلس إدارة الشركة ومن في حكمه.
الإدارة التنفيذية العليا	:	تشمل مدير عام الشركة أو المدير الإقليمي ونائب المدير العام أو نائب المدير الإقليمي ومساعد المدير العام أو مساعد المدير الإقليمي والمدير المالي ومدير العمليات ومدير إدارة المخاطر ومدير الخزينة (الاستثمار) ومدير الامتثال، بالإضافة لأي موظف في الشركة له سلطة تنفيذية موازية لأي من سلطات أي من المذكورين ويرتبط وظيفياً مباشرةً بالمدير العام.
بيئة تكنولوجيا المعلومات والاتصالات	:	هي مجموعة التجهيزات الحاسوبية الخاصة بالشبكات الداخلية والشبكات الخارجية والخوادم الرئيسية والبرمجيات العاملة عليها وجميع الأجهزة المساندة لها في الموقع الرئيسي والبديل

		للشركة.
المعلومات (Information)	:	أي بيانات شفوية أو مكتوبة أو سجلات أو إحصاءات أو وثائق مكتوبة أو مصورة أو مسجلة أو مخزنة إلكترونياً أو بأي طريقة أخرى تعد ذات قيمة للشركة.
البيانات (Data)	:	الحقائق الخام ويمكن توضيحها بالحروف والرموز والأرقام التي من الممكن أن تمثل الأشخاص أو الأشياء أو الأحداث.
أصول المعلومات (Information Assets)	:	أية معلومات أو ملفات إلكترونية أو غير إلكترونية أو أجهزة أو وسائط تخزين أو برامج أو أي من مكونات بيئة تكنولوجيا المعلومات والاتصالات المتعلقة بأعمال الشركة.
الفضاء السيبراني (Cyberspace)	:	بيئة افتراضية تتكون من تفاعل الأشخاص والبرمجيات والخدمات على الإنترنت عن طريق أجهزة وشبكات التكنولوجيا المتصلة بها.
الهجوم السيبراني (Cyber Attack)	:	أي محاولة تدمير أو كشف أو تغيير أو تعطيل أو سرقة أو محاولة استغلال نقاط الضعف أو نفاذ غير مشروع لأصول معلومات الشركة ضمن الفضاء السيبراني.
التكيف السيبراني (Cyber Resilience)	:	قدرة الشركة على توقع، وتحمل، واحتواء والتعافي بشكل سريع من الهجوم السيبراني.
الأمن السيبراني (Cyber Security)	:	الحفاظ على سرية وتكاملية وتوافرية المعلومات وأصول المعلومات التابعة للشركة ضمن الفضاء السيبراني من أي تهديد سيبراني عن طريق مجموعة من الوسائل والسياسات والتعليمات وأفضل الممارسات بهذا الخصوص.
التهديد السيبراني (Cyber Threat)	:	ظرف أو حدث يحتمل أن يستغل (عن قصد أو غير قصد) واحد أو أكثر من نقاط الضعف الموجودة في بيئة تكنولوجيا المعلومات والاتصالات للشركة، مما يؤثر على الأمن السيبراني فيها.
الحدث السيبراني	:	أي واقعة تدل على وجود تهديد سيبراني على بيئة تكنولوجيا

(Cyber Event)		المعلومات والاتصالات للشركة.
المخاطر السيبرانية (Cyber Risk)	:	مقدار توليفي ناتج عن احتساب احتمال وقوع حدث سيبراني في نطاق أصول المعلومات للشركة، وأثر ذلك الحدث على الشركة.
الحوكمة السيبرانية (Cyber Governance)	:	ترتيبات الشركة لوضع وتنفيذ ومراجعة نهجها لإدارة المخاطر السيبرانية.
حوكمة البيانات (Data Governance)	:	هي عملية إدارة توافرية، وأمن، وسهولة استخدام، وسلامة البيانات المستخدمة في الشركة.
الشيفرات الخبيثة (Malicious Code)	:	برمجيات أو ملفات ضارة تتضمن وظائف لها قدرات تؤثر بشكل سلبي سواء بشكل مباشر أو غير مباشر على بيئة تكنولوجيا المعلومات والاتصالات المستخدمة في الشركة.
الحماية (Protection)	:	توظيف الإجراءات والضوابط والتدابير الملائمة لتقديم خدمات وأعمال الشركة بصورة موثوقة.
الكشف (Detection)	:	توظيف الضوابط والإجراءات المناسبة من أجل العلم بوقوع الحدث السيبراني فوراً.
الاستجابة (Response)	:	توظيف الضوابط والإجراءات المناسبة لاحتواء الحدث السيبراني عند كشفه.
الاستعادة (Restore)	:	عملية استرجاع المعلومات المخزنة على وسائط النسخ الاحتياطية عند تلف أو فقدان المعلومات الاصلية أو الحاجة اليها بعد مدة من الزمن لإعادة سير عمل الشركة.
التعافي (Recovery)	:	مجموعة الإجراءات التي يتم اتخاذها واتباعها لإعادة الأعمال في الشركة الى وضعها الطبيعي وإعادة تشغيل موارد التكنولوجيا المعتمد عليها في تشغيل عمليات الشركة إلى ما كانت عليه قبل وقوع الحدث.
نقاط الضعف (Vulnerabilities)	:	خلل أو نقص في ضوابط الحماية المستخدمة في أي من مكونات بيئة تكنولوجيا المعلومات والاتصالات المتعلقة بأعمال

		الشركة الممكن استغلالها في عمليات الاختراق والهجوم السيبراني.
ضوابط الوصول/النفاذ (Access Control)	:	القواعد والآليات المستخدمة للسماح باستخدام ونفاذ الأشخاص المخولين فقط إلى أصول المعلومات وبما يتوافق وطبيعة مسؤولياتهم في الشركة.
الامتيازات (Privileges)	:	مستوى الصلاحيات التي يتم منحها للمستخدمين للوصول/للنفاذ واستخدام أي من مكونات بيئة تكنولوجيا المعلومات والاتصالات في الشركة.
إدارة التغيير (Change Management)	:	إدارة وضبط وتوثيق أي تغيير يتم إجراؤه على أي من مكونات بيئة تكنولوجيا المعلومات والاتصالات في الشركة أو أي تغيير في الإجراءات المعمول بها في الشركة من قبل الأطراف المخولة بالموافقة.
تصنيف المعلومات (Information Classification)	:	تحديد مستوى الحساسية المناسب للمعلومات التي يتم إنشاؤها أو تغييرها أو نقلها أو تعديلها أو حفظها على أية وسائل كانت وبأية تقنيات ممكنة، اعتمادا على المخاطر المترتبة على الاطلاع والاستخدام غير المشروع لتلك المعلومات.
السرية (Confidentiality)	:	حماية المعلومات من عمليات الاطلاع والنشر والإفصاح والاستخدام غير المشروع.
التوافرية (Availability)	:	امكانية استخدام والوصول/النفاذ الى المعلومات والأنظمة في الشركة واسترجاعها عند الطلب.
التكاملية (Integrity)	:	دقة واكتمال وسلامة المعلومات أو نظم المعلومات أو أي جزء منها والتحقق من أنه لم يطرأ عليها أي زيادة أو نقصان أو تغيير غير مشروع.
زمن التعافي المستهدف (Recovery Time Objective -	:	اقصى وقت مسموح به لإعادة تشغيل الخدمة أو العملية بعد حدوث الانقطاع لخدمات تكنولوجيا المعلومات.

RTO)		
نقطة الاسترجاع المستهدفة (Recovery Point Objective-RPO)	:	هو العمر الاقصى المسموح للبيانات التي قد تفقد عند استعادة الخدمة بعد حدوث انقطاع.
ادارة المخاطر السيبرانية (Cyber Risk Management)	:	عمليات تحديد وقياس وضبط ومراقبة المخاطر السيبرانية.
العمليات الحرجة (Critical Operations)	:	العمليات التي لا يمكن تحمل توقفها لفترات زمنية طويلة بحسب دراسات تحليل الأثر على الأعمال في الشركة، وتلك العمليات ذات المخاطر والأهمية النسبية للشركة.
البريد الإلكتروني (E-mail)	:	الخدمة التي يمكن توفيرها للمستخدمين من إنشاء وإرسال واستقبال وتخزين الرسائل الإلكترونية باستخدام أنظمة الاتصالات الإلكترونية.
التشفير (Encryption)	:	عملية تحويل المعلومات إلى شكل غير مقروء أو مفهوم.
الطرف الثالث (Third Party)	:	الجهة التي تعهد اليها الشركة لتولي الأعمال الفنية والتقنية بشكل كلي أو جزئي لمساعدتها للقيام بالأعمال المرخصة لها بما لا يتعارض مع أحكام التشريعات النافذة.
الاسناد الخارجي (Outsourcing)	:	الاستعانة بطرف ثالث أو توظيف موارده لتسيير أعمال الشركة أو جزء من أعمالها التي تقع ضمن مسؤوليتها.
الأمن المادي (Physical Security)	:	معايير و إجراءات الحماية التي تراقب أو تحدد الدخول إلى أي من مرافق أو موارد أو معلومات الشركة المخزنة على وسائط فيزيائية أو لمنع الوصول الى الموارد المعلوماتية والأنظمة، مثل المباني وخزائن الملفات والأجهزة المكتبية والمحمولة والخوادم والمعدات.
أصحاب المصالح (Stakeholders)	:	أي ذي مصلحة في الشركة مثل المساهمين أو الموظفين أو الدائنين أو العملاء أو المزودين الخارجيين أو الجهات الرقابية

		المعنية.
سجلات الأحداث (Event log)	:	ملفات بيانات الأحداث الأمنية والتشغيلية التي تنتج عن مكونات النظام لفهم نشاط النظام وتشخيص المشاكل التي قد تحصل عليه.
سجلات التدقيق (Audit Trail)	:	ملفات بيانات تقدم أدلة مستنديه على تسلسل العمليات الوظائفية والإدارية التي تحدث على الأنظمة.
تقييم المخاطر (Risk Assessment)	:	قياس وتحديد احتمالية حدوث المخاطر وشدتها وتوقع مقدار تأثيرها على الشركة.
اختبارات الاختراق (Penetration Testing)	:	اختبار يحاول فيه المقيمون المختصون بالبحث عن الثغرات الأمنية والتحايل على الخصائص الأمنية لأنظمة المعلومات والضوابط الأمنية واستغلالها لمحاولة اختراق تلك الأنظمة من خارج أو داخل الشركة لمعرفة مدى فعالية الضوابط الأمنية المستخدمة من قبل الشركة لحماية انظمتها.
الوصول عن بعد (Remote Access)	:	تمكين الاتصال مع أنظمة الشركة من خارج الشبكة الداخلية الخاصة بها سواء كان ذلك التمكين لغايات عمل موظفيها عن بعد أو تأمين الاتصال مع شركاء العمل أو من قبل طرف ثالث.

ب. تعتمد التعاريف الواردة في قانون البنك المركزي وقانون المعاملات الإلكترونية وقانون البنوك وأية تعليمات ذات علاقة صادرة عن البنك المركزي حيثما ورد النص عليها في هذه التعليمات ما لم تدل القرينة على غير ذلك.

الفصل الثاني

أولاً: حوكمة الامن السيبراني

المادة (٦):

على الشركة الالتزام بما يلي:

أ. أن يضم مجلس الإدارة في عضويته ومن يفوض من لجانه والإدارة التنفيذية العليا أشخاص يتمتعون بالمهارات والمعارف المناسبة لفهم وإدارة المخاطر السيبرانية.

ب. يتولى المجلس أو من يفوض من لجانه المسؤوليات والمهام التالية كل بحسب موقعه:

١. اعتماد سياسة الأمن السيبراني (Cyber Security Policy)

٢. اعتماد برنامج الأمن السيبراني (Cyber Security Program)

٣. فحص الامتثال لسياسة وبرنامج الأمن السيبراني.

ج. تتولى الإدارة التنفيذية العليا المسؤوليات والمهام التالية كل بحسب موقعه:

١. ضمان تطبيق وتحديث سياسة الأمن السيبراني.

٢. ضمان تطبيق برنامج الأمن السيبراني بحيث يكون متكامل مع الإطار العام لإدارة مخاطر تكنولوجيا المعلومات، والاستمرار بتحديثه وتطويره.

٣. ضمان وجود سجل شامل خاص بالمخاطر السيبرانية (Cyber Risk Register) وضمان تحديثه بشكل مستمر وبحيث يكون متوافق مع ملف مخاطر تكنولوجيا المعلومات (IT Risk Profile) في الشركة.

٤. الاطلاع على ومراقبة مستوى المخاطر السيبرانية بشكل مستمر.

٥. اعتماد قوائم الصلاحيات المتعلقة بإدارة الأمن والمخاطر السيبرانية من حيث تحديد الجهة أو الجهات أو الشخص أو الأطراف المسؤولة بشكل أولي (Responsible)، وتلك المسؤولة بشكل نهائي (Accountable)، وتلك المستشارة (Consulted)، وتلك التي يتم اطلاعها (Informed)، لكافة عمليات إدارة وضبط تلك المخاطر والرقابة والتدقيق عليها.

ثانياً: برنامج وسياسة الأمن السيبراني

المادة (٧):

على الشركة تطبيق والاستمرار بتحديث برنامج الأمن السيبراني (Cyber Security Program) لضمان تحقيق متطلبات السرية والمصداقية والتوافرية للمعلومات في بيئة تكنولوجيا المعلومات والاتصالات، على أن يتضمن البرنامج بالحد الأدنى ما يلي:

أ. تحديد التهديدات الداخلية والخارجية للمخاطر السيبرانية.
ب. تحديد وتصنيف مخاطر وحساسية المعلومات في بيئة تكنولوجيا المعلومات والاتصالات.
ج. تحديد الجهات ذات القدرة على النفاذ والاستخدام للمعلومات وبيئة تكنولوجيا المعلومات والاتصالات.
د. تطبيق سياسة وإجراءات الأمن السيبراني وتشغيل وبيئة تكنولوجيا المعلومات والاتصالات اللازمة لضمان حماية أصول المعلومات والمعلومات الحساسة في الشركة من عمليات الاختراق غير المشروع.
ه. كشف محاولات الاختراق غير المشروع الناجحة والفاشلة فور حدوثها ما أمكن.
و. اتخاذ الإجراءات التصحيحية اللازمة للسيطرة على والحد من الآثار السلبية للمخاطر السيبرانية.
ز. إجراءات إعادة تشغيل عمليات الشركة بعد توقفها بما في ذلك المتعلقة بالخدمات والمتطلبات القانونية والرقابية خلال الفترة الزمنية المقبولة والمحددة ضمن خطة استمرارية العمل وبما يتوافق مع ما ورد في المادة(٣٢/و) في هذه التعليمات.

المادة (٨):

يجب أن تكون سياسة الأمن السيبراني وثيقة مخصصة للأمن السيبراني في الشركة، كما يراعى لدى إعداد السياسة وتحديثها مساهمة كافة الأطراف المعنية واعتماد أفضل الممارسات الدولية وتحديثاتها كالمراجع والدروس والعبر المستفادة من حوادث الأمن السيبراني، ويمكن للشركة تضمين سياسة الأمن السيبراني بسياسة أمن المعلومات تحت مسمى "سياسة أمن المعلومات والأمن السيبراني" وكذلك تضمين برامج الأمن السيبراني ضمن برنامج أمن المعلومات شريطة تحقيق جميع ما ورد في هذه التعليمات.

المادة (٩):

يجب أن تتضمن سياسة الأمن السيبراني المحاور التالية بالحد الأدنى:

أ. تحديد الأدوار والمسؤوليات بما في ذلك مسؤولية اتخاذ القرار داخل الشركة فيما يتعلق بإدارة المخاطر السيبرانية وبما يشمل حالات الطوارئ والأزمات.

ب. حوكمة البيانات وتصنيفها.

ج. أمن وإدارة المعلومات وبيئة تكنولوجيا المعلومات والاتصالات في الشركة.

د. خصوصية بيانات العملاء.

ه. إدارة المخاطر السيبرانية.

و. ضوابط الحماية للحد من والسيطرة على المخاطر السيبرانية.

ز. خطط استمرارية الأعمال والتعافي من الكوارث.

ح. التعاون مع الأطراف المعنية للاستجابة الفعالة للهجمات السيبرانية والتعافي منها.

ط. مراقبة الأنظمة والشبكات والتطبيقات وتطويرها.

ي. ضوابط الأمن المادي والبيئي.

ك. إدارة العمليات المسندة للطرف الثالث.

ل. توعية وتدريب الموظفين داخل الشركة بخصوص الأمن السيبراني لضمان تطبيق جميع الموظفين في الشركة لجميع بنود سياسة الأمن السيبراني.

م. تحديد آلية الإفصاح للأطراف المعنية عن بنود سياسة الأمن السيبراني كل بحسب دوره.

ن. تحديد الجهة المالكة ونطاق التطبيق ودورية المراجعة والتحديث وصلاحيات الاطلاع والتوزيع والأهداف والمسؤوليات وإجراءات العمل المتعلقة بها والعقوبات في حال عدم الامتثال وآليات فحص الامتثال.

المادة (١٠):

يجب على الشركة إدارة أمن المعلومات ذات العلاقة بالأمن السيبراني من خلال مدير أمن معلومات بحيث لا يتبع اداريا لدائرة تقنية المعلومات ويتمتع بالاستقلالية وبما يضمن عدم تضارب المصالح وأن يكون لديه الخبرة العملية والمعرفة المهنية اللازمة ليكون مسؤولا عن المهام التالية كحد أدنى:

أ. الإشراف بشكل مباشر على وضع برنامج وسياسة الأمن السيبراني وضمان تنفيذهما والعمل على مراجعتهما وتحديثهما باستمرار.

ب. تقييم مدى كفاية وكفاءة برنامج وسياسة الأمن السيبراني.

ج. مراجعة فعالية ضوابط الحماية المعتمدة في سياسة الأمن السيبراني لدى الشركة بشكل مستمر.

د. تحديد وتقييم المخاطر السيبرانية.

ه. رفع تقارير نصف سنوية على الأقل أو كلما دعت الحاجة للمجلس وللإدارة التنفيذية العليا فيما يخص الأمن السيبراني في الشركة، على أن يتضمن التقرير الأمور التالية بالحد الأدنى:

١. الانحرافات المتعلقة بتطبيق سياسة الأمن السيبراني وإجراءاتها.

٢. نتائج تقييم المخاطر السيبرانية.

٣. نتائج تقييم مدى كفاية وكفاءة برنامج وسياسة الأمن السيبراني.

٤. التوصيات والإجراءات والمتطلبات الواجبة التنفيذ.

٥. ملخص يستعرض أهم أحداث تهديدات واختراقات الأمن السيبراني التي تعرضت لها الشركة خلال فترة التقرير.

المادة (١١):

بالرغم مما ورد في المادة (١٠) أعلاه يحق للشركة إسناد مهام إدارة أمن المعلومات أو جزء منها لطرف ثالث على أن تلتزم بما يلي:

أ. الطلب من الطرف الثالث الالتزام بما يلبي متطلبات التعليمات فيما يخص إدارة أمن المعلومات.

ب. فحص امتثال الطرف الثالث لمتطلبات التعليمات فيما يخص إدارة أمن المعلومات.

المادة (١٢):

على الشركة قبل إجراء تغيير في بيئة تكنولوجيا المعلومات والاتصالات في الشركة أو العمليات أو الإجراءات أو بعد وقوع أي حدث يؤثر على أمن الشركة التأكد ما إذا كانت هناك حاجة إلى إدخال تغييرات أو تحسينات على سياسة وبرنامج الأمن السيبراني.

الفصل الثالث

إدارة المخاطر السيبرانية

أولاً: تحديد العمليات الحرجة وأصول المعلومات الداعمة في الشركة

المادة (١٣):

على الشركة تحديد ما يلي للتمكن من تقييم المخاطر السيبرانية التي قد تواجهها:

أ. الوظائف والعمليات الحرجة في الشركة.

ب. أصول المعلومات في الشركة وفهم عملياتها وإجراءاتها ونظمها وما يتعلق بها من موارد ونظم المعلومات وسبل الوصول إليها، بما في ذلك النظم الداخلية والخارجية المرتبطة بها.

المادة (١٤):

على الشركة تصنيف وظائفها والعمليات الحرجة فيها وأصول المعلومات وذلك من حيث أهميتها وحساسيتها، ومراجعة وتحديث التصنيفات بشكل مستمر.

ثانياً: تقييم المخاطر السيبرانية

المادة (١٥): على الشركة تحليل عوامل المخاطر السيبرانية (Cyber Risk Factor Analysis) بشكل مستمر من حيث تحديد الأمور التالية:

أ. التهديدات الداخلية.

ب. التهديدات الخارجية.

ج. مواطن الضعف في إدارة موارد بيئة تكنولوجيا المعلومات والاتصالات.

د. مواطن الضعف في قدرة بيئة تكنولوجيا المعلومات والاتصالات على تمكين عمليات الشركة.

ه. مواطن الضعف في إدارة مخاطر بيئة تكنولوجيا المعلومات والاتصالات.

المادة (١٦):

على الشركة تحليل سيناريوهات المخاطر السيبرانية (Cyber Risk Scenario Analysis) بشكل مستمر من حيث تحديد الأمور التالية بالحد الأدنى:

أ. مصدر التهديد السيبراني: إما داخلي أو خارجي.

ب. نوع التهديد السيبراني: إما طبيعي، أو مفتعل، أو تكنولوجي.

ج. الحدث السيبراني: على سبيل المثال لا الحصر إفصاح معلومات سرية أو تعطل أو تعديل غير مشروع أو سرقة أو تدمير أو تصميم غير فعال أو استخدام غير مقبول.

د. الأصول أو الموارد المتأثرة (Assets or Resources Affected): على سبيل المثال لا الحصر موارد بشرية أو هياكل تنظيمية أو عمليات أو بيئة تكنولوجيا المعلومات والاتصالات أو معلومات.

ه. الوقت: وقت الحدوث، ومدة الحدث، وعمر الحدث عند اكتشافه.

المادة (١٧):

على الشركة إنشاء والاستمرار بتحديث السجل الشامل الخاص بالمخاطر السيبرانية (Cyber Risk Register) على أن يتضمن ما يلي بالحد الأدنى:

أ. مالك الأصل، فريق التقييم، تاريخ التقييم، تاريخ التقييم اللاحق، ملخص تقييم المخاطر السيبرانية وخيارات إدارتها.

ب. تقييم المخاطر السيبرانية من حيث احتساب محوري المخاطر متمثلة باحتمالية الحدث (Potential) وحجم الأثر (Impact or Severity)، ويفضل استخدام مقياس معياري زوجي لمحاور التقييم، وإظهار حجم الأثر اعتماداً على أهداف وعمليات الشركة المتضمنة تكنولوجيا المعلومات باستخدام محاور التقييم لأحد النماذج العالمية التالية على سبيل المثال:

١. COBIT Information Criteria
٢. Balanced Scorecard (BSC)
٣. Extended BSC
٤. Wester man
٥. COSO ERM

٦. FAIR (Factor Analysis of Information Risk)

ج. مستوى المخاطر المقبول (Risk Appetite).

د. خيارات إدارة المخاطر (قبول، تخفيف، تجنب، تحويل).

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

و. معايير أداء رئيسية لمراقبة مستوى المخاطر (Key Risk Indicators) للتأكد من عدم تجاوز المخاطر المقبولة ودرجة تحمل المخاطر (نسبة الانحراف المضافة للمخاطر المقبولة).

ز. معايير لتقييم سرية، نزاهة، أمن وتوافر الأنظمة والمعلومات الحساسة.

ح. تحديد مسؤوليات موظفي الشركة تجاه تلك المخاطر.

المادة (١٨):

يحق للشركة الاستعانة بطرف ثالث لغايات تقييم المخاطر السيبرانية مع مراعاة أحكام التشريعات النافذة.

الفصل الرابع

ضوابط الحماية

أولاً: حماية الأنظمة والبرمجيات والشبكات والأجهزة الشبكية

المادة (١٩):

على الشركة توفير ضوابط الحماية التالية على سبيل المثال لا الحصر لجميع مكونات بيئة تكنولوجيا المعلومات والاتصالات مثل الأنظمة والبرمجيات والشبكات والأجهزة الشبكية الموجودة لديها من أي حدث سيبراني:

أ. فصل الشبكات بما يضمن عزل تأثير الأنظمة المعرضة للاختراق السيبراني عن غيرها في حال حدوثه وبما يمكن من تسهيل استعادة الخدمات بكفاءة وفعالية وبحسب تقييم الشركة للمخاطر السيبرانية.

ب. فصل مواقع البنية التحتية (المواقع الرئيسية وموقع التعافي من الكوارث) الخاصة بالأنظمة الحرجة بمنطقة آمنة محدودة الدخول وتوثيق سجلات دخول الزوار لها بالإضافة إلى وجود أنظمة مراقبة لمواقع البنية التحتية.

ج. فصل بيئة التجربة وبيئة التطوير للأنظمة الحرجة عن البيئة الفعلية.

د. تقييم مدى كفاءة وتصميم الربط الشبكي والأجهزة الشبكية بما فيها أجهزة الحماية (مثل Firewalls, IPS (Intrusion Prevention Systems) باستمرار لتلبية احتياجات العمل، والاحتفاظ بتصميم محدث للربط الشبكي في الشركة بالإضافة الى الاحتفاظ بقائمة محدثة للأجهزة المتصلة بشبكة الشركة ومخططات مركز معلومات المواقع الرئيسية وموقع التعافي من الكوارث للشركة بمكان آمن يمكن للمعنيين فقط الوصول إليه.

ه. توفير ضوابط وقائية تتعلق بمنع ربط أجهزة الغير أو المملوكة من قبل الموظفين مع الشبكات والخوادم والأنظمة الموجودة لدى الشركة بما في ذلك أجهزة الحاسوب والأجهزة المحمولة وأي أجهزة أخرى دون الحصول على الموافقات اللازمة، وتطبيق سياسات وقواعد أمن المعلومات والأمن السيبراني عليها في حال الموافقة على الربط، والعمل على توفير ضوابط رقابية للكشف عن أي أجهزة مرتبطة بشبكات وأنظمة الشركة بطرق غير مشروعة.

و. توفير الأجهزة والبرمجيات اللازمة لمراقبة وتحذير وكشف الاختراق الإلكتروني والوصول غير المشروع مثل أجهزة كشف النفاذ (Intrusion Detection Systems) وبرامج الحماية من الفيروسات والتأكد من تحديثها بشكل مستمر وتوظيفها بشكل فعال في عمليات المراقبة وكشف الاختراق.

ز. تحديث أنظمة التشغيل والبرمجيات المثبتة على الأجهزة والخوادم الخاصة بالأنظمة الحرجة لدى الشركة بآخر التحديثات الموصى بها من الشركة الموردة وخصوصا التحديثات المتعلقة بإغلاق الثغرات الأمنية من قبل المزودين لتلك الأنظمة لتفادي مخاطر الأنظمة غير المحدثة، وبما يتناسب مع سياسة "Patch Management Policy" للشركة مع الحرص على تطبيق سياسات وإجراءات التغيير بالسرعة الممكنة، واتخاذ قرارات مبنية على مخاطر تكنولوجيا المعلومات والمخاطر السيبرانية وتوفير ضوابط بديلة فعالة في حال تعذر ذلك بالإضافة الى حذف أي برمجيات أو ملفات مخزنة على خوادم الأنظمة الحرجة ليس لها علاقة بالبرامج المعمول بها لدى الشركة مع ضرورة إجراء الفحوصات اللازمة قبل تنفيذ هذه التحديثات على الأنظمة.

ح. حصر عمليات وصول الموظفين للإنترنت بالمواقع الموثوقة فقط.

ط. فصل عمليات وصول الموظفين للأنظمة الحرجة عن وصولهم للإنترنت وإذا دعت الحاجة إلى غير ذلك يجب أخذ الموافقة اللازمة وتوثيقها.

ي. وضع معايير للإعدادات الأمنية لبيئة تكنولوجيا المعلومات والاتصالات حسب أفضل الممارسات وتوثيق ذلك.

ك. وضع إجراءات ومبادئ توجيهية مصممة لضمان أمان عمليات تطوير البرامج والتطبيقات داخل بيئة الشركة بالإضافة الى إجراءات تقييم أو اختبار أمن البرامج والتطبيقات التي تم تطويرها خارج بيئة الشركة.

ل. مراجعة وتحديث جميع الإجراءات والمبادئ التوجيهية المصممة لضمان أمان ممارسات تطوير البرامج والتطبيقات بشكل دوري ومن قبل أشخاص مؤهلين وبحسب المعايير الدولية بهذا الخصوص.

م. على الشركة تحديد الأنشطة التي قد تشكل خطراً على أنظمتها وبالأخص الأنظمة المالية وتعميمها على الموظفين لمنع الانخراط فيها.

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

المادة (٢٠):

على الشركة استخدام أنظمة حماية من مصادر متنوعة ضمن مستويات مختلفة (Different Security Tiers) على جميع أنظمة الشركة الحرجة.

المادة (٢١):

على الشركة توفير ضوابط الحماية التالية للأنظمة الحرجة والبيانات الحساسة في الشركة الخاصة بالتوثق/التحقق من هوية مستخدمي تلك الأنظمة:

أ. استخدام ضوابط نفاذ قوية (Strong Authentication) وفعالة من خلال فئتين أو أكثر من فئات التوثق (Multi-factor Authentication) وبحسب مستوى المخاطر، مع ضمان فصلها بشكل مناسب بطريقة تقلل من احتمالية معرفة الغير لإحدى فئاتها من خلال الأخرى واستخدام الوسائل والتقنيات اللازمة بما يضمن المساءلة وعدم الإنكار.

ب. في حال الحاجة الماسة للوصول عن بعد (Remote Access)؛ فيجب أن يتم استخدامها بأضيق الحدود، مع ضرورة توفير ضوابط النفاذ من خلال وسائل التوثق/التحقق المتعدد واستخدام تقنيات تشفير ذات اعتمادية عالية والضوابط الأخرى المصاحبة للحد من مخاطر الاختراق غير المصرح به.

ج. تطبيق المعايير الامنية الدولية وأفضل الممارسات العالمية عند اختيار مواصفات كلمات السر.

المادة (٢٢):

على الشركة توفير ضوابط الحماية التالية الخاصة بالمعلومات المتعلقة بأعمالها:

أ. التخلص من أي معلومات حساسة والتي لم تعد ضرورية لتشغيل العمليات الحرجة في الشركة وبما يتوافق والقوانين والأنظمة والتعليمات الصادرة بهذا الخصوص.

ب. ضمان توافرية المعلومات الخاصة بعمل الشركة من خلال أخذ النسخ الاحتياطية لها بشكل دوري وبمواقع آمنة داخل وخارج أماكن عمل الشركة.

ج. الالتزام بسياسة تصنيف البيانات لدى إرسال رسائل ذات محتوى سري وتشفير تلك الرسائل حسب حساسيتها.

د. تفعيل الضوابط اللازمة لحماية سرية المعلومات الحساسة التي يتم الاحتفاظ بها أو تناقلها عبر الشبكات الخارجية بما في ذلك تشفير تلك المعلومات.

ه. في حال تعذر على الشركة القيام بتشفير المعلومات الحساسة المخزنة والمستخدمة في التراسل فعلى الشركة حماية المعلومات الحساسة بطرق بديلة وفعالة على أن يتم مراجعتها ومصادقتها من قبل مدير أمن المعلومات.

المادة (٢٣):

على الشركة توفير ضوابط الحماية التالية والخاصة بضوابط الوصول/النفاذ (Access Controls) الى أنظمتها:

أ. المراقبة المستمرة لنشاط المستخدمين المصرح لهم بالاستخدام والوصول/النفاذ الى أنظمة وشبكات الشركة واكتشاف الوصول لتحديد الاستخدام غير المصرح به أو العبث بالمعلومات الحساسة.

ب. توظيف ضوابط الحماية اللازمة للتحكم بالنفاذ لأنظمة وخوادم وبرمجيات الشركة، ومراجعة صلاحيات الاستخدام والنفاذ الممنوحة على تلك الأنظمة بشكل مستمر، والتأكد من مناسبتها لطبيعة العمل واستخدامها بشكل مشروع وحذف الصلاحيات ورموز التعريف غير المستخدمة وبشكل فوري، وذلك من خلال توفير مصفوفة دليل الصلاحيات (Authority Matrix) للأنظمة معتمدة من الإدارة التنفيذية العليا تبين الصلاحيات التي تمنح على مستوى الوظيفة لكافة الأنظمة، على أن تراعي مصفوفة الصلاحيات المبادئ التالي:

١- الفصل في المهام (Segregation of Duties).

٢- الرقابة الثنائية على العمليات الحساسة (Dual Control).

٣- منح الصلاحيات على قدر الحاجة.

ج. أن يتم مراجعة وتعديل الصلاحيات بشكل دوري وعند حدوث أي تغيير على الأنظمة أو المسميات الوظيفية.

د. الامتثال ومراقبة الامتثال لسياسة كلمة المرور، مع التركيز على ضرورة تغيير كلمات السر الافتراضية المصاحبة للأنظمة والأجهزة الجديدة وبشكل فوري عند استخدامها.

ه. تطبيق قاعدة منح الامتيازات بالحد الأدنى وحسب الحاجة للعمل (Least privileges and on a need to know need to do) وعلى أن يتم مراجعة هذه الامتيازات باستمرار.

و. الأخذ بقاعدة الوصول/النفاذ التي تفيد بأن الوصول/النفاذ بشكل عام ممنوع باستثناء ما هو مسموح.

ز. عدم استخدام الحسابات المشتركة (Shared / Generic Accounts).

المادة (٢٤):

على الشركة توفير ضوابط الحماية التالية والخاصة بمخاطر التهديد السيبراني الداخلي:

أ. مراقبة وتحليل أنشطة الأشخاص غير المصرح لهم بالنفاذ لبيئة تكنولوجيا المعلومات والاتصالات الخاصة بالشركة في حال محاولتهم النفاذ الغير مصرح به الى بيئة تكنولوجيا المعلومات والاتصالات.

ب. توظيف تقنيات التعرف على فقدان البيانات وتقنيات الحماية ضد تغيير أو تسريب البيانات المصنفة (Data Leakage) من شبكة الشركة.

ج. وضع أسس التعيين المناسبة للموظفين الجدد خاصة المرتبطة أعمالهم بالأنظمة الحرجة للتأكد من سجله الوظيفي إن وجد.

د. إجراء مراجعة شاملة للموظفين الجدد وإجراء عمليات مراجعة مماثلة على جميع الموظفين على فترات منتظمة طوال فترة عملهم، بما يتناسب مع صلاحيات النفاذ واستخدام الموظفين للأنظمة الحرجة.

ه. تفعيل الضوابط اللازمة لإدارة المخاطر المتعلقة بالموظفين الذين ينهون عملهم من الشركة أو ينقطعون عن العمل بشكل مؤقت لفترات طويلة خاصة بسبب سلوك مشبوه.

و. أن تتضمن العقود التي يتم توقيعها مع الموظفين بنود قانونية واضحة في حال قيامهم باختراق الأنظمة والنفاذ بشكل غير مصرح به أو توقيع نموذج تعهد بهذا الخصوص وفقا لما يتناسب مع التشريعات النافذة ذات العلاقة وأنظمة الشركة.

ثانياً: ضوابط الحماية الخاصة بالبريد الإلكتروني

المادة (٢٥):

أ. على الشركة تطبيق سياسة لإدارة وتعريف تطبيقات وبروتوكولات ونطاق البريد الإلكتروني الذي يحمل اسم الشركة على الإنترنت متضمنا تطبيق الضوابط والمعايير الآمنة لنظام البريد الالكتروني التالية بالحد الأدنى:

١. السماح لمستخدم البريد الإلكتروني بالنفاذ لحسابه فقط بعد التوثق من هويته ومن خلال اتباع طريقة توثق/تحقق الهوية يصعب على الغير اختراقها وقد يتم استخدام طريقة توثق/تحقق الهوية المتعدد (Multi-factor Authentication) خاصة للمستخدمين الذين تعتبر طبيعة عملهم حساسة وذات أثر ومخاطر على عمليات الشركة وسمعتها.

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

٣. تفعيل خاصية "Reverse DNS Check" للتحقق من مطابقة العنوان الرقمي (IP) لمرسل البريد الإلكتروني (الوارد) مع اسمي النطاق والجهاز الصادر عنهما.

٤. ايقاف خاصية استلام البريد من مصادر تسمح الـ "Open Mail Relay".

٥. تفعيل خاصية "Real-time Blocking List - RBL Check" بحيث يتم من خلالها حجب الرسائل الواردة من مصادر مشبوهة اعتمادا على قوائم بيانات دولية موثوقة ومحدثة بهذا الشأن بالإضافة لقوائم داخلية تبنى وتحدث لتحقيق ذات الغرض.

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

٧. النظر في إمكانية تفعيل خاصية "DNSSEC" ضمن مكونات البيئة التقنية لدى الشركة.

٨. حجب المرفقات والروابط المشبوهة ضمن رسائل البريد الإلكتروني من خلال فحصها بواسطة برمجيات معتمد عليها بهذا الخصوص، وحظر الملفات ذات الامتدادات التنفيذية (Executable Files) وتحديد سقف مسموح لحجم المرفق، مع ضرورة تفعيل سياسة مناسبة على نظام البريد الإلكتروني للتعامل مع تلك الرسائل بناء على درجة مخاطرها.

٩. النظر في إمكانية تعريف سقوف لعدد الاتصالات بخادم البريد الإلكتروني من المصدر الواحد وبما يتناسب ومواصفات خادم البريد الإلكتروني ومتطلبات العمل حيثما لزم.

١٠. توظيف خصائص التوافرية وخطط استمرارية العمل لخدمات البريد الإلكتروني حسب تحليل "Business Impact Analysis-BIA".

١١. الاحتفاظ بسجلات التتبع لأنظمة البريد الإلكتروني العاملة ملاك الشركة لفترة زمنية تحدد ضمن سياسة الاحتفاظ بالبيانات بحيث لا تقل عن ثلاثة أشهر.

ب. وضع سياسة تعنى باستخدام البريد الإلكتروني اعتمادا على أفضل الممارسات الدولية بهذا المجال مع الالتزام بسياسة تصنيف البيانات لدى إرسال رسائل ذات محتوى سري وتشفير تلك الرسائل.

ج. العمل على تطوير برنامج توعوي يحدث باستمرار ويوجه لمستخدمي البريد الإلكتروني متعلق بآلية التعامل مع وأساليب كشف رسائل البريد الإلكتروني الاحتيالية والمشكوك فيها، تتضمن على وجه الخصوص إمكانية التواصل مع مرسل البريد الإلكتروني في حال الشك بهوية المرسل وذلك من خلال وسائل الاتصالات الأخرى.

ثالثا: السجلات

المادة (٢٦):

على الشركة الالتزام بما يلي:

أ. توفير سجلات الأحداث وسجلات التدقيق لبيئة تكنولوجيا المعلومات والاتصالات والأنظمة العاملة عليها.

ب. وجود آلية لإدارة وتحليل ومراقبة سجلات الأحداث والتدقيق بشكل مستمر حسب تصنيف أهمية الأنظمة العاملة على بيئة تكنولوجيا المعلومات والاتصالات وتوثيق ذلك.

ج. تحديد أنواع السجلات التي يتعين الاحتفاظ بها وفترات الاحتفاظ وصلاحيات الاطلاع عليها.

د. توفير الحماية اللازمة لسجلات الأحداث والتدقيق لضمان توافريتها وتكامليتها.

ه. توفير آلية مناسبة للتحقق من مراجعة سجلات الأحداث لبيئة تكنولوجيا المعلومات والاتصالات من قبل جهة مستقلة داخل أو خارج الشركة وبما لا يتعارض مع أحكام التشريعات النافذة.

الفصل الخامس

الكشف عن الحوادث السيبرانية

المادة (٢٧):

على الشركة الكشف عن مواطن الضعف في أي من مكونات بيئة تكنولوجيا المعلومات والاتصالات في الشركة وينبغي أن تتصدى قدرات الكشف أيضا لسوء استخدام الغير لتلك الأنظمة، والتهديدات الداخلية المحتملة، وغير ذلك من أنشطة التهديد المتقدم (Advanced Persistent Threats).

المادة (٢٨):

على الشركة وضع ضوابط متعددة المراحل لعملية الكشف بحيث تغطي الأشخاص والعمليات والتكنولوجيا، مع استخدام كل مرحلة كشبكة أمان للمراحل السابقة، وينبغي على الشركة اتخاذ نهجاً يمكنها من تأخير أو تعطيل أو ايقاف القدرة على التقدم في مراحل تسلسل الهجوم السيبراني.

المادة (٢٩):

يجب أن تكون قدرات الكشف لدى الشركة قادرة على دعم عملية الاستجابة للحوادث وجمع المعلومات والأدلة اللازمة لعمليات التحقيق (Forensic IT Audit) كلما اقتضت الحاجة اليها.

المادة (٣٠):

على الشركة توفير الآليات والأنظمة اللازمة لعمل مراقبة مستمرة وايجاد ترابطات سببية(Correlations) للكشف عن الأنشطة والأحداث غير الاعتيادية التي قد تؤثر على أعمال الشركة أو تتسبب في خسارة مالية لها.

المادة (٣١):

يجب تنفيذ تدابير للكشف عن مواطن التسريبات المحتملة للمعلومات والشيفرات الخبيثة والتهديدات الأمنية ونقاط الضعف والثغرات الأمنية وضرورة متابعة آخر التحديثات الأمنية والتحقق وتطبيق هذه التحديثات أول بأول.

الفصل السادس

الاستجابة للحوادث السيبرانية الطارئة والتعافي منها

المادة (٣٢):

على الشركة توفير ضوابط الاستجابة التالية للحوادث السيبرانية الطارئة:

أ. وضع خطة للاستجابة للحوادث السيبرانية بحيث تكون مصممة للاستجابة الفورية والتعافي من أي حدث طارئ يتعلق بالأمن السيبراني للشركة.

ب. يجب أن تتضمن خطة الاستجابة للحوادث السيبرانية ما يلي بالحد الأدنى:

١. تعريف الأدوار والمسؤوليات لاتخاذ القرار بشكل واضح.

٢. العمليات الداخلية المعنية بالاستجابة للحوادث السيبرانية.

٣. أهداف خطة الاستجابة للحوادث السيبرانية.

٤. الاتصالات الخارجية والداخلية وتبادل المعلومات مع الأطراف المعنية.
٥. تحديد الاحتياجات اللازمة لمعالجة أي مواطن ضعف في أي من مكونات بيئة تكنولوجيا المعلومات والاتصالات وما يرتبط بها من ضوابط.
٦. مخاطر الحوادث السيبرانية.
٧. التوثيق والإبلاغ بشأن حوادث الأمن السيبراني وأنشطة الاستجابة للحوادث ذات الصلة.
٨. تقييم ومراجعة خطة الاستجابة للحوادث السيبرانية حسب الحاجة في أعقاب الحدث السيبراني.
٩. أماكن حفظ الخطة (Hard copy, Soft copy) والإجراءات الخاصة بها.

ج. عمل فحص لخطة الاستجابة للحوادث السيبرانية وتحديثها باستمرار بالاستناد إلى المعلومات الحالية عن التهديدات السيبرانية والدروس المستفادة من الأحداث السابقة التي تعرضت لها الشركة أو أي شركة أخرى داخل أو خارج المملكة.

د. التعاون والتنسيق مع الأطراف المعنية للمساعدة في الاستجابة للحوادث السيبرانية بغرض احتواء تلك المشاكل والأحداث غير المتوقعة والتقليل من آثارها خاصة إذا كانت أنظمة تلك الجهات مرتبطة بأنظمة الشركة والتعاون مع تلك الجهات عند وضع خطة الاستجابة للحوادث السيبرانية.

ه. إجراء تحقيق وتقييم شامل عند الكشف عن هجوم سيبراني ناجح أو محاولة لهجوم سيبراني، لتحديد طبيعته ومداه والأضرار التي لحقت بها، كما يجب أن تتخذ الشركة إجراءات فورية لاحتواء الحدث السيبراني لمنع المزيد من الأضرار ولاستعادة عملياتها استناداً إلى خطة الاستجابة للحوادث السيبرانية.

و. تصميم واختبار جميع أنظمتها وعملياتها بحيث يكون الزمن المستهدف لتعافي العمليات الحرجة فيها من الكوارث (RTO) متوافقاً مع تعليمات وتعاميم البنك المركزي التي تصدر بهذا الخصوص. وينبغي أيضا وضع سيناريوهات الاستجابة في حال فشل القدرة على الاستئناف خلال هذه الفترة.

ز. تصميم واختبار أنظمتها وعملياتها لتمكين استعادة البيانات الحساسة بعد حدوث الاختراق السيبراني، وينبغي وضع ضوابط صارمة لكشف وحماية تلك البيانات.

ح. يجب أن يتم الاتفاق مع الاطراف المعنية على نقاط الاسترجاع المستهدفة (RPO - Recovery Point Objective) ومقدار زمن التعافي المستهدف (RTO - Recovery Time Objective) لكل خدمة تكنولوجيا المعلومات وتوثيقها واستخدامها كمتطلبات لتصميم الخدمة وخطط استمرارية تكنولوجيا المعلومات.

ط. إجراءات تمكنها من تحديد الجهة المسؤولة عن معالجة مواطن الضعف التي تبينت نتيجة تحقيق في حدث سيبراني طارئ لمنع المزيد من الأضرار واحتواء الحدث وإصلاح الاضرار والحيلولة دون تكرار الحدث مستقبلا.

المادة (٣٣):

على الشركة وضع إجراءات للتعافي من الحوادث السيبرانية وعلى أن تتضمن هذه الإجراءات ما يلي:

أ. القضاء على آثار الحوادث الضارة.

ب. التأكد من عودة الأنظمة والبيانات لوضعها الطبيعي.

ج. تحديد وتخفيف ومعالجة نقاط الضعف التي تم استغلالها لمنع وقوع حوادث مماثلة.

د. التواصل بشكل مناسب مع جميع الجهات الداخلية والخارجية ذات العلاقة مع الشركة فيما يخص التعافي من الحدث السيبراني.

الفصل السابع

الاختبارات

المادة (٣٤):

على الشركة العمل على اختبار مكونات بيئة تكنولوجيا المعلومات والاتصالات بعد وقوع الحدث السيبراني وبالتنسيق مع الأطراف المعنية.

المادة (٣٥):

على الشركة الالتزام بما يلي:

أ. تنفيذ اختبارات الاختراق للأنظمة الحرجة على الاقل مرة واحدة سنوياً أو بعد إجراء تعديل جذري على نظام/أنظمة الشركة مع مراعاة ما يلي:

١. أن يتم بناء نطاق الفحص استنادا إلى حساسية الانظمة وما يرتبط بها من أنظمة مساندة وداعمة.

٢. أن يتم تنفيذ الاختبارات على مستوى التطبيقات والشبكات الداخلية والخارجية في الشركة.

٣. إمكانية تنفيذ الفحوصات من قبل طرف ثالث على ألا يتم إسنادها لنفس الطرف الثالث أكثر من سنتين على التوالي.

ب. تنفيذ تقييم نقاط الضعف والثغرات الأمنية للأنظمة الحرجة والأنظمة المساندة والداعمة لها والشبكات الداخلية والخارجية بشكل دوري حسب تعليمات وتعاميم البنك المركزي التي تصدر بهذا الخصوص واتخاذ الإجراءات الكفيلة بمعالجة الثغرات المكتشفة.

ج. القيام بالمراقبة على أنظمة الشركة بشكل مستمر وفعال للكشف عن أية خلل في أي من مكونات بيئة تكنولوجيا المعلومات والاتصالات التي قد تشير إلى وجود ثغرات جديدة.

المادة (٣٦):

على الشركة وضع برنامج اختبار شامل للتحقق من فاعلية سياسة وبرنامج الأمن السيبراني على أساس منتظم ومتكرر وعلى أن يتم إطلاع المجلس والإدارة التنفيذية العليا على النحو المناسب بنتائج هذا الاختبار.

الفصل الثامن

الإسناد الخارجي

المادة (٣٧):

على الشركة تقييم الحاجة لإسناد العمليات الحرجة للطرف الثالث بالاعتماد على تقييم شامل للمخاطر السيبرانية مع مراعاة أحكام التشريعات النافذة بهذا الخصوص.

المادة (٣٨):

في حال إسناد جزء من عمليات الشركة إلى طرف ثالث يجب الالتزام بما يلي:

أ. على الشركة التأكد من توفير ضوابط الحماية اللازمة للسيطرة على جميع المخاطر السيبرانية المتعلقة بالأنظمة والبيانات الحساسة للشركة وعملاؤها والمستضافة لدى الطرف الثالث وعمل فحوصات دورية ومنتظمة لتقييم تلك الضوابط من قبل جهات مستقلة والحصول على تطمينات موثقة

بحسب المعايير الدولية المقبولة بهذا الخصوص وبما يتفق وهذه التعليمات و/أو الإشراف والرقابة المستمرة على الخدمات المقدمة من قبل الطرف الثالث.

ب. على المجلس والإدارة التنفيذية العليا للشركة إنشاء نظام وآلية لإدارة الخدمات المقدمة من الطرف الثالث بغرض دعم عملية تقديم خدمات الشركة وتضمين ذلك بسياسة الإسناد الخارجي لديها.

ج. على الشركة توقيع اتفاقية عدم الافصاح (Non-disclosure Agreement) بينها وبين الطرف الثالث.

د. التشريعات النافذة وعلى وجه الخصوص تلك المتعلقة بالسرية المصرفية وسرية بيانات العملاء وحمايتها.

ه. أية شروط أو متطلبات يحددها البنك المركزي بهذا الخصوص.

المادة (٣٩):

يجب على الشركة تضمين البنود التالية بسياسة الإسناد الخارجي فيما يخص المخاطر السيبرانية مع مراعاة أحكام التشريعات النافذة:

أ. إجراءات ضبط وصول/ نفاذ الطرف الثالث عن بعد بما في ذلك ضرورة النفاذ عبر وسائل توثق / تحقق الهوية متعدد الفئات (Multi-factor Authentication) للحد من وصوله إلى الأنظمة ذات الصلة والمعلومات الحساسة.

ب. الضوابط الواجب استخدامها من قبل الطرف الثالث المتعلقة بالتشفير لحماية المعلومات الحساسة الخاصة بالشركة أثناء تناقلها أو تخزينها من قبله.

ج. الإشعار الواجب تقديمه للشركة في حالة وقوع حادث للأمن السيبراني يؤثر بشكل مباشر أو غير مباشر على أنظمة الشركة أو معلوماتها الحساسة التي يحتفظ بها الطرف الثالث.

المادة (٤٠):

أن تتضمن العقود المبرمة بين الشركة والطرف الثالث متطلبات هذه التعليمات وعلى وجه الخصوص ما يلي:

أ. على الشركة عند توقيع اتفاقيات إسناد (Outsourcing) مع الطرف الثالث التأكد من التزام الطرف الثالث بتطبيق بنود هذه التعليمات بالقدر الذي يتناسب مع أهمية وطبيعة عمليات الشركة والخدمات والبرامج والبنية التحتية المقدمة للشركة قبل وأثناء فترة التعاقد، وبما لا يعفي المجلس والإدارة

التنفيذية العليا من المسؤولية النهائية لتحقيق متطلبات التعليمات، على أن يتم توفيق أوضاع الشركات المتعاقد معها حالياً بتاريخ نفاذ هذه التعليمات أو خلال فترة التعاقد أيهما أسبق.

ب. حق التدقيق (Audit Right) للشركة لتقييم المخاطر السيبرانية الناشئة عن ممارسات الطرف الثالث والتي تؤثر على الشركة، وذلك من قبل طرف آخر محايد وموثوق يتضمن تقديم رسائل تطمين تقدم رأيه بخصوص فحص الضوابط ومدى كفايتها، وذلك بحسب المعايير الدولية المتبعة بهذا الخصوص.

ج. الحد الأدنى من ممارسات الأمن السيبراني المطلوب تلبيتها من قبل الطرف الثالث بما في ذلك الإجراءات الأمنية اللازمة فيما يتعلق بمستوى الخدمة (Service Level).

د. التزام الطرف الثالث بسياسة الأمن السيبراني لدى الشركة.

ه. قيام الطرف الثالث بتزويد الشركة بتقارير فورية حول أي محاولة اختراق سيبراني أو أحداث طارئة قد تتعرض لها بيانات وخدمات الشركة لديهم.

الفصل التاسع

أولاً :التدريب وزيادة الوعي

المادة (٤١):

على الشركة توعية وتدريب منتظم لجميع الموظفين في الشركة على جميع مستوياتهم بهدف تعزيز الثقافة بأهمية الأمن السيبراني داخلها على أن يتم تحديثه ليعكس المخاطر التي تحددها الشركة في تقييمها للمخاطر وأن يتضمن بالحد الأدنى ما يلي:

أ. التوعية بالأمن السيبراني وأنواع التهديدات السيبرانية.

ب. كيفية الكشف عن المخاطر السيبرانية ومعالجتها.

ج. كيفية الإبلاغ عن أي نشاط وحوادث غير عادية.

د. خطط الطوارئ وطرق الاستجابة للحالات الطارئة وحالات حدوث الاختلاس والتزوير والاختراق السيبراني.

ه. آلية تطبيق التعليمات والتوعية بالمهام والمسؤوليات وتبعات المساءلة في حالات عدم الامتثال.

و. أفضل الممارسات الدولية فيما يخص كيفية استخدام الأنظمة والشبكات للسيطرة على وإدارة مخاطر الاختراق السيبراني وتزويدهم واطلاعهم على سياسات أمن المعلومات وسياسة الامن السيبراني وتوقيعهم للإقرار بفهمها والالتزام بمحتواها.

المادة (٤٢):

على الشركة توفير تدريب خاص ومكثف للعاملين في مجال أمن المعلومات والأمن السيبراني والموظفين الذين لديهم صلاحيات الوصول إلى الأنظمة الحرجة والمعلومات الحساسة كل حسب اختصاصه.

المادة (٤٣):

على الشركة توفير برامج التوعية لأعضاء المجلس والإدارة التنفيذية العليا حول مخاطر تكنولوجيا المعلومات والأمن السيبراني وأفضل الممارسات الدولية في هذا الصدد على الأقل مرة واحدة في السنة.

المادة (٤٤):

أ. على الشركة توعية عملائها لتفادي مخاطر الاختراق السيبراني وضرورة اتباع الضوابط المرعية للحفاظ على بياناتهم المالية والمصرفية وأخذ الحيطة والحذر، ومنها:

١. تعلم وفهم سياسة الأمن والخصوصية لمواقع الويب والتطبيقات الخاصة بالشركة.
٢. حماية الهوية الشخصية وبيانات التعريف بالهوية من خلال استخدام معرفات مختلفة لتطبيقات الويب المختلفة، والتقليل من مشاركة المعلومات الشخصية على مواقع الويب أو التطبيقات التي تطلب هذه المعلومات.
٣. إبلاغ الأطراف المعنية عن الأحداث المشبوهة التي تواجههم.
٤. عدم مشاركة المعلومات المصرفية على مواقع الويب أو التطبيقات الغير موثوقة التي تطلب هذه المعلومات.
٥. ضرورة توعية العملاء بشكل مستمر عن كيفية التأكد من هوية الشركة على الإنترنت وعبر تطبيقات الهاتف أثناء استخدام خدماتها.

ب. على الشركة توضيح الطرق المعتمدة والآمنة للتبليغ عن أي حادث اختراق سيبراني أو سرقة للبيانات للجهات ذات العلاقة.

ثانياً: تبادل معلومات الحوادث السيبرانية

المادة (٤٥):

يجب على الشركة تبادل معلومات الحوادث السيبرانية وفي الوقت المناسب مع الجهات المعنية والجهات الموثوقة والمتخصصة بمواضيع المخاطر السيبرانية السائدة حالياً والتهديدات ونقاط الضعف والحوادث والاستجابات، لتعزيز الضوابط المفعلة في الشركة والحد من الأضرار وزيادة الوعي وبما يتوافق مع أي تعاميم أو تعليمات صادرة عن البنك المركزي بالخصوص.

المادة (٤٦):

على الشركة الاعتماد على بيانات الحوادث السيبرانية الداخلية والخارجية في تقييم المخاطر السيبرانية في الفصل الثالث أعلاه.

الفصل العاشر

أحكام عامة

المادة (٤٧):

على الشركة إيقاف العمل بالخدمات والأنظمة والأجهزة غير المستخدمة بسبب عدم الحاجة لها بشكل نهائي وفق سياسة الشركة المعتمدة بهذا الخصوص وبطريقة تضمن عدم تأثر الخدمات أو الأنظمة أو العمليات الأخرى.

المادة (٤٨):

على الشركة اعتماد وتفعيل سياسة شاملة لإدارة التغيير تأخذ بعين الاعتبار المخاطر السيبرانية قبل وأثناء وبعد التغييروعمل تقييم للمخاطر السيبرانية وأخذ الضوابط التي تنتج عن عملية تقييم المخاطر بالاعتبار عند تطبيق التغيير.

المادة (٤٩):

أ. على الشركة إخطار البنك المركزي في حال اكتشاف تعرضها لأي حدث سيبراني او أي محاولة للهجوم السيبراني تتسم بدرجة خطورة عالية على أنظمتها أو شبكاتها في موعد أقصاه ٧٢ ساعة من لحظة اكتشاف الحدث السيبراني وبحسب الآلية التي سيعتمدها البنك المركزي وإعلام الأجهزة الأمنية المختصة عن أي حالة اختلاس أو تزوير أو سرقة أو احتيال ناتجة عن الحدث السيبراني فور اكتشافه وبحسب القوانين والتعليمات ذات العلاقة.

ب. تزويد البنك المركزي بتفاصيل الأحداث السيبرانية وآثارها وإجراءات الاستجابة والإجراءات الوقائية التي تم اتخاذها بشكل دوري وبحسب الآلية التي سيعتمدها.

المادة (٥٠):

على الشركة الإفصاح عن سياسة الأمن السيبراني الخاصة بها مع أصحاب المصالح.

المادة (٥١):

على الشركة إعلام العميل عن أية تحديثات بالإجراءات الأمنية الواجب اتباعها من قبله وحسب الآلية المتفق عليها مع العميل.

المادة (٥٢):

شمول برامج المدقق الداخلي والمدقق الخارجي على آليات تضمن الرقابة والمتابعة المستمرة لبنود التعليمات أعلاه.

المادة (٥٣):

على الشركة التأكد من أن كافة الأنظمة والتجهيزات المستعلمة في الشركة متوافقة مع المعايير العالمية والمحلية.

المادة (٥٤):

للبنك المركزي الحق بطلب أية تقارير أو بيانات أو سجلات يراها مناسبة.

المحافظ
د. زياد فريز