الرقـم : ٢٦/٢/ ٦٤٦٦
التاريـخ : ١٦ شعبان، ١٤٣٩
الموافق : ٠٢ أيار، ٢٠١٨

تعليمات المتطلبات الفنية والتقنية لشركات خدمات الدفع والتحويل الإلكتروني للأموال رقم (٨/٢٠١٨)

صادرة استناداً لأحكام الفقرتين (د) و (هـ) من المادة (٥) وأحكام الفقرة (هـ) من المادة (٦) وأحكام الفقرة (أ) من المادة (٤٨) والمادة (٥٥) من نظام الدفع والتحويل الإلكتروني للأموال رقم (١١١) لسنة ٢٠١٧

المادة (١):

تسمى هذه التعليمات "تعليمات المتطلبات الفنية والتقنية لشركات خدمات الدفع والتحويل الإلكتروني للأموال" ويعمل بها من تاريخ إقرارها.

المادة (٢):

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

بيئة تكنولوجيا المعلومات والاتصالات	:	مجموعة التجهيزات الحاسوبية الخاصة بالشبكات الداخلية والشبكات الخارجية والخوادم الرئيسية والبرمجيات العاملة عليها وجميع الأجهزة المساندة لها في الموقع الرئيسي والبديل للشركة.
أصول المعلومات	:	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.
البيانات الحساسة	:	البيانات السرية و/أو السرية للغاية التي تعتبر غاية في الأهمية للشركة والتي تعرض أمنها وخصوصيتها والمتعاملين معها للخطر الشديد.

ب) تعتمد التعاريف الواردة في نظام الدفع والتحويل الإلكتروني للأموال النافذ المفعول أينما ورد النص عليها في هذه التعليمات ما لم تدل القرينة على غير ذلك.

نطاق التطبيق

المادة (٣):

تطبق أحكام هذه التعليمات على جميع الجهات التالية:

أ) الشركات العاملة في المملكة المرخص لها من البنك المركزي بما في ذلك فروع الشركات الأجنبية مزاولة أياً من أنشطة خدمات الدفع أو إدارة وتشغيل أنظمة الدفع الإلكتروني.

ب) البنوك العاملة في المملكة وشركات الصرافة التي تزاول أي من أنشطة خدمات الدفع أو إدارة وتشغيل أنظمة الدفع الإلكتروني وبما لا يتعارض مع التشريعات الناظمة لها.

المادة (٤):

يراعى عند تطبيق أحكام هذه التعليمات كل ما ورد في تعليمات التكيف مع المخاطر السيبرانية وتقرأ معها بشكل متكامل.

متطلبات بيئة تكنولوجيا المعلومات والاتصالات

المادة (٥):

أ) على الشركة توفير بيئة تكنولوجيا المعلومات والاتصالات اللازمة لتقديم خدمات الدفع أو إدارة وتشغيل أنظمة الدفع الإلكتروني وتوفير الدعم والصيانة اللازمة لها.

ب) على الشركة ضبط إعدادات أنظمة التشغيل وقواعد البيانات وأجهزة الشبكة وجميع مكونات بيئة تكنولوجيا المعلومات والاتصالات بما في ذلك الإعدادات الأمنية وتوثيق ذلك بما يضمن عملها بتوافرية وتكاملية وموثوقية.

ج) على الشركة مراجعة مكونات بيئة تكنولوجيا المعلومات والاتصالات بشكل دوري بما في ذلك أساليب الحماية والإجراءات المتبعة في تنفيذ العمليات للتأكد من سلامتها وتحسين أدائها وتحديثها باستمرار وتوثيق ذلك.

المادة (٦):

على الشركة وقبل الانتقال إلى بيئة العمل الفعلية الالتزام بما يلي:

أ) فحص مكونات بيئة تكنولوجيا المعلومات والاتصالات للتأكد من مدى كفايتها واعتماديتها وموثوقيتها وبما يؤدي الغرض المراد منها وتوثيق ذلك.

ب) تغيير كلمات السر المصاحبة لكافة مكونات بيئة تكنولوجيا المعلومات والاتصالات الجديدة (Default Passwords) بشكل فوري عند بدء استخدامها.

ج) التوثيق الشامل لكافة مكونات بيئة تكنولوجيا المعلومات والاتصالات ومراجعته باستمرار وتوفير الحماية المناسبة له.

متطلبات حماية بيئة تكنولوجيا المعلومات والاتصالات

المادة (٧):

على الشركة الالتزام بما يلي:

أ) استخدام قنوات اتصال آمنة ذات سعات اتصال مناسبة (Bandwidth) لاستيعاب حجم البيانات المتراسلة.

ب) استخدام قنوات اتصال ذات سرعات عالية لدعم متطلبات التحديث الآني (Real time update).

ج) توظيف تقنيات الفصل الافتراضي و/أو المادي للشبكات ما أمكن ذلك.

د) استخدام أجهزة الحماية الشبكية اللازمة لبيئة تكنولوجيا المعلومات والاتصالات، على سبيل المثال لا الحصر (Firewalls, Intrusion Detection and Prevention Systems).

هـ) وضع ضوابط ومعايير للربط الشبكي عن بعد (Remote Access) بالشبكات الخاصة بالشركة.

المادة (٨):

أ) على الشركة تحديث أنظمة التشغيل والبرمجيات المثبتة على أجهزة وخوادم بيئة تكنولوجيا المعلومات والاتصالات بآخر التحديثات الموصى بها من الشركة الموردة مع ضرورة إجراء الفحوصات اللازمة قبل تنفيذ هذه التحديثات وتوفير ضوابط بديلة فعالة في حال تعذر ذلك.

ب) على الشركة حذف أي برمجيات أو ملفات مخزنة على الأجهزة والخوادم ليست لها علاقة بالأنظمة المعمول بها لدى الشركة.

المادة (٩):

على الشركة تثبيت أنظمة الحماية من الفيروسات على الخوادم وأجهزة العاملين في الشركة والعمل على تحديثها باستمرار وتحديد جدولة المسح التلقائي لمكافحة الفيروسات على الخوادم وأجهزة المستخدمين بشكل دوري.

فصل بيئات العمل

المادة (١٠):

أ) على الشركة فصل بيئة العمل الفعلية للأنظمة العاملة لدى الشركة عن البيئات الأخرى مع مراعاة ما يلي:

١) تحديد وتوثيق قواعد نقل البرمجيات من بيئة التجربة والتطوير (إن وجدت) إلى بيئة العمل الفعلية.

٢) أن تحاكي بيئة التجربة بيئة العمل الفعلية بأكبر قدر ممكن.

ب) على الشركة عدم السماح لكوادر البرمجة والتطوير بالعمل على بيئة العمل الفعلية إلا في الحالات الاستثنائية على أن يتم منحهم أسماء وكلمات سر مؤقتة يتم تغييرها بعد انتهاء الغرض الذي منحت من أجله وأن يتم توثيق ومراقبة جميع هذه الخطوات.

إدارة الوصول

المادة (١١):

أ) على الشركة وضع الضوابط المناسبة للتحكم بالنفاذ غير المادي (Logical Access) إلى بيئة تكنولوجيا المعلومات والاتصالات الخاصة بها وفحصها بشكل مستمر على أن تشمل بالحد الأدنى ما يلي:

١) استخدام ضوابط نفاذ قوية وفعالة وبحسب مستوى المخاطر واستخدام الوسائل والتقنيات اللازمة بما يضمن المساءلة وعدم الانكار.

٢) الإجراءات الرسمية لعمليات منح صلاحيات الوصول المتعدد للمستخدمين الجدد وعمليات إيقاف وحذف هذه الصلاحيات لمختلف أنظمة بيئة تكنولوجيا المعلومات والاتصالات.

٣) منح الصلاحيات على قدر الحاجة للاستخدام فقط ولكل استخدام على حدا على أن يتم مراجعتها بشكل دوري مع مراعاة الصلاحيات ذات الحساسية والخصوصية الأعلى.

٤) حصر عدد رموز التعريف المستخدمة للوصول والاستخدام لأنظمة الشركة المختلفة من ذوي الامتيازات العليا.

ب) على الشركة وضع الضوابط المناسبة للتحكم بالنفاذ المادي (Physical Access) إلى بيئة تكنولوجيا المعلومات والاتصالات الخاصة بها على أن تشمل بالحد الأدنى ما يلي:

١) تعريف الأشخاص المصرح لهم بالدخول إلى مرافق بيئة تكنولوجيا المعلومات والاتصالات وتحديد الشروط الأمنية الواجب مراعاتها عند الدخول لهذه المرافق وتوثيق ذلك ضمن قوائم محددة ومراجعتها باستمرار.

٢) منح موظفي الدعم الفني من الجهات الخارجية صلاحيات نفاذ محدودة ومؤقتة لمرافق بيئة تكنولوجيا المعلومات والاتصالات وحسب الحاجة فقط على أن يتم مراقبة هذه الصلاحيات ومراجعتها باستمرار.

ج) على الشركة وضع الضوابط المناسبة للوصول إلى الشبكات من خلال صلاحيات وصول محددة لكل مستخدم على حدا تتناسب مع أهمية وحساسية التطبيقات والبرامج الموصولة بها أو زيادة خطورة المواقع التي يشغلها مستخدمو الأنظمة مع مراعاة ما يلي:

١) حصر وصول المستخدمين من خارج الشركة من خلال بوابات آمنة وإلى برامج محددة.

٢) التوثق/ التحقق من هوية المستخدم على الشبكات الخارجية.

٣) مخاطر العمليات والخدمات التي يتم تقديمها من خلال الشبكات.

السجلات

المادة (١٢):

أ) على الشركة الاحتفاظ بالبيانات التاريخية لكافة المعاملات التي تمت بواسطة أنظمتها الإلكترونية وفق المتطلبات القانونية النافذة مع توافر امكانية استرجاعها عند الطلب على أن تتوفر في هذه البيانات ما يدل على منشأ السجل وتاريخ ووقت حفظ هذه البيانات.

ب) على الشركة الاحتفاظ بكافة سجلات التدقيق وسجلات الأحداث التشغيلية والأمنية لمكونات بيئة تكنولوجيا المعلومات والاتصالات لمدة لا تقل عن خمس سنوات مع مراعاة ما يلي:

١) توفير آلية لإدارة وتحليل ومراقبة السجلات بشكل مستمر.

٢) توفير الحماية اللازمة للسجلات لضمان توافريتها وتكامليتها وحماية السجلات من عمليات التغيير والضياع والتدمير والتخريب والتزوير من قبل جميع المستخدمين بكافة صلاحياتهم وخاصة مديري الأنظمة (System Administrators).

إدارة البيانات

المادة (١٣):

على الشركة وضع وتطوير التقنيات اللازمة لإدارة البيانات مع مراعاة الحد الأدنى مما يلي:

أ) استخدام قواعد بيانات ذات سعات تخزينية مناسبة ومراجعة تلك السعات للنظر في مدى كفايتها وزيادة السعات التخزينية كلما تطلب الأمر ذلك.

ب) القدرة على تخزين واسترجاع البيانات بسرعة وكفاءة وضمان توافرية وتكاملية وموثوقية هذه البيانات.

ج) وضع ضوابط الحماية المناسبة لحماية قواعد البيانات من الوصول غير المصرح به.

د) التأكد من تشفير جميع البيانات الحساسة عند تناقلها وتخزينها.

هـ) تحديد آلية حفظ البيانات وأماكن تخزينها ومعالجتها وتناقلها بما يتناسب مع حساسية تلك البيانات.

و) وضع إجراءات محكمة لإتلاف البيانات الحساسة بما يشمل وسائط التخزين المستخدمة وذلك عندما تنتفي الحاجة من وجودها مع مراعاة الفترة القانونية للاحتفاظ بتلك البيانات.

ز) وضع الإجراءات المناسبة لمعالجة أخطاء ومشاكل إدارة البيانات ومراجعة مدى كفاية وكفاءة هذه الإجراءات بشكل مستمر.

المادة (١٤):

على الشركة إخضاع البيانات (سواء المخزنة أو المتناقلة) والنسخ الاحتياطية من هذه البيانات وخاصة الحساسة منها إلى ضوابط التشفير المناسبة مع الالتزام بالحد الأدنى مما يلي:

أ) توظيف تقنيات تشفير ذات اعتمادية عالية لضمان سرية البيانات الحساسة سواء كانت على مستوى البيانات الشخصية أو بيانات الحركات المالية والبيانات الخاصة بالعملاء وتلك التي يتم حفظها عند طرف ثالث بالشكل الذي يضمن عدم إساءة استخدامها.

ب) وضع وتوثيق سياسات وإجراءات مفصلة ومراجعتها بشكل دوري لتنظيم إدارة مفاتيح التشفير من حيث انشائها وتخزينها واستخدامها وايقافها وانتهاء صلاحيتها وتجديدها وارشفتها ومراجعتها ومراقبتها.

ج) توظيف تجهيزات أمنية كافية وكفؤة مثل الأجهزة الخاصة بتخزين مفاتيح التشفير (HSM) وغيرها من الأدوات والأنظمة المستخدمة لتشفير البيانات الحساسة للشركة في مرحلة تناقلها وضمان إنشاء وإدارة المفاتيح السرية المستخدمة في التشفير بشكل آمن.

النسخ الاحتياطي والاسترجاع

المادة (١٥):

على الشركة وضع اجراءات وآليات للنسخ الاحتياطي لضمان توافرية بيانات الشركة على أن تشمل بالحد الأدنى ما يلي:

أ) أخذ نسخ احتياطية بشكل دوري لقواعد البيانات والمعلومات والبيانات كافة وإعدادات بيئة تكنولوجيا المعلومات والاتصالات والاحتفاظ بها في وسائط تخزين خاصة لحفظ النسخ بشكل منفصل عن مصدر هذه النسخ.

ب) توفير مستوى مناسب من الحماية المادية وغير المادية للنسخ الاحتياطية.

ج) فحص استرجاع النسخ الاحتياطية بما يتفق مع إجراءات النسخ الاحتياطي المعتمدة لدى الشركة وتوثيق إجراءات ونتائج الاسترجاع.

د) اختبار مدى كفاية وفاعلية وسائط التخزين وتلبيتها لمتطلبات الشركة في دعم عمليات الاسترجاع.

المادة (١٦):

على الشركة وضع الإجراءات اللازمة لضمان عدم إجراء أي تعديل غير مصرح به على نسخ البرامج المصدرية (Source Code) وحفظها في أماكن آمنة ومخصصة لها ووفق مستويات حماية مناسبة.

التوافرية العالية

المادة (١٧):

على الشركة التأكد من وجود الضوابط الكافية لضمان التوافرية العالية لبيئة تكنولوجيا المعلومات والاتصالات وعلى وجه الخصوص الأنظمة الحرجة وذلك بمراعاة السعة الاستيعابية الكافية والأداء الموثوق به، ووقت الاستجابة السريع، وقابلية التوسع، والقدرة على استعادة العمل بسرعة.

المادة (١٨):

على الشركة التأكد من توافرية مكونات بيئة تكنولوجيا المعلومات والاتصالات لتقليل نقاط الفشل الوحيدة التي يمكن أن تؤدي إلى تعطل العمل وأن تحافظ على أجهزة وبرمجيات وشبكات احتياطية اللازمة لاستعادة العمل بسرعة.

المادة (١٩):

على الشركة العمل على تحقيق مبدأ تعدد قنوات الاتصال ما بين الأطراف المختلفة وأن تكون القنوات المختلفة مقدمة من قبل مزودي خدمة اتصال مختلفين لتجنب مخاطر التعامل مع مزود خدمة واحد.

استمرارية العمل

المادة (٢٠):

على الشركة أن تنشئ موقعاً بديلاً يكون مفصولاً جغرافياً عن الموقع الرئيسي لضمان استمرارية أعمال الشركة في حالة حدوث انقطاع في الموقع الرئيسي.

المادة (٢١):

على الشركة وضع خطة استمرارية العمل والتعافي من الكوارث بما في ذلك آليات بناء وفحص وتشغيل وتحديث تلك الخطة ومراجعة وتقييم نتائج الفحوصات لضمان توافرية عمليات الشركة بشكل سنوي على الأقل وكلما دعت الحاجة لذلك مع الأخذ بالاعتبار ما يلي:

أ) شروط تفعيل خطة استمرارية العمل والتعافي من الكوارث بما في ذلك إجراءات تنفيذ هذه الخطة قبل اعتمادها.

ب) إجراءات خطة استمرارية العمل والتعافي من الكوارث التي تبين الأمور الواجب اتباعها والقيام بها عند الحاجة إلى تفعيل الخطة.

ج) إجراءات تصف الخطوات التي يتم من خلالها تشغيل بيئة تكنولوجيا المعلومات والاتصالات في المواقع البديلة.

د) إجراءات التعافي التي يتم اتباعها لاستعادة العمل إلى وضعه الطبيعي.

هـ) جدول زمني يبين مكان وزمان فحص خطة استمرارية العمل والتعافي من الكوارث وإجراءات الفحص.

و) النشاطات التدريبية والتوعوية المصممة للتأكد من الفهم الصحيح لإجراءات خطة استمرارية العمل والتعافي من الكوارث.

ز) مهام ومسؤوليات الأفراد تجاه تنفيذ كل جزء من أجزاء خطة استمرارية العمل والتعافي من الكوارث.

ح) تحديد إجراءات إعادة تشغيل عمليات الشركة ومتطلبات استعادة النظام، وتحديد زمن التعافي المستهدف ونقطة الاسترجاع المستهدفة والمضمنة في خطة استمرارية العمل والتعافي من الكوارث ووضع سيناريوهات الاستجابة في حال فشل القدرة على الاستئناف خلال هذه الفترة.

ط) توثيق فترات الانقطاع في الخدمة وأسباب الانقطاع والإجراءات المتبعة في معالجة سبب الانقطاع في سجل خاص.

إدارة مراكز البيانات

المادة (٢٢):

على الشركة توفير ضوابط أمن مادي وبيئي لمراكز البيانات في الموقعين الرئيسي والبديل على أن تشمل بالحد الأدنى ما يلي:

أ) تأمين الحماية المادية لمراكز البيانات من المخاطر البيئية مثل الحفاظ على مستويات معينة من درجة الحرارة والرطوبة والغبار والوقاية من مخاطر المياه والحريق والعمل على توفير التبريد الموزع على كافة مساحة الغرفة بشكل يتناسب مع توزيع التجهيزات داخل الغرفة.

ب) تأمين الحماية المادية من خلال أبواب أمنية.

ج) توفير المراقبة التلفزيونية المسجلة لمداخل ومراكز البيانات.

د) الاحتفاظ بسجلات زوار و/أو مستخدمي مراكز البيانات عند الدخول والخروج.

هـ) أن تكون البنية التحتية بعيدة ومحمية عن تهديدات فيضانات وتسربات المياه والصرف الصحي المحتملة.

و) توفير مولدات كهرباء وأنظمة وبطاريات (UPS) بالقدرة الكافية لتشغيل أجهزة وعمليات الشركة (الحساسة على الأقل) في حال انقطاع مصدر الكهرباء الرئيسي واستخدام نقاط متعددة لتزويد الأجهزة الرئيسية وملحقاتها بالطاقة الكهربائية لتلافي خطر الاعتماد على مصدر وحيد للطاقة وأن يكون التحويل بينها بشكل أوتوماتيكي.

إدارة التغيير

المادة (٢٣):

على الشركة وضع القواعد والإجراءات اللازمة لإدارة التغييرات التي تطرأ على بيئة تكنولوجيا المعلومات والاتصالات وأسس الموافقة عليها وتنفيذها ومراجعتها بحيث تطبق هذه القواعد على التغييرات المتعلقة بالأنظمة والأمن والإجراءات التصحيحية وتحديثات البرامج ونظم التشغيل.

المادة (٢٤):

على الشركة قبل تطبيق التغييرات على البيئة الفعلية إجراء تحليل للمخاطر وأثر التغيير على بيئة تكنولوجيا المعلومات والاتصالات المتعلقة بأعمال الشركة وتحديد في ما إذا كان التغيير المعني سيؤدي إلى آثار أمنية أو مشاكل في توافق البرامج والأنظمة والتطبيقات.

المادة (٢٥):

على الشركة التأكد من أن التغييرات يتم الموافقة عليها من الجهة المخولة بمنح الصلاحيات على إجراء التغييرات وأن يتم فحص التغيير وتوثيق خطط اختبار التغيير.

المادة (٢٦):

على الشركة أخذ نسخ احتياطية من الأنظمة أو التطبيقات المعنية بالتغيير قبل إجراء عملية التغيير ووضع خطة للعودة إلى إصدار سابق من النظام أو التطبيق في حال حدوث أي مشاكل أثناء تطبيق التغيير أو بعده ووضع خيارات استعادة بديلة لمعالجة الحالات التي لا يسمح فيها التغيير للشركة بالعودة إلى الوضع السابق.

أحكام عامة

المادة (٢٧):

على الشركة وقبل منحها الترخيص النهائي تنفيذ فحص الثغرات الأمنية من قبل جهة مختصة بذلك وتزويد البنك المركزي بتقرير يبين نتائج هذه الفحوصات، وللبنك المركزي في أي وقت الطلب من الشركة إجراء أية فحوصات أمنية متعلقة بالنظام والبنية التحتية.

المحافظ

د. زياد فريز