وزارة المواصلات والاتصالات
MINISTRY OF TRANSPORT AND COMMUNICATIONS

المبادئ التوجيهية للتجارة الإلكترونية

الأمـــن

motc.gov.qa

المبادئ التوجيهية للتجارة الإلكترونية

الأمـــن

إعداد:

وزارة المواصلات والاتصالات

دولة قطر

٢٠١٩/٢٠١٨

حول الوثيقة

تحتوي هذه الوثيقة على المبادئ التوجيهية الموصى بها لإدارة منظومة أمن التجارة الإلكترونية في قطر. إن الهدف الرئيسي هو ضمان قيام شركات التجارة الإلكترونية والمؤسسات المالية ومقدمي خدمات تكنولوجيا المعلومات وشركاء الخدمات اللوجستية بتصميم وتطبيق أفضل الممارسات الأمنية لأعمالهم. يجب استعمال المبادئ التوجيهية كإطار عمل متكامل، والالتزام بها.

جدول المحتويات

١. مقدمة

١-١ لمحة عامة

أضحت التجارة الإلكترونية في يومنا هذا، وأكثر من أي وقت مضى، أمراً لا غنى عنه في مجال الأعمال، مع تطور وعي العملاء وازدياد توقعاتهم. إن انتشار البرودباند عالي السرعة وتوفر بنية تحتية متقدمة للإنترنت، والأجهزة المحمولة الداعمة لنظام الشبكة الإلكترونية ، توفر فرصًا اقتصادية متزايدة للحكومات والشركات والأفراد، قد تكون ذات أثر عميق في كيفية ممارسة التجارة الإلكترونية بين الشركات (B2B) وبين الشركات والعملاء (B2C) في المستقبل.

بالنسبة لمالك متجر التجارة الإلكترونية، فإن لا شيء أكثر أهمية من أمن التجارة الإلكترونية. غالبًا ما يستهدف مهاجمو الإنترنت نقاط الضعف في مواقع التجارة الإلكترونية ويستغلونها. مثل هذا الإخلال بالجانب الأمني من شأنه أن يعصف بالثقة التي يضعها العملاء في الشركة. لقد تكبدت سمعة الشركات التي وقعت ضحية للقرصنة واختراق البيانات بسبب عدم كفاية التدابير الأمنية ضرراً يتعذر إصلاحه ولعواقب مالية جمة. وعوضاً عن ذلك فإن بوسع تجربة تسوق آمنة عبر الإنترنت أن تزيد من حجم المبيعات، لأن المستهلكين يختارون بطبيعة الحال إجراء عمليات شراء من موقع ويب آمن. وتؤدي معرفة المزيد عن أهمية أمن التجارة الإلكترونية وكيفية تحسينها إلى ضمان الأمن المالي وازدهار الأعمال.

١-٢ التجارة الإلكترونية

التجارة الإلكترونية هي ذلك التوجه لنشاط الأعمال حينما تتم عملية تزويد العملاء بالسلع أو الخدمات عن طريق الأجهزة الإلكترونية والإنترنت. يضيف هذا النوع من التواصل وإنجاز عمليات المبيعات بعض الجوانب الجديدة لإدارة البيانات وقنوات البيع والإعلانات وعرض السلع والخدمات، وأكثر من ذلك، تنفيذ دورة العمليات التجارية الكاملة، بما في ذلك الدفع والتسليم والمبالغ المستردة.

١-٣ أصحاب المصلحة الرئيسيون

مع تزايد استخدام التكنولوجيا والمعلومات، ينبغي على المؤسسات أن تضع في اعتبارها الحاجة إلى الأمن وحماية مصالح أصحاب المصلحة الرئيسيين التاليين:

- العملاء / المشتركين الذين يحتاجون إلى الوثوق بشبكة المؤسسة والخدمات المقدمة، والتي تشمل توفر الخدمات وحماية معلومات التعريف الشخصية الخاصة بهم.
- السلطات التنظيمية التي تطلب تحقيق الأمن عبر التشريعات و/ أو التوجيهات من أجل ضمان توفر خدمات التجارة الإلكترونية وحماية الخصوصية.
- الموردين (مثل مقدمي خدمات تكنولوجيا المعلومات وشركاء الخدمات اللوجستية ومقدمي خدمات الدفع) الذين يحتاجون إلى أمن المعلومات لحماية العمليات اليومية المتعلقة بوظائف العمل والوفاء بالتزاماتهم تجاه العملاء.
- التجار العاملين والمؤسسات المالية العاملة بالتجارة الإلكترونية، والذين يحتاجون إلى ضمان تحقيق أهداف الأعمال، وإلى إبراز أن أمن المعلومات قد أصبح ثقافة مؤسسية، وإلى تعزيز ثقة المستثمرين بشكل عام، وإعطاء الإحساس للموردين والعملاء بالاطمئنان والارتياح للخدمات.

٢. المبادئ التوجيهية للأمن

٢-١ حماية البيانات والخصوصية

البيانات هي أحد الأصول القيّمة التي يجب على جميع تجار التجارة الإلكترونية والمؤسسات المالية وشركاء الخدمات اللوجستية ومزودي خدمات تكنولوجيا المعلومات (المشار إليهم فيما بعد باسم «المؤسسات») حمايتها وإدارتها. تقوم المؤسسات بجمع واستخدام وتخزين مجموعة واسعة من البيانات الشخصية، مثل سجلات المعلومات الشخصية للموظفين والعملاء، ومعلومات الهوية الوطنية، والتفاصيل الديموغرافية، وتفاصيل الاتصال، والمعلومات المالية، وما إلى ذلك من أجل تقديم الخدمات للعملاء.

يمكن جمع البيانات الشخصية عندما يقوم المستهلكون أو الأفراد الآخرون بتسجيل الدخول في موقع الويب، أو عندما يحتاجون إلى طلب منتج أو خدمة، أو عندما يرغبون في تلقي متابعات إخبارية، أو الدخول في مسابقة أو غير ذلك. في كل مرة يقوم فيها الفرد بتقديم بيانات شخصية يتم إعداد سجل في قاعدة بيانات تتعلق بهذا الفرد. إن جميع المعلومات عن أي شخص يتم تحديده أو يمكن التعرف عليه بشكل معقول عن طريق مزيج من المعلومات (مثل عنوان بروتوكول الإنترنت IP) يجب اعتبارها على أنها بيانات شخصية. بالإمكان أيضًا جمع البيانات المتعلقة بالفرد بطريقة أقل مباشرة أو أقل وضوحاً، على سبيل المثال: من خلال استخدام ملفات تعريف الارتباط التي تجمع البيانات المتعلقة بزائر موقع الويب. ويُعد هذا النوع من جمع البيانات أيضًا عملية معالجة للبيانات الشخصية إذا كان من الممكن تحديد الفرد المعني (صاحب البيانات). إن الاستخدام الفعال لهذه البيانات داخل المؤسسات وعبرها هو أمر بالغ الأهمية لتعزيز القدرة على صياغة السياسات وتقديم خدمات ملائمة تُركز على العملاء. وبالتالي، فقد أصبح من الضروري للمؤسسات أن تصيغ وأن تعمل على تنفيذ إجراءات مناسبة لضمان سرية ونزاهة وتوفر واتساق جميع البيانات الشخصية المخزنة في أشكال مختلفة. إن هذه الوثيقة التوجيهية تهدف إلى وضع عمليات لحماية البيانات والخصوصية في المؤسسات من أجل إدارة البيانات الشخصية طوال دورة حياتها.

إن على المؤسسات أن تدرك أن الإدارة الفعالة لخصوصية البيانات ضرورية لدعم وظائفها الأساسية، وللامتثال لالتزاماتها القانونية والتنظيمية وللمساهمة في الإدارة الفعالة بصورة عامة. هذه المبادئ التوجيهية توضح ايضاً كيفية حماية البيانات الشخصية للعميل داخل المؤسسات وخارجها.

تنطبق هذه المبادئ التوجيهية على جميع المعلومات/ السجلات/ البيانات الشخصية، التي تُنشئها أو تستلمها أو تحتفظ بها المؤسسة والموردون الخارجيون للمؤسسة ممن يمتلكون إمكانية الوصول إلى البيانات الشخصية للعميل في أي مكان تُخزن فيه سجلات البيانات هذه وفي أي شكل كانت، أثناء قيامهم بأداء واجباتهم ووظائفهم المحددة. إن للبيانات دورة حياة طبيعية، تبدأ من الإعداد والإنشاء مروراً بالتخزين والمعالجة والاستخدام وانتهاءً بتدميرها أو اتلافها في نهاية المطاف. قد تختلف قيمة أصول البيانات والمخاطر التي قد تتعرض لها أثناء دورة حياتها، غير أن حماية البيانات والخصوصية تظل أمراً مهماً في جميع المراحل.

٢-٢ التحقق من العميل

يشكل العملاء جوهر أي نشاط تجاري، لذا يصبح من الأهمية أن تتم المصادقة والتحقق من أولئك العملاء الذين يقومون بالتسجيل مع تاجر التجارة الإلكترونية. إن ذلك يضمن أمن التاجر من عمليات الاحتيال عبر الإنترنت وعمليات الاحتيال أثناء شحن الأجهزة المشتراة. إن التحقق من العميل هو خطوة في غاية الأهمية يتوجب على تجار التجارة الإلكترونية القيام بها قبل السماح للعملاء بالاستفادة من أي خدمات عبر الإنترنت.

إن الهدف من هذا المبدأ التوجيهي هو توفير أفضل الممارسات في التحقق من هوية العميل لتجار التجارة الإلكترونية لحمايتهم من عمليات الاحتيال. إن على التجار الالتزام بحماية أعمالهم من عمليات الاحتيال والخسائر في التجارة الإلكترونية. ينطبق هذا المبدأ التوجيهي على جميع تجار التجارة الإلكترونية والمؤسسات المالية في قطر.

لقد أصبح التحقق من هوية العميل أمرًا أساسياً مع ازدياد تعقيد هجمات التجارة الإلكترونية كل يوم. إن على المؤسسات، أثناء تسجيل العملاء، اتخاذ تدابير أمنية متنوعة تنطبق على نظامها البيئي.

٢-٣ تاريخ العميل وتحليل البيانات الشخصية

يُساعد سجل معاملات العملاء وتحليل بيانات المؤسسات على تحسين تجربة العملاء من خلال تقديم منتجات أفضل. كما يُساعد تحليل البيانات في تتبع سرعة الاستجابة لطلب العميل، ومعدل الطلبات المرتجعة، ومتوسط كمية المعاملات وغير ذلك من الأمور الأخرى. ويمكن لهذه البيانات أن تكون مفيدة في توفير أفكار عن السلوك الاحتيالي للعملاء، أو أي تهديد عبر الإنترنت أو غيرها، يوفر هذا المبدأ التوجيهي إرشادات لضمان أمن تجار التجارة الإلكترونية والمؤسسات المالية في دولة قطر.

٢-٤ تحليل المعاملات المجمعة من معاملات أطراف أخرى

إن إتاحة الوصول إلى البيانات لجميع المشاركين ذوي الصلة في السوق يخلق فرصاً لكل منهم لإعداد عروض أفضل، وفرصاً للمستهلكين لاتخاذ خيارات أفضل فيما يتعلق بالمنتجات. يغطي هذا المبدأ التوجيهي تحليل بيانات العملاء المجمعة من معاملات أطراف أخرى ومعاملات العملاء. وينطبق هذا المبدأ التوجيهي على جميع تجار التجارة الإلكترونية والمؤسسات المالية والأطراف الأخرى.

٢-٥ تعقب أجهزة الشراء

يحتاج مسوقو التجارة الإلكترونية إلى فهم أكثر وضوحًا لمسارات الأجهزة التي تجلب العائدات، والأجهزة التي يستخدمها العملاء لتصفح متجرك، والأجهزة المستخدمة لإجراء عمليات الشراء. يغطي هذا المبدأ التوجيهي تعقب الأجهزة المستخدمة من قبل العملاء لشراء السلع / الخدمات عبر الإنترنت. ويساعد التجار على حماية أنفسهم ضد سلوك المستهلك الاحتيالي.

٢-٦ أمور أخرى

- **استخدام المحفظة الإلكترونية**

إن الوصول إلى طرق دفع متعددة وإلى عملية دفع إلكترونية فعالة هو أمر ضروري للغاية لزيادة تبني التجارة الإلكترونية. في الوقت الحالي، يخضع التجار في قطر لعمليات متعددة من قبل البنوك الوطنية لتأسيس الدفع الإلكتروني. تُشير المحفظة الإلكترونية إلى حساب إلكتروني يسمح للمستهلك بإجراء معاملات إلكترونية بطريقة

أكثر سرعة وفعالية. تعتزم الحكومة تعزيز بوابة (QPAY) لتمكين استخدام البطاقات مسبقة الدفع، والبطاقات المدينة، وبطاقات الأجور لتأمين تحقيق دفعات آمنة عبر الإنترنت. ويهدف هذا المبدأ التوجيهي إلى ضمان أمن المعاملات التي تجري من خلال المحافظ الإلكترونية والبطاقات المدفوعة مسبقاً. وينطبق هذا المبدأ التوجيهي على جميع المؤسسات المصرح لها بتقديم خدمة المحافظ الإلكترونية (أدوات الدفع مسبقة الدفع (PPI)) وبطاقات الهدايا المشحونة مقدماً، في دولة قطر.

➢ أمن الشبكات

يُحدد المبدأ التوجيهي لأمن الشبكات متطلبات تأمين روابط اتصالات الشبكة وأصول المعلومات التي يتم نقلها داخل المؤسسة ومن المؤسسة. إن أمن الشبكات يساعد المؤسسات على ضمان التحكم في الوصول إلى كل من خدمات الشبكة الداخلية والخارجية، وأن وصول المستخدمين إلى الشبكات والخدمات الشبكية لا يؤثر على أمن الخدمات المتصلة بالشبكة. وهو يغطي إعداد متطلبات الأمن التقني عند المستوى القياسي (مثال: معدات الشبكات وتبادل المعلومات مع الطرف الثالث، ونقل المعلومات داخلياً وخارجياً، وحماية البريد الإلكتروني، واتفاقيات السرية / عدم الإفصاح). يهدف هذا المبدأ التوجيهي إلى منع الوصول غير المصرح به إلى الخدمات المتصلة بالشبكة. فضلاً عن ذلك يوضح هذا المبدأ التوجيهي للمؤسسة معايير متنوعة متعلقة بتأمين شبكتها والضوابط التي يجب تنفيذها لضمان أمن المعلومات في الشبكات وحماية الخدمات المتصلة من الوصول غير المصرح به.

➢ أمن البنية التحتية

تُمكن المبادئ التوجيهية لإدارة أمن البنية التحتية المؤسسات من تصميم وتنفيذ البنية التحتية بطريقة تضمن وجود الضوابط الأمنية المناسبة والتي تتناسب مع مستويات تصنيف البيانات وحساسية الأعمال. علاوة على ذلك يساعد هذا المبدأ المؤسسة على اقتراح الضوابط الأمنية الفعالة، بناءً على المخاطر، بما يُلبي مقاصد وزارة المواصلات والاتصالات وسياسات المؤسسة، فضلاً عن كونه يخلق نوعاً من المساءلة داخل الشبكة وموارد الحوسبة الأخرى التي يمكن للأفراد الوصول إلى أنظمتها.

إن الغرض من هذا المبدأ التوجيهي هو إنشاء إطار لإدارة أمن البنية التحتية لدى تجار التجارة الإلكترونية ومقدمي خدمات تكنولوجيا المعلومات وشركاء الخدمات اللوجستية والمؤسسات المالية في قطر. ينبغي أن تُمكن هذه العملية المؤسسات من التأكد من أن جميع الوظائف الأساسية للبنية التحتية يتم توثيقها وأن لديها عمليات تشغيلية وخطط للتعافي من الكوارث من أجل توفير استمرارية التشغيل.

➢ إدارة نقاط الضعف

التقييم الأمني هو العملية التي يتم بها تحديد نقاط الضعف في أنظمة تكنولوجيا المعلومات يدويًا أو بواسطة أدوات، وتقييم مخاطر استغلال نقاط الضعف تلك. يساعد هذا التقييم في تحديد الخطوات التالية لتصحيح نقاط الضعف والحد من المخاطر عن طريق اتخاذ الإجراءات التصحيحية. إن إدارة نقاط الضعف تتكون من استخدام برنامج حاسوبي لتحديد نقاط الضعف في الشبكات أو البنية التحتية للحاسوب أو التطبيقات. أما عملية إدارة عمليات التحديث فهي تشمل الوسائل والأساليب التي تهدف إلى تحديد التحديثات الأمنية والحصول عليها في الوقت المناسب، واختبار التحديثات القابلة للتطبيق، واستخدام التحديثات، فضلاً عن آلية الصيانة وإعداد التقارير.

يتمثل الغرض من هذا المبدأ التوجيهي في وضع إطار عمل لإدارة نقاط الضعف وإدارة عمليات التحديث وتقييمات الأمن الأخرى لدى تجار التجارة الإلكترونية والمؤسسات المالية في قطر. وستتيح لنا هذه العملية الرصد المستمر لنقاط الضعف في بيئة تقنية المعلومات لدى المؤسسة والمخاطر المرتبطة بها.

- **إدارة السجلات**

إن عملية إعداد السجلات هي عنصر لا غنى عنه في أمن الأنظمة وأجهزة الشبكة. ولذلك، تعتبر مراقبة السجلات وتحليلها من الأنشطة الضرورية، لأن ملفات السجل غالبًا ما تكون هي السجل الأفضل و/ أو السجل الوحيد للسلوكيات المشبوهة. يتناول المبدأ التوجيهي لإدارة السجلات جمع وتحليل السجلات والاحتفاظ بها والإجراءات التصحيحية المتخذة لضمان معرفة أي تهديد للأعمال والحد منه. يسعى هذا المبدأ التوجيهي إلى التأكد من تسجيل جميع الأحداث ذات الصلة بأمن الشركات وبيانات الأعمال وتوفر الأدلة ذات الصلة. يهدف هذا المبدأ التوجيهي إلى إبراز أهمية الضوابط والخطوات اللازمة لضمان تسجيل ومراقبة أنشطة النظام.

٣. المبادئ التوجيهية التفصيلية

٣-١ حماية البيانات والخصوصية

ينظم القانون رقم 13/2016 بشأن حماية خصوصية البيانات الشخصية جمع وتخزين واستخدام ونقل البيانات الشخصية للمستهلكين (وكذلك الموردين وغيرهم من جهات الاتصال) من قبل التجار أو مقدمي الخدمات. تعتبر الأنشطة العامة لجمع أو استلام أو تسجيل أو ترتيب أو حفظ أو إعداد أو تعديل أو استعادة أو استخدام أو الإفصاح عن أو نشر أو نقل أو حجب أو إلغاء أو حذف البيانات الشخصية «معالجة» للبيانات الشخصية.

المبادئ التوجيهية التالية مهمة من أجل مراعاة الأحكام والالتزامات القانونية الخاصة بالعناية الواجبة:

- يجب أن يكون التجار على الإنترنت على دراية بأنهم إذا قاموا بمعالجة البيانات المتعلقة بالعملاء الوطنيين، فإنهم يقومون بدور «المراقب» كما هو محدد في المادة ١ من القانون رقم 13/2016 بشأن حماية خصوصية البيانات الشخصية. فهم يقررون الغاية من معالجة البيانات وطريقة معالجتها، ويصدرون تعليمات لمعالج البيانات ليقوم فعلياً بمعالجة البيانات الشخصية نيابة عنهم. إن اعتبارك مراقباً أو معالج بيانات ينطوي على التزامات قانونية معينة والتزامات عامة تتعلق بالعناية الواجبة.

- يجب ألا تعالج البيانات الشخصية إلا وفق الشفافية والنزاهة واحترام كرامة الإنسان والممارسات المقبولة وفقا لأحكام القانون.

- لا يجوز معالجة البيانات الشخصية الحساسة إلا بعد الحصول على إذن من وزارة المواصلات والاتصالات (غير أنه لم يتم إصدار الإجراءات ذات الصلة حتى الآن). إن البيانات الشخصية الحساسة هي البيانات المتعلقة بالأصل العرقي والأطفال والصحة والحالة البدنية أو النفسية والدين والعلاقات الزوجية أو الحالة الجنائية.

- يجب أن تكون عملية جمع البيانات الشخصية ومعالجتها ذات صلة بالأغراض المشروعة، ويجب عدم معالجة البيانات غير ذات الصلة. علاوة على ذلك، فإنه يُمكن الاحتفاظ بالبيانات فقط خلال الفترة الضرورية لأداء الغرض ذي الصلة. لذا ينبغي حذف البيانات التي أصبحت قديمة أو مهملة.

- عندما يقوم المراقب بتوجيه معالج ليس موظفاً لديه (مثال: مقدم خدمة تكنولوجيا المعلومات، مسؤول موقع الويب) لمعالجة البيانات، فإن عليه التأكد من أن المعالج سوف يحترم القواعد والإجراءات اللازمة. وعلى المراقب والمعالج أن يضمنا الحماية الكافية للبيانات الشخصية ضد الفقد أو التلف أو التعديل أو الإفصاح أو الوصول من قبل أشخاص غير مرخصين أو الاستخدام غير القانوني لها، ويجب أن تكون تلك الاحتياطات متناسبة مع طبيعة البيانات وأهميتها.

- يجب على المعالج إبلاغ المراقب على الفور عن أي خرق أو انتهاك لاحتياطات السلامة («خرق البيانات»). يجب على المراقب إخطار الفرد المعني والإدارة المعنية في وزارة المواصلات والاتصالات إذا كان من المحتمل أن يتسبب هذا الخرق في أضرار خطيرة لخصوصية الأفراد. عندما تكون حماية البيانات على وجه التحديد معرضة للخطر، فإنه يُتوقع من المراقب تدقيق إجراءات المعالج.

- يجب على مشرف موقع الويب الموجه للأطفال نشر إشعار على موقع الويب حول طبيعة البيانات المتعلقة بالأطفال، وطريقة استخدام البيانات وسياسات الإفصاح. وعلاوة على ذلك، فإنه لا يُمكن جمع بيانات الأطفال إلا بعد الحصول على موافقة صريحة من آبائهم عبر الاتصال الإلكتروني أو غير ذلك، ويجب إيقاف المعالجة (وحذف البيانات) إذا طلب أحد الوالدين ذلك. يجب ألا تتوقف مشاركة الطفل في أي لعبة أو عرض جوائز أو أي نشاط آخر على شرط تقديم بيانات شخصية تتجاوز الحدود اللازمة لما هو مطلوب من أجل تلك المشاركة. يجب تقديم معلومات حول نوع البيانات التي تتم معالجتها والغرض من ذلك، لدى طلب أحد الوالدين ذلك، بالإضافة إلى نسخة من البيانات التي تم جمعها وتخزينها.

- لا يجوز استخدام البيانات الشخصية لأغراض التسويق المباشر عبر الاتصالات الإلكترونية إلا إذا أعطى الشخص موافقة مسبقة على استخدام بياناته لذلك الغرض. وستكون ممارسة جيدة لو تم وضع مربع اختيار فارغ بجوار أي شكل لجمع البيانات، مصحوباً بعبارة «أوافق على استخدام بياناتي لأغراض التسويق المباشر من خلال الوسائل الإلكترونية». يُمكن، حينئذ، للشخص الذي يرغب في التعبير عن موافقته على تلقي الاتصالات التسويقية المباشرة وضع علامة في مربع الاختيار، ويجب تخزين هذه الموافقة كمعلومات شخصية تتعلق به.

- يجب أن توضح الاتصالات التسويقية المباشرة هوية منشئ التسويق، ويجب أن تتضمن عنواناً يسهل الوصول إليه يمكن للفرد من خلاله إرسال طلب لوقف المزيد من الاتصالات التجارية، أو لسحب موافقته السابقة على ذلك

تجدر الإشارة إلى أن المبادئ التوجيهية للأحكام والشروط تحتوي على سياسة خصوصية نموذجية يمكن استخدامها لإعلام زوار موقع التاجر وعملائه بالمبادئ والضمانات التي سيراعيها التاجر فيما يتعلق بمعالجة البيانات الشخصية

- **حوكمة البيانات**

- يتعين على المؤسسات تحديد إطار عمل لحماية البيانات والخصوصية
- يجب على الإدارة تعيين مسؤول كبير، تكون مسؤوليته هي الإشراف على إدارة ومراقبة حماية البيانات والخصوصية. ويجب تعيين المسؤول على أساس المؤهلات المهنية والخبرة والمعرفة بحماية البيانات والخصوصية.
- وستكون مسؤوليات الشخص المعين كما يلي:
  - المشاركة في جميع القضايا المتعلقة بمتطلبات حماية البيانات الشخصية والخصوصية
  - التأكد من توفر عمليات وإجراءات مناسبة لإدارة دورة حياة المعلومات بما يكفي لإنشاء وتخزين وإدارة ومعالجة البيانات معالجة شاملة وبدقة وفي الوقت المناسب
  - إشعار وتقديم النصح للمراقب والمعالج والموظفين الذين يقومون بأنشطة المعالجة
  - مراقبة الامتثال باللوائح المعمول بها مثل لوائح حماية البيانات العامة (GDPR) ولوائح منظمة التعاون الاقتصادي والتنمية (OECD) وغيرها من اللوائح
  - إجراء التدريب والتوعية حول عمليات المعالجة وحماية البيانات والخصوصية
  - الاتصال والتعاون مع حكومة قطر
- يجب إحالة جميع القضايا المتعلقة بإدارة البيانات وحمايتها وخصوصيتها ومشاركتها إلى الإدارة. تقوم الإدارة بالإشراف وضمان المواءمة وتوفير التوجيه العام والمشورة بشأن قضايا حماية البيانات لتسهيل مشاركة البيانات مع مراقبي البيانات ومعالجيها ضمن الإطار التشريعي الساري.

مراقب ومعالج البيانات

- يجوز لمراقب البيانات جمع ومعالجة البيانات الشخصية عندما يمنح الفرد (صاحب البيانات) موافقته على ذلك، إلا إذا اعتبرت المعالجة ضرورية لتحقيق غرض مشروع للمراقب أوللطرف الثالث الذي ستُنقل البيانات الشخصية إليه
- قبل معالجة أي بيانات شخصية، يجب على مراقب البيانات إبلاغ صاحب البيانات حول:
  - تفاصيل مراقب البيانات أو المعالج الذي يقوم بأعمال مراقب البيانات
  - الغرض المشروع الذي يُريد مراقب البيانات أو الطرف الثالث معالجة البيانات الشخصية لأجله (مثال: إدارة العملاء والتسويق)
  - وصف شامل ودقيق لأنشطة المعالجة ودرجات الكشف عن البيانات الشخصية للغرض المشروع
  - أي معلومات أخرى ضرورية للمعالجة المشروعة
- يجب على مراقبي البيانات ومعالجيها اتخاذ التدابير التقنية والتنظيمية المناسبة لضمان مستوى من الأمن يتناسب مع حجم المخاطر. ويجب عليهم ضمان ما يلي:
  - تنفيذ المعالجة وفقًا للوائح المعمول بها مثل قانون حماية خصوصية البيانات الشخصية - القانون رقم (13) لسنة 2016 في قطر، لوائح حماية البيانات العامة في الاتحاد الأوروبي (EU GDPR) وغيرها من اللوائح
  - مراجعة هذه الضوابط وتحديثها في حالة حدوث أي تغييرات في العمليات أو عند الضرورة
  - تنفيذ سياسات مناسبة لحماية البيانات
  - الامتثال للسياسات المعمول بها لحماية البيانات
  - اعتماد الخصوصية في مبادئ التصميم
  - استخدام تدابير مثل الاسماء المستعارة والتشفير ومبدأ حماية البيانات وتقنيات الحد من البيانات
  - الحصول على الموافقة من الأفراد، أصحاب البيانات، عند جمع البيانات، ويجب أن تكون الموافقة صريحة ومحددة، ويجب الاحتفاظ بها طوال الفترة التي قد تكون المعالجة مطلوبة خلالها
  - يقتصر الوصول إلى البيانات الشخصية على الأفراد المصرح لهم فقط
  - تجري معالجة البيانات الشخصية الضرورية فقط وللغرض المحدد فقط
  - ضمان سرية البيانات الشخصية وسلامتها وتوفرها
  - القيام دورياً باختبار وتقييم فعالية الإجراءات التقنية والتنظيمية
  - ضمان مرونة نظام المعالجة وميزة استعادة الخدمات وإمكانية الوصول إلى البيانات في الوقت المطلوب في حالة وقوع أي حادثة
  - منع التدمير العرضي أو غير المشروع للبيانات أو فقدانها أو تغييرها أو الكشف عنها أو الوصول إليها
- يجب أن يتأكد المعالجون الذين يعملون بالنيابة عن المراقبين من وجود التدابير التقنية والتنظيمية الكافية لحماية البيانات الشخصية لصاحب البيانات
- لا يجوز للمعالج إشراك معالج آخر بدون إذن خطي من المراقب
- يجب إبلاغ مراقب البيانات بأي تغييرات في معالجي البيانات
- عندما يتعاقد المعالج مع معالج آخر في الباطن، تسري على المعالج الآخر نفس الالتزامات المتعلقة بحماية البيانات
- يتوجب على المعالج الذي يمتلك إمكانية الوصول إلى البيانات أن يقوم بمعالجة البيانات فقط بناءً على تعليمات المراقب، ما لم يكن غير ذلك مطلوباً بموجب القانون القطري

- يجب على مراقبي ومعالجي البيانات نشر بيان خصوصية على موقعهم الإلكتروني
- يجب على مراقبي ومعالجي البيانات تنفيذ عمليات التخلص من البيانات أو إتلافها بشكل آمن عندما لا تعود هناك حاجة لها، لمنع الأطراف غير المصرح لها من الوصول إلى تلك البيانات
- جمع البيانات:
  - يجب أن يكون مراقب أو معالج البيانات، الذي يكون بحوزته البيانات الخاصة بصاحب البيانات، قادرًا على إثبات الحصول على الموافقة (لغرض جمع أو استخدام أو الكشف عن البيانات الشخصية لطرف ثالث أو منظمة أخرى لغرض معالجة معاملات الخدمة) من صاحب البيانات
  - يجب على مراقبي ومعالجي البيانات التأكد من أن جميع المعلومات أو السجلات المخزنة مادياً أو إلكترونيًا في أنظمتهم، يتم تصنيفها وتأمينها بما يتماشى مع سياسة تأمين المعلومات الوطنية، الإصدار 2.0. يجب على المؤسسات أيضا إنشاء والحفاظ على سجل لمثل هذه البيانات الأساسية وأصول المعلومات
  - يجب على مراقبي ومعالجي البيانات التأكد من أن البيانات يتم تجميعها بواسطة وسائل قانونية نزيهة، وأن تقتصر على ما هو ضروري لتحقيق المتطلبات القانونية أو المتعلقة بالأعمال
  - جب على مراقبي البيانات إجراء مراجعات لتحديد الخدمات التي يمكن فيها الاستغناء عن الوثائق أو تعبئة النماذج بواسطة أصحاب البيانات والشركات أو الحد منها إلى أقصى حد ممكن

➢ مشاركة البيانات

- يتعين على مراقبي البيانات الحصول على موافقة من أصحاب البيانات في نموذج طلب الخدمة على النسخة المطبوعة أو الإلكترونية عبر الإنترنت، على السماح بإعادة استخدام البيانات الشخصية ومشاركتها لغرض تقديم الخدمات لهم. وقد تكون تلك الموافقة على شكل بيان يُفيد أنه «بتقديم الطلب للحصول على الخدمة المطلوبة، فإن مقدم الطلب يسمح بمشاركة بياناته الشخصية وإعادة استخدامها بين المؤسسات في دولة قطر، فقط لغرض تقديم الخدمات الحالية والمطلوبة مستقبلاً إليهم.»
- بالنسبة للبيانات الشخصية الحساسة، يجب على مراقبي البيانات العمل مع معالج البيانات لتحديد الحد الأدنى من البيانات اللازمة للوفاء بمتطلبات المستخدم مع ضمان وجود ضمانات كافية لحماية البيانات؛ على سبيل المثال، من خلال تحديد ما إذا كان من الممكن تحقيق الهدف دون الكشف عن هوية صاحب البيانات.
- يجب أن تقتصر البيانات التي يتعين مشاركتها على ما قد يكون ضرورياً لتحقيق أغراض الخدمة المطلوبة.
- الغرض من مشاركة البيانات: يجوز للمؤسسات مشاركة البيانات مع مؤسسة أخرى فقط للغرض المحدد وهو تلبية طلب الخدمة. وحسب الاقتضاء، ينبغي صياغة اتفاقيات لمشاركة البيانات، إن لزم الأمر، لإلزام جميع الأطراف ذات الصلة في مبادرة المشاركة. يجب أن تتضمن اتفاقية مشاركة البيانات الغرض من مشاركة البيانات والمؤسسات المعنية ومجموعات البيانات / العناصر التي ستتم مشاركتها، وقواعد الاحتفاظ ببنود البيانات المشتركة وحذفها، وإجراءات التعامل مع إنهاء اتفاقية مشاركة البيانات.
- فيما يتعلق بنقل البيانات الشخصية إلى أشخاص آخرين، يجب ملاحظة أن هذا النقل يعتبر معالجة للبيانات، وبالتالي فإن طلب الموافقة أو ضرورة تحقيق غرض قانوني ينطبق على هذه الحالة. لا ينص القانون على متطلبات محددة لنقل البيانات داخل قطر أو خارجها، غير أنه من المنصوص عليه أنه لا يجوز للمراقب أن يتخذ أي قرار أو إجراء قد يعيق تدفق البيانات الشخصية عبر الحدود، ما لم تكن معالجة تلك البيانات انتهاكًا لأحكام قانون الخصوصية أو قد تتسبب في أضرار خطيرة للبيانات أو خصوصية الفرد.

حقوق الأفراد أصحاب البيانات

- في وقت الحصول على المعلومات، يجب عل مراقب البيانات تقديم تفاصيل الاتصال الخاصة به، والمسؤول الرئيسي لحماية البيانات، والغرض من جمع البيانات، ومتلقي البيانات، ونقلها إلى بلد ثالث أو منظمة دولية، إلى صاحب البيانات
  - وللمعالجة النزيهة والشفافة، يتعين على المراقب أن يقدم أيضاً ما يلي:
  - فترة تخزين البيانات
  - شرط التصحيح أو الحذف؛ الحق في تقديم شكوى لدى هيئة مختصة. منطق الإعداد الآلي للملفات، وأهميته وتأثيره على صاحب البيانات، إن وجد
  - يحق لصاحب البيانات الحصول على المعلومات التالية من المراقب عند معالجة البيانات
  - نسخة عن البيانات الشخصية
  - رسوم معقولة للطلبات المتكررة من صاحب البيانات
  - الغرض من المعالجة
  - فترة تخزين البيانات والمعايير المستخدمة لتحديد ذلك
  - مستلمي البيانات المفصح عنها
  - الشروط المتعلقة بالتصحيح أو الحذف
  - الحق في تقديم شكوى لدى هيئة مختصة
  - منطق إعداد الملفات الآلي وأهميته وتأثيره على صاحب البيانات، إن وجد
  - النقل إلى بلد ثالث أو منظمة دولية، والضمانات المطبقة ومصدر البيانات عند عدم جمعها من صاحب البيانات
- بإمكان صاحب البيانات طلب حذف البيانات الشخصية فقط إذا لم تعد البيانات مطلوبة للغرض الذي تم الحصول عليها من أجله من قبل مراقب البيانات
- يجب على المراقب إبلاغ أي تصحيح أو حذف إلى كل مستلم تم الكشف عن بيانات شخصية له، ما لم يتطلب الأمر جهداً أو بيانات غير متناسبة ومالم يتسبب في تأخير غير مبرر
- يجوز لصاحب البيانات في أي وقت ما يلي:
  - سحب موافقته المسبقة بشأن معالجة بياناته الشخصية
  - الاعتراض على المعالجة إذا كانت غير ضرورية للأغراض المحددة، أو عندما تكون تمييزية أو ضارة أو مخالفة للقانون
  - طلب حذف بياناته الشخصية وفقًا لهذه الشروط
  - تقديم طلب للحصول على حق الوصول إلى بياناته الشخصية، وأن يتم إبلاغه عن عملية المعالجة وأغراضها، والحصول على نسخة منها (قد يكون ذلك بعد دفع رسوم معقولة)، وتقديم طلب لتصحيح البيانات مع المستندات الداعمة.
  - يجوز للمراقب رفض الامتثال للطلبات إذا كشف عن الأسباب الكامنة خلف ذلك الرفض. لكن إذا كان الأمن القومي أو علاقات الدولة الدولية أو المصالح الوطنية الاقتصادية أو المالية، أو عمليات منع الجريمة، على المحك، فلا يجب الكشف عن السبب. لا يجب منح حق الوصول إلى بيانات الفرد إذا كان ذلك يؤدي إلى تضرر المصالح التجارية لشخص آخر، أو إذا كان هذا سيؤدي إلى الكشف عن البيانات الشخصية لشخص آخر لم يوافق على ذلك، أو إذا كان من المحتمل أنها ستسبب أضرار مادية أو معنوية لذلك الشخص.

- يجب على مراقب البيانات صياغة قواعد داخلية لتلقي ودراسة الشكاوى، وطلبات الوصول إلى البيانات، وطلبات تصحيح البيانات أو حذفها، وإتاحة هذه القواعد للأفراد (على سبيل المثال: في سياسة الخصوصية)
- القواعد والإجراءات المتعلقة بحقوق الأفراد سيتم تحديدها بموجب قرارلم يتم إصداره بعد

٢-٣ التحقق من العميل

أثناء تسجيل العملاء، يجب على المؤسسات القيام بما يلي حسبما ينطبق على منظومتهم:

- إجراء التحقق من العنوان البريدي، حيثما أمكن ذلك، عن طريق التحقق من العنوان ومن ثم توفيرخيارات وسائل الدفع
- إجراء التحقق من خلال المعرفات الشخصية مثل معرف البريد الإلكتروني ورقم الهاتف المحمول. يمكن القيام بذلك عن طريق إرسال رابط التحقق على البريد الإلكتروني أورمز المرور الذي سيُطلب من المستخدم تقديمه إلى المؤسسة قبل إنشاء الحساب
- اختيارخدمة التحقق من العنوان (AVS) : خدمة التحقق من العنوان هي خدمة تسمح للتجار الذين يقبلون المعاملات غير المباشرة بمقارنة عنوان إرسال الفواتير الذي يقدمه العميل مع العنوان الموجود على ملف جهة إصدار البطاقة قبل معالجة المعاملة. يعتبرعدم التطابق مؤشراً قوياً للاحتيال. ويتم ذلك كجزء من طلب التاجر للحصول على إذن بطاقة الائتمان للمعاملة. يُرسل معالج البطاقة الائتمانية رمز الاستجابة مرة أخرى إلى التاجر مشيراً إلى درجة مطابقة العنوان، والتي يتم على أساسها قبول أورفض معاملة البطاقة الائتمانية
- استخدام ميزة البحث عبر الموقع الجغرافي: باستخدام أداة البحث عبر الموقع الجغرافي، يمكن للمؤسسات تحديد العنوان البريدي التقريبي لأي موقع على خريطة العالم بسرعة
- التحقق من هوية العميل من خلال رقم التحقق من البطاقة (CVN / CVV). مما يُساعد على مصادقة المستخدم / البطاقة مقارنة رقم التحقق المطبوع على شريط التوقيع على ظهر البطاقة مع المعلومات الموجودة في الملف لدى البنك الذي أصدر البطاقة
- استخدام المصادقة متعددة العوامل: يجب على المؤسسات تبني المصادقة متعدد العوامل والتأكد من أن جميع المعاملات المالية تتبع نفس العملية
- مصادقة الدافعين: تطبيق آلية التحقق الآمن ثلاثية الأبعاد (3D Secure) التحقق بواسطة بطاقة(Visa) أو الرمز الآمن (Securecode) بواسطة بطاقة (Mastercard) لمنع المعاملات الاحتيالية باستخدام البطاقات الائتمانية والبطاقات المدينة عبر الإنترنت. وهي عملية من ثلاثة أجزاء تضم الأطراف المعنية، وهم البائع والمشتري (المصرف الذي يعالج الدفع) ومصدري البطاقات (أي بطاقات Visa أو MasterCard)
- استخدام التحقق عبررقم الهاتف / البحث العكسي للتأكد عند إدخال المستخدم لبيانات غير صحيحة
- تنفيذ المصادقة متعددة العوامل، عبر الهاتف، لمصادقة العملاء. يمكن القيام بذلك بواسطة رمز مرور ديناميكي صالح لمرة واحدة يتكون عادةً من 4 إلى 6 أرقام. يُمكن إرسال الرمز إلى أجهزة العملاء الجوالة عن طريق رسالة قصيرة أو إخطارعبر الإنترنت أويُمكن إنشاؤه عن طريق مولد لرموز المرور (تطبيق) لمرة واحدة
- توثيق المستخدمين من خلال القياسات الحيوية كلما كان ذلك ممكنا. الطرق الأكثرشيوعا هي من خلال بصمات الأصابع والتعرف على الصوت
- كلما كان ذلك ممكنًا، يجب على المؤسسات إجراء فحص لتاريخ الائتمان للمعاملات ذات القيمة العالية
- توفيرالخيارلتمكين العملاء من تسجيل الدخول من خلال / ربط حسابات الشبكات الاجتماعية بحساب التجارة الإلكترونية

٣-٣ تاريخ العميل وتحليل البيانات الشخصية

يجب على المؤسسات استخدام الآليات التالية لتحليل تاريخ العميل والبيانات لتتبع أي سلوك احتيالي:

- **سجل طلبات العميل**
  - يجب أن يكون الوصول إلى سجل طلبات العميل مقصوراً على أغراض التحليل فقط، ولا يجوز مشاركته مع أي شخص خارج نطاق دائرة الاستخدام الداخلي
  - يجب الاحتفاظ بسجل طلب العميل في قاعدة بيانات آمنة
  - يجب تشفير بيانات طلب العميل
  - يجب أن تكون البيانات متاحة فقط للموظفين المصرح لهم بعد الحصول على الموافقات السليمة.
  - يجب مراجعة إعدادات كلمة المرور وتهيئة وحدة الخادم وجدار الحماية مراجعة دورية

- **القوائم السلبية**
  - يجب تحديد عملية لتصنيف العميل ضمن قائمة إيجابية أو سلبية بناءً على سمات محددة مسبقًا
  - ينبغي تصنيف العملاء الذين لديهم «معدل طلبات مرتجعة» معين ضمن القائمة السلبية
  - يجب ألا يكون العميل قادرًا على تقديم طلبات باستخدام نفس رقم البريد الإلكتروني/ رقم الهاتف الذي تم وضعه في القائمة السوداء
  - بعد تجاوز عدد مرات فشل المصادقة، يجب قفل هوية العميل وطلب مصادقة إضافية
  - يجب تقييم العملاء على أساس عناوين بروتوكولات الإنترنت (IP) الخاصة بأجهزتهم، ويجب حظرهم إذا وردوا في عناوين (IP) غير مرغوب فيها

- **مراقبة سرعة الطلب**
  - يجب على الشركة أن تجري على أساس دوري فحص سرعة للكشف عن أي معاملات احتيالية. يتمثل الهدف من سرعة الاستخدام هو البحث عن أي سلوك مشبوه استناداً إلى عدد المعاملات ذات الصلة التي يحاول المستهلك القيام بها. ويتم الفحص بناء على حساب عدد الاستخدامات لعنصر البيانات داخل إطار زمني محدد مسبقاً
  - يجب على التجار تتبع عدد المعاملات التي تجرى عبر جهاز واحد في يوم واحد
  - يجب على التجار إجراء فحص السرعة المتقدم مثل عدد الحسابات التي تمت رؤيتها على عنوان (IP) معين في ال 30 يومًا الأخيرة وما إلى ذلك

- **نموذج نقاط عمليات الاحتيال**
  - يجب على تجار التجارة الإلكترونية تطوير إجراءات/ نظام أو إطار عمل داخلي لنقاط عمليات الاحتيال في المعاملات. يتيح نظام نقاط عمليات الاحتيال المصمم تصميماً جيداً للتجار إمكانية تخصيص نقاط للعناصر المختلفة لأي معاملة احتيالية. وتتضمن تلك العناصر عادةً ما يلي: عنوان بروتوكول الإنترنت (IP) وعنوان البريد الإلكتروني والوقت (من اليوم) الذي قدم فيه الطلب ورمز نتيجة (AVS) وقيمة المبيعات ونوع البضائع وطريقة الشحن وعناوين الشحن والفواتير المختلفة والرموز البريدية
  - يجب على المؤسسات أن تحدد بوضوح المسؤوليات المتعلقة بالكشف عن عمليات الاحتيال وعمليات مراجعة العمليات المشبوهة

- يجب على المؤسسات تتبع أداء مراقبة عمليات الاحتيال لفهم تأثير الاحتيال على الأعمال
- يجب على المؤسسات تسجيل جميع العناصر الرئيسية للمعاملات الاحتيالية مثل الأسماء وعناوين البريد الإلكتروني وعناوين الشحن وأرقام تعريف العملاء وكلمات المرور وأرقام الهواتف وأرقام البطاقات المستخدمة

- **تحليل سلوك العميل في الموقع**
  - يجب على المؤسسات مراقبة المعاملات باستمرار وتطبيق التحليلات السلوكية للكشف عن أي معاملة احتيالية
  - يجب على المؤسسات مراقبة دورة حياة الطلب الاعتيادية لضمان تقديم خدمة سلسة للعملاء
  - يجب على المؤسسات تحليل طلبات العملاء السابقة لتقديم منتجات وخدمات أفضل
  - يجب الحصول على موافقة العميل قبل تحليل بياناته
  - يجب نشر سياسة الخصوصية على الموقع تشير بوضوح إلى أن جميع بيانات العملاء سوف تُستخدم لأغراض التحليل

٣-٤ تحليل المعاملات المجمعة من معاملات أطراف أخرى

إن إتاحة الوصول إلى البيانات لجميع المشاركين ذوي الصلة في السوق يخلق فرصاً لإعداد عروض أفضل، وفرصاً للمستهلكين لاتخاذ خيارات أفضل فيما يتعلق بالمنتجات

- **سرعة الشراء للتجار المتعددين:**
  - يُستحسن أن تجري المؤسسات تحليلاً لمعاملات عملائها باستخدام واجهات برمجة التطبيقات. واجهات برمجة التطبيقات تسمح بمراقبة معاملة جارية والتنبؤ بالمعاملات المستقبلية للعملاء وتوفير منتجات أفضل لمعاملاتهم التالية

- **القوائم السلبية المشتركة وقوائم العناوين الهامة المشتركة**
  - يوصى بأن تتعقب المؤسسات العملاء المحتالين بناءً على واجهات برمجة التطبيقات
  - يُوصى بأن يقوم تجار التجارة الإلكترونية والمؤسسات المالية باستخدام مكونات إضافية يمكنها التحقق من «القائمة السوداء» أثناء كل عملية شراء، وأن تحظر أي عميل يتطابق عنوانه مع عنوان البريد الإلكتروني و/ أو عنوان بروتوكول (IP) في القائمة السلبية
  - يجب على تجار التجارة الإلكترونية والمؤسسات المالية الاحتفاظ بسجلات الأحداث التي توفر معلومات حول محاولات الشراء التي يقوم بها عميل من القائمة السلبية
  - يجب على تجار التجارة الإلكترونية والمؤسسات المالية أن يضعوا العملاء الذين لديهم «معدل طلبات مرتجعة» ضمن القائمة السوداء

٣-٥ تعقب أجهزة الشراء

- يُوصى بأن يقوم تاجر التجارة الإلكترونية بتعقب عنوان (IP) وتحديد الموقع الجغرافي لجهاز الشراء
- يوصى بأن يقوم تجار التجارة الإلكترونية بتعقب العميل على أساس مزيج من هوية المستخدم وهوية العميل. هوية المستخدم هي القيمة التي يرسلها العميل إلى (Google Analytics)، والتي تحدد هوية العميل كمستخدم تمت مصادقته

- يُستحسن تشغيل توحيد الجلسات على الوضع الافتراضي. توحيد الجلسة هو إعداد لهوية المستخدم يُمكّن من جمع النتائج قبل تعيين هوية المستخدم أو ربطه تلقائيًا بهوية المستخدم.
- يجب على المؤسسات وضع ضوابط تساعد على تحديد ما إذا كان العميل / المستخدم قد قام بالتسجيل من جهاز جديد، ويجب إخطار المستخدم بذلك على الفور.
- يجب على المؤسسات تزويد العميل / المستخدم بخيار لتذكر الأجهزة التي يستخدمها بشكل متكرر.
- يُوصى بتتبع أجهزة الشراء بناءً على بصمات الجهاز.

٦-٣ أمور أخرى

➢ استخدام المحفظة الإلكترونية

- يجوز للبنوك التي سُمح لها بتقديم معاملات بنكية عبر الهاتف المحمول من قبل المشرع / الحكومة إطلاق أدوات الدفع المدفوعة مقدما على الهاتف المحمول (المحافظ الإلكترونية)
- يتعين على البنوك إصدار وسيلة دفع مسبقة الدفع بعد التطبيق الكامل لمبدأ «اعرف عميلك» (KYC).
- يجب وضع حد يومي محدد مسبقاً، لأدوات الدفع المدفوعة مسبقاً عبر النظام المفتوح الصادرة عن المصارف في قطر وللسحب النقدي من نقاط البيع
- ويُفضل السماح للشركات المالية غير المصرفية (NBFCs) بإصدار أدوات الدفع بنظام شبه مغلق فقط، بما في ذلك أدوات الدفع المدفوعة مسبقاً باستخدام على الهاتف المحمول
- تخضع المصارف والمؤسسات المالية غير المصرفية وغيرها من الكيانات غير المصرفية المسموح لها بإصدار أدوات هدايا شبه مغلقة ومغلقة مسبقة الدفع، للشروط التالية:
  - يجب تحديد الحد الأقصى لصلاحية أدوات الهدايا المدفوعة مسبقا
  - يجب تحديد القيمة القصوى لكل أداة دفع من هذا القبيل
  - لا يجوز أن تكون هذه الأدوات قابلة لإعادة التحميل
  - لا يجوز السماح بالسحب النقدي لمثل هذه الأدوات
  - يجب الاحتفاظ بمستندات «اعرف عميلك» الكاملة لمشتريّ هذه الأدوات بأكثر من الحد المحدد مسبقاً.
  - يجب أن تحتفظ الجهة المصدرة بتفاصيل الأشخاص الذين صدرت لهم هذه الأدوات وإتاحتها عند الطلب. يجب أن تضمن الجهة المصدرة أيضًا الحصول على التفاصيل الكاملة للمستفيد النهائي من أجل تقديمها إلى الجهة التنظيمية أو الحكومة، عند الطلب
  - قد تتبنى الكيانات نهجًا قائمًا على المخاطر، معتمداً حسب الأصول قبل الإدارة العليا، في تحديد عدد تلك الأدوات التي يمكن إصدارها إلى العميل، وحدود المعاملة الخ
- يجب على المؤسسات التي تصدر أدوات الدفع المدفوعة مسبقاً أن تحتفظ بسجل يضم جميع المعاملات التي تتم باستخدام هذه الأدوات. يجب أن تكون هذه البيانات متاحة للتدقيق من قبل مصرف قطر المركزي أو أي وكالة / وكالات أخرى على النحو الذي قد تطلبه الحكومة / الجهة التنظيمية
- يتعين على الجهات المصدرة لأدوات الدفع المدفوعة مسبقاً توفير أنظمة وبنية تحتية كافية لأمن المعلومات والبيانات للوقاية من اكتشاف عمليات الاحتيال. ومن الضروري وجود قاعدة بيانات مركزية / نظام معلومات إدارة (MIS) لدى الجهة المصدرة لمنع شراء أدوات الدفع المتعددة في مواقع مختلفة، مما يؤدي إلى التحايل على الحدود المحددة لأدوات الدفع هذه، إن وجدت
- يجب على جميع الجهات المصدرة لأدوات الدفع المدفوعة مسبقاً الإفصاح عن جميع الأحكام والشروط الهامة بلغة واضحة وبسيطة (ويفضل أن تكون باللغتين العربية والإنجليزية) ومفهومة للمستهلكين أثناء إصدار الأدوات. تشمل هذه الإفصاحات:

- جميع الرسوم والمصاريف المرتبطة باستخدام الأداة
  - فترة الصلاحية والشروط والأحكام المتعلقة بانتهاء صلاحية الأداة
  - أرقام هواتف خدمة العملاء وعنوان URL لموقع الويب
- يطلب من الجهات المصدرة لأدوات الدفع المدفوعة مسبقاً الإبلاغ عن عمليات الاحتيال، إن وجدت، التي تتعلق بأدوات الدفع المدفوعة مسبقاً الصادرة من قبلها، وذلك على أساس ربع سنوي (أو أقل) إلى الحكومة / الجهة التنظيمية
- للحد من الخسائر المرتبطة بالتعرض للمخاطر، يجب على الجهات المصدرة لأدوات الدفع المدفوعة مسبقاً تنفيذ إجراءات وضوابط داخلية للكشف عن ومنع الاحتيال بما ينطبق على بيئة العمل
- يجب على الجهات المصدرة لأدوات الدفع المدفوعة مسبقاً تمكين آلية المصادقة للمستخدم قبل إجراء أي معاملات من خلال المحفظة الإلكترونية. يمكن التأكد من ذلك عن طريق إصدار رمز الحماية وكلمة مرور منيعة والقياسات الحيوية وغيرها
- يتعين على الجهات المصدرة لأدوات الدفع المدفوعة مسبقاً تعيين فرد أو مجموعة متخصصة في مراقبة عمليات الاحتيال لتوفير التوجيه الذي تحتاجه المؤسسة للتصدي لعمليات الاحتيال
- يجب على الجهات المصدرة لأدوات الدفع المدفوعة مسبقاً إجراء مراجعة أمنية سنوية للمحافظ الإلكترونية وفقاً لضوابط تتضمن، على سبيل المثال لا الحصر، ما يلي:
  - الضوابط العامة لتكنولوجيا المعلومات (إدارة التغيير وإدارة ضبط وصول المستخدم وإدارة الحوادث والمشاكل وإدارة التحديث والمعالجة وإدارة السجلات)
  - ضوابط معالجة الأعمال (السياسات والإجراءات التنظيمية وغيرها)
  - تقييم أمن التطبيقات (عبر الشبكة والهاتف المحمول)
  - مراجعة تهيئة الإعدادات الأمنية
  - مراجعة أمن البنية التحتية
  - الامتثال لأية معايير دولية مثل (TCG Framework) ، (NIST Cybersecurity Framework)

- **أفضل الممارسات للمستهلكين**
  - تمكين كلمات المرور على الأجهزة: يجب تمكين كلمات المرور المنيعة على الهواتف المحمولة والأجهزة اللوحية والأجهزة الأخرى الخاصة بالمستخدم قبل استخدام المحافظ الإلكترونية. يجب استخدام الطبقات الأمنية الإضافية التي توفرها هذه الأجهزة
  - استخدام اتصالات الشبكة الآمنة: من المهم أن تكون متصلاً فقط بالشبكات الموثوقة. تجنب استخدام شبكات (Wi-Fi) العامة. يجب استخدام اتصالات (Wi-Fi) الأكثر أمانًا وثقة، والتي تم تعريفها بأنها اتصالات "(WPA) أو (WPA2)"، والتي تتطلب استخدام كلمات مرور منيعة
  - تثبيت التطبيقات من المصادر الموثوقة: يجب على المستخدم التحقق من أن مزود المحفظة الإلكترونية يتمتع بسجل حافل من الأمن والموثوقية في التعامل مع البيانات المالية الحساسة بطريقة آمنة وموثوقة وملائمة وتوفير دعم العملاء (في حالة فقدان البطاقة أو الاحتيال في الحساب)
  - الحفاظ على أمن وثائق المصادقة اللازمة لتسجيل الدخول: تجنب تدوين المعلومات المستخدمة للوصول إلى المحافظ الرقمية في مكان ظاهر أو تخزينها في ملف غير محمي لتجنب سوء استخدامها
  - إنشاء كلمة مرور مميزة للمحفظة الإلكترونية: استخدام كلمة مرور مميزة يصعب تخمينها للمحفظة الرقمية لمنع مخاطر الوصول غير المصرح به إليها
  - البقاء على يقظة ووعي بحالة الاتصال عبر شبكة الهاتف المحمول، وقم بالتسجيل للتنبيهات من خلال الرسائل القصيرة والرسائل الإلكترونية

- تحديد نقاط الاتصال في حالة وقوع الأحداث الاحتيالية: بالنسبة لأي نشاط احتيالي يحدث على حساب المستخدم كما في سيناريوهات فقد الهاتف المحمول أوسرقته، فقدان بطاقة شخصية مخزنة في المحفظة أو اختراق الحساب، فعلى المستخدم أن يكون على علم بنقطة الاتصال المناسبة لمعالجة هذه القضية. يجب أن يفهم المستخدم فهماً كاملاً شروط وأحكام عقد مقدمي خدمة المحفظة الإلكترونية.

➢ أمن الشبكات

- **مراقبة الشبكة وضوابطها**

- يجب على المؤسسة أن تنسق أنشطة الإدارة تنسيقاً جيداً لتحسين الخدمات المقدمة إلى المؤسسة وضمان تطبيق الضوابط باستمرار على كل البنية التحتية لمعالجة المعلومات
- لا ينبغي تنفيذ اتصال شبكة مخصص بين شبكة المؤسسة وأي طرف خارجي إلا بعد معالجة المخاطر الناشئة عن الاتصال معالجة مناسبة. يجب تحديد هذه المخاطر من خلال إجراء فحوصات أمنية دورية لشبكة المؤسسة
- يجب على المؤسسة تقييد استخدام برنامج أداة النظام على الأنظمة الحية، مثل تلك التي تسهل الوصول عن بعد، أو تدير تسجيل الأحداث وسياسات المجموعة على مسؤولي النظام وموظفي خدمات الدعم الحاسوبية فقط. يجب الاحتفاظ بنسخ رئيسية من هذه البرامج بشكل آمن
- يجب أن تتأكد المؤسسة من أنه بالنسبة للأنظمة التي تقوم بتشغيل بروتوكولات إدارة الشبكة البسيطة (SNMP)، فإنه يجب تكوين بروتوكولات إدارة الشبكة البسيطة بشكل آمن، وتغيير كل سلسلة المجتمع الافتراضية من قبل المسؤول
- يجب أن تكون هناك تدابير أمنية مناسبة لحماية سرية وسلامة البيانات التي تمر عبر الشبكات العامة والشبكات المحلية والشبكات اللاسلكية وجميع الأنظمة والتطبيقات المتصلة. يجب منع استخدام البروتوكولات غير الآمنة مثل (ftp) و (telnet) منعاً باتاً
- يجب وضع جميع الأنظمة التي يكون من الضرورة الوصول إليها من الإنترنت، على سبيل المثال لا الحصر، خوادم البريد الإلكتروني وخوادم الويب والخوادم الوكيلة، ضمن المنطقة المحايدة (DMZ)
- يجب تدقيق جميع الأنظمة/ الموجهات التي تتعامل مع الإنترنت على فترات منتظمة وفقًا لمعايير أمن قياسية (benchmarked) لضمان ضبط الوصول إلى الشبكة بشكل سليم وسلامة البيانات المنقولة عبرها
- يجب تحديد المعايير التقنية المطلوبة للتوصيل الآمن مع خدمات الشبكة وفقاً لقواعد اتصال وأمن الشبكة
- يجب تطبيق تقنيات المصادقة والتشفير وضوابط اتصال الشبكة من أجل أمن خدمات الشبكة
- يجب إنشاء وتوثيق إجراءات استخدام خدمة الشبكة لتقييد الوصول إلى خدمات أو تطبيقات الشبكة، حسب الضرورة
- يجب التأكد من إزالة أو تعطيل جميع خدمات الشبكة غير المستخدمة أو غير المرغوب فيها داخل شبكة المؤسسة
- يجب الحفاظ على قائمة موثقة من الخدمات والمنافذ المطلوبة لأغراض الأعمال وتحديثها بانتظام
- يجب عدم السماح بعمليات تحميل وتنزيل الملفات غير الآمنة من / إلى الإنترنت
- يجب تقييم أي خدمة إنترنت جديدة لتقييم المخاطر المرتبطة بها والحصول على الموافقات الضرورية من الموظفين المعتمدين داخل المؤسسة قبل اعتماد أي خدمة من هذا القبيل. يجب أن تتضمن جميع الوصلات بين شبكة المؤسسة والإنترنت (الشبكة العامة) جدار حماية معتمد وآلية ضبط الوصول المصاحب له
- لضمان تثبيت الأنظمة وصيانتها بطريقة تمنع الوصول غير المصرح به والاستخدام غير المصرح به والأعطال، يجب تنفيذ عناصر الضبط التالية:
  - يجب تعزيز جميع الأنظمة التي تدعم العمليات التجارية وفقًا لأفضل الممارسات في هذا المجال قبل الاتصال بشبكة المؤسسة: مركز أمن الإنترنت؛ المعهد الوطني للمعايير والتكنولوجيا (NIST) ؛ ومعهد (SANS)

- يجب تهيئة أجهزة الشبكة مثل نقاط الوصول اللاسلكية وجدران الحماية وأجهزة التوجيه وغيرها وفق آخر تحديثاتها وفقًا لتهيئات الأمان الضرورية والمعمول بها
- يجب على المؤسسة النظر في تنفيذ نظام كشف التسلل/ نظام منع التطفل (IDS / IPS) فور توفير نظام الأمن الأساسي. يجب مراعاة الآتي أثناء تقييم نظام (IDS / IPS) والتوصية به:
  - اكتشاف جميع أنواع الهجمات الأمنية على النظام بما في ذلك الحرمان من الاستخدام والتنكر إلخ.
  - اكتشاف عمليات التطفل على الشبكة
  - مراقبة حركة مرور الشبكة والدفاع ضد الهجمات عن طريق مطابقة النمط ضد ملف نمط قابل للتحديث
  - يجب أن يكون النظام قادرًا على إنشاء تنبيهات مختلفة مثل: سجل الأحداث، البريد الإلكتروني، الفاكس، الصوت، النداء، تعريف المستخدم، وما إلى ذلك
  - يجب تغيير كلمة المرور على أساس منتظم
  - يجب إجراء نسخ احتياطي لأحدث نظم التشغيل (IDS / IPS) بشكل منتظم
  - يجب أن تقتصر نسخ ملفات التهيئة على الأفراد المصرح لهم
- يجب الحفاظ على جميع الوثائق الهامة التي تصف العمليات والإجراءات ذات الصلة لإدارة معدات الشبكة مثل أجهزة التوجيه والتبديل وجدران الحماية وضبطها بشكل ملائم. يجب أن تقوم المؤسسة بتوثيق وإجراء التحديثات اللازمة بشكل واضح لتعكس التغييرات في بنية الشبكة. يقتصر الوصول إلى وثائق هيكل الشبكة على الأفراد المصرح لهم فقط داخل المؤسسة
- يجب الاحتفاظ بتفاصيل تهيئة الشبكة بشكل آمن للتأكد من أنها متوفرة عند الحاجة، كما هو الحال في أوقات تعطل النظام. ويجب حمايتها لأنها تخزن معلومات هامة حول شبكة المؤسسة
- كما يجب أن تتضمن تفاصيل تهيئة الشبكة ما يلي:
  - مخططات الشبكة واسعة النطاق (WAN)
  - مخططات الشبكة الواسعة المحلية (LAN)
  - جهاز التوجيه والتبديل
  - تهيئة جدار الحماية
  - تفاصيل الجهاز
  - عناوين بروتوكول الإنترنت IP المستخدمة داخل المؤسسة
  - تفاصيل التهيئة الخاصة بأجهزة الشبكة المهمة الأخرى

- **المصادقة**

- يجب تطبيق آليات المصادقة المناسبة للمعدات الخاصة بالمستخدمين وأنظمة المعلومات المتصلة بشبكة المؤسسة. يجب تسجيل جميع أجهزة الكمبيوتر المحمولة التي تتصل بشبكة المؤسسة على النطاق الخاص بها
  - يجب عرض شعار التحذير عند تسجيل الدخول إلى أي نظام داخل شبكة المؤسسة
  - يجب استخدام النظام فقط من قبل المستخدمين المصرح لهم
  - يعتبر استمرار المستخدم في استخدام النظام إقراراً منه بأنه / أنها مستخدم مرخص
  - استخدام هذا النظام يشكل موافقة على المراقبة
- يجب ألا يشتمل الشعار على أي نظام أو معرّفات للتطبيقات، والتي يمكن أن توفر معلومات قيّمة لأي متطفل محتمل، على سبيل المثال: الأجهزة ونظام التشغيل على المضيف، أو معلومات حول المؤسسة أو الأمور الداخلية الأخرى
- يجب تمكين شعار التحذير لأجهزة الشبكة (أجهزة التوجيه والمفاتيح وغيرها) والخوادم

- **فصل الشبكة**
  - يجب على المؤسسات اتباع نهج قائم على المخاطر لإجراء الفصل بين الشبكات
  - يجب تقسيم أمن شبكة المؤسسة إلى نطاقات شبكة منطقية منفصلة، مثل: نطاقات الشبكة الداخلية ونطاقات الشبكة الخارجية وغيرها. كما يجب حماية كل نطاق من هذه النطاقات بمحيط أمان محدد. يجب تطبيق مجموعة من عناصر التحكم في نطاقات الشبكة المنطقية المختلفة لمزيد من فصل بيئات أمن الشبكة.
  - يجب تصميم شبكات المناطق المحلية الافتراضية (VLAN) ، بحيث يتم فصل الشبكات بشكل منطقي. وخلال تصميم شبكات (VLAN)، يجب التأكد من أن أنظمة المعلومات الحساسة / الحرجة معزولة عن الأنظمة الأخرى وأن تكون على شبكة محلية ظاهرية منفصلة، بناء على فصل البيانات والسرية ومتطلبات العمل الأخرى. يجب ضبط الوصول إلى شبكة (VLAN) هذه، ومنح حق الوصول إليها فقط على أساس الحاجة إلى المعرفة.
  - يجب تحديد مناطق الشبكة من أجل تصنيف مجموعة المستخدمين والخدمات وتقسيمها تبعاً لاعتبارات معينة مثل أهمية وحساسية الأعمال التجارية، وسلامة تكنولوجيا المعلومات، وتصنيف معلومات البيانات، ومستويات ثقة المستخدم، واتفاقيات الأعمال، والاعتبارات الأمنية. إن تحديد نطاق الشبكة يحد من تعقيد الخيارات المتاحة في منح الوصول إلى موارد الشبكة، كما أنه يُلبي غالبية الاحتياجات الأمنية. يجب تقسيم الشبكة إلى المناطق التالية:
    - المنطقة العامة - تكون المنطقة العامة مفتوحة بالكامل وتشمل الشبكات العامة مثل شبكة الإنترنت العامة، وشبكة الهاتف العامة المزودة بمفتاح، وغيرها من الشبكات والخدمات الأساسية لشبكة الجوال العامة. سيكون فرض القيود والمتطلبات صعباً أو مستحيلاً على هذه المنطقة لأنها خارج نطاق سيطرة المؤسسة. يجب تقوية أي أنظمة يتم تنفيذها أو التفاعل معها في المنطقة العامة ضد أي هجوم.
    - منطقة العمليات - منطقة العمليات هي البيئة القياسية التي تجري فيها المؤسسة عملياتها الروتينية. وهي البيئة التي يتم فيها تثبيت معظم أنظمة المستخدم النهائي وخوادم مجموعة العمل. ولكن، حتى مع وجود ضوابط أمان مناسبة في الأنظمة النهائية، تظل هذه المنطقة غير مناسبة للمستودعات الكبيرة للبيانات الحساسة أو التطبيقات المهمة، دون وجود ضوابط أمان إضافية قوية وجديرة بالثقة.
    - المنطقة المحظورة - يجب أن توفر المنطقة المحظورة بيئة شبكة مضبوطة، تتلاءم عمومًا مع خدمات تكنولوجيا المعلومات الهامة والحساسة (مثال: تلك التي لها متطلبات موثوقية متوسطة، حيث يؤدي اختراق خدمات تكنولوجيا المعلومات إلى تعطل الأعمال) أو المستودعات الكبيرة للمعلومات الحساسة (مثال: في مركز بيانات). يجب المصادقة على جميع كيانات طبقات الشبكة في المنطقة المحظورة، إما صراحةً من خلال تنفيذ خدمة مصادقة الكيان النظير أو ضمنيًا من خلال مزيج من الأمن المادي وضبط التهيئة. إن المنطقة المحظورة تقلل من تهديدات الأشخاص داخل النظام عن طريق الحد من الوصول ومن خلال المراقبة الإدارية.
    - منطقة الوصول الخاصة - يجب أن تكون منطقة الوصول الخاصة بيئة شبكة مضبوطة بإحكام بما يناسب احتياجات المعالجة الخاصة. يجب تطوير متطلبات منطقة الوصول الخاصة على أساس كل حالة على حدة لتلبية احتياجات المعالجة الخاصة للبيئة. على سبيل المثال، قد يحتاج فريق يعمل على مشروع بحثي سري إلى إنشاء منطقة وصول خاصة.
    - المنطقة المحايدة - يجب على المؤسسة الحد من الوصول إلى البيانات والأنظمة الواردة من الإنترنت. يجب تنفيذ هذا الحد من خلال استخدام منطقة محايدة (DMZ)، وهي جزء من بنية جدار الحماية. ويجب ألا يمنح الجمهور، في أي حال من الأحوال، إمكانية الوصول للدخول إلى البيانات مباشرة على الخوادم الموجودة على الشبكة الموثوقة الخاصة بالمؤسسة، والتي توجد داخل نظام جدار الحماية. عند الاستجابة لطلب لمنطقة محايدة، فإن من الأشياء التي يجب أخذها في الاعتبار: انخفاض طفيف في الأداء، وانخفاض مستوى الوصول إلى المهاجم.

- **أمن الشبكات**
  - يجب أن يقتصر الوصول المنطقي إلى الشبكة على المستخدمين المصرح لهم فقط، للتأكد من أنه يمكن فقط للمستخدمين المسموح لهم الوصول إلى أجزاء الشبكة والخدمات
  - يعتبر التعرف التلقائي على المعدات وسيلة لمصادقة الاتصالات من مواقع ومعدات محددة
  - يجب ضبط الوصول إلى منافذ التشخيص داخل المؤسسة بشكل آمن
  - يجب ضبط الوصول إلى أدوات التحكم في النظام المحلية (مثل ملفات Batch ونصوص Unix وغيرها). يقتصر الوصول إلى هذه الأدوات على الموظفين المصرح لهم فقط
  - بخلاف القائمة المعيارية للخدمات والمنافذ، إذا كانت هناك أي حاجة لتمكين أي خدمة أخرى أو منفذ آخر على الخادم وفقًا لمتطلبات العمل، فيجب اتباع عملية إدارة التغيير بحيث يكون تنفيذه خاضعاً للموافقة والاختبار، بالإضافة إلى مراعاة الضوابط الضرورية/ البديلة، إذا لزم الأمر
  - يجب توثيق تفاصيل هذا الاختبار وعملية الموافقة
  - كممارسة جيدة، يجب إجراء تقييم للمخاطر قبل السماح بتدفق المعلومات بين أنظمة معلومات الأعمال المختلفة أو منح الوصول إلى أي طرف ثالث
  - يجب تطبيق التسجيل والمراقبة المناسبين لتمكين تسجيل وكشف الأفعال التي قد تؤثر على، أو تكون على صلة، بأمن المعلومات. يجب تسجيل جميع الإجراءات والتي تشمل، على سبيل المثال لا الحصر، تسجيل الدخول / الخروج من الحسابات الإدارية أو واجهة جهاز التوجيه أو الربط لأحداث جيدة/ سيئة، وأحداث بدء / إيقاف تشغيل النظام، ومسارات التدقيق، ومحاولات الهجوم، تسجيلاً سليماً كاملاً
  - يجب تأمين ملفات السجل من الوصول أو التعديل غير المصرح به. يجب إجراء مراجعة منتظمة لملفات السجل لتحديد أي نشاط خبيث أو غير طبيعي
  - يجب تنفيذ ضوابط الأمن التالية (مثل الضوابط التقنية، العقود / الاتفاقيات) في تبادل المعلومات التجارية مع أصحاب المصلحة
    - يتم توفير المكالمات الهاتفية والبريد الصوتي والفاكسات والمحادثات عن بعد وأي أنظمة اتصالات سرية أخرى من قِبل المؤسسة بغرض استخدامها فيما يتعلق بعمل المؤسسة، ويحظر أي استخدام آخر باستثناء الاستخدام الشخصي المعقول وفي حالات خاصة
    - يجب حماية جميع المعلومات المنقولة، من خلال الإنترنت كوسيلة النقل، بين شبكة المؤسسة وشركائها / أطراف ثالثة، حماية كافية باستخدام تقنية تشفير معتمدة
  - يجب على المؤسسة تحديد وتسجيل جميع مكونات الشبكة لديها مع التفاصيل في قائمة الموجودات
  - يجب على المؤسسة تقييم وتنفيذ الضوابط اللازمة للحد من استخدام مكونات الشبكة
  - يجب تأمين الوصول إلى وظائف معالجة المعلومات الحساسة من خلال الحد من المحطات التي يمكن من خلالها تنفيذ هذه الوظائف وتقييد هذه المحطات مادياً و / أو منطقيًاً

- **سجل الشبكة**
  - يجب أن تحتفظ المؤسسة بسجل لجميع محاولات الدخول الناجحة وغير الناجحة، ويجب مراجعة سجل هذه المحاولات مراجعة دورية من قبل مسؤولي النظام داخل المؤسسة
  - يجب على المؤسسة أن تقيد إمكانية الوصول إلى المرافق التي تعيد تشكيل آليات التسجيل على المستخدمين المصرح لهم فقط
  - يجب على المؤسسة أن تحدد وتنفذ عملية لمراقبة السجلات التي يتم جمعها مراقبة دورية
  - يجب حماية ملفات السجل من الوصول إليها أو تعديلها أو حذفها من قبل المستخدمين غير المصرح لهم إما عن طريق تشفير السجلات أو من خلال تحديد مستويات الوصول
  - يجب تنفيذ برنامج مراقبة سلامة السجلات واكتشاف التغيير عليها، لضمان تعذر تغيير بيانات السجل الحالية دون صدور تنبيهات بذلك

- يجب الاحتفاظ، بصورة منتظمة، بنسخ احتياطية من المستندات التي يحتاجها التدقيق، وتخزينها في موقع مقيد الوصول إليه

➢ أمن البنية التحتية

- **أمن دفاع المحيط FA27 2F94 998D FDB5 DE3D F8B5 06E4 A169 4E46**
  - يجب على المؤسسة تحديد هيكل الشبكة وضمان حمايته حماية كافية
  - ويجب عليها تطبيق التسجيل الذكي بالمستوى الذي يؤمن تعقب أي هجوم
  - يجب على المؤسسة صياغة عملية لتتبع عمليات الاقتحام، إن وجدت، وتحليلها تحليلاً مفصلاً لاتخاذ إجراءات تصحيحية لهيكل البنية التحتية الأمنية
  - يجب أن تحتفظ المؤسسة بوثائق مفصلة لتهيئات الفلتر (الموجه والوكيل) وأن تتبع عملية إدارة التغيير لإدخال أية تغييرات على التهيئات
  - يجب على المؤسسة تثبيت الفلاتر المناسبة. فيما يلي مراجع للمؤسسة:
    - يمنع رقم قائمة الوصول أي (ICMP) أي إعادة توجيه لمنع حزم (ICPM)
    - مكافحة الانتحال لضبط الوصول من خلال جهاز التوجيه قد توقف الحزم مع عنوان المصدر من خلال عناوين (IP) داخلية من الوصول
  - يجب على المؤسسة ضبط ومراقبة تهيئات الفلتر من حيث الامتيازات واستخدامها، ومن يستطيع التعديل ومن قام بالتعديل ومتى أجري التعديل ولماذا تم التعديل وما إلى ذلك
  - يجب على المؤسسات إجراء تقييم المخاطر قبل تشغيل أي جهاز في الشبكة. يجب الإبلاغ عن المخاطر التي يتم التعرف عليها إلى الإدارة
  - يجب على المؤسسة إعداد آلية لتحديث الفلاتر كلما تطلب الأمر تنفيذ تغييرات في الشبكة، أو تثبيت إصدارات برامج جديدة، لمنع الهجمات المستقبلية التي قد تستغل نقاط الضعف الموجودة أو التي تم اكتشافها حديثًا
  - يجب على المؤسسة تهيئة برنامج مكافحة الفيروسات للمسح في الوقت الحقيقي على البوابة
  - يجب اختبار هذه الفلاتر بشكل دوري، واختبار الفواصل للتأكد من أن القواعد لا تزال تعمل
  - يجب إجراء تقييم دوري لأمن الشبكة مثل تقييم مدى التعرض للمخاطر، واختبار الاختراق وما إلى ذلك

- **أمن نظام التشغيل وخادم التطبيق**
  - يجب على المؤسسات تقييم نظام التشغيل وقاعدة البيانات تقييماً دورياً قياساً على الضوابط العامة لتكنولوجيا المعلومات وغيرها من ضوابط مستوى النظام
  - يجب أن تخضع حقوق الوصول المنطقي (القراءة / الكتابة / التعديل) لرقابة صارمة، ويجب إتاحة الوصول إليها فقط بعد الحصول على الموافقات المناسبة من مالك نظام المعلومات أو الإدارة العليا.
  - يجب إصدار حقوق الوصول على أساس «الامتيازات الأقل»
  - يجب على المؤسسة التأكد من أن خوادمها آمنة ماديًا. يجب أن يقتصر الوصول المادي على الأفراد المصرح لهم فقط. إذا كان هناك مستخدمون غير مصرح لهم يحتاجون إلى الوصول المادي إلى خادم الشبكة أو الاقتراب منه، فيجب أن يتم اصطحابهم بواسطة موظفين مخولين
  - يجب على المؤسسة تنفيذ ورصد متطلبات إجراء التدقيق بمسارات محددة لتحديد مخالفات الوصول المادي أو الوصول غير المصرح به
  - يجب وضع جميع الخوادم (أنظمة التشغيل وخوادم التطبيقات وخوادم الويب وخوادم البريد) في شبكة المؤسسة في منطقة آمنة توفر عناصر تحكم بيئية ملائمة، بما في ذلك التهوية تكييف الهواء، ومزودة بوحدة حماية الطاقة غير المنقطعة (UPS) ووحدة تكييف الهواء وإطفاء الحرائق

- يجب على المؤسسة إدارة ومراقبة خوادمها بطريقة ملائمة وترددات محددة
- يجب على المؤسسة أن تأخذ بعين الاعتبار الممارسات التالية لتأمين أجهزة الخادم الخاصة بها:
  - تجنب استخدام وحدات تحكم الخادم قدر الإمكان
  - مطابقة توافق الأجهزة أثناء شراء / تثبيت الخادم
  - تعطيل ميزة الإقلاع عبر القرص المضغوط أو القرص المرن
- يجب إعداد التهيئة الملائمة لضبط الوصول ووضعها على جميع أجهزة الشبكة ذات إمكانية تسجيل الدخول عن بُعد
- يجب وضع أجهزة الشبكة، إن أمكن، داخل خزانة شبكة مناسبة أو خزانة اتصالات أو في غرفة خادم معينة
- يجب تعطيل هويات المستخدم الافتراضية
- يجب مراقبة استخدام كلمات المرور الافتراضية مراقبة صارمة
- يجب مراقبة أنشطة حساب النظام

- **أمن المضيف**
  - تقييم المخاطر: يجب على المؤسسة إجراء تقييم للمخاطر الأمنية فيما يتعلق بجميع عناصر بنيتها التحتية. ستحدد تقييمات المخاطر التدابير الأمنية المضادة المناسبة اللازمة للحماية من الانتهاكات المحتملة في السرية والسلامة والوفرة
  - الأمن المادي والبيئي: يجب وضع جميع معدات المؤسسة في بيئة محكومة وآمنة
    - يجب وضع المعدات الهامة أو الحساسة للبنى التحتية في مناطق آمنة ومحمية بمحيط آمن مع وجود حواجز أمنية مناسبة وضوابط دخول
    - يجب وضع المعدات الهامة أو الحساسة للبنية التحتية في بيئة قابلة للتحكم من ناحية درجة الحرارة والرطوبة وإمدادات الطاقة
    - يجب أن تتأكد المؤسسة من تسجيل دخول وخروج جميع الزوار الذين يمكنهم الوصول إلى مناطق البنية التحتية. سيحتوي السجل على الاسم والمنظمة والغرض من الزيارة والتاريخ ووقت الدخول والخروج
    - يجب على المؤسسة التأكد من أن جميع الموظفين المسؤولين على علم بإجراءات الزوار، وأن يتم مراقبة الزوار، عند الضرورة
  - الوصول إلى الشبكة: يجب توفير الوصول إلى البنية التحتية داخل المؤسسة عبر إجراءات تسجيل دخول آمنة، مُصممة لتقليل فرصة الوصول غير المصرح به
  - يجب أن يكون لدى المؤسسة إجراءات رسمية وموثقة للتسجيل وإلغاء التسجيل للوصول إلى الشبكة
  - النسخ الاحتياطي للبيانات واستعادتها: يجب أن تتأكد المؤسسة من تسجيل معلومات التهيئة الضرورية للسماح باستعادة الأنظمة الأساسية
  - فيما يلي بعض الخصائص الأساسية المتعلقة بأمن محطة العمل
    - صياغة سياسة وصول المستخدم وتنفيذها
    - تحديث ملفات المعالجة (patches)/ الإصلاحات العاجلة (hotfixes) لنظام تشغيل وتطبيقات محطة العمل
    - الحد من الوصول إلى موارد الشبكة من محطات العمل. التعيين على أساس «المطلوب فقط».
    - تثبيت برنامج مكافحة الفيروسات وتحديثه بانتظام على جميع محطات العمل
    - التأكد من إدخال بيانات محطة العمل في سياسة النسخ الاحتياطي والجدول الزمني للمؤسسة
- التعافي من الكوارث: من أجل التخفيف من تأثير فقد الاتصال المحلي أو الكلي للشبكة، وتسهيل التعافي السريع لخدمات الشبكة في حالة وقوع كارثة، تطلب المؤسسة تطبيق ما يلي على جميع مرافق الحوسبة:
  - يجب توثيق الخطط، وتطوير إجراءات الاستجابة والتعافي والموافقة عليها، بما يوضح كيفية قيام المؤسسة بإدارة أي حدث مدمر والحفاظ على استمرارية أعمالها إلى مستوى محدد مسبقًا، وفق الأهداف المعتمدة من الإدارة

- يجب على المؤسسات تحديد متطلبات الأعمال من إتاحة البيانات
- يجب إعداد نسخة احتياطية بشكل روتيني عن جميع البيانات التي تعتبر «هامة/حساسة» لتشغيل المؤسسة ككل، أو للخدمات المقدمة من قبل إدارة معينة، من قبل الطرف المسؤول عن تلك البيانات، مع تخزين ملفات الأرشيف خارج الموقع على فترات منتظمة
- يجب اختبار البيانات المنسوخة بشكل دوري للتأكد من أن الوسائط وإجراءات الاستعادة تعمل، وأن البيانات يمكن استرجاعها فعلياً

- **إدارة السحابة**
  - يخضع استخدام الخدمات السحابية لأغراض العمل لإصدار تفويض رسمي من المؤسسة.
  - يجب إخضاع مورد خدمات السحابة لإجراءات العناية الواجبة قبل تعيين مزوّد الخدمة.
  - يجب أخذ الموافقات اللازمة من جميع الموظفين داخل المؤسسة فيما يتعلق بالأمن والخصوصية وجميع متطلبات إدارة تكنولوجيا المعلومات الأخرى، التي يجب معالجتها معالجة كافية من قبل مورد الحوسبة السحابية
  - بالنسبة لأي خدمات سحابية تتطلب من المستخدمين الموافقة على شروط الخدمة، يجب مراجعة هذه الاتفاقيات والموافقة عليها من قبل إدارة المؤسسة
  - يجب أن يتوافق استخدام مثل هذه الخدمات مع سياسة الاستخدام المقبول / سياسة استخدام الكمبيوتر / سياسة استخدام الإنترنت / ساسة إحضار جهازك الخاص (BYOD)
  - يجب أن تحدد المؤسسة المخاطر المتعلقة بعدم الامتثال للتوجيهات الداخلية وقوانين ولوائح التجارة الإلكترونية في قطر ولوائح مركز قطر للاستجابة لطوارئ الحاسب الآلي (كيوسيرت)، والتي قد تؤدي إلى فرض غرامات أو تشويه السمعة أو خسائر أخرى
  - يجب أن تحدد المؤسسة المخاطر المتعلقة بتغيير مستوى السيطرة في الحوكمة الأمنية
  - يجب أن تحدد المؤسسة المخاطر المتعلقة بتقديم الخدمة والاستمرارية وكذلك الضوابط الدفاعية مثل الحماية من البرمجيات الخبيثة وإدارة نقاط الضعف والحرمان من الخدمة وحماية البيانات بسبب الأعطال ونقص العمليات والضوابط والمنهجية وما إلى ذلك
  - يجب تقديم برامج التدريب والتوعية التي تُركز على إدارة الخدمات السحابية والمخاطر المرتبطة بها إلى جميع مسؤوليّ الخدمات السحابية والمستخدمين والموظفين المسؤولين والمقاولين. ويجب أن تشمل برامج التدريب والتوعية ما يلي:
    - معايير وإجراءات استخدام الخدمات السحابية
    - مخاطر أمن المعلومات ذات الصلة بالخدمات السحابية وكيفية إدارة هذه المخاطر
    - مخاطر بيئة النظام والشبكة المتعلقة باستخدام الخدمات السحابية
    - الامتثال القانوني والتنظيمي المعمول به
  - يجب أن توضح قوائم الجرد في المؤسسة تفاصيل كمية أصول المعلومات والأصول المرتبطة بها المخزنة في بيئة الحوسبة السحابية. يجب أن توضح السجلات الموقع الذي يتم فيه الاحتفاظ بالأصول، أي، بعبارة أخرى، تحديد الخدمة السحابية
  - يجب أن تتأكد المؤسسة من تسمية المعلومات والأصول المرتبطة بها المحفوظة في بيئة الحوسبة السحابية وفقاً لإجراءات المؤسسة المعتمدة للتسمية
  - يجب على المؤسسة تحديد متطلباتها لتسجيل الأحداث والتحقق من أن الخدمة السحابية تلبي هذه المتطلبات
  - في حالة تم تفويض عملية مميزة إلى المؤسسة، فإنه يتم تسجيل تشغيل هذه العملية وأدائها. ويجب أن تحدد المؤسسة ما إذا كانت إمكانيات التسجيل التي يوفرها مزود الخدمة السحابية ملائمة أم أن عليها توفير إمكانات تسجيل إضافية

- يجب على المؤسسات صياغة وتنفيذ خطط إدارة الطاقة الاستيعابية
- يجب على مزودي الخدمات السحابية توفير طاقة استيعابية كافية للوفاء بمتطلبات السعة المطلوبة والأداء المتفق عليها
- يجب تحديد البيانات السحابية التي سيتم نسخها احتياطياً مع تحديد وتيرة النسخ ومدة الاحتفاظ من قبل المؤسسات
- يجب على المؤسسة، إذا لزم الأمر، تنفيذ ضوابط تشفير لاستخدام الخدمات السحابية، بعد إجراء تقييم للمخاطر. يجب أن تكون الضوابط قوية بما يكفي للحد من المخاطر المحددة، سواء تم تطبيق تلك الضوابط من قبل المؤسسة أو من قبل مقدم الخدمة السحابية
- يجب على المؤسسة تحديد مفاتيح التشفير لكل خدمة سحابية، ووضع إجراءات مناسبة لإدارة المفاتيح
- يجب أن تتأكد المؤسسة من أن الوصول إلى المعلومات في الخدمة السحابية سيكون مقيدًا وفقًا لسياستها لضبط الوصول. ويتضمن ذلك تقييد الوصول إلى الخدمات السحابية، ووظائف الخدمات السحابية، وبيانات المؤسسة التي يتم الاحتفاظ بها في الخدمة السحابية

- **التكامل مع التاجر والبنوك**
  - يُوصى بأن تلتزم المؤسسات بمتطلبات (PCI DSS) عند تنفيذ الاندماج مع التجار والبنوك
  - يجب أن تأخذ المؤسسة النقاط التالية في الاعتبار أثناء دمج منصاتها/ أنظمتها مع التجار والبنوك:
    - تقنية التشفير المستخدمة من قبل بوابات الدفع
    - استخدام عنوان بروتوكول IP الديناميكي
    - استخدام جدران حماية متينة بما فيه الكفاية لتكون فعالة دون التسبب في إزعاج حاملي البطاقات أو الموردين
    - استخدام التوقيعات الرقمية
  - يجب على المؤسسة تطبيق تدابير قوية لمراقبة الوصول في الأنظمة المدمجة
  - يجب على المؤسسة مراقبة واختبار شبكاتها بانتظام
  - يجب على المؤسسة امتلاك برنامج لإدارة نقاط الضعف وأن تقوم بعمليات مسح دورية ومن ثم تنفيذ المعالجات والأعمال التصحيحية اللازمة
  - تدابير أمنية إضافية للمؤسسات
  - البرمجيات الخبيثة: يجب على المؤسسة التأكد من وجود إجراءات تقنية كافية للحد من مخاطر اقتحام البرمجيات الخبيثة. يجب تدريب جميع المستخدمين وتوعيتهم بمسؤوليتهم تجاه عدم القيام بأي أفعال قد تؤدي إلى دخول برمجيات خبيثة إلى النظام
  - فقدان البيانات: يجب على المؤسسة التأكد من وجود إجراءات تقنية كافية للحد من مخاطر فقدان البيانات. يجب تدريب جميع المستخدمين وتوعيتهم بمسؤوليتهم فيما يتعلق بفقدان البيانات
  - نقاط ضعف اليوم الصفري: يجب على المؤسسة التأكد من وجود إجراءات تقنية كافية للحد من مخاطر نقاط الضعف المكتشفة للتو والتي لم تعالج بعد
  - البرامج غير المصرح بها: يجب على المؤسسة التأكد من وجود إجراءات تقنية كافية للحد من مخاطر البرامج غير المصرح بها. يجب تدريب جميع المستخدمين وتوعيتهم بمسؤوليتهم فيما يتعلق بالبرامج غير المصرح بها
  - التهيئة الخاطئة للنظام: يجب على المؤسسة التأكد من وجود إجراءات تقنية وتشغيلية كافية للحد من المخاطر الناجمة عن التهيئة الخاطئة للأنظمة
  - أي مخاطر أخرى يتم تحديدها: يجب على المؤسسة أن تتأكد، حسب الاقتضاء، من تطبيق تدابير تقنية لاكتشاف أي مخاطر أخرى وحماية أنظمة البنية التحتية الخاصة بها عند تحديد تلك المخاطر

➢ إدارة نقاط الضعف

- **إدارة نقاط الضعف**
  - يجب على المؤسسات تحديد وتنفيذ إطار عمل لإدارة نقاط الضعف يغطي جميع الأنظمة الداخلية والخارجية
  - يجب على المؤسسات تطبيق دورة تقييم الثغرات، التي تشمل المراحل التالية:
    - مرحلة الإعداد: لتحديد وتصنيف أصول تكنولوجيا المعلومات لدى المؤسسة
    - مرحلة المسح الأولي: لفحص جميع نقاط الضعف الموجودة في شبكاتها وأجهزتها وأنظمتها
    - مرحلة الإصلاح: لتحديد أولويات الإصلاح على أساس المخاطر
    - مرحلة تنفيذ إجراء الإغلاق: لتثبيت ملف التصحيح أو تثبيت الترقيات اللازمة للأنظمة
    - مرحلة إعادة المسح: لإعادة الفحص والتحقق من تخفيف المخاطر
  - يمكن للمؤسسات الرجوع إلى المبادئ التوجيهية الصادرة عن المعهد الوطني للمعايير والتكنولوجيا (NIST) ومشروع (OWASP) وغيرها لإجراء عمليات المسح هذه
  - يجب أن تحتفظ المؤسسات بجرد كامل وحديث للأصول يضم معلومات محددة مثل تفاصيل مورد البرامج / الأجهزة، وأرقام الإصدارات، وحالة التشغيل الحالية (على سبيل المثال: ما هي البرامج المثبتة على الأنظمة أو الأجهزة التي يتم تشغيلها) والشخص (الأشخاص) داخل المؤسسة المسؤول عن البرامج الخاصة بالإدارة الفعالة لنقاط الضعف التقنية
  - يجب أن تتخذ المؤسسات الإجراءات المناسبة وفي الوقت المطلوب للتصدي لنقاط الضعف التقنية المحتملة التي تم تحديدها في أنظمتها وشبكاتها
  - يجب على المؤسسة صياغة وتحديد الأدوار والمسؤوليات المتعلقة بإدارة نقاط الضعف التقنية
  - يجب أن تشمل نقاط الضعف رصد مدى التعرض للمخاطر، وتقييم مخاطر التعرض، وتصحيح الأخطاء، وتتبع الأصول وأي مسؤوليات تنسيق مطلوبة
  - يجب تحديد الجداول الزمنية اللازمة للاستجابة لإخطارات نقاط الضعف التقنية المحتملة
  - تصنف نقاط الضعف على مستويات شدة مرتفعة أو متوسطة أو منخفضة على أساس عوامل متعددة مثل نطاق المدى والتأثير على النظام والمخاطر المرتبطة بنقاط الضعف وغيرها
  - يجب على المؤسسات تحديد وتنفيذ عملية تضمن تحديد نقاط الضعف خلال دورة تطوير البرمجيات، وأن تتأكد من اشتمال جميع التغييرات الرئيسية عنصراً من عناصر إدارة مواطن الضعف
  - يجب على المؤسسات وضع إجراءات لمعالجة الحالات التي يتم فيها تحديد نقطة الضعف، ولكن لا يوجد إجراء مضاد مناسب لها. في مثل هذه الحالات، يجب على المؤسسة تقييم المخاطر المتعلقة بنقطة الضعف المحددة، وتحديد إجراءات الكشف اللازمة والإجراءات التصحيحية المناسبة

- **سجل التدقيق**
  - يجب الاحتفاظ بسجل تدقيق لجميع الأنشطة المنفذة، ويجب الاحتفاظ بالسجلات اللازمة لضمان فعالية وكفاءة عملية إدارة نقاط الضعف

- **إدارة ملفات التصحيح (patch)**
  - يجب على جميع المؤسسات أن تحدد إطار عمل، وأن تقوم بتوثيق السياسات المعمول بها
  - تنفيذ جدول ملف التصحيح الذي يتضمن: الإخطارات الاستشارية والجدول الزمني لتقديم المشورة بشأن التخفيف المخاطر من تاريخ إصدار الشركة المصنّعة للمعدات الأصلية (OEM)، والاستثناءات المطلوبة قبل تنفيذ عمليات التصحيح، والتقارير الدورية عن إدارة التصحيح داخل المؤسسة
  - يجب على المؤسسات صياغة معايير لتصنيف درجات الخطورة لملفات التصحيح. سيساعد هذا على تحديد مدى الحاجة لمعالجة نقاط الضعف وتفعيل التحديثات ذات الصلة

- يجب اتباع عملية إدارة التغيير قبل تشغيل ملفات التصحيح على الأنظمة الحية. يجب أن يتضمن ذلك تحليل التأثيرات على التطبيقات/ الأجهزة الرفع والتنزيل، وخطة الاستعادة، وخطة النسخ الاحتياطي، والجدول الزمني للتنفيذ المحدد مسبقًا، وخطة التوقف المعتمدة وإخطار التوقف إلخ
- يجب تقييم المخاطر المرتبطة بتثبيت ملف التصحيح (يجب مقارنة المخاطر التي فرضتها نقاط الضعف مع مخاطر تثبيت ملف التصحيح)
- يجب اختبار ملفات التصحيح وتقييمها قبل تثبيتها للتأكد من فعاليتها وأنه لن ينتج عنها آثار جانبية غير مقبولة؛ وإذا لم يتوفر ملف التصحيح، فيجب التفكير في ضوابط أخرى، مثل:
  - إيقاف تشغيل الخدمات أو الإمكانيات المرتبطة بنقاط الضعف الأمنية
  - تكييف أو إضافة ضوابط الوصول، مثال: جدران الحماية على حدود الشبكة
  - زيادة المراقبة للكشف عن الهجمات الفعلية
  - زيادة الوعي بنقاط الضعف

- **تقييم أمني آخر**
  - اختبار الاختراق هو محاولة لتقييم أمن البنية التحتية لتكنولوجيا المعلومات من خلال محاولة استغلال نقاط الضعف بطريقة آمنة. وقد توجد نقاط الضعف هذه في أنظمة التشغيل والخدمات وعيوب التطبيقات وعمليات التهيئة الخاطئة أو سلوك المستخدم النهائي المحفوف بالمخاطر
  - يوفر اختبار الاختراق صورة عن النظام في حالة محددة في وقت محدد. تقتصر الصورة على أجزاء النظام التي تم اختبارها فعليًا أثناء محاولة (محاولات) الاختراق
  - يجب على المؤسسات إجراء اختبارات الاختراق الدورية للشبكة والخوادم وقواعد البيانات، من شبكة خارجية لتحديد نقاط الضعف الموجودة
  - يجب على المؤسسات تحليل جميع نقاط الضعف وإرسالها إلى خبراء المجال التقني داخل المؤسسة للحصول على توصيات الإصلاح ولتحديد الإيجابيات الكاذبة (يجب تقديم مبررات للإيجابيات الكاذبة)
  - بمجرد تفعيل ملف الإصلاح، يجب على خبراء المجال التقني داخل المؤسسة تقديم تأكيد خلال الفترة الزمنية المحددة في خطط المعالجة الموضوعة من قبل المؤسسة
  - يجب على المؤسسات إجراء عملية إعادة مسح للتحقق من صحة معالجة نقاط الضعف ومشاركة نتائج إعادة المسح مع مالكي النطاقات التقنية، وقد تقوم أيضاً بمشاركتها مع الإدارة في وحداتها، حسب الاقتضاء
  - يجب على المؤسسات إجراء مراجعة دورية للتهيئة والتأكد من أن تهيئة النظام تتماشى مع ممارسات الأمن الرائدة
  - يوصى بأن تقوم المؤسسات، بصورة دورية، بإجراء التقييم الأمني للتطبيقات على التطبيقات الهامة/الحساسة

➢ إدارة السجلات

- **مراقبة السجلات**
  - يجب إعداد سجلات الأحداث التي تسجل أنشطة المستخدم والاستثناءات والأعطال وأحداث أمن المعلومات، وتخزينها بصورة آمنة
  - يجب على المؤسسات صياغة وتنفيذ إجراءات وضوابط تقنية لحماية مرافق التسجيل، ويجب حماية معلومات السجلات من العبث والوصول غير المصرح به إليها

- يجب أن تتضمن سجلات الأحداث، حسبما تقتضيه الحاجة، ما يلي: هويات المستخدم وأنشطة النظام والتواريخ والأوقات وتفاصيل الأحداث الرئيسية، مثال: تسجيل الدخول وتسجيل الخروج؛ هوية الجهاز أو موقعه، إذا أمكن، ومعرف النظام؛ سجلات محاولات الوصول الناجحة والمرفوضة من قبل النظام؛ سجلات البيانات الناجحة والمرفوضة ومحاولات الوصول إلى الموارد الأخرى؛ والتغييرات على تهيئة النظام، استخدام الامتيازات واستخدام أدوات وتطبيقات النظام؛ الملفات التي تم الوصول إليها ونوع الوصول؛ وعناوين الشبكة والبروتوكولات والإنذارات التي أثارها نظام ضبط الوصول؛ تنشيط وإلغاء تفعيل أنظمة الحماية مثل أنظمة مكافحة الفيروسات وأنظمة كشف التسلل، وسجلات المعاملات التي ينفذها المستخدمون في التطبيقات. وينبغي النظر في المجموعة التالية من الإمكانيات التقنية للتأكد من أن إدارة السجل تغطي جميع الضوابط أدناه:
  - مراقبة الملفات التي تتطلب امتيازات أعلى
  - إمكانيات عمليات نظام المكافحة
  - تثبيت برامج غير مصرح بها أو من المحتمل أن تكون ضارة (برنامج الوصول من الباب الخلفي وحصان طروادة وغيرها)
  - تعديل أو حذف المعلومات الحساسة
  - استغلال نقاط الضعف لاكتساب امتيازات أعلى أو مختلفة
- يجب تصنيف جميع السجلات ومراجعتها. فيما يلي بعض الأمثلة للرجوع إليها:
  - في حالة نظام تشغيل ويندوز: سجلات النظام الخاصة بالأخطاء والتحذيرات لأعطال الأجهزة. يجب مراجعة السجل الأمني لمحاولات النجاح والفشل.
  - في حالة عدم وجود نظام تشغيل ويندوز: مراجعة سجلات نشاط المسؤول وسجلات المصادقة وسجلات الأخطاء الموجودة في الدليل / (logs) / (var) وسجلات بدء التشغيل والإيقاف وسجلات التدقيق وما إلى ذلك
  - سجلات أجهزة الشبكة: المراجعة الدورية للسجلات من جدار الحماية، ونظام اكتشاف/ منع التطفل، الذي يلتقط التفاصيل التالية:
    ١. الحزم الواردة والصادرة
    ٢. معلومات حول خوادم معينة مثال: خادم الويب
    ٣. سجلات التدقيق، ومحاولات الدخول المصرح بها وغير المصرح بها
    ٤. نشاط المسؤول - سجلات المستخدم المميزة للتغييرات في النظام، على سبيل المثال، إضافة / حذف المساروأي تغييرات أخرى في التهيئة
    ٥. الحزم التي تم إسقاطها
    ٦. التجسس على النظام
    ٧. السجلات الهامة التي تم إنشاؤها بواسطة الأجهزة (التنبيهات على الحزم المشبوهة، تحديد المجسات، إحصائيات الهجوم)
  - سجلات خادم التطبيق: يجب مراجعة المجموعة التالية من السجلات الخاصة بخوادم التطبيقات المختلفة مراجعة دورية:
    ١. سجلات خادم الويب: مثال: سجلات الأخطاء، سجلات الوصول
    ٢. سجلات خادم البريد: مثال: حالة الاتصال، قوائم انتظار (SMTP)، حالة البروتوكول (SMTP ،POP3)
    ٣. سجلات خادم (FTP): مثال: عمليات تسجيل الدخول الحالية، الأوامر المنفذة، الملف الذي تم تحميله وتنزيله
    ٤. سجلات خادم قاعدة البيانات: مثال: سجلات نشاط المستخدم، سجلات التدقيق للوحدة الخلفية (إنشاء الجدول، الحذف، التعديل، البحث، إلخ.)، الوصول إلى الأشكال
- قد تحتوي سجلات الأحداث بيانات حساسة ومعلومات تعريف شخصية. يجب اتخاذ تدابير حماية الخصوصية المناسبة.

- **التخزين**
  - تمثل السجلات محافظ السجل الأساسي لأنشطة النظام والشبكة. وعند حدوث إخفاقات أمنية، يكون السجل مفيدًا بشكل خاص لتحديد تسلسل الأحداث الزمني. وبالتالي، ينبغي حماية جميع مرافق التسجيل ومعلومات السجل من العبث والوصول غير المصرح به
  - يجب وضع ضوابط للحماية من التغييرات غير المصرح بها على معلومات السجل والمشاكل التشغيلية في أداة تسجيل الدخول، بما في ذلك:
    - أي تعديلات على أنواع الرسائل التي تم تسجيلها
    - ملفات السجل التي يتم تحريرها أو حذفها
    - تجاوز سعة تخزين وسائط ملفات السجل، مما يؤدي إلى فشل تسجيل الأحداث أو الإفراط في الكتابة للأحداث المسجلة السابقة
  - يجب تحديد فترة الاحتفاظ بالسجل لجميع أجهزة البنية التحتية والتطبيقات وخادم البريد والبيانات المالية وأي متطلبات قانونية وتنظيمية وامتثالية معمول بها. يجب أرشفة السجلات كجزء من سياسة الاحتفاظ بالسجلات أو وفقًا لمتطلبات جمع الأدلة والاحتفاظ بها
  - يمكن النظر في المجموعة التالية من الضوابط لتأمين تخزين السجل وحمايته:
    - يجب إجراء جميع عمليات جمع السجلات والدمج على خادم مستقل ومخصص
    - يجب تشفير محتويات بيانات السجل بشكل صحيح للحماية الموقعة رقمياً لضمان السلامة
    - يجب تعيين ملفات السجل على «إلحاق فقط» لتجنب الحذف والشطب والكتابة فوقها
    - يجب إجراء نسخ احتياطي منتظم لجميع ملفات السجل على فترات دورية، ويجب أن تكون هناك قواعد مناسبة لتسمية المعلومات لتوضيح التاريخ والوقت والنوع والخادم
    - يجب دمج السجل الاحتياطي مع النسخة الاحتياطية الكلية للشركة
    - يجب توفر الأدوات الضرورية لتصفية (فلترة) الأحداث الرئيسية من سجلات جميع الأحداث وسوف يساعد ذلك على إدارة تكاليف سعة التخزين وقضايا الامتثال التي تتطلب متطلبات تدقيق هائلة الحجم
    - يجب على المؤسسات صياغة سياسات التخلص الآمن لمسح بيانات السجلات ووسائطها وإتلافها

- **سجلات المسؤول والمشغل**
  - يجب تسجيل أنشطة جميع مسؤولي النظام وأنشطة مشغلي النظام، وحماية السجلات ومراجعتها بانتظام للحفاظ على مساءلة المستخدمين أصحاب الامتيازات.
  - يُمكن استخدام نظام كشف التسلل، تتم إدارته خارج سيطرة النظام ومسؤولي الشبكات، لمراقبة أنشطة إدارة النظام والشبكة من أجل الامتثال.

- **اعتبارات النظام**
  - يجب مراعاة ما يلي عند إعداد آليات التسجيل:
    - استخدام خادم سجل نظام مركزي
    - آليات تحذير لتنبيه المسؤول في حالة وجود أي نشاط ضار يتم اكتشافه في السجلات
    - استخدم تنسيق السجل المدمج لتخزين سجل النقل
    - اختيار أسماء مختلفة لملفات السجلات لمواقع الويب الافتراضية المختلفة، والتي يمكن تنفيذها كجزء من خادم ويب فعلي واحد
    - التأكد من وجود الإجراءات الضرورية بحيث لا تملأ ملفات السجلات محركات الأقراص الثابتة
    - التأكد من تخزين ملفات السجلات بشكل منتظم وتأمينها وتحليلها

- **سياسة التدقيق وإدارة السجلات**
  - التدقيق هو فحص رسمي ومراجعة للإجراءات التي يتخذها مستخدمو النظام. يتيح تدقيق الأحداث التسجيل الموثوق والدقيق والقابل للتهيئة لمجموعة متنوعة من أحداث النظام ذات الصلة بالجانب الأمني، بما في ذلك عمليات تسجيل الدخول وتغييرات التهيئة والوصول إلى الملفات والشبكات.
  - تقوم سياسة التدقيق باكتشاف ومنع اختراق نظام الكمبيوتر في المؤسسة، وتكشف عن حالات إساءة الاستخدام. ويمكن إجراء عمليات التدقيق بغرض:
    - ضمان السرية والسلامة والتوفر من خلال مراجعة سجلات التدقيق والحفاظ عليها.
    - التأكد من تقييد الوصول إلى سجلات التدقيق والحفاظ على الفصل بين الواجبات.
    - التحقق من الحوادث الأمنية الممكنة وإعادة بناء تسلسل الأحداث التي تسبق المشكلة وكل ما يحدث بعدها.
  - يجب على المؤسسات تحديد جميع متطلبات التدقيق لمضيفي نظام (Windows)، ومضيفي نظام (Linux)، وخوادم الويب وخوادم قواعد البيانات وغيرها، حسب الاقتضاء، وتحديد سياسة التدقيق الخاصة بكل منها.
  - يجب أن تجري المؤسسة تقييماً دوريًا والعلاقات المتبادلة بين السجلات من جدران الحماية، ونظام (IDS IPS /)، وخوادم التطبيقات (الويب والبريد وقاعدة البيانات)، والأنظمة إلخ. وأن تستخلص استنتاجات حول نوع الحدث ووقته، ونقاط الضعف التي تم استغلالها وأسبابها الجذرية. يجب أن توفر هذه السجلات مدخلات حيوية لإدارة حوادث أمن الكمبيوتر، سواء لمنع الحوادث أو الاستجابة لها.
  - يجب إعداد تقارير إدارية منتظمة لتتبع، بصورة صحيحة، أحداث النسخ الاحتياطي والتخلص والكشف عن أي تشابهات قد تنشأ في الأنظمة.

الملحق ١:
المصطلحات والتعاريف

الرقم	المصطلح	التعريف
١.	الموافقة	موافقة صاحب البيانات تعني أي إشارة ممنوحة بحرية ومحددة ومستنيرة ولا غموض فيها لرغبة صاحب البيانات يفيد/تفيد بموجبها، من خلال بيان أو إجراء تأكيدي واضح، بالموافقة على معالجة البيانات الشخصية الخاصة به.
٢.	البيانات	تشير إلى جميع البيانات والمعلومات (مثل المعلومات الشخصية والمعلومات المالية لصاحب البيانات وما إلى ذلك) الموجودة في شكل إلكتروني، والتي يحصل عليها أو يستردها أو يشاركها تجار التجارة الإلكترونية والمؤسسات المالية لغرض تقديم خدمات التجارة الإلكترونية للجمهور.
٣.	مراقب البيانات	يُشير إلى أي كيان (شخص طبيعي أو اعتباري أو سلطة عامة أو وكالة أو أي هيئة أخرى) يحدد (إما بمفرده أو مشتركًا مع أشخاص آخرين) الأغراض التي من أجلها عولجت أي بيانات شخصية والأسلوب الذي عولجت به أو ستتم معالجتها بها.
٤.	معالج البيانات	معالج البيانات هو أي كيان (شخص طبيعي أو اعتباري أو سلطة عامة أو وكالة أو أي هيئة أخرى) يقوم بمعالجة البيانات نيابة عن مراقب البيانات. يجب أن يقرر مراقب البيانات الغرض والأسلوب الواجب اتباعهما لمعالجة البيانات.
٥.	صاحب البيانات	صاحب البيانات يعني الفرد الذي هو موضوع البيانات الشخصية. وبعبارة أخرى فإن صاحب البيانات هو الفرد الذي تتعلق به بيانات شخصية معينة.
٦.	معالجة البيانات	يُشير إلى تنفيذ أي عملية أو مجموعة من العمليات على البيانات، بما في ذلك جمع أو استلام أو تسجيل أو تنظيم أو تخزين أو تكييف أو تغيير أو استرجاع أو استشارة أو استخدام أو كشف أو نشر أو نقل أو حجب أو محو أو إتلاف تلك المعلومات.
٧.	مشاركة البيانات	تعني الإفصاح عن البيانات من أي وكالة أو كيان أو أكثر إلى وكالة/ كيان أو وكالة/ كيان من طرف ثالث أو وكالات/ كيانات، أو مشاركة البيانات بين أجزاء من الوكالة / الكيان.
٨.	وزارة المواصلات والاتصالات	تُشير إلى وزارة المواصلات والاتصالات - قطر
٩.	المؤسسة	تُشير إلى تجار التجارة الإلكترونية والمؤسسات المالية.
١٠.	البيانات الشخصية	تشير إلى: • أي معلومات عن شخص تكون هويته ظاهرة أو يمكن التحقق منها بشكل معقول بناءً على تلك المعلومات أو من مجموعة من تلك المعلومات وغيرها، و / أو • أي معلومات، بما في ذلك بيانات الموقع، التي يُمكن أن ترتبط بشكل معقول بفرد معين بغض النظر عما إذا كانت هوية الفرد واضحة من تلك المعلومات أو من مزيج منها بالإضافة إلى المعلومات الأخرى.
١١.	الطرف الثالث/ الآخر	يشير إلى أي شخص أو كيان، بخلاف مراقب البيانات، يقوم بمعالجة البيانات نيابة عن المراقب، ويشمل أي شخص أو كيان آخر معين من قبل طرف ثالث للغرض المذكور.

الرقم	المصطلح	التعريف
١٢.	البيانات الشخصية الحساسة	تتعلق بمعلومات ترتبط بإثنية صاحب البيانات أو أصله العرقي أو آرائه السياسية أو معتقداته الدينية أو أنشطته النقابية أو صحته البدنية أو العقلية أو الجنسية أو تفاصيل جرائمه الجنائية.
١٣.	خدمة التحقق من العنوان (AVS):	تتحقق خدمة التحقق من العنوان (AVS) من العنوان الشخصي الذي يقدمه العميل عند إجراء معاملة البطاقة الائتمانية.
١٤.	المصادقة	المصادقة هي عملية التعرف على هوية المستخدم. إنها آلية ربط طلب وارد مع مجموعة من بيانات وثائق المصادقة التعريفية.
١٥.	رقم التحقق من البطاقة	رقم التحقق من البطاقة (CVV) هو آخر ثلاثة أرقام مطبوعة على لوحة التوقيع الموجودة على ظهر البطاقة الائتمانية / البطاقة المدينة. إن ميزة (CVV / CID) هي ميزة أمان تسمح لتاجر التجارة الإلكترونية وبنك المصدر للبطاقة الائتمانية بتحديد حامل البطاقة وتوفير حماية إضافية ضد الاحتيال.
١٦.	سجل الائتمان	سجل الائتمان هو سجل لسداد المقترض المسؤول عن الديون. يُعد تقرير الائتمان سجلاً للتاريخ الائتماني للمقترض من عدد من المصادر، بما في ذلك البنوك وشركات البطاقات الائتمانية ووكالات التحصيل والحكومات.
١٧.	التحقق	تقييم أوراق اعتماد المستخدم للتأكد من أنها صحيحة وكاملة.
١٨.	تحديد الموقع الجغرافي IP	تحديد أو تقدير الموقع الجغرافي الحقيقي للجسم، مثل مصدر رادار أو هاتف جوال أو محطة حاسوب متصلة بالإنترنت. في أبسط أشكاله، ينطوي تحديد الموقع الجغرافي على توليد مجموعة من الإحداثيات الجغرافية، ويرتبط ارتباطا وثيقا باستخدام أنظمة تحديد المواقع، ولكن الاستفادة الأمثل منه تتعزز عبر استخدام هذه الإحداثيات لتحديد موقع ذي معنى، مثل عنوان الشارع.
١٩.	بصمة الجهاز	بصمة الجهاز أو بصمة الآلة أو بصمة المتصفح هي المعلومات التي يتم جمعها حول جهاز حاسوب بعيد بغرض تحديد الهوية. يمكن استخدام البصمات لتحديد المستخدمين الأفارد أو الأجهزة بشكل كامل أو جزئي حتى عند إيقاف تشغيل ملفات تعريف الارتباط
٢٠.	المستهلكون	الأفراد / المؤسسات الذين يحصلون على أدوات دفع مدفوعة مسبقاً لشراء السلع والخدمات، بما في ذلك الخدمات المالية
٢١.	الجهة المصدرة	هي الكيان الذي يدير أنظمة الدفع التي تصدر أدوات دفع مدفوعة مسبقاً للأفراد / المؤسسات. يتم استخدام الأموال التي يتم جمعها من قبل هذا الكيان لدفع الدفعات إلى التجار، الذين هم جزء من ترتيبات القبول، مباشرة أو من خلال اتفاقية تسوية.
٢٢.	أدوات الدفع المدفوعة مسبقاً	أدوات الدفع مسبقة الدفع هي أدوات دفع تُسهل شراء السلع والخدمات، بما في ذلك تحويل الأموال، مقابل القيمة المخزنة على تلك الأدوات. تمثل القيمة المخزنة على هذه الأدوات القيمة التي يدفعها حاملو الأدوات نقدًا أو على شكل دين إلى حساب مصرفي أو من خلال بطاقة ائتمانية.

الرقم	المصطلح	التعريف
.٢٣	أدوات الدفع عبر النظام المفتوح:	يُمكن استخدام أدوات الدفع هذه لشراء السلع والخدمات، بما في ذلك الخدمات المالية، مثل تحويل الأموال في أي بطاقة تقبل مواقع التاجر (محطات نقاط البيع) وأيضاً السماح بالسحب النقدي في أجهزة الصراف الآلي
.٢٤	أدوات الدفع عبر النظام المغلق:	هي أدوات دفع صادرة عن أي كيان لتسهيل شراء السلع والخدمات منه. هذه الأدوات لا تسمح بالسحب النقدي أو الاسترداد. وبما أن هذه الأدوات لا تسهل الدفعات والتسوية لخدمات الطرف الثالث، فإن إصدار وتشغيل هذه الأدوات لا يتم تصنيفه كأنظمة دفع.
.٢٥	أدوات الدفع عبر النظام شبه المغلق:	يُمكن استخدام أدوات الدفع هذه لشراء السلع والخدمات، بما في ذلك الخدمات المالية في مجموعة من المواقع / المنشآت التجارية المحددة بوضوح والتي لها عقد محدد مع الجهة المصدرة لقبول أدوات الدفع. هذه الأدوات لا تسمح بالسحب النقدي أو الاسترداد من قبل حاملها
.٢٦	الحدود	تُشير جميع "الحدود" على قيمة الأدوات المذكورة في المبادئ التوجيهية إلى القيمة القصوى لهذه الأدوات التي يمكن إصدارها لأي حامل.
.٢٧	نقاط الضعف	نقاط الضعف هي خلل أو ضعف في تصميم أو تنفيذ أو تشغيل أو إدارة النظام، يمكن استغلاله لتهديد أغراض أمن النظام.
.٢٨	تقييم نقاط الضعف	تقييم نقاط الضعف هو مسح يتم إجراؤه من الشبكة الداخلية، ويقدم نظرة عامة على نقاط الضعف التي يمكن رؤيتها من الشبكة المحلية، مع الأخذ بعين الاعتبار المراقبة الأمنية القائمة على المضيف والموجودة على النظام المستهدف. من خلال إجراء مسح داخلي أو خارجي لكل مكون في الهيكل، يمكن أن توفر النتائج معلومات حول مدى أمان كل طبقة. ("الدفاع في العمق")
.٢٩	التهديد/المهدد	التهديد/المهدد هو أي (مهاجم خارجي خبيث، مستخدم داخلي، عدم استقرار في النظام، إلخ) قد يضر بالأصول المملوكة من قبل أي تطبيق (موارد ذات قيمة، مثل البيانات في قاعدة بيانات أو في نظام الملفات) عن طريق استغلال نقاط الضعف.
.٣٠	الاختبار	الاختبار هو إجراء لإثبات أن التطبيق يلبي المتطلبات الأمنية لأصحاب المصلحة
.٣١	ملف التصحيح	ملف التصحيح عبارة عن جزء من برنامج مصمم لإصلاح مشكلات أو تحديث برنامج كمبيوتر أو بياناته الداعمة.
.٣٢	ملف تصحيح أمني	هو ملف تصحيح طورته "الشركات المصنّعة للمعدات الأصلية" (OEMs) لإصلاح نقاط الضعف المحددة.
.٣٣	الاستشارات الأمنية	إشعار تصدره الشركات المصنّعة للمعدات الأصلية عن أي نقاط ضعف محددة يمكن إصلاحها من خلال تطبيق ملفات التصحيح المقترحة أو إجراء بعض التغييرات على التهيئة.
.٣٤	إصدار البرنامج	هو إشعار تصدره الشركات المصنّعة للمعدات الأصلية حول ترقية البرامج الرئيسية / الثانوية التي تتناول إصلاحات الأخطاء والتحسينات البرمجية.

الملحق ٢:
قائمة المصادر

قائمة المصادر

- معيار الآيزو 27001: 2013
- إدارة الهوية - معهد SANS
- المبادئ التوجيهية لأمن تطبيق WASP
- المبادئ التوجيهية لإمكانية الوصول إلى محتوى الويب 2.0 (WCAG)
- مخاطر التكنولوجيا الحديثة والخدمات المصرفية الإلكترونية رقم الملحق (192)
- الآيزو/ آي إي سي دي آي اس 29115 - تكنولوجيا المعلومات - تقنيات الأمن - إطار ضمان مصادقة الكيان
- معايير أمن بيانات بطاقات الدفع
- إطار عمل (COBIT 5)
- المبادئ التوجيهية للأمن ثلاثي الأبعاد (3D Secure)
- نظام حماية البيانات العامة
- IRDAI - إطار أمن المعلومات
- إطار عمل الأمن السيبراني في البنوك - بنك الاحتياطي الهندي
- دليل تجار فيزا للتجارة الإلكترونية لإدارة المخاطر
- الاستراتيجية الوطنية للأمن السيبراني - وزارة المواصلات والاتصالات.
- إطار عمل الأمن السيبراني لدى المعهد الوطني للمعايير والتكنولوجيا (NIST)

MOTC
motc.gov.qa