وزارة المواصلات والاتصالات
MINISTRY OF TRANSPORT AND COMMUNICATIONS

المبادئ التوجيهية للتجارة الإلكترونية

تكنولوجيا المعلومات

motc.gov.qa

المبادئ التوجيهية للتجارة الإلكترونية

تكنولوجيا المعلومات

إعداد:

وزارة المواصلات والاتصالات

دولة قطر

٢٠١٩/٢٠١٨

حول الوثيقة

تحتوي هذه الوثيقة على المبادئ التوجيهية الموصى بها لإدارة التكنولوجيا لمنظومة 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 التكنولوجية. يجب استعمال المبادئ التوجيهية كإطار عمل متكامل، والالتزام بها عند صياغة الضوابط التكنولوجية للأعمال.

جدول المحتويات

١. مقدمة

١-١ تمهيد

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.

عندما يتعلق الأمر بممارسات التجارة الإلكترونية الجيدة، فإن التكنولوجيا هي المفتاح. تؤدي التكنولوجياً دورا حيوياً في جميع جوانب تنفيذ نظام التجارة الإلكترونية الفعال وسلسلة القيمة. من خلال مواكبة أفضل الممارسات ذات الصلة بأحدث التكنولوجيا بالنسبة لأعمالك، يمكنك تعزيز الأمن وزيادة الكفاءة والمبيعات بما يكفل تجربة عملاء أفضل.

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 التكنولوجيا وحماية مصالح أصحاب المصلحة الرئيسيين التاليين:

- العملاء / المشتركون 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.
- الموردون (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 وتجار التجزئة 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 للتكنولوجيا

٢-١ أمن المعلومات

تنطبق هذه المباديء التوجيهية على جميع المعلومات ونظم المعلومات، طوال دورة حياتها، لدى كافة تجار التجارة الإلكترونية ومقدمي خدمات تكنولوجيا المعلومات وشركاء الخدمات اللوجستية والمؤسسات المالية (يُشار إليها فيما يلي باسم «المؤسسات») أينما وجدت المعلومات ونظم المعلومات.

وتهدف هذه المباديء التوجيهية إلى تنفيذ مراقبة ضوابط أمن المعلومات على نطاق المؤسسة. تلتزم المؤسسات بتوفير الحماية الشاملة لأصولها المعلوماتية ضد عواقب اختراقات السرية أو السلامة و/ أو انقطاع توفر تلك الأصول.
يجب على المؤسسات تحديد الأطر الأمنية المناسبة، وهياكل تنظيم الأمن، وتحديد المسؤوليات والموارد اللازمة لإدارة أمن المعلومات في جميع أنحاء المؤسسة.

يجب على الإدارة إثبات القيادة والالتزام فيما يتعلق بأمن المعلومات من خلال:
- التأكد من وضع سياسة أمن المعلومات وأهداف أمن المعلومات والتي تتسق مع التوجه الاستراتيجي للمؤ سسة
- ضمان دمج متطلبات أمن المعلومات في عمليات المؤسسة
- التأكد من توفر وكفاءة الموارد اللازمة لتلبية أهداف ومتطلبات أمن المعلومات
- إبراز أهمية أمن المعلومات الفعال والامتثال لمتطلبات نظام إدارة أمن المعلومات من قبل المستخدمين وكذلك الموردين
- التأكد من أن أمن المعلومات يحقق النتائج المرجوة
- تحديد وتنفيذ تدابير لمراقبة فعالية أهداف أمن المعلومات داخل المؤسسة
- تعزيز عملية التحسين المستمرة
- يجب على الإدارة أن تنظر في تنفيذ أو مواءمة متطلبات أمن المعلومات داخل مؤسساتها، بناء على مدى أهمية وحساسية الأنشطة التي تقوم بها، مع المسؤوليات والسياسات والمبادئ التوجيهية التي تتبعها الحكومة، ومع المعايير الدولية المختلفة مثل الآيزو 27001 ونظام (PCI DSS) وغيره.
- دعم أدوار الإدارة الأخرى ذات الصلة لإظهار قيادتها كما تنطبق على مجالات مسؤوليتها.

يجب على الإدارة العليا وضع سياسة أمن المعلومات بحيث:
- تكون مناسبة لأغراض المؤسسة
- تتضمن أهداف أمن المعلومات أو توفر إطاراً لوضع أهداف أمن المعلومات
- تتضمن التزاماً بتلبية المتطلبات السارية المتعلقة بأمن المعلومات
- تتضمن التزاماً بالتحسين المستمر لنظام إدارة أمن المعلومات

يجب على الإدارة العليا التأكد من أنه قد تم تحديد المكلفين بالمسؤوليات والأدوار المتصلة بأمن المعلومات وأنه قد تم الإبلاغ بذلك. وعلى الإدارة العليا تحديد المسؤوليات والصلاحيات فيما يتعلق بما يلي:
- التأكد من أن أمن المعلومات يتسق مع متطلبات هذا المعيار الدولي
- رفع التقارير عن الأداء إلى الإدارة العليا

٢-٢ إدارة الهوية - تسجيل الدخول

ينطبق هذا المبدأ التوجيهي على جميع التطبيقات والمعلومات وأنظمة المعلومات الخاصة بمؤسسات التجارة الإلكترونية.

تُعالج إدارة الهوية الاستخدام الصحيح لوثائق المصادقة اللازمة لتحديد هوية المستخدمين وتوثيقها بشكل فريد. مع نمو المؤسسات وإضافة المزيد من الخدمات، ودمج وظائف أعمال جديدة مثل المشاريع المشتركة والمشاريع متعددة الفترات، أصبح ضبط الوصول إلى موارد معلومات الشركة مهمة أكثر صعوبة. فمع استمرار نمو وتمدد نطاق التحكم في الوصول عبر أنظمة متعددة وتطبيقات متعددة، يُمكن لكل نظام أن يستخدم طريقة مختلفة لضبط الوصول

ومصادقة المستخدم. إن الوصول إلى أصول المعلومات يجب أن يضبط وفقاً لمتطلبات الأعمال والأمن، وبما يتناسب مع سياسات المنظمة. يجب تطبيق ضوابط الوصول بناءً على مبدأ «رفض كل شيء ما لم يُؤذن به صراحةً» لحماية أصول المعلومات من الوصول غير المصرح به. تتمثل أهداف إدارة الهوية في:

- تقييد الوصول إلى أصول المعلومات وفقًا لمتطلبات الأعمال
- منع الوصول غير المصرح به إلى أنظمة المعلومات وخدمات الشبكة وأنظمة التشغيل والمعلومات الموجودة في أنظمة قواعد البيانات والتطبيقات
- التأكد من أن مرافق الحوسبة المتنقلة والعمل عن بعد محمية بضوابط الأمن المناسبة
- التأكد من تنفيذ ضوابط الوصول إلى المعلومات لتلبية أي متطلبات تعاقدية ذات صلة، حسب الاقتضاء

٢-٣ تأكيد الدفع

إن مدفوعات التجارة الإلكترونية، والتي هي واحدة من أسرع المنظومات تغيراً في العالم، في حالة دائمة من التغيروعدم الثبات. فمع التقدم المستمروالتبني المتزايد لنمط الحياة الرقمي (أي نمط الحياة الذي تتيح فيه الأجهزة المتصلة بالإنترنت للأشخاص العمل والتسوق واللعب والإبداع والمشاركة والتواصل والتعامل بطريقة متكاملة ووفقًا لشروطهم الخاصة على مدار الساعة في جميع أنحاء العالم) يتوقع المستهلكون المزيد من السرعة والراحة. ذلك لا ينطبق فقط على تجربة الدفع، وإنما أيضاً على طريقة التفاعل مع واستعمال الخدمات المالية الأخرى أيضاً.

هذا المبدأ التوجيهي يقدم إرشادات لإدارة أمن الدفع بواسطة تجار التجارة الإلكترونية والمؤسسات المالية العاملة فيها، ويوضح الممارسات الأمنية للعملاء. ينطبق هذا المبدأ التوجيهي على جميع مؤسسات التجارة الإلكترونية الخاضعة لنظم وزارة المواصلات والاتصالات. يضع هذا المبدأ التوجيهي في اعتباره جميع وسائل الدفع المعمول بها لدى كافة المؤسسات. تتضمن أدوات الدفع المختلفة التي يوفرها تجار التجارة الإلكترونية في سبيل خدمة العملاء بسلاسة ما يلي:

- البطاقات الائتمانية: تستخدم البطاقات الائتمانية على نطاق واسع دولياً، وتحظى بقبول على نطاق واسع كطريقة دفع متعارف عليها. وعلى الرغم من ذلك فقد طرأ انخفاض تدريجي في استخدام البطاقة الائتمانية على المستوى الدولي، مع اكتساب المحافظ الإلكترونية والبدائل الأخرى المزيد من الانتشار. فهذه التطورات، خطت بطاقات الولاء خطوات واسعة نحو النمو.
- البطاقة المدينة: علاوةً على كون البطاقة مفيدة للدفعات في المعاملات خارج الإنترنت، فقد تزايد استخدام البطاقات المدينة في المعاملات عبر الإنترنت أيضًا. وإذ تعمل البطاقة المدينة بطريقة تشبه إلى حد كبير البطاقة الائتمانية، دون أن تنطوي على المخاطر العديدة للديون، فقد شاع استخدام هذه البطاقات مؤخراً.
- المحفظة الإلكترونية: المحفظة الإلكترونية هي أداة رقمية تُمكن المستهلكين من حفظ أموالهم. ويمكن أن ينظر إليها على أنها النظير الرقمي لمحفظتنا المادية. يمكن للمحافظ الإلكترونية أن تحتوي على بطاقات ائتمانية (مسجلة مسبقا) وبطاقات مدينة وبطاقات هدايا وبطاقات ولاء، وأن توفر إمكانية الوصول إلى طرق دفع بديلة مثل التحويلات المصرفية عبر الإنترنت. وتتيح بعض المحافظ الإلكترونية للمستهلكين إمكانية (شحن) الأموال في محافظهم مسبقاً. إن المحافظ الإلكترونية توفر تجربة دفع محسنة وتبسط عملية الدفع عبر الإنترنت والهاتف المحمول.
- الدفعات الإلكترونية المصرفية عبر الإنترنت (OBeP): إن نظام الدفعات الإلكترونية المصرفية عبر الإنترنت (OBeP) هو نوع من شبكات الدفعات المصممة لتسهيل التحويلات المصرفية عبر الإنترنت. في هذا النظام، تتم المصادقة على المستهلك آنياً من قبل المؤسسة المالية التي يتعامل معها، وكذلك يتم التحقق من توفر الأموال آنياً، وتقدم المؤسسة المالية التي يتعامل معها المستهلك ضمانًا بالدفع للتاجر في حالة إجراء الدفع كتحويل ائتماني (دفع مباشر): مع شروع المستهلك / المشتري في عملية الدفع، يتلقى التاجر الضمان آنياً حتى يتمكن من متابعة التنفيذ.
- الأدوات مسبقة الدفع: الأدوات 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 دفعها حاملو تلك الأدوات نقدًا أو بالخصم إلى حساب مصرفي أو من خلال بطاقة ائتمانية.

- الدفعات النقدية/الدفع نقدًا عند التسليم: الدفع نقداً عند التسليم (COD) هي طريقة دفع يتم فيها نقل البضائع المطلوبة إلى مكان المشتري، لكن تُسلم فقط عند السداد الكامل. تجري معظم الدفعات في دولة قطر على أساس الدفع نقداً عند التسليم، وهناك بعض طرق الدفع الالكتروني المحدودة (البطاقات المدينة والبطاقات مسبقة الدفع والمحافظ الرقمية وغيرها).

٢-٤ أفضل ممارسات التصميم

تتطلب أفضل ممارسات التصميم والتطوير الآمن أن تكون الشيفرات والعمليات التي تدخل في تطوير التطبيقات آمنة. حيث يحتوي التطوير الآمن على استخدام عددٍ من العمليات، بما في ذلك تنفيذ دورة حياة التطوير الأمني (SDLC) والتشفير الآمن نفسه.

إن الهدف من هذه الوثيقة هو تحديد الضوابط التي يلزم دمجها والتحقق من صحتها في مختلف التطبيقات لضبط الوصول إلى وحماية سرية وسلامة وتوفر المعلومات التي تتم معالجتها أو تخزينها في تلك التطبيقات.

تضع هذه المبادئ التوجيهية في اعتبارها ضرورة وضع المتطلبات ذات الصلة بأمن المعلومات ضمن متطلبات أنظمة المعلومات الجديدة أو متطلبات تحسينات نظم المعلومات القائمة لدى كافة تجار التجارة الإلكترونية والمؤسسات المالية العاملة فيها (يُشار إليها فيما بعد بالمؤسسات) بما يضمن أن أمن المعلومات قد تم تصميمه وتطبيقه في إطار دورة حياة نظم المعلومات.

٢-٥ إمكانية الوصول

يساعد هذا المبدأ التوجيهي في إدارة وتنفيذ تطبيقات يسهل الوصول إليها للمؤسسات. توفر مبادرة الوصول إلى شبكة الإنترنت (WAI) W3C Web Accessibility Initiative مجموعة من معايير الوصول التي تم التعارف عليها والاعتراف بها من قبل الحكومات والمؤسسات في جميع أنحاء العالم. وتشمل:

تنطبق المبادئ التوجيهية للوصول إلى محتوى الويب (WCAG 2.0) على جميع محتويات الويب والتطبيقات، بما في ذلك تلك الموجود ة على الهواتف المحمولة وأجهزة التلفاز وقنوات التسليم الأخرى.

تنطبق المبادئ التوجيهية لإمكانية الوصول لأداء التأليف (ATAG 2.0) على مواقع الويب التي توفر للمستخدمين فرصة إنشاء محتوى، مثل إضافة التعليقات أو النشر في المنتديات أو تحميل الصور أو مقاطع الفيديو. وتنطبق هذه المبادئ التوجيهية أيضًا إذا كانت مؤسستك توفر أدوات، مثل نظم إدارة المحتوى (CMS)، للموظفين أو العملاء لإدارة مواقع الويب ومحتوياتها.

تنطبق المبادئ التوجيهية للوصول إلى وكيل المستخدم (UAAG 2.0) عند توفير مكونات إضافية، مثل مشغلات الوسائط، لتقديم المحتوى أو عند تطوير ضوابط التحكم المخصصة لتوفير وظائف غير قياسية.

٣. المبادئ التوجيهية التفصيلية

٣-١ أمن المعلومات

➢ إدارة أصول المعلومات وتصنيف المعلومات

- **إدارة أصل المعلومات**

يوفر هذا القسم المبادئ التوجيهية لتحقيق والحفاظ على الحماية المناسبة للأصول التنظيمية. كما يحدد أيضاً المبادئ التوجيهية للتعرف على التفاصيل الهامة للأصل، وفهم أهميته لتوفير مستوى مناسب من الحماية للصيانة.

يجب أن يقوم جميع رؤساء الوظائف / الإدارات / المجموعات (أو ممثليهم المعينين) باختيار مالك معين لكل أصل. يجب تتبع أصول المعلومات عبر دورة حياتها وتحديد وتوثيق وتنيفذ القواعد المتعلقة بالاستخدام المقبول لها. ويجب إعادة أصول المعلومات تلك عند إنهاء أو انتهاء الخدمة أو العقد أو الاتفاق. يجب على المؤسسة اتخاذ التدابير المناسبة لمنع إساءة استخدام وضمان حماية أصولها.

- **تصنيف المعلومات**

تعتبر أصول المعلومات في أي مؤسسة ذات أهمية قصوى، ولذا يجب الحفاظ على سريتها وسلامتها وتوفرها بشكل مناسب. ويجب على المؤسسات التأكد مما يلي:

- تصنيف أصول المعلومات من حيث المتطلبات القانونية والقيمة والأهمية والحساسية، إزاء الإفشاء أو التعديل غير المصرح به.
- أن مالكي أصول المعلومات مسؤولون عن تصنيفها. يجب أن يتضمن نظام التصنيف أعراف التصنيف والمعايير التي ستتبع لمراجعة التصنيف بين آونة وأخرى في المستقبل. ينبغي تقييم مستوى الحماية في النظام من خلال تحليل السرية والسلامة والتوفر وأي متطلبات أخرى للمعلومات قيد النظر.
- يجب تضمين التصنيف في عمليات المؤسسة، وأن يكون متسقًا ومتماسكًا في كل المؤسسة.

➢ ضبط الدخول

- يجب وضع سياسة لضبط الوصول وتوثيقها ومراجعتها بناء على متطلبات أمن المعلومات والأعمال.
- يجب ضبط الوصول إلى أصول المعلومات بناءاً على متطلبات الأعمال والأمن، وبما يتناسب مع تصنيف أصول المعلومات. يجب تطبيق ضوابط الوصول بناء على المبدأ الأمني «رفض كل شيء ما لم يؤذن به صراحةً» لحماية أصول المعلومات من الوصول غير المصرح به. ويمكن للمؤسسات الرجوع إلى ما يلي للإطلاع على مبادئ توجيهية تفصيلية:
  - يجب على المؤسسات وضع إجراءات رسمية للتسجيل وإلغاء التسجيل لمنح أوحجب الوصول إلى أي من أنظمة المعلومات والخدمات.
  - ينبغي النظر في كل من ضوابط الوصول المنطقي والمادي معاً.
  - يجب أن تتحكم المؤسسة في تخصيص كلمات المرور من خلال عملية إدارية رسمية.
  - يجب على المؤسسة القيام بمراجعة دورية لحقوق وصول المستخدمين من خلال عملية رسمية.
  - يجب على المؤسسة أن تحدد وتنفذ تدابير لحماية وصول المستخدم النهائي وكلمات المرور.
  - يجب على المؤسسة أن تحد من وصول موردي الطرف الثالث إلى الأنظمة الحساسة، وإذا لزم الأمر يجب إعطائهم إمكانية الوصول بعد إجراء عمليات التحقق المناسبة.
  - يجب أن تنفذ المؤسسة «ضبط الوصول القائم على الدور» وينطبق الأمر ذاته على جميع الأنظمة والمستخدمين بما في ذلك العملاء/المستخدمين النهائيين/المستخدمين المميزين،
  - بالنسبة لمعاملات التجارة الإلكترونية الهامة، يتعين على المؤسسات تنفيذ المصادقة متعددة العوامل قبل إتاحة الوصول إلى أنظمة المؤسسة.

- **مسؤوليات المستخدم**
  - يجب على المؤسسة التأكد من أن المستخدمين يتبعون ممارسات أمان جيدة في اختيار واستخدام كلمات المرور المعقدة
  - يجب على المؤسسة تنفيذ واعتماد سياسة المكتب النظيف فيما يتعلق بالأوراق، ووسائط التخزين القابلة للإزالة
  - يجب على المؤسسة تنفيذ سياسة الشاشة النظيفة لوحدات معالجة المعلومات. يجب ترك أجهزة الحاسوب والأجهزة الطرفية، عندما تكون غير مراقبة، على وضعية تسجيل الخروج، أو حمايتها باستخدام شاشة التوقف. كما يجب حمايتها بواسطة مفاتيح المرور أو كلمات المرور أو عناصر التحكم المشابهة عند ما لا تكون قيد الاستخدام.

- **ضبط الوصول إلى الشبكة**
  - يجب تزويد المستخدمين بإمكانية الوصول فقط إلى خدمات الشبكة التي تم تفويضهم باستخدامها بالتحديد. يجب التأكد من استخدام طرق المصادقة الملائمة من قبل المستخدمين عن بعد للحصول على إمكانية الوصول.
  - يجب على المؤسسة تطبيق آلية الفصل بين الشبكات حينما تتعلق بمجموعات من خدمات المعلومات والمستخدمين وأنظمة المعلومات

- **ضبط الوصول إلى النظام والتطبيقات**
  - على المؤسسة أن تتحكم في الوصول إلى الأنظمة والتطبيقات وفقاً لسياسة مراقبة الدخول وعبر إجراء تسجيل دخول آمن
  - يجب أن يكون استخدام الوصول المميز والمراجعات من خلال عملية رسمية
  - يجب استخدام كلمات مرور منيعة ومعقدة للحصول على إمكانية الوصول
  - يجب على المؤسسة تنفيذ ضوابط صارمة إضافية للمستخدمين ذوي إمكانية الوصول المميز
  - يجب تسجيل أنشطة جميع مستخدمي الوصول المميز ورصدها على أساس دوري
  - يجب تقييد برامج المرافق التي قد تكون قادرة على تجاوز النظام وضوابط التطبيق، ومراقبتها
  - يجب أن تتحكم المؤسسة وتقيّد الوصول إلى شيفرة مصدر البرنامج

➢ أمن الموارد البشرية

- يهدف هذا المبدأ التوجيهي إلى ضمان إجراء التوظيف وفقاً للقوانين واللوائح ذات الصلة مثل سياسة تأمين المعلومات الوطنية ومعيار أمن نظام الاتصالات الداخلي (ICS) الوطني ومتطلبات العمل. ويوضح المبدأ أن المستخدمين يجب أن يكونوا مناسبين للأدوار التي تم توظيفهم فيها، وأنه قد تم تعريفهم بمسؤولياتهم تجاه حماية سرية وسلامة أصول المعلومات.وهو يحدد أيضاً متطلبات أمن المعلومات التي يتعين دمجها في عمليات الموارد البشرية أثناء التوظيف والخدمة والفصل. يهدف هذا المبدأ التوجيهي إلى معالجة مخاطر الأخطاء البشرية والسرقة والاحتيال أو سوء استخدام المرافق، فضلاً عن مساعدة جميع الموظفين في خلق بيئة حوسبة آمنة.

- **يجب ضمان ما يلي:**
  - أن المستخدمين يفهمون مسؤولياتهم المتعلقة بأمن المعلومات
  - ممارسة التحقق من الخلفية حسب العملية المعتمدة
  - توقيع اتفاقية السرية / عدم الإفصاح من قبل المستخدمين فور التحاقهم بالعمل
  - تدريب المستخدمين على استخدام نظم المعلومات بأمان
  - التأكد من خروج المستخدمين وفق العملية المعتمدة

- يجب على المؤسسات اتخاذ إجراءات تأديبية في حق المستخدمين الذين يثبت تورطهم في خروقات وانتهاكات أمنية.

➢ الأمن المادي والبيئي

- يقدم هذا المبدأ التوجيهي إرشادات عن تطوير وتنفيذ ضوابط الأمن المناسبة الضرورية لحماية أصول المعلومات ومرافق التصنيع في المؤسسة من المهددات المادية والبيئية. يجب أن تكون مرافق معالجة المعلومات ومراكز البيانات ومراكز العمليات وموقع التعافي من الكوارث والمواقع الأخرى التي تحددها الإدارة محمية حماية مناسبة.

- **المناطق الآمنة**
  - يجب تعريف حدود المحيط الآمن واستخدامها لحماية المناطق التي تحتوي على معلومات ومرافق معالجة معلومات حساسة أو حرجة
  - يتعين على المؤسسات تصميم وتطبيق الحماية المادية ضد المهددات الخارجية والبيئية، مثل الوصول غير المصرح به والأضرار الناجمة عن الحريق والفيضانات والزلازل والانفجار والاضطرابات المدنية وغيرها من أشكال الكوارث الطبيعية أو تلك التي هي من صنع الإنسان.

- **أمن المعدات**
  - يجب تنفيذ ضوابط أمن المعدات لمنع فقد أو تلف أو سرقة أو اختراق أنظمة المعلومات وانقطاع أنشطة المؤسسة.
  - يجب حماية جميع المعدات من التهديدات البيئية والوصول غير المصرح به وانقطاع التيار الكهربائي وغير ذلك من الاضطرابات المماثلة الناجمة عن الأعطال في المرافق المساندة
  - يجب تخزين المعدات غير المراقبة مثل الخوادم والشبكات والأجهزة اللاسلكية وأجهزة الاتصالات في حاويات مسيجة آمنة
  - في الحالات التي تستضاف فيها الأجهزة على السحابة أو مبان عائدة لطرف ثالث، يجب على المؤسسة التأكد من ضمان تنفيذ مقدم خدمة السحابة أو الطرف الثالث لضوابط تتماشى مع سياسة أمن معلومات المؤسسة.
  - يجب أن تكون جميع المعدات، مثل أشرطة النسخ الاحتياطية وما إلى ذلك، محمية أثناء النقل بشكل مناسب بما في ذلك الجوانب الأمنية المادية والبيئية.
  - يجب حماية جميع الكابلات، بما في ذلك كابلات الطاقة والشبكة، من التلف أو الاعتراض غير المصرح به
  - يجب على المؤسسات تطبيق المعايير الأمنية على المعدات خارج الموقع للحد من مخاطر العمل خارج حدود المؤسسة.
  - يجب أن تقوم المؤسسة بتطبيق آلية للتخلص الآمن، ويجب أن تتضمن أي عملية لإعادة استخدام المعدات نقاط مراجعة للتأكد من أنه قد تمت إزالة أي بيانات حساسة أو برامج مرخصة أو أنه قد تم طمسها بشكل آمن قبل التخلص منها.
  - يجب الحصول على تفويض مسبق لترحيل أو إزالة أي أصول معلومات إلى خارج مباني المؤسسة

➢ أمن العمليات

- يوفر هذا المبدأ التوجيهي الإرشادات اللازمة لضمان التشغيل الملائم والآمن لمرافق معالجة المعلومات، حيث من شأن هذا أن يقلل من فرص التعديل غير المصرح به أو غير المقصود أو إساءة استخدام أصول معلومات المؤسسة.

- **إجراءات التشغيل الموثقة**
  - يجب على المؤسسة توثيق إجراءات الأنشطة التشغيلية المرتبطة بمرافق معالجة المعلومات والاتصالات
  - يجب إتاحة هذه الوثائق للمستخدمين لاستخدامها فقط على أساس الحاجة للاستخدام
  - يجب أن تُعامل إجراءات التشغيل والإجراءات الموثقة لأنشطة النظام كمستندات رسمية وألا يتم إحداث تغييرات عليها إلا بتفويض من قبل الإدارة. وحيثما كان ذلك ممكنا من الناحية التقنية، ينبغي إدارة نظم المعلومات بطريقة متسقة، وباستخدام نفس الإجراءات والأدوات والمرافق

- **إدارة التغيير**
  - يجب أن تتحكم المؤسسة في تنفيذ التغييرات في مرافق وأنظمة معالجة المعلومات
  - يجب توفر مسؤوليات وإجراءات إدارية رسمية لضمان السيطرة الضرورية على جميع التغييرات
  - يجب أن تتم جميع التغييرات المصرح بها لأي نظام لمعالجة المعلومات من خلال عملية إدارة التغيير
  - يجب الاحتفاظ بجميع سجلات التغييرات ومراجعتها بصورة دورية
  - يجب الاحتفاظ بسجلات التغيير وفقا للقوانين واللوائح ذات الصلة مثل «سياسة تأمين المعلومات الوطنية ومعيار أمن نظام الاتصالات الداخلي (ICS) الوطني» ووفقاً لمتطلبات العمل.

- **إدارة السعة (الطاقة الاستيعابية)**
  - يجب على المؤسسة تحديد متطلبات السعة، آخذة في الاعتبار أهمية وحساسية النظام المعني للنشاط التجاري
  - ينبغي تطبيق موالفة النظام ومراقبته للتأكد من، وحيثما كان ذلك ضرورياً، تحسين توفر وكفاة الأنظمة
  - لضمان تحقيق الأداء المطلوب للنظام، يجب على المؤسسة مراقبة وموالفة استخدام موارد النظام
  - يجب دراسة الإسقاطات والتوقعات المتعلقة بمتطلبات السعة مستقبلياً من أجل ترشيد موارد النظام

- **الفصل بين الواجبات**
  - يجب على المؤسسات الفصل بين الواجبات والمسؤوليات المتضاربة للحد من فرص التعديل غير المصرح به أو غير المقصود أو إساءة استخدام أصول المعلومات الخاصة بالمؤسسة
  - ينبغي الحرص على عدم إمكانية وصول شخص واحد إلى أصول المعلومات وتعديلها أو استخدامها دون تصريح أو دون أن يكتشف ذلك. يجب فصل الشروع في الفعل عن التفويض والتصريح به

- **فصل بيئات التطوير والاختبار والتشغيل**
  - يجب أن يكون لدى المؤسسة مناطق منفصلة للتطوير والاختبار والتشغيل للحد من مخاطر الوصول غير المصرح به أو التغييرات في النظام التشغيلي
  - ينبغي تحديد المستوى الضروري للفصل بين بيئات التشغيل والاختبار والتطوير لمنع المشاكل التشغيلية ومن ثم تطبيق ذلك المستوى

- **الحماية من الشيفرات الخبيثة والبرمجيات الخبيثة**

  يجب على المؤسسات ما يلي:
  - وضع ضوابط كافية للكشف عن الشيفرات الخبيثة والبرمجيات الخبيثة ومنعها والتعافي منها
  - وضع ضوابط ضد استخدام شيفرة الهاتف المحمول
  - ضمان وضع الإجراءات الوقائية المناسبة في أنظمة المعلومات لمنع تنفيذ شيفرات الهاتف المحمول غير المصرح بها
  - اكتشاف ومنع استخدام البرامج غير المصرح بها (مثال: القائمة البيضاء للتطبيقات)

- تحديد الإجراءات والمسؤوليات للتعامل مع برامج حماية الأنظمة من البرمجيات الخبيثة، والتدريب على استخدامها، وإعداد التقارير بخصوصها والتعافي من هجمات البرمجيات الخبيثة

- **النسخ الاحتياطي**
  - يجب وضع سياسة نسخ احتياطي لتحديد متطلبات المؤسسة للنسخ الاحتياطي للمعلومات والبرامج والأنظمة
  - يجب أن تحتفظ المؤسسة بنسخ احتياطية عن المعلومات والبرامج وصور النظام واختبارها بانتظام وفق سياسة نسخ احتياطية متفق عليها
  - يجب توفير مرافق كافية للنسخ الاحتياطي لضمان إمكانية استعادة جميع المعلومات والبرامج الأساسية / الهامة عقب وقوع كارثة أو عطل في الوسائط

- **التسجيل والمراقبة**
  - يجب على المؤسسة تفعيل تسجيل الأحداث وفقًا لمتطلبات ضبط النظام ومواصفات الشركة الصانعة
  - يجب أن يُسجل السجل الأخطاء والاستثناءات وأحداث النظام والأحداث الأمنية وما إلى ذلك. كما يجب وضع ضوابط لحماية السجلات ضد العبث والوصول غير المصرح به إليها
  - يجب مراقبة أنشطة مسؤول النظام والمشغل وفقاً للقوانين ذات الصلة مثل سياسة تأمين المعلومات الوطنية ومعيار أمن نظام الاتصالات الداخلي (ICS) الوطني، الاستراتيجية الوطنية للأمن السيبراني، والمبادئ التوجيهية لمصرف قطر المركزي المتعلقة بقواعد المراقبة البنكية ووفقًا للمتطلبات الأمنية.
  - يجب مزامنة جميع الساعات ذات الصلة بأنظمة معالجة المعلومات أو مجال الأمن مع مصدر زمني مرجعي واحد
  - يجب على المؤسسة الاحتفاظ بسجل لجميع سجلات أوامر التشغيل والصيانة وفقًا لشروط الترخيص

- **قابلية التعرض للمخاطر و إدارة البرامج**
  - يجب على المؤسسة أن تطور وتحتفظ بآلية لمعرفة نقاط الضعف التقنية باستخدام فحص قابلية التعرض للمخاطر واختبار اختراق الشبكات لأنظمة المعلومات المستخدمة وتعرضها لتلك المخاطر
  - على المؤسسة التأكد من إجراء مراجعات دورية للبنية التحتية بما في ذلك أجهزة وتطبيقات الشبكة لتحديد أي نقاط ضعف
  - يجب اتخاذ الإجراءات لتقليل قابلية التعرض للمخاطر بشكل ملائم وفي الوقت المناسب
  - يجب اتخاذ إجراءات دورية لإصلاح المشاكل ومنع تكرارها

- **إدارة أمن الشبكات**
  - يجب على المؤسسة إدارة الشبكة ومراقبتها لحماية المعلومات في الأنظمة والتطبيقات
  - يجب تطبيق الفصل بين الشبكات عن طريق تجميع خدمات المعلومات والمستخدمين ونظم المعلومات
  - يجب على المؤسسة تطبيق ضوابط أمنية على الشبكة لضمان تشفير المعلومات المنقولة من خلال أنظمة الشبكة الحساسة
  - يجب أن تتأكد المؤسسة من رصد سجلات الأحداث الخاصة بأجهزة الشبكة وأن يتم تنفيذ التدابير المناسبة لتحديد أي حوادث أمنية حدثت أو ربما تحدث
  - يجب أن تتأكد المؤسسة من أن أمن خدمات الشبكة محدد ومُدرج في أية اتفاقية لخدمات الشبكة، سواء داخل المؤسسة أو خارجها. ويتضمن ذلك ميزات الأمان ومستويات الخدمة ومتطلبات الإدارة لكافة خدمات الشبكة
  - يجب القيام بتعزيز الشبكة وتقويتها كإجراء تحسين مستمر لضمان عمليات الضبط والتهيئة

- **الأجهزة المحمولة والعمل عن بعد**
  - يجب على المؤسسة تطبيق التدابير الأمنية المناسبة ضد مخاطر استخدام الأجهزة المحمولة
  - يجب أن يكون لدى المؤسسة تدابيراً أمنية لحماية معلومات أنشطة العمل عن بعد
  - يجب أن تكون إمكانية الوصول عن بعد من موقع أجنبي متاحة على أساس الحاجة فقط

- **جمع المعلومات ونقلها**
  - يجب على المؤسسة الحصول على موافقة الفرد (المستخدم النهائي) قبل جمع معلومات هويته لأغراض المصادقة، وينبغي التأكد من أن المعلومات المجمعة تُستخدم فقط لغرض المصادقة على هوية المستخدم.
  - يجب على المؤسسة حماية المعلومات أثناء نقلها عبر جميع أنواع مرافق الاتصالات، بما في ذلك الرسائل الإلكترونية واستخدام الإنترنت والوسائط المادية المتنقلة
  - يجب أن يكون لدى المؤسسة القدرة على النقل الآمن لمعلومات الأعمال مع أطراف خارجية. يجب استخدام اتفاقات السرية أو اتفاقيات عدم الإفصاح لحماية نقل المعلومات

- **التشفير**
  - يجب على المؤسسة استخدام ضوابط تشفير تتسق مع القوانين واللوائح ذات الصلة مثل سياسة تأمين المعلومات الوطنية ووفقًا للمتطلبات الأمنية. يجب تطوير وتنفيذ رقابة إدارة المفاتيح، والتي تتضمن الشهادات الرقمية ومفاتيح التشفير لحماية المفاتيح طوال دورة حياتها.

➢ **الاستحواذ على النظام وتطويره وصيانته**

- **المتطلبات الأمنية لأنظمة المعلومات**
  - يجب تحديد المتطلبات الملائمة المتعلقة بالأمن وإدراجها خلال تطوير أنظمة معلومات جديدة أو تحسينات لأنظمة المعلومات القائمة
  - على المؤسسة التأكد من التطوير الآمن للبرمجيات والأنظمة من خلال تطبيق الضوابط الأمنية على عمليات التطوير وبناء بيئة التطوير الآمنة. يجب اتباع عملية إدارة التغيير للحكم في التغييرات في دورة حياة التطوير
  - على المؤسسة التأكد من إجراء التحسين المستمر لتأمين خدمات التطبيقات والمعاملات على الشبكات العامة مثل الإنترنت
  - بالنسبة لتفعيل عناصر الشبكة في الشبكة، يجب اختبار عناصر الشبكة وفقًا لمعايير الأمان الدولية ذات الصلة، حسب الاقتضاء، على سبيل المثال: المعايير الخاصة بنظام إدارة أمن المعلومات وفقاً لسلسلة معايير شهادة الآيزو ISO 27000.
  - يتم الاحتفاظ بنسخ نتائج الاختبارات والشهادات / تقارير الاختبارات لفترة محددة من تاريخ شراء المعدات
  - يجب تحديد الخصائص الأمنية العصرية ذات الصلة والميزات المتعلقة بأمن الاتصالات وتنفيذها في الشبكة. يجب الاحتفاظ بقائمة بخصائص الأمن والمعدات والبرامج وما إلى ذلك إلى حين استخدامها
  - يجب على المؤسسة إجراء مراجعة واختبار تقني للتطبيقات بعد تغيير نظام التشغيل أو ترقيته للتأكد من عدم وجود أي تأثير سلبي على العمليات التنظيمية أو الأمن. يجب على المؤسسة فرض قيود على التغييرات في حزم البرامج من أجل الحد من التغييرات، وتثبيط التعديلات على حزم البرامج وفرض رقابة صارمة على التعديلات.
  - يجب على المؤسسة وضع المبادئ الهندسية الآمنة للنظام مثل التعزيز والاختبار وغيرها من المبادئ، وتطبيقها على أنظمة المعلومات. يجب على المؤسسة مراقبة تطوير البرمجيات المستندة إلى أطراف خارجية والإشراف على ذلك، وذلك في حال تطوير التطبيق من قبل مورد خارجي.

- يجب إجراء اختبار أمن النظام المناسب واختبار قبول النظام (اختبار قبول المستخدم) لاختبار أنظمة المعلومات قبل نقلها إلى بيئة الإنتاج
- يجب أن تكون بيانات الاختبار المستخدمة للاختبار محمية ومراقبة بشكل مناسب

➢ أمن الموردين

- الموردون هم أولئك الذين يجري التعاقد معهم لتوريد الأجهزة والبرامج والخدمات المتخصصة الضرورية لإدارة العمليات التقنية (مثال: الشبكة وتكنولوجيا المعلومات وغيرها) والخدمات المتخصصة لإدارة العمليات التجارية والعمليات (مثال: مركز الاتصال وطباعة الفواتير ومعالجة الفواتير والأمور اللوجستية وغير ذلك.) و/ أو أي تركيبة مما ذكر أعلاه. يجب على المؤسسات اتباع المبادئ التوجيهية أدناه لضمان أمان وسلامة العلاقات مع الموردين.
  - يجب أن توافق المؤسسات وتوثق متطلبات أمن المعلومات من أجل تخفيف المخاطر المرتبطة بوصول الموردين إلى أصول المعلومات الخاصة بالمؤسسة
  - يجب أن تكون هناك اتفاقيات مع الموردين لإدراج متطلبات معالجة مخاطر أمن المعلومات المرتبطة بخدمات تكنولوجيا المعلومات والاتصالات وسلسلة توريد المنتجات
  - يجب أن تقوم المؤسسات بصورة منتظمة بمراقبة ومراجعة وتدقيق تقديم الموردين للخدمات
  - ينبغي إدارة التغييرات في تقديم الخدمات من قبل الموردين، بما في ذلك الحفاظ على وتحسين سياسات وإجراءات وضوابط أمن المعلومات القائمة، مع مراعاة مدى أهمية وحساسية معلومات الأعمال والنظم والعمليات ذات الصلة، وإعادة تقييم المخاطر

➢ إدارة حوادث أمن المعلومات

- **إدارة الحوادث الأمنية والتحسينات**
  - يجب أن يكون لدى المؤسسة عملية موثقة لضمان الاستجابة السريعة والفعالة والمنظمة لأحداث أمن المعلومات. يجب إبلاغ الإدارة بأحداث أمن المعلومات بناءً على المعايير المحددة في الوقت المناسب
  - يجب على المؤسسة توفير آلية للمستخدمين للإبلاغ عن أي نقاط ضعف أمنية في الأنظمة أو الخدمات تمت ملاحظتها أو الاشتباه في وجودها
  - يجب على المؤسسات الإبلاغ عن حوادث أمن المعلومات وعمليات الاحتيال إلى مركز قطر للاستجابة لطوارئ الحاسب الآلي (كيوسيرت) خلال 72 ساعة دون أي تأخير غير مبرر
  - في حالة التأخير يجب على المؤسسة تقديم المبررات الصحيحة
  - يجب إنشاء قاعدة معرفة بناء على الدروس المستفادة من حوادث أمن المعلومات.
  - يجب تطبيق الضوابط المناسبة لتحديد وجمع وامتلاك وحفظ المعلومات التي يمكن استخدامها كأدلة. يجب تطبيق علم الأدلة الجنائية الشبكية على الحوادث الأمنية لتحديد مقدار التعرض للمخاطر والأسباب الجذرية لذلك.

➢ إدارة استمرارية أمن المعلومات

- يجب على المؤسسة تخطيط وتطبيق استمرارية أمن المعلومات التي تخاطب متطلبات أمن المعلومات اللازمة في الأوقات الصعبة
- يجب على المؤسسة تطوير خطط استمرارية العمل والحفاظ عليها لضمان استمرارية العمليات في الأوقات الصعبة
- يجب بناء وحدات احتياطية إضافية ملائمة لتلبية متطلبات التوفر وفقًا لما تقتضيه متطلبات العمل
- يجب اختبار خطط الاستمرارية وتطويرها (إذا لزم الأمر) على أساس منتظم للتأكد من فعاليتها وحداثتها

➢ إدارة الالتزام بأمن المعلومات

- يجب تحديد جميع المتطلبات التشريعية والتنظيمية والتعاقدية ذات الصلة ونهج المؤسسة لتلبية تلك المتطلبات بشكل علني وتوثيقها وتحديثها لكل نظام معلومات وللمؤسسة ككل أيضاً
- يجب تطبيق الإجراءات المناسبة لضمان الامتثال للمتطلبات التشريعية والتنظيمية والتعاقدية المتعلقة بحقوق الملكية الفكرية واستخدام البرمجيات المسجلة الملكية
- يجب على المؤسسة أن تراجع بصورة مستقلة نهجها في إدارة أمن المعلومات وتنفيذه (أي: أهداف الرقابة وضوابط وسياسات وعمليات وإجراءات أمن المعلومات) في الفترات المخططة أو عند حدوث تغييرات مهمة
- يجب مراجعة أنظمة المعلومات بانتظام للتأكد من امتثالها لسياسات ومعايير أمن المعلومات الخاصة بالمؤسسة.

➢ التدقيق الداخلي

- يجب على المؤسسة إجراء عمليات تدقيق داخلية في فترات زمنية مخططة لمعرفة ما إذا كان إطار عمل أمن المعلومات يتوافق مع:
  - المتطلبات المحددة ذاتيًا لإدارة أمن المعلومات.
  - متطلبات أي معايير ذات صلة مثال:QCB Framework ، PCI DSS ، ISO 27001: 201 إلخ.
  - يجب على المؤسسة ضمان تنفيذ خطة التدقيق الداخلي تنفيذاً فعالاً والمحافظة على ذلك.
  - يجب على المؤسسات التأكد من أن نتائج عمليات التدقيق يتم إبلاغها إلى الإدارة ذات الصلة.

➢ أفضل الممارسات لتأمين التجارة الإلكترونية

- استخدم بروتوكول التشفير TLS 1.1 أو بروتوكول أعلى منه عند نقل بيانات حامل البطاقة داخليًا (على سبيل المثال، عند نقل بيانات حامل البطاقة لدى نقاط الدخول والخروج) عبر الشبكة.
- بسبب الطبيعة الديناميكية لبيئات التجارة الإلكترونية والتغييرات المتكررة في مواقع الويب وتطبيقات الويب، إدرس جدوى تثبيت جدار حماية لتطبيقات الويب (WAF).
- يُستحسن أيضًا وضع قواعد جدار الحماية لضمان عدم وصول حركة المرور غير المرغوب فيها (سواءً الدخول والخروج) إلى الشبكة. من المهم فهم نوع وطبيعة أي جدران حماية مثبتة في بيئة مقدم الخدمة وتتحكم في الوصول إلى الخدمات أو البيئات المقدمة للتاجر
- راجع بانتظام أي روابط (مثال: عناوين URL و iFrames وواجهات برمجة التطبيقات وغيرها) بدءاً من موقع التاجر على الويب وانتهاء ببوابة الدفع للتأكد من أن الروابط لم يتم تغييرها لإعادة التوجيه إلى مواقع غير مصرح بها.
- يُفضل أن يتحقق التاجر من مزود الخدمة الخاص به لضمان تشغيل برامج مكافحة الفيروسات / برامج مكافحة البرمجيات الخبيثة على الأنظمة المقدمة للتاجر. إذا لم يقم موفر الخدمة بتشغيل برنامج مكافحة الفيروسات نيابة عن التاجر، فمن المستحسن أن يفهم التاجر سبب ذلك، وأن يُطبق حلاً خاصاً به لهذه الأنظمة. من المستحسن أيضًا أن يكون للتاجر برنامج لمكافحة الفيروسات يعمل على الأنظمة التي يديرها.
- يُنصح التجار بأن يسألوا مزودي الخدمات الذين يتعاملون معهم عن الأنظمة الموجودة لديهم لكشف حالات الاختراق/ منع الاختراق ومراقبة سلامة الملفات. ويُوصى التجار أيضاً بضمان مراقبة أي اختراقات لأنظمتهم.

➢ أفضل الممارسات لأمان المستخدم النهائي

- يجب على المستخدمين النهائيين تحديث كلمات المرور الخاصة بهم بانتظام والاحتفاظ بكلمة مرور معقدة يصعب تخمينها (مزيج من الأحرف الخاصة والحروف الهجائية والأرقام)
- يجب على المستخدمين عدم الإفصاح عن معلوماتهم (مثل رقم الحساب ورقم التعريف الشخصي وتفاصيل بطاقة الائتمان وغيرها) عبر المكالمات الهاتفية لأن هذا يمكن أن يكون هجوماً باستخدام حيل الهندسة الاجتماعية
- يجب على المستخدمين توخي الحذر أثناء الوصول إلى رسائل البريد الإلكتروني من مرسل مجهول، والتحقق دائمًا من المصدر قبل النقر على أي روابط قد تكون موجودة في البريد
- يجب على المستخدمين دائمًا استخدام برامج مكافحة الفيروسات على الأجهزة الشخصية
- يجب على المستخدمين الحفاظ على تحديث أنظمة التشغيل والبرامج على أجهزتهم
- يجب مراجعة حسابات الإنترنت وتقارير الائتمان بصورة دورية
- يجب على المستخدمين أثناء ربط حسابات الشبكات الاجتماعية قراءة سياسة الخصوصية الخاصة بتاجر التجارة الإلكترونية وفهمها بدقة، ومعرفة كيفية استخدام معلوماتهم
- يجب اختيار أعلى مستوى متاح لإعدادات الخصوصية والأمان وتفعيله على أي موقع من مواقع الوسائل الاجتماعية
- تجنب استخدام شبكات Wi-Fi العامة، والتي تعتبر من الأهداف الغنية للصوص عبر الإنترنت
- يجب على المستخدمين عمل نسخ احتياطية عن الملفات بشكل منتظم على محرك أقراص خارجي (لاستعادة البيانات بأمان في حالة وقوع أي حوادث)
- الاشتراك في صفحات الشبكات الاجتماعية التي تم التحقق منها، واستخدام تطبيقات الجوال الرسمية المرتبطة بموقع ويب رسمي
- إبلاغ البنك بالتغييرات في رقم الهاتف المحمول لضمان عدم إرسال إشعارات الرسائل القصيرة SMS إلى شخص آخر
- ومن أفضل الممارسات تجنب استخدام خيار «تذكر رقم بطاقتي» على المواقع التي تجري فيها المعاملات

٣-٢ إدارة الهوية - تسجيل الدخول

➢ إدارة الهوية للمؤسسات

- يجب تحديد وتطبيق إطار عمل رسمي أو سياسة لإدارة الهوية معتمدة من الإدارة العليا
- يجب تطبيق عمليتي التسجيل وإلغاء التسجيل بشكل رسمي للمستخدمين لتفعيل منح حقوق الوصول
- يجب أن يكون لكل مستخدم هوية مميزة لربط المستخدمين بتعاملاتهم وتحميلهم المسؤولية عنها
- يجب عدم السماح باستخدام الهويات المشتركة إلا إذا كانت ضرورية لأسباب تجارية أو تشغيلية، ويجب الموافقة على ذلك وتوثيقه
- ينبغي، وعلى الفور، تعطيل أو إزالة هويات المستخدمين الذين تركوا المؤسسة
- يجب تحديد وإزالة / تعطيل هويات المستخدمين التي لم تعد مطلوبة بصورة دورية. يجب أن تتأكد المؤسسات من عدم إصدار هويات تعريف المستخدمين تلك لأي مستخدمين آخرين

- يجب أن تكون هناك عملية رسمية لمنح حقوق الوصول للمستخدمين، لمنح أو إلغاء حقوق الوصول لجميع أنواع المستخدمين لجميع الأنظمة والخدمات
- يجب أن تتضمن عملية تعيين أو إلغاء حقوق الوصول الممنوحة لمعرفات المستخدمين ما يلي:
  - الحصول على تفويض من إدارة / مالك نظام أو خدمة المعلومات لغرض استخدام نظام أو خدمة المعلومات
  - التحقق من أن مستوى الوصول الممنوح متوافق مع سياسات الوصول لدى المؤسسة
  - التأكد من عدم تفعيل حقوق الوصول قبل إتمام إجراءات التفويض
  - الاحتفاظ بسجل مركزي يضم حقوق الوصول الممنوحة لهوية المستخدم للوصول إلى نظم وخدمات المعلومات
  - تعديل حقوق الوصول للمستخدمين الذين قاموا بتغيير الأدوار أو الوظائف، وإجراء مراجعة دورية لحقوق الوصول مع مالكي نظم المعلومات أو الخدمات
- يجب تقييد تخصيص واستخدام حقوق الوصول المميزة ومراقبتها
- يجب تقييد الوصول إلى المعلومات ووظائف نظام التطبيق وفقاً لسياسة ضبط الوصول لدى المؤسسة.
- تمكين الدخول الموحد (SSO). وباستخدامك ميزة الدخول الموحد (SSO)، ستوفر للمستخدمين لديك إمكانية استخدام نفس مجموعة بيانات وثائق المصادقة اللازمة لتسجيل الدخول والوصول إلى الموارد التي يحتاجون إليها، بغض النظر عن موقع هذا الموارد
- استخدام ضبط الوصول القائم على الدور - يعد تقييد الوصول بالحاجة إلى المعرفة والمبادئ الأمنية القائمة على أقل الامتيازات أمراً لا غنى عنه للمؤسسات التي ترغب في فرض سياسات أمن للوصول إلى البيانات

إدارة الهوية لهويات العملاء

- يجب تطبيق وتوثيق عملية رسمية لإنشاء هوية العميل، لتمكين العملاء من إنشاء حساب مع تجار التجارة الإلكترونية
- يجب أن يحظى كل عميل بهوية مستخدم مميزة تُخصص له وتتمتع بالحماية من خلال كلمة مرور منيعة.
- يجب على المؤسسة توفير مستوى التأكيد - 2 وفقاً لمعايير الآيزو / IEC DIS 29115 لغرض تسجيل المستخدم.
- يجب على المؤسسات التأكد من إصدار بطاقة هوية واحدة لكل عميل يتم ربطها بمعرّف شخصي، على سبيل المثال لا الحصر رقم الهاتف المحمول والبريد الإلكتروني وغير ذلك
- يجب على المؤسسات توفير خيار للعملاء لربط هويات تسجيل الدخول الخاصة بهم مع موقع فيسبوك أو جوجل أو أي حساب على وسائل التواصل الاجتماعي الأخرى
- يجب على المؤسسات مراجعة هويات العملاء بصورة دورية وتعطيل / إزالة جميع الهويات غير النشطة
- يجب فرض المصادقة متعددة العوامل (MFA) على العملاء.

٣-٣ تأكيد الدفع

ضوابط الأمن لأدوات الدفع

- البطاقات (البطاقات الائتمانية والبطاقات المدينة): تستخدم البطاقات الائتمانية والبطاقات المدينة على نطاق واسع في معاملات التجارة الإلكترونية. ينبغي الرجوع إلى المبادئ التوجيهية التالية لتعزيز أمن الدفع بالبطاقات:
  - يجب على التجار العاملين في مجال التجارة الإلكترونية أن يختاروا المستلم/معالج الدفع ومزود الخدمة المناسب. وعليهم أن يعقدوا شراكات مع مستلم/معالج دفع قادر على توفير دعم فعال لإدارة المخاطر وبوسعه إثبات فهمه الشامل لمخاطر الاحتيال على الإنترنت والمسئولية المترتبة على ذلك.
  - التركيز على الحد من المخاطر: التقاط تفاصيل البطاقة وحامل البطاقة الأساسية فقط من خلال التركيز على حقول بيانات المعاملة المطلوبة، والتحقق من البطاقة وبيانات العميل التي يتم تلقيها عبر الإنترنت.
  - إنشاء آلية لمنع الاحتيال الداخلي: يجب إنشاء بنية تحتية لإدارة المخاطر، وملفات متينة لتجنب عمليات الاحتيال الداخلية، وضوابط ذكية للمعاملات
  - تطبيق الفحص ضد الاحتيال: طرق الفحص ضد عمليات الاحتيال يمكن أن تساعد في تقليل عمليات الاحتيال في مبالغ الشراء الكبيرة والمعاملات عالية المخاطر. من خلال فحص معاملات البطاقة عبر الإنترنت بعناية، يمكن للمؤسسات تجنب أنشطة الاحتيال قبل أن تؤدي إلى خسارات باهظة للأعمال.
  - يجب على المؤسسات تشفير جميع تفاصيل حامل البطاقة التي يتم تخزينها
  - يجب على المؤسسات عدم تخزين رقم التحقق من البطاقة (CVV) لحاملي البطاقات.
  - استخدم آلية التحقق الأمن ثلاثية الأبعاد 3D Secure (المتحقق منها بواسطة بطاقة Visa أو Secure-code أو Mastercard) أو أي معيار صناعي رائد آخر لضمان أمن المعاملات
  - حماية حساب التاجر من الاقتحام: باستخدام أجهزة حاسوب متطورة وأدوات عالية التقنية، يتمكن المهاجمون السيبرانيون من الوصول إلى عربة التسوق وأنظمة معالجات بوابة الدفع، ومهاجمة حسابات التاجر الإلكترونية الضعيفة، وإجراء عمليات التزوير في إيداعات التاجر. لكن عبر اتخاذ إجراءات استباقية، يمكن للمؤسسات أن تقلل من هذه الهجمات السيبرانية والمخاطر المرتبطة بها
  - يجب إنشاء عملية آمنة لتوجيه عملية منح التفويض: قبل قبول أي بطاقات للدفع عبر الإنترنت، تأكد من وجود عملية آمنة وفعالة لتقديم طلبات التفويض عبر الإنترنت
  - يجب أن تحافظ المؤسسات على سرية بيانات حامل البطاقة من خلال الالتزام بمعايير (PCI DSS) أو المبادئ التوجيهية لمصرف قطر المركزي أو أي معايير رائدة أخرى في هذا المجال.
  - يجب استخدام المصادقة متعددة العوامل أو مستوى المصادقة - 3 من معايير الآيزو (ISO / IEC DIS 29115) وما فوق هذا المستوى للمعاملات

- **المحافظ الرقمية وأدوات الدفع مسبقة الدفع**
  - يجب على المؤسسات إجراء مراجعات أمنية دورية للتطبيق وبنيتة التحتية لكشف وتحديد أي مخاطر متأصلة.
  - يجب إجراء تقييم لتطبيقات الهاتف المحمول دورياً لتحديد نقاط الضعف فيها والمخاطر المرتبطة بها.
  - ينبغي إبلاغ جميع أصحاب المصلحة بنقاط الضعف تلك، وصياغة خطة معالجة مع تحديد الجداول الزمنية لمعالجة هذه النقاط

- يجب على المؤسسات تحديد المتطلبات القانونية والتنظيمية المعمول بها وضمان الامتثال بها
- الجهة المُنظمة؛
- يجب على المؤسسات إجراء مراجعة أمنية سنوية للمحافظ الإلكترونية وفقاً لضوابط تتضمن، على سبيل المثال لا الحصر، ما يلي:
  ١. الضوابط العامة لتكنولوجيا المعلومات (إدارة التغييروإدارة ضبط وصول المستخدم وإدارة الحوادث والمشاكل وإدارة التحديث والمعالجة وإدارة السجلات)
  ٢. ضوابط عمليات الأعمال (السياسات والإجراءات التنظيمية وغيرها)
  ٣. تطبيق تقييم الأمن (عبر الشبكة والهاتف المحمول)
  ٤. مراجعة تهيئة الإعدادات الأمنية
  ٥. مراجعة أمن البنية التحتية.
  ٦. الامتثال لأية معايير دولية مثل TCG Framework، NIST Cybersecurity Framework.
- يجب مراعاة متطلبات خصوصية البيانات وإدراجها لضمان خصوصية بيانات العميل
- يجب على المؤسسات إجراء مراجعات لتهيئة الإعدادات الأمنية استنادًا إلى المبادئ التوجيهية لمركز قطر للاستجابة لطوارئ الحاسب الآلي (كيوسيرت)/ معهد (NIST) الخاصة بأجهزة الشبكة لتحديد نقاط الضعف والمخاطر المرتبطة بها. علاوة على ذلك، يجب تحديد أولويات نقاط الضعف هذه على أساس درجة الخطورة، وضمان معالجة هذه النقاط ضمن الفترات الزمنية المحددة.

- **الدفعات الإلكترونية المصرفية عبر الإنترنت (OBeP):**
  - يتعين على المؤسسات المصرفية إنشاء بنية تحتية قوية وحديثة لتكنولوجيا المعلومات والالتزام بمتطلبات مصرف قطر المركزي
  - يجب على المؤسسات المصرفية استخدام آليات المصادقة متعددة العوامل في المصادقة على هويات المستهلكين
  - يجب على المؤسسات المصرفية استخدام حل لمراقبة عمليات الاحتيال لمنع عمليات الاحتيال المالي عبر الإنترنت
  - تُوصى المؤسسات بصياغة إطار أمن سيبراني قوي وأن تجري تقييمات دورية لضمان الامتثال للسياسات والإجراءات المعتمدة
  - يجب مراقبة جميع المعاملات عالية المخاطر وإرسال الإخطارات إلى العملاء عبر الرسائل القصيرة / البريد الإلكتروني
- يجب أن تكون مجالس إدارات المؤسسات المالية على علم بالمخاطر المرتبطة بالخدمات المصرفية الإلكترونية وبتقييم المخاطر الناتجة عنها. يجب على البنوك أن تتصدى لهذه المخاطر من خلال استراتيجية واضحة مدفوعة من الأعلى، ويجب ضمان مراعاة هذه الاستراتيجية لتأثيرات الأعمال المصرفية الإلكترونية، حيثما كان ذلك ذا صلة. يجب نشر مثل هذه الاستراتيجية بشكل واضح في كل مجالات الأعمال، ودعمها بخطة أعمال واضحة مع وسائل فعالة لمراقبة أدائها.

- **الدفع نقداً عند التسليم**
  - يجب تطبيق أمن النقد من قبل جميع الموظفين والإدارة تطبيقاً حرفياً
  - يجب تقسيم المناطق جغرافياً عند توفير خيار الدفع النقدي للعملاء
  - يجب أن تكون عقود الطرف الثالث التي تحدد شروط وأحكام الخدمات مع شركاء الخدمات اللوجستية سارية المفعول. يجب أن تُحدد العقود بوضوح اتفاقيات مستوى الخدمة.
  - يجب على تاجر التجارة الإلكترونية أن يراقب بصفة دورية اتفاقيات مستوى الخدمة المتفق عليها مع مزود الخدمات اللوجستية، وإبقاء أصحاب المصلحة في الصورة

- **ممارسات الدفع الآمنة للعملاء**
  - حفظ رقم التعريف الشخصي (PIN) وكلمات المرور الخاصة بالمعاملات المصرفية لأنها معلومات شخصية. تجنب تدوين أو كتابة رقم التعريف الشخصي (PIN) وكلمات المرور الخاصة بالمعاملات المصرفية
  - يجب ألا تشارك معلومات رقم التعريف الشخصي (PIN) وكلمات المرور الخاصة بالمعاملات المصرفية مع أي شخص
  - حدث معلوماتك المصرفية / الشخصية مباشرة في فرع البنك
  - اتصل بالبنك على الفور في أي من الحالات التالية:
    - فقدان بطاقة الدفع، أو
    - حصول معاملة مشبوهة
  - احتفظ بجميع الإيصالات وسجلات المعاملات
  - تغيير كلمات مرور المعاملات المصرفية عبر الإنترنت بشكل دوري
  - مراجعة معاملات الحساب المصرفي مراجعة دورية لتحديد أي معاملات مشبوهة
  - القيام بالبحث لجمع المعلومات عن التاجر قبل تقديم الطلب: احرص دائماً على الشراء من المواقع الإلكترونية للوسطاء والمتاجر ذات السمعة الجيدة
  - التحقق من المبلغ قبل تقديم الطلب
  - انتحال الموقع - وهي مواقع الويب التي تبدو مصممة بحرفية ومهنية وكأنها قانونية بهدف جمع معلومات حساسة من الزائرين غير الحذرين. يمكن اكتشاف مواقع الويب هذه من خلال التحقق بعناية من عنوان(URL).
  - عدم الاستجابة أو فتح روابط الإنترنت أو المرفقات في رسائل البريد الإلكتروني غير المرغوب فيها
  - التسوق في مواقع الويب الآمنة: يستخدم موقع الويب الآمن تقنية التشفير لنقل المعلومات من الحاسوب إلى النظام الحاسوبي للتاجر عبر الإنترنت، مما يحافظ على سلامة وأمن المعلومات السرية مثل تفاصيل بطاقة الائتمان وما إلى ذلك.
  - ابحث عن بروتوكول "(Https)" في عنوان الويب أو عنوان (URL) (عند إدخال معلومات شخصية). هذا يعني أن المعلومات مشفرة بين المتصفح والتاجر، وهذا من شأنه الحفاظ على أمنها وحمايتها من الوصول غير المصرح به.
  - لا تدع المواقع تخزن معلومات البطاقة الائتمانية في ملفاتها
  - تأكد من وجود قفل صغير مغلق في شريط العنوان، أو في الزاوية اليمنى السفلى من النافذة
  - تحقق دائمًا من رمز "قفل" المتصفح، ولكن يجب أن تُدرك أن هذا يُشير فقط إلى قناة اتصال آمنة، وليس بالضرورة إلى موقع ويب شرعي
  - تثبيت وتحديث برامج الأمان (برامج جدار الحماية، ومكافحة الفيروسات، وبرامج مكافحة التجسس). من الأهمية بمكان تثبيت وتحديث هذه البرامج، وإجراء عمليات فحص منتظمة للحواسيب للمساعدة في الحماية من التهديدات مثل الفيروسات وبرامج التجسس والبريد العشوائي وحماية المعلومات الشخصية بشكل عام.
  - الحفاظ على تحديث برنامج النظام ومتصفح الويب
  - استخدام أجهزة شخصية وشبكة (Wi-Fi) خاصة للتسوق عبر الإنترنت بدلاً من جهاز حاسوب عام وشبكة (Wi-Fi) عامة
  - التأكد من تسجيل الخروج من موقع التسوق
  - تجنب الكشف عن كلمات المرور الخاصة بالدفع والتسوق عبر الإنترنت

٤-٣ أفضل ممارسات التصميم

➢ أمن التطبيق

- يجب على المؤسسة التأكد من الآتي في جميع التطبيقات التي تم تطويرها داخلياً أو التطبيقات المستخدمة من قبلها:
  - الحفاظ على سلامة نظم معالجة البيانات الآلية في جميع الأوقات
  - الحفاظ على خصوصية البيانات
  - توفر آليات داخلية كافية لمراجعة ورصد وتقييم ضوابطها وأنظمتها وإجراءاتها ووسائل حمايتها.
- يجب أن تضمن المؤسسة حماية المعلومات الواردة في معاملات خدمات التطبيقات لمنع النقل غير المكتمل أو التوجيه الخاطيء، أو التغيير غير المصرح به للرسالة أو الكشف غير المصرح به أو تكرار الرسائل غير المصرح به أو إعادة التشغيل.
- يجب على المؤسسة النظر في اتباع مجموعة الضوابط التالية لضمان أمن تطبيقاتها:
  - اتباع التطوير الآمن لبناء خدمة آمنة وهيكل وبرمجيات ونظام يُراعي أمن مرحلة التصميم وبيئة التطوير ونقاط الفحص المناسبة في دورة التطوير.
  - يجب أن تظل برمجيات تطبيقات الأعمال قيد التطوير منفصلة تمامًا عن برامج تطبيقات الإنتاج من خلال أنظمة حاسوبية منفصلة ماديًا أو الدلائل أو المكتبات المنفصلة مع فرض ضوابط الوصول الصارمة عليها.
  - يجب إعداد الوثائق التي تعكس الطبيعة والموافقة والأداء لجميع التغييرات الهامة على أنظمة الحاسوب والاتصالات الخاصة بالانتاج التي تملكها المؤسسة، واعتماد تلك الوثائق قبل الشروع بأي تغيير.
  - يجب على الإدارة التأكد من أن جميع أنشطة تطوير البرامج وأنشطة صيانة البرامج التي يقوم بها الموظفون الداخليون متوافقة مع سياسات المؤسسة ومعاييرها وإجراءاتها واتفاقيات تطوير الأنظمة لديها
  - يجب أن يكون كل تغيير غير طارئ على أنظمة الإنتاج في المؤسسة متوافقاً مع هيكل أمن المعلومات، وأن توافق عليه الإدارة كجزء من الإجراءات الرسمية لمراقبة التغيير
- يجب على المؤسسة تصميم مبادئ هندسة نظم معلومات آمنة في جميع الطبقات المعمارية، وبالتحديد: الأعمال والبيانات والتطبيقات والتكنولوجيا.
- يجب على المؤسسة وضع معايير قبول لأنظمة المعلومات الجديدة ومرافق معالجة المعلومات والتحديثات والإصدارات الجديدة لها، بالإضافة إلى إجراء الاختبارات المناسبة للأنظمة أثناء التطوير وقبل وضعها قيد الإنتاج الفعلي.
- يجب إجراء الاختبارات الأمنية من قبل المؤسسات لمعالجة نقاط الضعف في مشروع أمن تطبيقات الويب المفتوحة مقابل المتطلبات الأمنية المحددة في مرحلة التخطيط وتحديد مواطن الضعف، والتي يمكن استغلالها من قبل مصدر التهديد الداخلي/ الخارجي، في النماذج التي يجري تطويرها.
- يجب مراعاة الضوابط التقنية التالية عند دراسة ضوابط تنفيذ سياسات أمن التطبيقات:
  - ضمان حماية التطبيق ضد الوصول غير المصرح به أو التغيير للسجلات والبيانات أو إتلافها أو الكشف عنها أو نشرها
  - تنفيذ مبدأ حق الوصول بأقل الامتيازات، الذي يحد إمكانية وصول المستخدمين إلى الوظائف والبيانات ومعلومات النظام المطلوبة لتنفيذ مهامهم فقط
  - يجب تسجيل محاولات المصادقة الفاشلة في سجل التدقيق، بما في ذلك التاريخ والوقت ومعرّف المستخدم وعنوان المصدر لمحاولة تسجيل الدخول
  - ضمان أمان الشبكة التي يتم من خلالها إنشاء وسائل الاتصال الإلكترونية بين المشاركين في السوق عبر التطبيق ضد الدخول أو الوصول غير المصرح بهما

- يحتوي التطبيق/ موقع الويب على صيغ إرسال وتشفير قياسية بين المشاركين في السوق على المنصة من أجل حماية المعلومات من أي خلل أو قرصنة وما إلى ذلك
- تنفيذ التشفير في نقل جميع المعلومات الحساسة. يجب أن يتضمن ذلك بروتوكول التشفير (TLS) لحماية الاتصال، ويمكن إتمام ذلك بتشفير منفصل للملفات الحساسة أو الاتصالات التي لا تعتمد على بروتوكول (HTTP).
- يجب أن تكون شهادات بروتوكول التشفير (TLS) صالحة وأن تحمل اسم النطاق الصحيح، وليست منتهية الصلاحية، ويتم تثبيتها بشهادات وسيطة عند اللزوم.
- يجب تنفيذ جميع وظائف التشفير المستخدمة لحماية الأسرار من مستخدم التطبيق على نظام موثوق به (مثال: الخادم).
- أن يكون لدى التطبيق / موقع الويب الإجراءات والتسهيلات الكافية لضمان حمايته من الفقد أو التدمير، واتخاذ الترتيبات اللازمة للتعافي بعد الكوارث في مكان مختلف عن المكان الموجود.
- تمتع التطبيق / موقع الويب بنظام معلومات الإدارة الذي يدعم عمليات التجارة الإلكترونية القائمة على الإنترنت من أجل تحقيق اتصال آني مع الأنظمة الأساسية للتجارة الإلكترونية وضمان الفصل الفعال بين أنظمة التطبيقات الأخرى، وتجنب النقل الخارجي وانتشار مخاطر أمن المعلومات.
- تمتع التطبيق/ موقع الويب بجدار حماية قوي، وميزة كشف التسلل، وتشفير البيانات، والتعافي من الكوارث وغيرها من أنظمة إدارة أمن معلومات الإنترنت
- تمتع التطبيق / موقع الويب بالوسائل التي تضمن أن المعلومات والعمليات والإجراءات وأي آلية أخرى بصرف النظر عن اسمها، المعروضة والمنفذة على المنصة، موجودة ومتاحة في كل الأوقات للتحقق والتدقيق.
- توفير طريقة للمستخدمين لتسجيل الخروج من التطبيق. يجب أن يؤدي تسجيل الخروج إلى مسح حالة الجلسة بالكامل وإزالة أو إبطال أي ملفات تعريف ارتباط متبقية
- استخدام مولد أرقام زائفة عشوائية مشفرة بشكل جيد لتوليد رموز جلسة العمل. استخدام التشفير (مثل صفحات الويب المشفرة باستخدام بروتوكول SSL) لحماية سرية الجلسة وأمنها.
- يجب فحص البيانات المستلمة من مصادر البيانات غير الموثوقة قبل الاستخدام الأول.
- استخدام الحد الأدنى من أذونات نظام الملفات على جميع المنصات. استخدام قيود "ch'-rooted" وسياسات الوصول المشفرة لتقييد مكان الحصول على الملفات أو حفظها
- استخدام واجهات برمجة التطبيقات المدمجة الخاصة بالمهام لتنفيذ مهام نظام التشغيل. عدم السماح للتطبيق بإصدار الأوامر مباشرة إلى نظام التشغيل، خاصةً من خلال استخدام واجهات الأوامر (command shells) التي فعلها التطبيق.
- استخدام الفحص الجزئي أو الكلي للتحقق من تكامل الشيفرة المفسرة والمكتبات والملفات التنفيذية وملفات التهيئة
- استخدام القفل لمنع الطلبات المتعددة المتزامنة أو استخدام آلية تزامن لمنع حالات السباق
- حماية المتغيرات والموارد المشتركة من الوصول المتزامن غير الصحيح
- تهيئة جميع المتغيرات ومخازن البيانات الأخرى بشكل صريح، إما أثناء الإقرار أو قبل الاستخدام الأول مباشرةً
- تحديد أساليب (HTTP) والحصول (Get)أو النشر (Post)، التي سيدعمها التطبيق، وما إذا كان سيتم التعامل معه بشكل مختلف في الصفحات المختلفة في التطبيق.
- تعطيل أساليب (HTTP) غير الضرورية، مثل ملحقات (WebDAV). إذا كانت هناك حاجة لطريقة (HTTP) موسعة تدعم معالجة الملفات، فيجب استخدام آلية مصادقة تم فحصها جيدًا.
- مراجعة جميع التطبيقات الثانوية ورمز الطرف الثالث والمكتبات لتحديد ضرورات العمل والتحقق من الوظيفة الآمنة، حيث يمكن أن تؤدي إلى نقاط ضعف جديدة.

- تنفيذ التحديث الآمن: إذا كان التطبيق يستخدم التحديثات التلقائية، فيجب استخدام التواقيع المشفرة للرموز، والتأكيد على عملاء التنزيل أن يتحققوا من هذه التواقيع. استخدام القنوات المشفرة لنقل الرمز من الخادم المضيف.

- يجب أن ترجع المؤسسة إلى أفضل الممارسات في هذا المجال، أفضل 10 ممارسات لدى (OWASP)، والمبادئ التوجيهية لدى مركز قطر للاستجابة لطوارئ الحاسب الآلي (كيوسيرت)، والمبادئ التوجيهية لدى (TCG) وغيرها أثناء تصميم الضوابط لضمان أمن تطبيقها.

➢ متطلبات التصميم

- يجب على المؤسسات تقييم التصميم المقترح والضوابط والمنهجية الأمنية والتأكد من أن التصميم يتكامل مع مبادئ أمن المعلومات. ينبغي النظر في أمن المعلومات في جميع جوانب دورة حياة تطوير البرمجيات
- ينبغي أن تدرس المؤسسة طرقاً مختلفة مثل متطلبات الامتثال المستمدة من السياسات واللوائح، أو نماذج التهديدات، أو مراجعات الحوادث، أو استخدام المستويات الأولى لنقاط الضعف لتحديد متطلبات أمن المعلومات. يجب توثيق هذه المتطلبات ومراجعتها من قبل جميع أصحاب المصلحة.
- يجب على المؤسسة تحليل المخاطر الأمنية لأي تقنية جديدة ومراجعة التصميم ضد أنماط الهجوم المعروفة. يجب مراجعة هذه المبادئ على فترات دورية للتأكد من أنها تسهم بفعالية في تعزيز معايير الأمن في إطار العملية الهندسية.
- يجب على المؤسسات وضع بيان واضح ومختصر لسياسة الخصوصية وإتاحته لزوار الموقع من خلال الروابط الموجودة على الصفحة الرئيسية. قد تخضع هذه الممارسة للمتطلبات القانونية. للحد من مخاوف العملاء حول تقديم البيانات الشخصية، يجب أن تحدد سياسة الخصوصية ما يلي:
  - ما هي بيانات العملاء التي يتم جمعها وتتبعها
  - مع من تتم مشاركة هذه المعلومات
  - كيف يمكن للعملاء الانسحاب
- إنشاء حقول بيانات المعاملة التي يمكن أن تساعد المؤسسات على اكتشاف المواقف التي تنطوي على مخاطر، والطلب من العميل تعبئتها. يمكن أن تؤدي بعض حقول بيانات المعاملات المعينة دورًا هاماً في تقييم مخاطر الاحتيال في المعاملة. تشمل حقول بيانات المخاطر الرئيسية ما يلي:
  - المعلومات الديموغرافية، مثل: أرقام الهاتف، التي يمكن التحقق من صحتها باستخدام عمليات البحث العكسية في الدليل
  - عنوان البريد الإلكتروني خاصة عندما يتعلق الأمر بخدمة "شخص مجهول"
  - اسم حامل البطاقة وعنوان الفواتير، والذي يمكن التحقق من صحته باستخدام خدمات البحث في الدليل
  - اسم وعنوان الشحن، خاصةً إذا كانت هذه المعلومات مختلفة عن معلومات فواتير حامل البطاقة
  - قيمة التحقق من البطاقة 2 (CVV2)، خاصة لمواقع الويب التي تبيع سلع أو خدمات عالية المخاطر
- يُوصى بأن تقوم المؤسسات بفحص العناوين الدولية عالية المخاطر. قد يحمل قبول المعاملات من بعض المواقع الدولية مستويات عالية من المخاطر. التقاط عنوان بروتوكول الإنترنت (IP) وترجمته لتحديد مصدر الشبكة الحاسوبية.
- استخدام برنامج / خدمة الموقع الجغرافي لتحديد دولة عنوان بروتوكول الإنترنت (IP).
- مطابقة دولة بروتوكول الإنترنت (IP) مع دولة عنوان الفواتير والشحن. إذا لم تتطابق البلدان، فاختر ترتيب المراجعة الإضافية.

➢ التكامل مع وسائل التواصل الاجتماعي والمنتديات والمدونات

- يجب أن تركز المؤسسات على "اختبار الاستجابة والتفاعل - (testing waters)" للتأكد مما إذا كان يمكن استخدام وسائل التواصل الاجتماعي كقناة تفاعلية ثنائية الاتجاه للاستماع وإشراك قاعدتها الإعلامية الاجتماعية التي تمتد عبر عملائها وشركائها وعامة الجمهور والموظفين.
- يجب على المؤسسات التي تركز على تطوير وتحسين التطبيقات الاجتماعية أن تأخذ مجموعة الضوابط التالية بعين الاعتبار:
  - صياغة استراتيجية وسائل التواصل الاجتماعي التي تضم: تعريف الاستراتيجية و الرؤية، ونموذج الحوكمة وتقييم نضج وسائل التواصل الاجتماعي وتحليل المشاعر و المؤثرات وغيرها من العوامل
  - يجب على المنظمات تحديد وتعيين الأفراد أو الإدارات داخل المؤسسة لمراقبة قنوات وسائل التواصل الاجتماعي ضمن مجموعات منفصلة
  - إجراء التدقيق الروتيني لتقييم المخاطر واعتبارات الخصوصية
  - قياس ورصد وتحليل وتحسين مؤشرات الأداء الاجتماعي لإنشاء كفاءات تشغيلية أكبر
- يُوصى بأن تستخدم المؤسسات أساليب الاستفادة الأمثل من محركات البحث وآلية التسويق عبر محركات البحث لتعزيز مستويات ظهور مواقع الويب

➢ تقييم المنتج

- **يجب على جميع المؤسسات التي تعرض منتجات عبر الإنترنت أن تلفت انتباه العملاء إلى المعلومات ونواحي المشاركة التالية:**
  - نوع المستهلك الذي يستهدفه المنتج
  - السمات الرئيسية للمنتج
  - الخيارات والتغطية التي يقدمها المنتج، حسب ما هو مطبق
  - الاستثناءات والقيود المرتبطة بالمنتج، إن وجدت
  - إجمالي الأقساط والرسوم الأخرى التي يجب على المستهلك دفعها (بما في ذلك جميع الضرائب السارية) أو إذا لم يكن بالإمكان تحديد مبلغ محدد، يذكر أساس احتساب المبلغ لكي يكون بالإمكان التحقق منه.
  - جوانب "حق الإلغاء" إن وجدت، وكذلك مدة الإلغاء وإجراءات ممارسة هذا الحق
  - الأطر الزمنية لتجهيز الطلبات وإرسال تأكيد بالبريد الإلكتروني للعملاء وملخص الطلب خلال يوم عمل واحد من تاريخ الطلب الأصلي
  - أي مهلة زمنية للتحقق من صحة المعلومات المقدمة

➢ تحديث المحتوى

- **يجب مراعاة النقاط التالية في أي وقت تحتاج فيه حزمة البرامج إلى التعديل:**
  - مخاطر اختراق الضوابط المدمجة وسلامة العمليات
  - ما إذا كان يجب الحصول على موافقة البائع
  - إمكانية الحصول على التغييرات المطلوبة من البائع كتحديثات قياسية للبرنامج
  - التأثير إذا كانت المؤسسة ستصبح مسؤولة عن الصيانة المستقبلية للبرنامج نتيجة للتغيرات
  - التوافق مع البرامج الأخرى المستخدمة

- إذا كانت التغييرات ضرورية، فيجب الاحتفاظ بالبرنامج الأصلي وتطبيق التغييرات على نسخة معينة. يجب تنفيذ عملية إدارة تحديث البرامج للتأكد من تثبيت أحدث التصحيحات المعتمدة وتحديثات التطبيق لكافة البرامج المعتمدة.
- يجب اختبار جميع التغييرات وتوثيقها بشكل كامل، بحيث يمكن إعادة تطبيقها، إذا لزم الأمر، على التحديثات اللاحقة للبرامج. ينبغي اختبار التعديلات والتحقق من صحتها بواسطة هيئة تقييم مستقلة، إذا لزم الأمر
- يجب على المؤسسات أن تكشف كشفاً كاملاً للعميل في صفحة الدفعات الخاصة بموقع الويب عن العمليات والمعلومات الحالية في البلد المتعلقة بالعملة المستخدمة في معاملة الشراء

٣-٥ إمكانية الوصول

- يُوصى بأن يدعم موقع الويب ميزة اللغات المتعددة (مثال: اللغة العربية والإنجليزية وغيرهما)
- يجب على المؤسسات الامتثال لمعايير مجلس هندسة الإنترنت (IAB) الخاصة بالإعلان الرقمي.

الملحق ١:
المصطلحات والتعاريف

الرقم	المصطلح	التعريف
١	ضبط الوصول	يشير إلى التأكد من أن الوصول إلى أصول المعلومات مصرح به ومقيّد بناءً على متطلبات العمل والأمن.
٢	الأصل	هو أي شيء له قيمة معينة بالنسبة لأي مؤسسة
٣	الهجوم	هو محاولة تدمير أو فضح أو تغيير أو تعطيل أو سرقة أو الوصول غير المصرح به إلى الأصل أو استخدامه بدون تصريح.
٤	المصادقة	هي توفير تأكيد بأن السمة المزعومة للمنشأة صحيحة.
٥	التفويض	التفويض هو العملية المستخدمة لمنح الأذونات للمستخدمين المصادق عليهم. يمنح التفويض المستخدم، من خلال التكنولوجيا أو العملية، الحق في استخدام أصول المعلومات، ويُحدد نوع الوصول المسموح به (للقراءة فقط أو الإنشاء أو الحذف و/ أو التعديل). يجب أن يُحدد النظام أو التطبيق ما إذا كان المستخدم لديه إذن لتنفيذ العملية المطلوبة.
٦	التوفر	هي خاصية أن يكون الشيء متاحاً ويمكن استخدامه عند الطلب من قبل جهة مخولة.
٧	السرية	هي سمة عدم إتاحة المعلومات أو الكشف عنها لأفراد أو كيانات أو عمليات غير مصرح لها.
٨	التحسين المستمر	يُعرف على أنه النشاط المتكرر لتحسين الأداء.
٩	الفعالية	هو مدى تحقيق الأنشطة المخطط لها وتحقيق النتائج المخطط لها.
١٠	المعلومات	تنطبق على أي عملية تخزين أو اتصال أو تلقي لأي معارف، مثل: الحقائق والبيانات والآراء، بما في ذلك النماذج الرقمية أو الرسومية أو السردية، سواء كانت شفهية أو محفوظة على أي وسيط للتخزين.
١١	أصل المعلومات	هي المعلومات التي تتمتع بقيمة هامة لشركتنا بما في ذلك الأشخاص والورق و (المعلومات) المنطقية والمادية والبرمجيات والخدمات والموقع
١٢	مرافق معالجة المعلومات	هي أي نظام أو خدمة أو بنية تحتية لمعالجة المعلومات، أو الموقع المادي الذي يحتويها.
١٣	أمن المعلومات	يُعرف على أنه عملية الحفاظ على سرية المعلومات وسلامتها وتوفرها.
١٤	حدث أمن المعلومات	يُعرف على أنه حدوث حالة للنظام أو الخدمة أو الشبكة تشير إلى انتهاك محتمل لسياسة أمن المعلومات أو فشل الضوابط، أو حالة غير معروفة سابقاً قد تكون ذات صلة بالأمن.

الرقم	المصطلح	التعريف
١٥	حادثة أمن المعلومات	هو حادثة مفردة أو سلسلة من الحوادث لأمن المعلومات غير المرغوب فيها أو غير المتوقعة، والتي من المحتمل، بصورة كبيرة، أن ينتج عنها خرق للعمليات التجارية وتهديد أمن المعلومات.
١٦	سلامة المعلومات	وهي سمة التمتع بالدقة والشمولية.
١٧	المخاطر	وهي الجمع بين احتمال وقوع حدث وتأثيره
١٨	التهديد	التهديد هو السبب المحتمل لحدث غير مرغوب فيه قد يؤدي إلى إلحاق الضرر بمؤسسة وأصولها.
١٩	الفيروس	فيروس الحاسوب هو جزء من برنامج ضار يهدف إلى إرفاق نفسه ببرامج أخرى ونسخ نفسه في برامج أخرى، وفي النهاية، قد يصيب كل برنامج في النظام. يوجد أيضاً شكل مختلف يُعرف باسم فيروس الماكرو ، والذي يربط نفسه بوحدات الماكرو، والتي تعد جزءاً من بعض برامج معالجة النصوص وجداول البيانات. هناك برامج ضارة أخرى تحمل أسماء مثل الديدان أو أحصنة طروادة أو القنابل الموقوتة. يمكن أن تكون كل هذه الأشياء ضارةً جداً بنظام ما، لكنها مستقلة بذاتها عوضاً عن نسخ المرفقات.
٢٠	قابلية التعرض للمخاطر	هو عيب أو ضعف في إجراءات أمن النظام أو التصميم أو التنفيذ أو الضوابط الداخلية التي يمكن ممارستها (تفعل بطريق الخطأ أو استغلالها عمداً) وينتج عنه خرق أمني أو انتهاك لسياسة أمن النظام.
٢١	قيمة التحقق من البطاقة	قيمة التحقق من البطاقة (CVV) هو نظام تقوم شركات بطاقات الائتمان بتقديمه للمساعدة في الحماية من عمليات الاحتيال. وهو رمز مكون من ٣ أرقام يتم احتسابه من البيانات الموجودة على الشريط المغناطيسي ولا يمكن تزويره.

الملحق ٢:
قائمة المصادر

قائمة المصادر

- معيار الآيزو 27001: 2013
- إدارة الهوية - معهد SANS
- المبادئ التوجيهية لأمن تطبيق OWASP
- المبادئ التوجيهية لإمكانية الوصول إلى محتوى الويب (WCAG 2.0)
- 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
- معالجة دفعات التجارة الإلكترونية – فيزا
- تقرير طرق الدفع في التجارة الإلكترونية لعام 2016 - The Paypers
- الدفع بواسطة الهاتف المحمول: حرب المحافظ ، 015 - إيرنست آند يونج
- سياسة تأمين المعلومات الوطنية
- معيار أمن نظام الاتصالات الداخلي (ICS) الوطني
- الاستراتيجية الوطنية للأمن السيبراني
- المبادئ التوجيهية لمصرف قطر المركزي حول قواعد الرقابة المصرفية

MOTC
motc.gov.qa