هذا المربع مخصّص لأغراض توجيهية. احذف جميع المربعات التوجيهية بعد تعبئة النموذج. يجب تحرير البنود الملوّنة باللون الأزرق بصورة مناسبة. ويجب إزالة التظليل الملون بعد إجراء التعديلات.

أدخل شعار الجهة بالضغط على الصورة الموضحة.

نموذج سياسة التشفير

استبدل <اسم الجهة> باسم الجهة في مجمل صفحات الوثيقة.
وللقيام بذلك، اتبع الخطوات التالية:

1. اضغط على مفتاحي "Ctrl" و"H" في الوقت نفسه.
2. أضف "<اسم الجهة>" في مربع البحث عن النص.
3. أدخل الاسم الكامل لجهتك في مربع "استبدال" النص.
4. اضغط على "المزيد" وتأكّد من اختيار "Match case".
5. اضغط على "استبدل الكل".
6. أغلق مربع الحوار.

اختر التصنيف

التاريخ: اضغط هنا لإضافة نص

الإصدار: اضغط هنا لإضافة نص

المرجع: اضغط هنا لإضافة نص

اعتماد الوثيقة

الدور	الاسم	التاريخ	التوقيع
اختر الدور	<أدخل الاسم الكامل للشخص>	اضغط هنا لإضافة نص	<أدخل التوقيع>

نسخ الوثيقة

النسخة	التاريخ	عُدلَ بواسطة	أسباب التعديل
<أدخل رقم النسخة>	اضغط هنا لإضافة نص	<أدخل الاسم الكامل للشخص>	<أدخل وصف التعديل>

قائمة المحتويات

الأهداف

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير لضمان الاستخدام السليم والفعال للتشفير لحماية الأصول المعلوماتية الإلكترونية الخاصة بـ<اسم الجهة> وللتقليل من المخاطر السيبرانية والتهديدات الداخلية والخارجية من خلال التركيز على الأهداف الأساسية للحماية وهي: سرية المعلومات، وسلامتها، وتوافرها.

تهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم ٢-٨-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع الأصول المعلوماتية الإلكترونية الخاصة بـ<اسم الجهة>، وتنطبق على جميع العاملين في <اسم الجهة>، بما في ذلك الجهات التي تتعامل معها والأطراف الخارجية.

بنود السياسة

1- البنود العامة

1-1 يجب على <اسم الجهة> تطوير وتوثيق واعتماد إجراءات ومعايير خاصة بالتشفير بناءً على حاجة العمل وعلى تحليل المخاطر في <اسم الجهة> وبحيث يتوافق المستوى الأمني مع المعايير الوطنية للتشفير الصادرة من قبل الهيئة الوطنية للأمن السيبراني. وتشمل هذه الإجراءات على حلول التشفير المعتمدة والقيود المطبقة عليها (تقنياً وتنظيمياً)، وطرق استخدامها وآلية إصدار المفاتيح ونشرها واستعادتها، بالإضافة إلى إدارة النسخ الاحتياطية للمفاتيح وإجراءات إتلاف مفاتيح التشفير. (ECC-2-8-3-1)

2-1 يجب تشفير البيانات أثناء النقل والتخزين بناءً على تصنيفها وحسب السياسات والإجراءات التنظيمية لـ<اسم الجهة>، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

3-1 يجب استخدام طرق وخوارزميات ومفاتيح وأجهزة تشفير محدثة وفقاً لما تصدره الهيئة بهذا الشأن. (CSCC-2-7-1-3)

4-1 يجب تشفير جميع بيانات الأنظمة الحساسة، أثناء النقل (Data-In-Transit). (CSCC-2-7-1-1)

5-1 يجب تشفير جميع بيانات الأنظمة الحساسة، أثناء التخزين (Data-at-Rest) على مستوى الملفات، وقاعدة البيانات، أو على مستوى أعمدة محددة داخل قاعدة البيانات. (CSCC-2-7-1-2)

6-1 يجب تحديد وتوثيق الأدوار والمسؤوليات المتعلقة بإدارة البنية التحتية لمفاتيح التشفير (Key Management Infrastructure "KMI")، للأدوار التالية على الأقل:

1-6-1 مسؤول مفاتيح وأنظمة التشفير (Keying Material Manager) باعتباره <مدير الإدارة المعنية بالأمن السيبراني>.

1-6-2 مشرفو التشفير المسؤولون عن حماية مفاتيح التشفير (Key Custodians).

1-6-3 الجهات المعنية بإصدار الشهادات (Certification Authorities "CAs")، بحيث تكون موثوقة وآمنة.

1-6-4 الجهات المعنية بتسجيل الشهادات (Registration Authorities "RAs")، بحيث تكون موثوقة وآمنة.

2- الاستخدام الآمن للتشفير

2-1 يجب تحديد وتوثيق كافة حلول التشفير المستخدمة (بما في ذلك الخوارزميات والبرامج والوحدات (Modules) والمكتبات (Libraries) ومكونات التشفير الأخرى) وتقييمها واعتمادها من قبل <الإدارة المعنية بالأمن السيبراني> قبل تطبيقها في <اسم الجهة>.

2-2 يجب التأكد من تطبيق التشفير وفقاً لحلول التشفير المعتمدة لدى <اسم الجهة>.

2-3 يُمنع استخدام خوارزميات التشفير المطورة داخلياً وفقاً لدليل التشفير الخاص بمشروع أمان تطبيق الويب المفتوح (OWASP).

2-4 يجب استخدام طرق التحقق الآمن (مثل استخدام مفاتيح التشفير العامة والتواقيع الرقمية والشهادات الرقمية) للحد من المخاطر السيبرانية ووفقاً لحلول التشفير المعتمدة في <اسم الجهة>.

2-5 يجب استخدام التحقق من هوية المستخدم لنقل البيانات السرية للغاية إلى أطراف خارجية باستخدام شهادات التشفير الرقمية (Digital Certificates) المعتمدة، ووفقاً لسياسة حماية البيانات والمعلومات المعتمدة في <اسم الجهة>.

2-6 يجب استخدام وسيلة تحقق من الهوية متعددة العناصر (Multi-Factor Authentication "MFA") للتحقق من صلاحية المستخدم للوصول إلى الأنظمة الحساسة وفقاً لسياسة حماية البيانات والمعلومات المعتمدة لدى <اسم الجهة>.

3- إدارة مفاتيح التشفير

3-1 يجب إدارة مفاتيح التشفير بطريقة آمنة خلال عمليات دورة حياتها (Key Lifecycle Management) والتأكد من استخدامها بشكل سليم وفعّال. (ECC-2-8-3-2)

3-2 يجب أن يتم إصدار شهادات التشفير عن طريق جهة إصدار الشهادات الداخلية في <اسم الجهة> للخدمات المحلية أو عن طريق جهة خارجية موثوقة.

3-3 يجب حفظ معلومات المفاتيح الخاصة (Private Key) في مكان آمن (وخاصة إذا كانت تستخدم للتوقيع الإلكتروني)، ومنع الوصول غير المصرح به، بما في ذلك جهات إصدار الشهادات.

3-4 يجب توفير التقنيات اللازمة لحماية مفاتيح التشفير عند تخزينها (Tamper Resistant Safe).

3-5 يجب حماية المفاتيح الخاصة (Private Key) من خلال تأمينها بكلمة مرور و/أو من خلال تخزينها على وسيط آمن، ووفقاً لإجراءات التشفير المعتمدة.

3-6 يجب تصنيف مفاتيح التشفير الخاصة باعتبارها معلومات "سرية للغاية" وفقاً لسياسة تصنيف البيانات المعتمدة في <اسم الجهة>.

3-7 يجب تفعيل سجلات الأحداث لحلول إدارة مفاتيح التشفير ومراقبتها دورياً.

8-3 يجب تحديد مدة لاستخدام مفاتيح التشفير وتاريخ الإنشاء وتاريخ الانتهاء لكل مفتاح.

9-3 يجب تجديد مفاتيح التشفير قبل انتهاء صلاحيتها.

10-3 يجب استخدام قائمة محدثة لشهادات التشفير الملغية (Certificate Revocation List) وذلك لضمان عدم استخدام شهادات التشفير منتهية الصلاحية أو التي تعرضت لانتهاك أمني في التعاملات مستقبلاً.

11-3 في حال تعرض مفتاح التشفير الخاص (Private Key) المُستخدم من قبل <اسم الجهة> إلى انتهاك أمني أو في حال عدم توفر المفتاح (بسبب تلف وسائط تخزين المفاتيح)، يجب إبلاغ الجهة المعنية بإصدار الشهادات على الفور لإلغائه وإعادة إصدار مفتاح التشفير الخاص (Private Key).

12-3 يجب إلزام الجهة المعنية بإصدار الشهادات، في حال تعرضت مفاتيح التشفير الخاصة بها (Private Keys) إلى انتهاك أمني، بإبلاغ <اسم الجهة> وإلغاء جميع الشهادات فوراً واستبدال المفتاح الخاص بالجهة المعنية بإصدار الشهادات.

13-3 في حال عدم إمكانية تبادل المفاتيح بشكل آمن وموثوق عبر شبكات الاتصالات، يجب نقل مفاتيح التشفير باستخدام قنوات بديلة آمنة ومستقلة (out-of-band channels).

14-3 يجب مراجعة وتحديث متطلبات طول مفاتيح التشفير بناءً على آخر التطورات التقنية ذات العلاقة مرة في السنة على الأقل وبما يتوافق مع معايير التشفير الوطنية.

15-3 مشرفو التشفير هم المسؤولون عن حماية مفاتيح التشفير (Key Custodians) وهم المصرح لهم فقط باستبدال مفاتيح التشفير عند الحاجة.

16-3 يُمنع حفظ مفاتيح التشفير على الذاكرة الرئيسية أو حفظها بنفس الأنظمة المطبق عليها التشفير. وعوضاً عن ذلك، يُوصى بحفظها على أجهزة مستقلة (Peripheral Hardware Devices)، مثل أجهزة حماية مفاتيح التشفير (Hardware Security Modules "HSM")، وأنظمة تخزين المفاتيح (Key Loaders)، أو أي أجهزة أخرى مخصصة لهذا الغرض.

4- متطلبات أخرى

1-4 يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر للاستخدام السليم والفعال للتشفير.

2-4 يجب مراجعة كافة متطلبات الأمن السيبراني الخاصة بالتشفير دورياً. (ECC-2-8-4)

3-4 تتم مراجعة هذه السياسة مرة واحدة في السنة؛ على الأقل.

الأدوار والمسؤوليات

1- **راعي ومالك وثيقة السياسة:** <رئيس الإدارة المعنية بالأمن السيبراني>.

2- **مراجعة السياسة وتحديثها:** <الإدارة المعنية بالأمن السيبراني>.

3- **تنفيذ السياسة وتطبيقها:** <الإدارة المعنية بتقنية المعلومات> و<الإدارة المعنية بالأمن السيبراني>.

الالتزام بالسياسة

1- يجب على <رئيس الإدارة المعنية بالأمن السيبراني> ضمان التزام <اسم الجهة> بهذه السياسة دورياً.

2- يجب على كافة العاملين في <اسم الجهة> الالتزام بهذه السياسة.

3- قد يعرض أي انتهاك لهذه السياسة صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في <اسم الجهة>.