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

اختر التصنيف

التاريخ: اضغط هنا لإضافة تاريخ

الإصدار: اضغط هنا لإضافة نص

المرجع: اضغط هنا لإضافة نص

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

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

إخلاء المسؤولية

طُور هذا النموذج عن طريق الهيئة الوطنية للأمن السيبراني كمثال توضيحي يمكن استخدامه كدليل ومرجع للجهات. يجب أن يتم تعديل هذا النموذج ومواءمته مع أعمال <اسم الجهة> والمتطلبات التشريعية والتنظيمية ذات العلاقة. كما يجب أن يُعتمد هذا النموذج من قبل رئيس الجهة أو من يقوم/تقوم بتفويضه. وتخلي الهيئة مسؤوليتها من استخدام هذا النموذج كما هو، وتؤكد على أن هذا النموذج ما هو إلا مثال توضيحي.

اعتماد الوثيقة

الدور	المسمى الوظيفي	الاسم	التاريخ	التوقيع
اختر الدور	<أدخل المسمى الوظيفي>	<أدخل الاسم الكامل للموظف>	اضغط هنا لإضافة تاريخ	<أدخل التوقيع>

نسخ الوثيقة

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

جدول المراجعة

معدل المراجعة	التاريخ لأخر مراجعة	تاريخ المراجعة القادمة
مره واحدة كل سنة	اضغط هنا لإضافة تاريخ	اضغط هنا لإضافة نص

اختر التصنيف

الإصدار <١,٠>

قائمة المحتويات

اختر التصنيف

الإصدار <١,٠>

الغرض

تهدف هذه السياسة إلى تحديد متطلبات الأمن السيبراني المتعلقة بالتشفير لحماية الأصول المعلوماتية الإلكترونية الخاصة ب<اسم الجهة> لتحقيق الغرض الأساسي وهو تقليل المخاطر السيبرانية الناتجة عن التهديدات الداخلية والخارجية في <اسم الجهة>.

هذه المتطلبات تمت موائمتها مع متطلبات الأمن السيبراني الصادرة من الهيئة الوطنية للأمن السيبراني ويشمل ذلك على سبيل المثال لا الحصر: الضوابط الأساسية للأمن السيبراني (ECC – ١: ٢٠١٨)، ضوابط الأمن السيبراني للأنظمة الحساسة (CSCC – ١: ٢٠١٩)، المعايير الوطنية للتشفير (NCS – ١: ٢٠٢٠) وغيرها من المتطلبات التشريعية والتنظيمية ذات العلاقة.

نطاق العمل

تطبق هذه السياسة جميع الأصول المعلوماتية والتقنية الخاصة ب<اسم الجهة>، وعلى جميع العاملين (الموظفين والمتعاقدين) في <اسم الجهة>، بما في ذلك الجهات التي تتعامل معها والأطراف الخارجية.

بنود السياسة

١- البنود العامة

١-١ 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 (NCS-١:٢٠٢٠) الصادرة من قبل الهيئة الوطنية للأمن السيبراني.

١-٢ يجب تشفير البيانات أثناء النقل والتخزين بناءً على تصنيفها وحسب السياسات والإجراءات التنظيمية ل<اسم الجهة>، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

١-٣ يجب تطبيق خوارزميات وطرقها المحدثة والآمنة عند التشفير وفقًا للمتطلبات التشريعية والتنظيمية ذات العلاقة.

١-٤ يجب تشفير البيانات والمعلومات المنقولة إلى الخدمات السحابية، أو المنقولة منها، بحسب المتطلبات التشريعية والتنظيمية ذات العلاقة.

١-٥ يجب تشفير جميع بيانات الأنظمة الحساسة، أثناء النقل (Data-In-Transit).

١-٦ يجب تشفير جميع بيانات الأنظمة الحساسة، أثناء التخزين (Data-at-Rest) على مستوى الملفات، وقاعدة البيانات، أو على مستوى أعمدة محددة داخل قاعدة البيانات.

١-٧ يجب مراجعة تطبيق متطلبات الأمن السيبراني للتشفير في <اسم الجهة> دورياً.

١-٨ يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر والاستخدام الصحيح والفعال لمتطلبات التشفير.

٢- الاستخدام الآمن للتشفير

١-٢ يجب حصر كافة حلول التشفير المستخدمة (بما في ذلك الخوارزميات والبرامج والوحدات (Modules) والمكتبات (Libraries) ومكونات التشفير الأخرى) وتقييمها واعتمادها من قبل إدارة الأمن السيبراني في <اسم الجهة> قبل تطبيقها في <اسم الجهة>.

٢-٢ يجب التأكد من تطبيق أساسيات التشفير المستخدمة (مثل الخوارزميات المتماثلة Symmetric) (algorithm والخوارزميات غير المتماثلة (Asymmetric algorithm) بناءً على المعايير الوطنية للتشفير (NCS-١:٢٠٢٠).

٣-٢ يجب التأكد من تطبيق التشفير وفقًا لحلول التشفير المعتمدة لدى <اسم الجهة>.

٤-٢ يُمنع استخدام خوارزميات التشفير المطورة داخليًا وفقًا لدليل التشفير الخاص بمشروع أمان تطبيق الويب المفتوح (OWASP) وبناءً على المعايير الوطنية للتشفير (NCS-١:٢٠٢٠).

٥-٢ يجب استخدام طرق التحقق الآمن (مثل استخدام المفاتيح العامة والتواقيع الرقمية والشهادات الرقمية) وفقًا لحلول التشفير المعتمدة لدى <اسم الجهة> للتقليل من المخاطر السيبرانية.

٦-٢ يجب استخدام التحقق من هوية المستخدم لنقل البيانات السرية للغاية إلى أطراف خارجية باستخدام شهادات التشفير الرقمية (Digital Certificates) المعتمدة، ووفقًا لسياسة حماية البيانات والمعلومات المعتمدة لدى <اسم الجهة> وتوافقها مع المتطلبات التشريعية والتنظيمية.

٧-٢ يجب أن تحدد معايير التشفير الى مستويين اثنين من مستويات القوة لمعايير التشفير، وهي المستوى الأساسي (Moderate) والمستوى المتقدم (Advanced)، وذلك لضمان مرونة التنفيذ وكفاءته بناءً على المعايير الوطنية للتشفير (NCS-١:٢٠٢٠).

٨-٢ يجب أن تكون تقنيات التشفير المستخدمة في بيئة شبكات أنظمة التحكم الصناعي (OT/ICS) متوائمة مع المعاير الوطني للتشفير (NCS-١:٢٠٢٠).

٩-٢ يجب استخدام طرق وخوارزميات محدثة وآمنة للتشفير عند الإنشاء والحفظ والنقل وعلى كامل الاتصال الشبكي المستخدم لنقل البيانات المصنفة سري وسري للغاية وفقًا للمستوى المتقدم (Advanced) بناءً على ضوابط الأمن السيبراني للبيانات (DCC-١:٢٠٢١).

١٠-٢ يجب استخدام طرق وخوارزميات محدثة وآمنة للتشفير عند الإنشاء والحفظ والنقل وعلى كامل الاتصال الشبكي المستخدم لنقل البيانات المصنفة مقيد وفقا للمستوى المتوسط (Moderate) بناءً على ضوابط الأمن السيبراني للبيانات (DCC-١:٢٠٢١).

١١-٢ يجب الالتزام باستخدام طرق وخوارزميات ومفاتيح وأجهزة تشفير محدثة وآمنة للمستوى المتقدم (Advanced) عند استخدام الخدمات السحابية بناءً على ضوابط الأمن السيبراني للحوسبة السحابية (CCC-١:٢٠٢٠).

٢-١٢ يجب استخدام طرق وخوارزميات محدثة وآمنة للتشفير على كامل الاتصال الشبكي المستخدم للعمل عن بعد وفقًا للمستوى المتقدم (Advanced) ضمن المعايير الوطنية للتشفير بناءً على ضوابط الأمن السيبراني للعمل عن بعد (TCC-١:٢٠٢١).

٢-١٣ يجب التأكد من استخدام تصاميم التشفير وطرق تشفيرها (مثل طرق عمليات التشفير الكتلية ورموز توثيق الرسائل (MAC) والتشفير والتوثيق باستخدام البيانات المرتبطة (AEAD) وغيرها من التصاميم) بناءً على المعايير الوطنية للتشفير (NCS-١:٢٠٢٠).

٣- بروتوكولات التشفير الشائعة

٣-١ يجب التأكد والأخذ بعين الاعتبار استخدام بروتوكولات التشفير مثل (بروتوكول الإنترنت الأمن (IPSec) وبرتوكول طبقة النقل الآمنة (TLS) بناءً على المعايير الوطنية للتشفير-NCS (١:٢٠٢٠).

٣-٢ يجب التأكد من استخدام الإصدارات المقبولة للبروتوكولات المستخدمة في (الاتصال الآمن عن بعد والبلوتوث ونظام الاتصالات المتنقلة العالمية (UMTS/LTE/٥G) والوصول الآمن للشبكة اللاسلكية WIFI) بناءً على المعايير الوطنية للتشفير (NCS-١:٢٠٢٠).

٤- البنية التحتية للمفاتيح العامة

٤-١ يجب التأكد من استخدام خوارزميات الشهادات للبنية التحتية للمفاتيح العامة (Public Key Infrastructure (PKI) بناءً على المعايير الوطنية للتشفير (NCS-١:٢٠٢٠).

٤-٢ يجب التأكد من صلاحية الشهادات المستخدمة (Validity of the certificates) بناءً على المعايير الوطنية للتشفير (NCS-١:٢٠٢٠).

٤-٣ يجب إدارة البيانات والمعلومات المستخدمة مع المفاتيح بصورة آمنة.

٤-٤ يجب حصر الأدوار والمسؤوليات المتعلقة بإدارة البنية التحتية لمفاتيح العامة (Public Key Infrastructure (PKI)، للأدوار التالية على الأقل:

٤-٤-١ مسؤول مفاتيح وأنظمة التشفير (Keying Material Manager) باعتباره <مدير الإدارة المعنية بالأمن السيبراني>.

٤-٤-٢ مشرفو التشفير المسؤولون عن حماية المفاتيح (Key Custodians) وهم فقط المصرح لهم باستبدال المفاتيح عند الحاجة.

٤-٤-٣ الجهات المعنية بإصدار الشهادات (Certification Authorities "CAs")، بحيث تكون موثوقة وآمنة.

٤-٤-٤ الجهات المعنية بتسجيل الشهادات (Registration Authorities "RAs")، بحيث تكون موثوقة وآمنة.

٥- إدارة دورة المفاتيح

٥-١ يجب إدارة دورة المفاتيح بطريقة آمنة خلال عمليات دورة حياتها الكاملة (Key Lifecycle Management) والتأكد من استخدامها بشكل سليم وفعّال وفقًا لمعيار التشفير المعتمد لدى <اسم الجهة>.

٥-٢ يجب أن يتم إصدار شهادات التشفير عن طريق <جهة إصدار الشهادات الداخلية> في <اسم الجهة> للخدمات المحلية أو عن طريق جهة خارجية موثوقة.

٥-٣ 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.

٥-٤ يجب توفير التقنيات اللازمة لحماية المفاتيح عند تخزينها (Tamper Resistant Safe).

٥-٥ يجب حماية المفاتيح الخاصة (Private Key) من خلال تأمينها بكلمة مرور و/أو من خلال تخزينها على وسيط آمن وفقًا لمعيار التشفير المعتمد لدى <اسم الجهة>.

٥-٦ يجب الالتزام بالمتطلبات الخاصة بعمليات إدارة دورة المفاتيح (KLM Processes) لكل عملية ضمن دورة حياة المفاتيح منذ إنشائها وحتى إتلافها وفقًا لمعيار التشفير المعتمد لدى <اسم الجهة> مثل:

- إنشاء المفاتيح (Key Generation)
- تسجيل / تصديق المفاتيح (Key Registration/Certification)
- استخدام المفاتيح (Key Use)
- تخزين المفاتيح (Key Storage)
- الغاء المفاتيح والتحقق من صحتها (Key Revocation/Validation)
- أرشفة المفاتيح (Key Archive)
- إتلاف المفاتيح (Key Destruction)
- المحاسبة على المفاتيح (Key Accounting)

٥-٧ يجب تصنيف المفاتيح الخاصة باعتبارها معلومات "سرية للغاية" وفقًا لسياسة تصنيف البيانات والمعلومات المعتمدة في <اسم الجهة>.

٥-٨ يجب منع حفظ المفاتيح على الذاكرة الرئيسية أو حفظها بنفس الأنظمة المطبق عليها التشفير. وعوضًا عن ذلك، يجب حفظها على أجهزة مثل أجهزة حماية وحدات التشفير (Hardware Cryptographic Modules “HCM”)، أو وحدات تخزين المفاتيح (Key Storage)، أو أي أجهزة أخرى مخصصة لهذا الغرض.

٥-٩ يجب تحديد مدة لاستخدام المفاتيح وتاريخ الإنشاء وتاريخ الانتهاء لكل مفتاح.

٥-١٠ يجب تجديد المفاتيح قبل انتهاء صلاحيتها.

٥-١١ 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 مستقبلًا.

٥-١٢ في حال تعرض المفتاح 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 المفتاح الخاص (Private Key).

٥-١٣ يجب إلزام الجهة المعنية بإصدار الشهادات، في حال تعرضت المفاتيح الخاصة بها (Private Keys) إلى انتهاك أمني، بإبلاغ <اسم الجهة> وإلغاء جميع الشهادات فورًا واستبدال المفتاح الخاص بالجهة المعنية بإصدار الشهادات.

٥-١٤ في حال عدم إمكانية تبادل المفاتيح بشكل آمن وموثوق عبر شبكات الاتصالات، يجب نقل المفاتيح باستخدام قنوات بديلة آمنة ومستقلة (Out-of-band channels).

٥-١٥ يجب مراجعة وتحديث متطلبات طول المفاتيح بناءً على آخر التطورات التقنية ذات العلاقة مرة واحدة في السنة على الأقل وبما يتوافق مع المعايير الوطنية للتشفير (NCS-١:٢٠٢٠).

الأدوار والمسؤوليات

١- **مالك السياسة:** <رئيس الإدارة المعنية بالأمن السيبراني>.

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

٣- **تنفيذ السياسة وتطبيقها:** <الإدارة المعنية بتقنية المعلومات>.

٤- **قياس الالتزام بالسياسة:** <الإدارة المعنية بالأمن السيبراني>.

التحديث والمراجعة

يجب على <الإدارة المعنية بالأمن السيبراني> مراجعة السياسة سنويًا على الأقل أو في حال حدوث تغييرات في السياسات أو الإجراءات التنظيمية في <اسم الجهة> أو المتطلبات التشريعية والتنظيمية ذات العلاقة.

الالتزام بالسياسة

١- يجب على <رئيس الإدارة المعنية بالأمن السيبراني> التأكد من التزام <اسم الجهة> بهذه السياسة دوريًا.

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

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