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 معيار 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.

اختر التصنيف

الإصدار <1.0>

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	عُدِلَ بواسطة	أسباب التعديل
<أدخل رقم النسخة>	اضغط هنا لإضافة تاريخ	<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 تاريخ

اختر التصنيف

الإصدار <1.0>

قائمة المحتويات

اختر التصنيف

الإصدار <1.0>

الغرض

الغرض من هذا المعيار هو تحديد متطلبات الأمن السيبراني التفصيلية المتعلقة بالتشفير في <اسم الجهة> لتقليل المخاطر السيبرانية وحمايتها من التهديدات الداخلية والخارجية.

تمت موائمة هذه المعيار مع سياسة التشفير والضوابط والمعايير الصادرة من الهيئة الوطنية للأمن السيبراني والمتطلبات التنظيمية والتشريعية ذات العلاقة.

نطاق العمل

يغطي هذا المعيار جميع الأنظمة والتطبيقات وأجهزة معالجة المعلومات الخاصة ب<اسم الجهة>، وينطبق على جميع العاملين (الموظفين والمتعاقدين) في <اسم الجهة>.

المعايير

1	استخدام التشفير
الهدف	ضمان إدارة التشفير واستخدامه بصورة آمنة وملائمة عند الحاجة.
المخاطر المحتملة	يمكن أن يؤدي عدم استخدام التشفير بصورة ملائمة وعند الضرورة إلى مخاطر شديدة قد تتسبب بسرقة المعلومات أو الكشف عنها أو الوصول غير المصرح به إليها.
المعايير المطلوبة	
1-1	استخدام شهادات تشفير صحيحة لأمن طبقة النقل (TLS) وذلك لكافة المعلومات المحمية المنقولة أو المستخدمة بين العميل والخادم والخوادم الأخرى.
2-1	استخدام شهادات تشفير أمن طبقة النقل (TLS) الصادرة عن جهة إصدار شهادات معترف بها لكافة خدمات الإنتاج في <اسم الجهة>.
3-1	إعداد متصفحات الإنترنت لتجنب البروتوكولات غير الآمنة (مثل "SSLv3" أو "SSLv2") وخوارزميات التشفير الضعيفة (مثل "DES" أو "MD5") مع التأكد من أن استخدام البروتكولات متوائم مع المعايير الوطنية للتشفير (NCS-1:2020).
4-1	استخدام القنوات المشفرة لكافة عمليات المصادقة.
5-1	ضمان حماية النسخ الاحتياطية بصورة ملائمة عن طريق الأمن المادي والتشفير عند تخزينها ونقلها عبر الشبكة، ويشمل هذا النسخ الاحتياطية عن بعد والخدمات السحابية.

اختر التصنيف

الإصدار <1.0>

6-1	إدارة كافة أجهزة الشبكة باستخدام جلسات مشفرة.
7-1	في حال اكتشاف خطأ في المعلومات المستلمة خلال عملية التشفير، وطلب المتلقي أن تكون المعلومات صحيحة بالكامل (على سبيل المثال لا الحصر، عندما لا يكون المتلقي قادراً على متابعة أعماله عند وجود خطأ في المعلومات)، يجب تنفيذ الآتي: • عدم استخدام المعلومات. • إعادة إرسال المعلومات بناءً على طلب المتلقي (على أن تكون إعادة إرسالها مقتصرة على عدد محدد من المرات). • تخزين المعلومات المتعلقة بالحادثة في سجل التدقيق لتحديد مصدر الخطأ لاحقاً.
8-1	يجب تصميم مستويات القوة لتستهدف مستوى أمن 128 -بت بالنسبة للمستوى الأساسي ومستوى أمن 256-بت بالنسبة للمستوى المتقدم بناء على المعايير الوطنية للتشفير (NCS-1:2020).
2	تشفير البيانات والمعلومات
الهدف	ضمان تشفير البيانات والمعلومات عند الضرورة.
المخاطر المحتملة	تنطوي البيانات والمعلومات غير المشفرة على مخاطر كبيرة قد تتسبب بسرقة المعلومات أو الكشف عنها أو الوصول غير المصرح به إليها.
المعايير المطلوبة	
1-2	يجب استخدام برنامج تشفير القرص الكامل المعتمد لتشفير القرص الصلب في كافة الأجهزة المحمولة.
2-2	يجب فك تشفير كافة أنواع حركة بيانات الشبكة المشفرة عند الخادم الوكيل على حدود الشبكة قبل تحليل المحتوى. ويمكن لـ<اسم الجهة> استخدام قائمة محددة من التطبيقات لمواقع مسموحة يمكن الوصول إليها عبر خادم وكيل دون فك تشفير حركة البيانات.
3-2	يجب على كافة عمليات الوصول وتسجيل الدخول عن بعد إلى شبكة <اسم الجهة> تشفير البيانات قيد الاستخدام والنقل.
4-2	يجب مراقبة كافة أنواع الحركة التي تخرج من <اسم الجهة> وكشف أي استخدام غير مصرح به للتشفير.
5-2	في حال استخدام أجهزة التخزين (USB)، يجب تشفير البيانات المخزنة بناءً على تصنيفها على هذه الأجهزة.

اختر التصنيف

الإصدار <1.0>

6-2	يجب تشفير جميع المعلومات المحمية أثناء الاستخدام والنقل.
7-2	يجب تشفير جميع المعلومات المحمية أثناء التخزين باستخدام أداة تتطلب آلية تحقق ثانوية غير مدمجة في نظام التشغيل من أجل الوصول إلى المعلومات.
8-2	يجب تشفير جميع البيانات اللاسلكية أثناء الاستخدام والنقل.
9-2	يجب تشفير أو اختزال كافة بيانات الاعتماد باستخدام بيانات عشوائية عند تخزينها.
10-2	يجب ضمان أن جميع أسماء المستخدمين وبيانات التحقق الخاصة بالحسابات تُنقل عبر الشبكات باستخدام قنوات مشفرة.
11-2	يجب تشفير وسائط تخزين الخوادم، بما في ذلك الأقراص الثابتة أو التخزين المتصل بالشبكة (NAS) أو التخزين المتصل بشبكة منطقة التخزين (SAN) أو أي نوع آخر من وحدات التخزين المتصلة.
12-2	يجب تشفير قواعد البيانات لمنع الاطلاع غير المصرح به للبيانات المصنفة مقيد وسري وسري للغاية.
13-2	يجب نقل البيانات عبر الشبكة وبين الأنظمة باستخدام آليات تشفير قوية بما يكفي لتقليل مخاطر تعرض البيانات.
14-2	يجب تشفير ملفات قاعدة البيانات على مستوى قاعدة البيانات أو المستوى الميداني، وفقًا للسياسات والإجراءات ذات الصلة الخاصة بـ<اسم الجهة>.
15-2	يجب تشفير أشرطة النسخ الاحتياطي التي تخزن نسخًا احتياطية، ولا يجوز تخزين المفتاح في نفس الأشرطة بنص عادي.
16-2	يجب تشفير البيانات للمسؤول أو المستخدم أو التطبيق من وإلى نظام إدارة قواعد البيانات (DBMS).
17-2	يجب تطبيق التشفير بين الطرفيات (end-to end encryption) لاتصالات تطبيقات الويب من الخادم والعميل.
3	المعلومات الأخرى ذات العلاقة بالتشفير
الهدف	ضمان إدارة البيانات والمعلومات المستخدمة مع المفاتيح بصورة آمنة.
المخاطر المحتملة	قد تؤدي الإدارة غير الآمنة للبيانات والمعلومات المستخدمة مع المفاتيح إلى مخاطر كبيرة قد تتسبب بسرقة المعلومات أو الكشف عنها أو الوصول غير المصرح به إليها.

اختر التصنيف

الإصدار <1.0>

المعايير المطلوبة	
1-3	يجب حماية كافة المعلومات المستخدمة مع خوارزميات التشفير والمفاتيح.
2-3	يجب حماية الخصائص المشتركة لمعلومات التشفير وفقاً لنوعها.
3-3	يجب الحصول على ضمان بشأن صلاحية "معيار النطاق" لكافة خوارزميات المفاتيح العامة الخاصة بالدخول المنفصل لضمان صحة معايير النطاق حسابياً. وذلك من خلال إحدى الطرق التالية: • الحصول على ضمان من الجهة المسؤولة عن المفتاح أو الجهة المسؤولة عن التحقق من المفتاح أو طرف خارجي موثوق. • التحقق من المفاتيح العامة اعتماداً على الخوارزميات المستخدمة.
4-3	يجب إدراج آليات لا تعتمد على التشفير في أنظمة الاتصالات لضمان توافر المعلومات المشفرة المنقولة بعد استلامها بنجاح، بدلاً من الاعتماد على إعادة إرسالها من قبل المرسل الأصلي لغايات توافرها مستقبلاً.
4	خوارزميات التشفير وتصاميمها
الهدف	ضمان استخدام خوارزميات وتصاميم التشفير المعتمدة والآمنة عند التشفير.
المخاطر المحتملة	ينطوي استخدام خوارزميات وتصاميم التشفير غير الآمنة أو غير المعتمدة على مخاطر كبيرة قد تتسبب بسرقة المعلومات أو الكشف عنها أو الوصول غير المصرح به إليها.
المعايير المطلوبة	
1-4	يجب استخدام خوارزميات دوال الاختزال المشفرة فقط بحيث لا يكون من الممكن العثور على نص له نتيجة اختزال معينة (مقاومة عكس الخوارزمية)، أو العثور على نصين لهما نفس نتيجة الاختزال (مقاومة التصادم).
2-4	يجب استخدام خوارزميات دوال اختزال مشفرة المقبولة بناء على المعايير الوطنية للتشفير(NCS-1:2020).
3-4	يجب استخدام أطوال المفاتيح التي لا تقل عن 128 بت في جميع خوارزميات المفاتيح المتماثلة.
4-4	يجب استخدام شفرة التحقق من الرسائل (MAC) لضمان سلامة البيانات والتأكد من قيام الجهة المتوقعة بحساب شفرة التحقق من الرسائل (MAC).

اختر التصنيف

الإصدار <1.0>

5-4	يجب استخدام خوارزميات شفرة التحقق من الرسائل (MAC) بناءً على خوارزميات التشفير الكتلي (Block Cipher)، (مثل شفرة التحقق من الرسائل باستخدام التشفير "CMAC")، أو بناءً على خوارزميات حساب ملخص النص المميز (شفرة التحقق من الرسائل المجزأة "HMAC").
6-4	يجب عدم استخدام نفس المفتاح لغايات التشفير واحتساب شفرة التحقق من الرسائل (MAC) في حال استخدام نفس خوارزمية التشفير الكتلي (Block Cipher).
7-4	يجب استخدام خوارزميات التواقيع الرقمية المعتمدة لتوفير التحقق الآمن والتحقق من سلامة المعلومات ودعم عدم إنكار صحة البيانات.
8-4	يجب استخدام خوارزميات التواقيع الرقمية التالية مع أطوال المفاتيح المعتمدة لكل من: • خوارزمية التوقيع الرقمي (خوارزمية "DSA"). • خوارزمية ريفست وشامير وإديلمان (خوارزمية "RSA"). • خوارزمية التوقيع الرقمي للمنحنى الإهليلجي (خوارزمية "ECDSA"). • خوارزمية ميركل (خوارزمية "Merkle ") .
9-4	يجب إصدار التواقيع الرقمية باستخدام مفاتيح تلبي أو تتجاوز أطوال المفاتيح المعتمدة للخوارزمية.
10-4	يجب استخدام طرق تبادل المفاتيح المعتمدة التالية لإعداد المفاتيح بين الجهات التي تقوم بالاتصالات: • نقل المفاتيح: يجب نقل مواد صياغة المفاتيح من جهة إلى أخرى باستخدام خوارزمية متماثلة (أي باستخدام مفاتيح تشفير المفاتيح) أو باستخدام خوارزمية غير متماثلة. • الاتفاق على المفاتيح: يجب أن تتعاون الجهات في إنشاء مواد صياغة المفاتيح المشتركة باستخدام خوارزميات متماثلة أو غير متماثلة.
11-4	يجب استخدام طرق تبادل المفاتيح المعتمدة باستخدام أطوال المفاتيح المعتمدة. وتشمل هذه الطرق خوارزمية ديفي- هيلمان (خوارزمية "DH") وخوارزمية "RSA" وخوارزمية "Elliptic Curve Diffie-Hellman" ("ECDH") للمستوى المتقدم.
12-4	يجب استخدام درجة قوة لا تقل عن 256 بت لخوارزميات التشفير المستخدمة للأنظمة الحساسة بناء على المعايير الوطنية للتشفير (NCS-1:2020).

اختر التصنيف

الإصدار <1.0>

13-4	يجب استخدام درجات قوة لا تقل عن 256 بت لخوارزميات الاختزال المستخدمة للأنظمة الحساسة.
14-4	يجب استخدام التشفير والتوثيق باستخدام البيانات المرتبطة والتصاميم المقبولة لذلك مثل: • Galois Counter Mode (GCM) • Counter with CBC-MAC (CCM)
15-4	عند استخدام تصاميم التشفير الهجينة يجب استخدام التصاميم المقبولة لها مثل • Elliptic Curve Integrated Encryption Scheme (ECIES) • Discrete Logarithm Integrated Encryption Scheme (DLIES) • RSA with Optimal Asymmetric Encryption Padding (RSA-OAEP)
5	بروتوكولات التشفير الشائعة
الهدف	ضمان استخدام برتوكولات التشفير المعتمدة والآمنة عند التشفير.
المخاطر المحتملة	ينطوي استخدام بروتوكولات التشفير غير الآمنة أو غير المعتمدة على مخاطر كبيرة قد تتسبب بسرقة المعلومات أو الكشف عنها أو الوصول غير المصرح به إليها.
المعايير المطلوبة	
1-5	يجب استخدام خوارزميات بروتوكول الإنترنت الآمن (IP Security) وبالنسبة للتوثيق، يجب استخدام حقل التوثيق (AH) وتغليف البيانات الآمن (ESP) مع تصاميم التوثيق (MAC) مثل HMAC-SHA3-256 , HMAC-SHA2-384.
2-5	يجب استخدام الإصدارات المقبولة لبروتوكول طبقة النقل الآمنة (TLS) مثل (TLS 1.2) و (TLS 1.3) .
3-5	يجب استخدام بروتوكول نظام اسم النطاق الآمن (DNSSEC) والمتطلبات المقبولة لتوقيع بيانات المنطقة ولتوثيق الرسائل مثل (ECDSA_P384_SHA-384) و (HMAC_SHA- 384).
4-5	يجب استخدام الإصدارات والمتطلبات المقبولة لبروتوكول الاتصال الآمن عن بعد مثل (SSH-2) و (AEAD_AES_128_GCM).

اختر التصنيف

الإصدار <1.0>

5-5	يجب استخدام الإصدارات والمتطلبات المقبولة للبلوتوث مثل (Bluetooth 4.1) و (Security Mode 4) و (AES-CCM).
6-5	يجب استخدام المتطلبات المقبولة لنظام الاتصالات المتنقلة العالمية (UMTS) / الجيل الرابع (4G) / الجيل الخامس (5G) مثل: • لنظام الاتصالات المتنقلة العالمية (UMTS) يتم استخدام (UEA1-128) مع (UA1-128) • للجيل الرابع (4G) يتم استخدام (128-EEA2) مع (128-EIA2) • للجيل الخامس (5G) يتم استخدام (128-NEA2) مع (128-NIA2)
7-5	يجب استخدام الإصدارات المقبولة للوصول الآمن للشبكة اللاسلكية مثل (WPA3-Enterprise).
8-5	يجب استخدام بروتوكول كيربيروس والمتطلبات المقبولة له للمستويين الأساسي والمتقدم مثل: • (CAMELLIA128-CTS-CMAC) • (AES256-CTS-HMAC-SHA3)
9-5	يجب استخدام بروتوكول إدارة الخادم الذي يدعم التشفير أو اعداد التشفير لبروتوكولات إدارة الخادم، مثل (LDAP) عبر (TLS) و (SNMPv3) مع المصادقة والخصوصية و (Kerberos) مع (TLS) وسجل النظام المشفر وما إلى ذلك.
10-5	يجب اعداد التشفير لتطبيق الخادم وبروتوكولات اتصال قاعدة البيانات، مثل (HTTPS) أو (Secure API) أو (TDE) أو (SQL) مع (TLS) و (SFTP) و (SSHv2) وما إلى ذلك.
11-5	لا يجوز استخدام البروتوكولات غير المشفرة أو الخدمات غير الآمنة (مثل (HTTP) و (FTP) وما إلى ذلك)، ويجب استخدام (HTTPS) و (SFTP) وما إلى ذلك بدلاً من ذلك.
12-5	يجب تنفيذ تقنيات التشفير، مثل بروتوكول أمان طبقة النقل (TLS) والشبكات الخاصة الافتراضية (VPN) ، لحماية آليات المصادقة أثناء الإرسال.
13-5	يجب تخصيص الاعدادات لبروتوكولات تطبيقات الويب لاستخدام التشفير حيثما كان ذلك ممكنًا (على سبيل المثال لا الحصر، (HTTPS) ، و (SFTP) عبر (TLS) ، وما إلى ذلك).

اختر التصنيف

الإصدار <1.0>

14-5	يجب تقييد استخدام بروتوكولات الإدارة المشفرة الآمنة مثل (Secure Shell (SSH)) v2 وبروتوكول سطح المكتب البعيد (RDP) عبر (TLS).

الأدوار والمسؤوليات

1- **مالك المعيار:** <رئيس الإدارة المعنية بالأمن السيبراني>.

2- **مراجعة المعيار وتحديثه:** <الإدارة المعنية بالأمن السيبراني>.

3- **تنفيذ المعيار وتطبيقه:** <الإدارة المعنية بتقنية المعلومات>.

4- **قياس الالتزام بالمعيار:** <الإدارة المعنية بالأمن السيبراني>.

التحديث والمراجعة

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

الالتزام بالمعيار

1- يجب على <رئيس الإدارة المعنية بالأمن السيبراني> التأكد من التزام <اسم الجهة> بهذا المعيار دورياً.

2- يجب على كافة العاملين في <اسم الجهة> الالتزام بهذا المعيار.

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

اختر التصنيف

الإصدار <1.0>