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

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>

اختر التصنيف

الإصدار 1.0

قائمة المحتويات

الأهداف

الغرض من هذا المعيار هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بالتشفير الخاصة بـ<اسم الجهة> لتقليل المخاطر السيبرانية وحمايتها من التهديدات الداخلية والخارجية من خلال التركيز على الأهداف الأساسية للحماية وهي: سرية المعلومات، وسلامتها، وتوافرها. كما يجب أن تتوافق مع المعايير الوطنية للتشفير الصادرة من الهيئة الوطنية للأمن السيبراني كمرجع أساسي بأعلى أولوية لمتطلبات الأمن السيبراني الخاصة بالتشفير.

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

نطاق العمل وقابلية التطبيق

يغطي هذا المعيار جميع الأنظمة والتطبيقات وأجهزة معالجة المعلومات الخاصة بـ<اسم الجهة>، وتنطبق على جميع العاملين في <اسم الجهة>.

المعايير

1	استخدام التشفير (Use of Cryptography)
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.
الإجراءات المطلوبة	
1-1	استخدام شهادات تشفير صحيحة لأمن طبقة النقل (TLS) وذلك لكافة المعلومات المحمية المنقولة أو المستخدمة بين العميل والخادم والخوادم الأخرى. Valid Transport Layer Security (TLS) certificates shall be used for all sensitive information in transit between the client, server and other servers.
2-1	استخدام شهادات تشفير أمن طبقة النقل (TLS) الصادرة عن جهة إصدار شهادات معترف بها لكافة خدمات الإنتاج في <اسم الجهة>. TLS certificates shall be obtained from a recognized Certificate Authority (CA) for all production services at <entity name>.

3-1	إعداد متصفحات الإنترنت لتجنب البروتوكولات غير الآمنة (مثل "SSLv3" أو "SSLv2") وخوارزميات التشفير الضعيفة (مثل "DES" أو "MD5"). Internet browsers shall be configured to avoid insecure and weak protocols (e.g., SSLv3 or SSLv2), and weak ciphers (e.g., DES or MD5).
4-1	استخدام القنوات المشفرة لكافة عمليات المصادقة. Encrypted channels shall be used for all authentication.
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. It shall be ensured that backups are properly protected via physical security and encryption when they are stored and moved across the network. Such backups shall include remote backups and cloud services.
6-1	إدارة كافة أجهزة الشبكة باستخدام جلسات مشفرة. All network devices shall be managed using encrypted sessions.
7-1	في حال اكتشاف خطأ في المعلومات المستلمة خلال عملية التشفير، وطلب المتلقي أن تكون المعلومات صحيحة بالكامل (على سبيل المثال، 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. During a cryptographic process, if an error is detected in the received information, and the receiver requires that the information be entirely correct (e.g., the receiver cannot proceed when the information is in error), then the following shall be performed: • The information shall not be used. • The recipient may request that the information be resent (retransmissions shall be limited to a predetermined maximum number of times).

	• Information related to the incident shall be stored in an audit log to later identify the source of the error.
2	إدارة مفاتيح التشفير (Cryptographic Key Management)
الهدف	ضمان إدارة مفاتيح التشفير بصورة آمنة خلال دورة إدارة مفاتيح التشفير الكاملة.
المخاطر المحتملة	تنطوي إدارة مفاتيح التشفير غير الآمنة على مخاطر شديدة قد تتسبب بسرقة المعلومات أو الكشف عنها أو الوصول غير المصرح به إليها.
الإجراءات المطلوبة	
1-2	يجب إدارة مفاتيح التشفير وفقاً لعمليات إدارة مفاتيح التشفير المعتمدة في <اسم الجهة> وإجراءاتها وإرشاداتها، ويشمل ذلك إصدار المفاتيح وتخزينها ونسخها احتياطياً واستعادتها وغيرها من العمليات. Cryptographic keys shall be managed in accordance with <entity name>'s cryptographic key management processes, procedures, and guidelines. This shall include key generation, key storage, key backup, key recovery, etc.
2-2	يجب تحديد فئات مفاتيح التشفير وفقاً لتصنيفها (عامة، أو خاصة، أو متماثلة) واستخدامها. Cryptographic keys shall be categorized according to their classification (public, private, or symmetric) and use.
3-2	يجب حماية مفاتيح التشفير وفقاً لنوعها. Cryptographic keys shall be protected according to their type and the required protection.
4-2	يجب حماية الخصائص المشتركة لمفاتيح التشفير وفقاً لنوعها. Associations for the cryptographic keys shall be protected according to their type.
5-2	يجب الحصول على ضمان بشأن صلاحية المفاتيح العامة للتأكد من أن مفاتيح التشفير صحيحة 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 المباشر من المفاتيح العامة اعتماداً على الخوارزميات المستخدمة.

An assurance of public-key validity shall be obtained to ensure that the cryptographic key is arithmetically correct, through one of the following methods: • Assurance from the key owner, key verifier, or trusted third party. • Explicit public key validation depending on the algorithm used.	
يجب استخدام خوارزميات توفر ضماناً بشأن ملكية المفتاح العام أو الحصول على هذا الضمان مباشرة للتأكد من أن الجهة الخارجية (أي الطرف الخارجي) التي توفر المفتاح العام تملك فعلياً المفتاح الخاص المصاحب للمفتاح العام. Algorithms that provide an assurance of private-key possession shall be used. Alternatively, such assurance shall be obtained explicitly to ensure that the external entity (i.e., third party) providing a public key actually possesses the associated private key.	6-2
يجب توفير الحماية الأمنية الواردة في الضابط 2-2 لفترة زمنية معينة وفقاً لنوع مفتاح التشفير. The security protections highlighted in control 2-2 shall be provided for a period of time as per the cryptographic key type.	7-2
يجب تعيين مدة تشفير لمفاتيح التشفير. Cryptoperiods shall be assigned to the cryptographic keys.	8-2
يجب إتلاف كافة المفاتيح المتماثلة والمفاتيح الخاصة في نهاية فترة حمايتها كما هو مبين في الضابط 2-6. All symmetric keys and all private keys shall be destroyed at the end of their period of protection as highlighted in control 2-6.	9-2
يجب استخدام أطوال مفاتيح التشفير التي لا تقل عن 128 بت في جميع خوارزميات المفاتيح المتماثلة. Cryptographic key lengths that are at least 128 bits shall be used in all symmetric key algorithms.	10-2
يجب استخدام مفاتيح نظام التشفير غير المتماثلة ذات الطول الكافي لكي تكون بنفس درجة قوة أطوال المفاتيح المتماثلة.	11-2

اختر التصنيف

	Asymmetric cryptosystem keys that are of sufficient length shall be used to yield equivalent strength to symmetric key lengths.
12-2	بالنسبة للأنظمة الحساسة، من المستحسن استخدام أطوال مفاتيح تشفير متماثلة لا تقل عن 256 بت، وأطوال مفاتيح تشفير غير متماثلة (Elliptic Curve Cryptography ECC) لا تقل عن 512 بت. For critical systems, it is recommended to employ symmetric cryptographic key lengths that are at least 256 bits, and asymmetric Elliptic Curve Cryptography ECC key lengths that are at least 512 bits.
3	تشفير البيانات والمعلومات (Data and Information Encryption)
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.
الإجراءات المطلوبة	
1-3	يجب استخدام برنامج تشفير القرص الكامل المعتمد لتشفير القرص الصلب في كافة الأجهزة المحمولة. Approved whole disk encryption software shall be used to encrypt the hard drive of all mobile devices.
2-3	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. All encrypted network traffic shall be decrypted at the boundary proxy prior to analyzing the content. However, <entity name> may use whitelists of allowed sites that can be accessed through the proxy without decrypting the traffic.
3-3	يجب على كافة عمليات الوصول وتسجيل الدخول عن بعد إلى شبكة <اسم الجهة> تشفير البيانات قيد الاستخدام والنقل، واستخدام التحقّق من الهوية متعدّد العناصر. All remote login access to <entity name>'s network shall be required to encrypt data in transit and use multi-factor authentication.

4-3	يجب مراقبة كافة أنواع الحركة التي تخرج من <اسم الجهة> وكشف أي استخدام غير مصرح به للتشفير. All traffic leaving <entity name> shall be monitored, and any unauthorized use of encryption shall be detected.
5-3	إذا كانت أجهزة التخزين (USB) مطلوبة، يجب تشفير البيانات المخزنة بناءً على تصنيفها على هذه الأجهزة. If USB storage devices are required, data stored on such devices shall be encrypted while at rest, based on the data classification.
6-3	يجب تشفير جميع المعلومات المحمية أثناء الاستخدام والنقل. All protected information in transit shall be encrypted.
7-3	يجب تشفير جميع المعلومات المحمية أثناء التخزين باستخدام أداة تتطلب آلية تحقق ثانوية غير مدمجة في نظام التشغيل من أجل الوصول إلى المعلومات. All protected information at rest shall be encrypted using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.
8-3	يجب تشفير جميع البيانات اللاسلكية أثناء الاستخدام والنقل. All wireless data in transit shall be encrypted.
9-3	يجب تشفير أو اختزال كافة بيانات الاعتماد باستخدام بيانات عشوائية عند تخزينها. All authentication credentials shall be encrypted or hashed with a salt when stored.
10-3	يجب ضمان أن جميع أسماء المستخدمين وبيانات التحقق الخاصة بالحسابات تُنقل عبر الشبكات باستخدام قنوات مشفرة. It shall be ensured that all account usernames and authentication credentials are transmitted across networks using encrypted channels.
4	المعلومات الأخرى ذات العلاقة بالتشفير (Other Cryptographic Related Information)
الهدف	ضمان إدارة البيانات والمعلومات المستخدمة مع مفاتيح التشفير بصورة آمنة.

اختر التصنيف

المخاطر المحتملة	قد تؤدي الإدارة غير الآمنة للبيانات والمعلومات المستخدمة مع مفاتيح التشفير إلى مخاطر كبيرة قد تتسبب بسرقة المعلومات أو الكشف عنها أو الوصول غير المصرح به إليها.
الإجراءات المطلوبة	
1-4	يجب حماية كافة المعلومات المستخدمة مع خوارزميات التشفير ومفاتيح التشفير. All information used in conjunction with cryptographic algorithms and cryptographic keys shall be protected.
2-4	يجب حماية الخصائص المشتركة لمعلومات التشفير وفقاً لنوعها. Associations for cryptographic information shall be protected according to their type.
3-4	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. An assurance of domain parameter validity shall be obtained for all discrete log public key algorithms to ensure that the domain parameters are arithmetically correct, using one of the following methods: • Assurance from the key owner, key verifier, or trusted third party • Explicit validation depending on the algorithm used
4-4	يجب توفير الحماية الأمنية الواردة في الضابط 2-2 لفترة زمنية معينة وفقاً لنوع معلومات التشفير. The security protections highlighted in control 2-2 shall be provided for a period of time.

5-4	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. Non-cryptographic mechanisms shall be incorporated in communication systems to ensure the availability of transmitted cryptographic information after it has been successfully received, rather than relying on retransmission by the original sender for future availability.
5	بروتوكولات التشفير وخوارزميات التشفير المدعومة (Encryption Protocols and Cipher Suites)
الهدف	ضمان استخدام خوارزميات التشفير المعتمدة والآمنة عند التشفير.
المخاطر المحتملة	ينطوي استخدام خوارزميات التشفير غير الآمنة أو غير المعتمدة على مخاطر كبيرة قد تتسبب بسرقة المعلومات أو الكشف عنها أو الوصول غير المصرح به إليها.
الإجراءات المطلوبة	
1-5	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). Only cryptographic hash functions shall be used to ensure that it is not feasible to find a message that produces a given hash value (Pre-image Resistance), or find two messages that produce the same hash value (Collision Resistance).
2-5	يجب استخدام خوارزميات دوال اختزال مشفرة وفقاً لمعايير الخوارزميات ذات العلاقة. Cryptographic hash functions shall be used as directed by the relevant algorithm standards.
3-5	يجب استخدام أطوال مفاتيح التشفير التي لا تقل عن 128 بت في جميع خوارزميات المفاتيح المتماثلة. Cryptographic key lengths that are at least 128 bits shall be used in all symmetric key algorithms.
4-5	يجب استخدام شفرة التحقق من الرسائل (MAC) لضمان سلامة البيانات والتأكد من قيام الجهة المتوقعة بحساب شفرة التحقق من الرسائل (MAC).

اختر التصنيف

Message Authentication Codes (MACs) shall be used to provide assurance of the data's integrity, and that the MAC was computed by the expected entity.	
يجب استخدام خوارزميات شفرة التحقق من الرسائل (MAC) بناءً على خوارزميات التشفير الكتلي (Block Cipher)، (مثل شفرة التحقق من الرسائل باستخدام التشفير "CMAC" أو شفرة غاليوس للتحقق من الرسائل "GMAC")، أو بناءً على خوارزميات حساب ملخص النص المميز (شفرة التحقق من الرسائل المجزأة "HMAC"). Only MAC algorithms shall be used based on block cipher algorithms (CMAC or GMAC) or based on hash functions (HMAC).	5-5
يجب عدم استخدام نفس المفتاح لغايات التشفير واحتساب شفرة التحقق من الرسائل (MAC) في حال استخدام نفس خوارزمية التشفير الكتلي (Block Cipher). The same key shall not be used if the same block cipher algorithm is used for both encryption and MAC computation.	6-5
يجب استخدام خوارزميات التواقيع الرقمية المعتمدة لتوفير التحقق الآمن والتحقق من سلامة المعلومات ودعم عدم إنكار صحة البيانات. Approved digital signature algorithms shall be used to provide source authentication, integrity authentication, and support for non-repudiation.	7-5
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"). Only the following digital signature algorithms shall be used with the approved key sizes for each of the following: • Digital Signature Algorithm (DSA) • RSA Algorithm • ECDSA Algorithm	8-5
يجب إصدار التواقيع الرقمية باستخدام مفاتيح تلبي أو تتجاوز أطوال المفاتيح المعتمدة للخوارزمية. Digital signatures shall be generated using keys that meet or exceed the approved key sizes of the algorithm.	9-5

10-5	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. Only the following approved key-exchange scheme types shall be used to set up keys between communicating entities: • Key Transport: The keying material shall be transported from one entity to another using a symmetric algorithm (i.e., using a key-wrapping key), or using an asymmetric algorithm. • Key Agreement: Entities shall co-create shared keying material using symmetric or asymmetric algorithms.
11-5	يجب استخدام طرق تبادل المفاتيح المعتمدة باستخدام أطوال المفاتيح المعتمدة. وتشمل هذه الطرق خوارزمية ديفي- هيلمان (خوارزمية "DH") وخوارزمية "RSA". Approved key-exchange schemes with approved key sizes shall be used. These schemes include Diffie-Hellman (DH) and RSA algorithms.
12-5	يجب استخدام درجة قوة لا تقل عن 256 بت لخوارزميات التشفير المستخدمة للأنظمة الحساسة حسب ما تصدره الهيئة الوطنية للأمن السيبراني في هذا الخصوص. Security strengths of at least 256 bits shall be employed for cryptographic algorithms used for critical systems following what the NCA issues in this regards.
13-5	يجب استخدام درجات قوة لا تقل عن 256 بت لخوارزميات حساب ملخص النص المميز المستخدمة للأنظمة الحساسة. Security strengths of at least 256 bits shall be employed for hash functions used for critical systems.

الأدوار والمسؤوليات

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

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

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

الالتزام بالمعيار

1- يجب على <رئيس الإدارة المعنية بالأمن السيبراني> ضمان التزام <اسم الجهة> بهذا المعيار باستمرار.

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>.