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 إدارة مفاتيح 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	عُدِّلَ بواسطة	تفاصيل الإصدار
<أدخل رقم النسخة>	اضغط هنا لإضافة تاريخ	<أدخل الاسم الكامل للموظف>	<أدخل وصف الإصدار>

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

الغرض

الغرض من هذا المعيار هو تحديد متطلبات الأمن السيبراني التفصيلية المتعلقة بعملية إدارة مفاتيح التشفير في <اسم الجهة>. تمت مواءمة هذه المتطلبات مع متطلبات الأمن السيبراني الصادرة عن الهيئة الوطنية للأمن السيبراني، وتشمل على سبيل المثال لا الحصر: الضوابط الأساسية للأمن السيبراني (ECC – 1: 2018) والمعايير الوطنية للتشفير (NCS-1:2020) وغيرها من المتطلبات التشريعية والتنظيمية ذات العلاقة بالأمن السيبراني.

نطاق العمل

يغطي هذا المعيار جميع الأصول المعلوماتية والتقنية لدى <اسم الجهة>، وينطبق على جميع العاملين (الموظفين والمتعاقدين) في <اسم الجهة>.

المعايير

1	المتطلبات العامة (General requirements)
الهدف	تحديد المتطلبات العامة لعملية إدارة مفاتيح التشفير لضمان الإدارة الآمنة والمناسبة لمفاتيح التشفير التي تستخدمها <اسم الجهة> خلال دورة حياتها.
المخاطر المحتملة	في حال عدم استخدام مفاتيح التشفير بصورة صحيحة وعدم تنفيذ عملية إدارتها بما يتماشى مع معايير التشفير العامة، فسيؤثر ذلك على عمليات التواصل وتبادل البيانات، ما قد يترتب عليه سرقة المعلومات والكشف عنها والوصول غير المصرح به إليها.
الإجراءات المطلوبة	
1-1	أن تتوافق إدارة مفاتيح التشفير مع الضابط 2-8-3 من الضوابط الأساسية للأمن السيبراني (ECC-1:2018).
2-1	إدارة المفاتيح من خلال الأنشطة التي تتضمن التعامل مع المفاتيح والمعايير الأمنية ذات الصلة مثل متجهات التهيئة خلال دورة المفتاح، بما في ذلك إنشاء المفتاح وتخزينه وإعداده وإدخاله وإخراجه واستخدامه وإتلافه.
3-1	تقسيم المفاتيح وفقًا لتصنيفها (عامة أو خاصة أو مشتركة أو متماثلة) وطبيعة استخدامها.
4-1	حماية المفاتيح وارتباطها وفقًا لنوعها والحماية المطلوبة.
5-1	أن تستوفي عملية استخدام وحدات تشفير الأجهزة المتطلبات التالية:

	• يجب ألا تكون المفاتيح الخاصة صالحة لأكثر من 5 سنوات (وهذا لا يحد من عمر الشهادات الصادرة عن هيئة إصدار الشهادات) لمعايير التشفير من المستوى المتوسط. • يجب ألا تكون المفاتيح الخاصة صالحة لأكثر من 3 سنوات (وهذا لا يحد من عمر الشهادات الصادرة عن هيئة إصدار الشهادات) لمعايير التشفير من المستوى المتقدم.
6-1	أن تستوفي عملية استخدام وحدات تشفير البرمجيات المتطلبات التالية: • يجب ألا تكون المفاتيح الخاصة صالحة لأكثر من سنتين لمعايير التشفير من المستوى المتوسط. • لا تكون مقبولة لمعايير التشفير من المستوى المتقدم.
2	إنشاء المفاتيح (Key Generation)
الهدف	تحديد متطلبات عملية إنشاء المفاتيح لضمان إنشاء المفاتيح بشكل سليم وفقًا للقواعد الأمنية المعمول بها.
المخاطر المحتملة	إذا لم يتم إنشاء مفاتيح التشفير بشكل صحيح بما يتماشى مع العملية المحددة، فقد يؤدي ذلك إلى إنشاء مفاتيح ضعيفة يمكن أن يكون لها تداعيات خطيرة قد يترتب عليها سرقة المعلومات والكشف عنها والوصول غير المصرح به إليها.
الإجراءات المطلوبة	
1-2	أن يتم إنشاء المفاتيح بناءً على: • إنشاء مفتاح باستخدام مُنشئ البتّات العشوائية (تم تحديد منشئات البتّات العشوائية في المنشور الخاص للمعهد الوطني للمعايير والتكنولوجيا 800-90ar1) • اشتقاق مفتاح من مفتاح آخر. • اشتقاق مفتاح من اتفاقية المفاتيح الموثقة بكلمة المرور بين طرفين باستخدام مخطط اتفاقية مفاتيح معتمد.
2-2	أن يتم إنشاء مفاتيح هيئة إصدار الشهادات في بيئة مؤمنة ماديًا من قبل العاملين (الموظفين والمتعاقدين) الذي يتمتعون بأدوار موثوقة خاضعة لرقابة مزدوجة، كحد أدنى، حيث تنطوي الرقابة المزدوجة على الاستعانة بشخصين أو أكثر لمراقبة عملية إنشاء المفاتيح ليكونا جزءًا من إجراء إنشاء المفاتيح الرسمي.

3-2	اعتماد طرق إنشاء أزواج المفاتيح غير المتماثلة وإدراجها وضمان امتثالها لوثيقة المعايير الوطنية للتشفير.
4-2	إنشاء زوج المفاتيح الثابت غير المتماثل من خلال: ● الطرف الذي يملك زوج المفاتيح (أي الطرف الذي يستخدم المفتاح الخاص في حسابات التشفير). ● منشأة تقوم بتوزيع زوج المفاتيح. ● المالك والمنشأة في عملية تعاونية.
5-2	أن تكون المفاتيح المتماثلة إما: ● مُنشأة بواسطة طريقة معتمدة ومُدرجة ومتوافقة مع وثيقة المعايير الوطنية للتشفير ● مشتقة من مفتاح رئيسي/مفتاح اشتقاق المفاتيح باستخدام خوارزمية اشتقاق مفاتيح معتمدة ومتوافقة مع وثيقة المعايير الوطنية للتشفير - وظيفة اشتقاق المفاتيح.
6-2	إنشاء المفتاح السري المتماثل المستخدم لتطبيق الحماية المشفرة على المعلومات وإزالة الحماية أو التحقق منها من خلال: ● جهة أو أكثر من الجهات التي ستتشارك المفتاح، ● طرف موثوق يوفر المفتاح للجهات المشاركة المقصودة بطريقة آمنة. ويجب أن يكون الطرف الموثوق محل ثقة من جميع الجهات التي ستشارك المفتاح وأن يلتزم بعدم الإفصاح عن المفتاح لأطراف غير مصرح لها أو إساءة استخدام المفتاح بأي شكل آخر.
7-2	أن تتوافق أطوال المفاتيح المستخدمة في خوارزميات المفاتيح المتماثلة مع وثيقة المعايير الوطنية للتشفير.
8-2	إنشاء جميع المفاتيح المتماثلة والمفاتيح المشاركة ضمن وحدة تشفير منصوص عليها في وثيقة المعايير الوطنية للتشفير.
9-2	بالنسبة للأنظمة الحساسة، من الضروري استخدام مفاتيح متماثلة بأطوال لا تقل عن 256 بت، ومفاتيح تشفير المنحنى البيضاوي (ECC) غير المتماثل بأطوال لا تقل عن 512 بت.

3	تسجيل/مصادقة المفاتيح (Key Registration/Certification)
الهدف	تحديد متطلبات عملية تسجيل/مصادقة المفاتيح لضمان تنفيذ عملية تسجيل/مصادقة المفاتيح وفقًا للقواعد الأمنية.
المخاطر المحتملة	في حال عدم تسجيل مفاتيح التشفير بما يتماشى مع المتطلبات المحددة، فقد يؤدي ذلك إلى: تسجيل المفاتيح لدى هيئة إصدار شهادات غير موثوقة وغير مصرح لها، ما قد يؤدي إلى تداعيات خطيرة قد يترتب عليها سرقة المعلومات والإفصاح عنها والوصول غير المصرح به إليها.
المعايير المطلوبة	
1-3	ربط المفاتيح بمالكها (مستخدمها) من خلال شهادة.
2-3	توزيع الشهادات الصادرة عن هيئة إصدار شهادات موثوقة على الأطراف المعتمدة والموقعين عليها.
3-3	الاستعانة بهيئة إصدار شهادات موثوقة.
4-3	أن يؤدي تسجيل المفاتيح إلى ربط مواد إنشاء المفاتيح بالمعلومات المرتبطة بجهة معينة. تشمل المفاتيح التي سيتم تسجيلها المفتاح العام لزوج مفاتيح غير متماثل والمفتاح المتماثل المستخدم لتحويل الجهة إلى نظام.
5-3	أن يكون الربط من قبل طرف خارجي موثوق. ومن الأمثلة على الأطراف الخارجية الموثوقة خادم كيربيروس ريلم (Kerberos realm) أو هيئة إصدار شهادات البنية التحتية للمفاتيح العامة (PKI).
6-3	في حال تم تنفيذ عملية الربط من خلال خادم كيربروس ريلم، يجب تخزين مفتاح متماثل على هذا الخادم مع البيانات الوصفية ذات العلاقة.
7-3	في حال قيام هيئة إصدار الشهادات بإجراء الربط، يجب وضع المفتاح العام والمعلومات المرتبطة به في شهادة المفتاح العام التي توقعها هيئة إصدار الشهادات رقميًا.
8-3	إذا قدمت هيئة إصدار الشهادات شهادة لمفتاح عام، يجب التحقق من المفتاح العام للتأكد من ارتباطه بالمفتاح الخاص المعروف من قبل المالك المفترض للمفتاح العام.
4	توزيع المفاتيح وتثبيتها (Key Distribution and Installation)
الهدف	تحديد متطلبات عملية توزيع المفاتيح وتثبيتها لضمان توزيع المفاتيح وتثبيتها بشكل سليم وفقًا للقواعد الأمنية.

المخاطر المحتملة	في حال عدم توزيع مفاتيح التشفير وتثبيتها بما يتماشى مع المتطلبات المحددة، فقد يؤدي ذلك إلى: اختراق المفاتيح وفك تشفيرها أو توزيعها على طرف خارجي غير مصرح له، ما قد يكون لذلك تداعيات خطيرة قد يترتب عليها سرقة المعلومات والكشف عنها والوصول غير المصرح به إليها.
الإجراءات المطلوبة	
1-4	ضمان سلامة وموثوقية مفتاح التحقق من التواقيع الخاص بهيئة إصدار الشهادات (المفتاح العام) وأي معايير مرتبطة به أثناء توزيعه على الأطراف المعوّلة.
2-4	توزيع المفاتيح على مستخدميها بشكل آمن وتحت إشراف المستخدمين.
3-4	نقل المفاتيح بشكل آمن من خلال حماية سريتها وموثوقيتها بما يتماشى مع وثيقة المعايير الوطنية للتشفير وعلى النحو المنصوص عليه فيها.
4-4	عدم توزيع المفاتيح الخاصة والسرية من خلال نص عادي.
5-4	تثبيت جميع نسخ المفاتيح وتخزينها بشكل آمن.
6-4	تأمين المفاتيح العامة لمنع اعتراضها والتلاعب بها إلى حين توزيعها.
7-4	نقل المفاتيح العامة، ويجب حماية الموثوقية (وليس الخصوصية) باستخدام الشهادات.
8-4	حماية المفاتيح الخاصة والتصريح بها من قبل المالك أو الطرف الخارجي أو هيئة إصدار الشهادات.
9-4	نقل المفاتيح التي يتم إنشاؤها باستخدام قنوات آمنة فقط (عندما يكون النقل ضروريًا).
10-4	عدم مشاركة المفاتيح أو توزيعها خارج تلك الجهات أو الأجهزة المحددة التي تتطلب استخدام المفتاح للأغراض المعتمدة.
11-4	أن تكون المفاتيح الموزعة يدويًا إما: ● محمية من خلال التشفير، مثل تلك المخصصة للتوزيع الإلكتروني. ● أو حاصلة على حماية مادية وتخضع للتوزيع المُراقب باستخدام طريقة آمنة ومعتمدة بين كل من منشأة معالجة المفاتيح والجهة النهائية.
12-4	عدم توزيع المفاتيح المستخدمة فقط لتخزين المعلومات إلا لأغراض النسخ الاحتياطي أو إلى الجهات المصرح لها الأخرى التي قد تتطلب الوصول إلى المعلومات المخزنة المحمية بواسطة المفاتيح.

13-4	الحفاظ على سرية المفتاح الخاص لزوج المفاتيح غير المتماثل. إذا تم نقل المفتاح، فيجب إخراجه ونقله بطريقة تضمن سريته وسلامته وموثوقيته بالشكل الملائم.
14-4	أن تكون الطريقة المستخدمة لنقل المفاتيح المتماثلة أو تشفير المفاتيح داعمة لمنظومة الحماية الأمنية اللازمة لحماية البيانات المستهدفة.
15-4	عدم نقل البيانات المشفرة والمفتاح المستخدم لتشفيرها معًا ما لم يتم حماية مفتاح التشفير عبر تشفير ثانوي، على سبيل المثال: تشفير المفتاح العام.
5	استخدام المفاتيح (Key Use)
الهدف	تحديد متطلبات عملية استخدام المفاتيح لضمان الاستخدام السليم للمفاتيح وفقًا للقواعد الأمنية.
المخاطر المحتملة	في حال عدم استخدام مفاتيح التشفير بما يتماشى مع المتطلبات المحددة، فقد يؤدي ذلك إلى: سوء استخدام المفتاح أو استخدامه بشكل غير مصرح به، ما قد يترتب عليه مخاطر شديدة قد تتسبب بسرقة المعلومات أو الكشف عنها أو الوصول غير المصرح به إليها.
الإجراءات المطلوبة	
1-5	حماية المفاتيح من الاستخدام غير المصرح به خلال دورات حياتها.
2-5	أن تخضع المفاتيح لآليات التحقق من التفويض لمنع المالكين من إساءة استخدامها.
3-5	استخدام كل مفتاح لغرض واحد فقط (مثل: التشفير أو المصادقة على السلامة أو تشفير المفاتيح بمفتاح آخر أو إنشاء البتات العشوائية أو التواقيع الرقمية).
4-5	ربط المفاتيح وأغراض استخدامها بطريقة موثوقة (تشفير المفاتيح بمفاتيح أخرى). وتخبر معلومات استخدام المفتاح النظام على متى يمكن (ومتى لا يمكن) استخدام المفتاح.
5-5	يجب تحديد فترة تشفير لكل مفتاح من أزواج المفاتيح غير المتماثلة.
6-5	يجوز تغيير المفتاح في الحالات التالية: • عند اختراق المفتاح. • عند اقتراب انتهاء صلاحية فترة تشفير المفتاح. • من المستحسن الحدّ من كمية البيانات المحمية باستخدام أي مفتاح معين (إنشاء مفتاح مشفر جديد - وهي عملية يتم فيها تغيير المفتاح المستخدم في جلسة الاتصال الجارية من أجل الحد من كمية البيانات التي يتم تشفيرها باستخدام المفتاح ذاته).

6	تخزين المفاتيح (Key Storage)
الهدف	تحديد متطلبات عملية تخزين المفاتيح لضمان التخزين السليم للمفاتيح وفقًا للقواعد الأمنية المعمول بها.
المخاطر المحتملة	في حال عدم تخزين مفاتيح التشفير بما يتماشى مع المتطلبات المحددة، فقد يؤدي ذلك إلى: تسرب بيانات المفتاح وفك تشفيره نتيجة لذلك، ما قد يؤدي إلى مخاطر شديدة قد تتسبب بسرقة المعلومات أو الكشف عنها أو الوصول غير المصرح به إليها.
الإجراءات المطلوبة	
1-6	على الجهة أن تفرض إعداد نسخ احتياطية آمنة للمفاتيح (للاستخدام الداخلي أو لاستخدام جهات إنفاذ القانون) عندما يكون التشفير مدعومًا.
2-6	يجب تحديد قواعد تخزين معلومات المفاتيح ووقت الاحتفاظ بها من قبل <اسم الجهة>.
3-6	أن تخضع المفاتيح المستخدمة في ضمان عدم إنكار صحة البيانات لرقابة المستخدم وحده.
4-6	استخدام معرفات المفاتيح أو الأسماء المميزة لتحديد المفاتيح بشكل صحيح.
5-6	على <اسم الجهة> معالجة كيفية قيام جهاز أو تطبيق التشفير بتخزين وحماية معلومات المفاتيح، بما في ذلك مدة تخزينها.
6-6	أن توضح <اسم الجهة> كيفية تحديد معلومات المفتاح (مثل: معرف المفتاح، والاسم المميز، والملكية، ومستخدمي المفتاح، وتاريخ الإنشاء، وتاريخ انتهاء الصلاحية، وهيئة إصدار الشهادات المعنية) خلال فترة تخزينه (مثل: باستخدام اسم مميز أو معرف مفاتيح). كما يجب إدراج متطلبات سعة التخزين لتخزين معلومات المفتاح.
7-6	تخزين المفاتيح الخاصة غير المتماثلة بإحدى الطرق التالية: • داخل جهاز واحدة من أجهزة تأمين وإدارة المفاتيح الرقمية بصيغة نص عادي (أو مشفرة بمفتاح رئيسي). • خارج أجهزة تأمين وإدارة المفاتيح الرقمية مع التأكد من تشفيرها بواسطة خوارزمية تشفير المفاتيح بمفاتيح أخرى وفقًا للمعايير الوطنية للتشفير. • داخل عدة أجهزة من أجهزة تأمين وإدارة المفاتيح الرقمية بصيغ نص عادي متفرقة (أو مشفرة بمفتاح رئيسي).
8-6	يجب تخزين المفاتيح المتماثلة داخل أجهزة تأمين وإدارة المفاتيح الرقمية. وفي حال كان هناك استثناء يستدعي تخزين المفتاح خارج وحدة التشفير، يجب أن تعتمد آلية الحماية على مستوى التأثير المرتبط بالبيانات المحمية بواسطة المفتاح.

9-6	تشفير قاعدة البيانات المستخدمة لتخزين المفاتيح باستخدام وحدة معتمدة تمتثل لوثيقة معايير الأمن الوطني.
7	إلغاء المفاتيح/التحقق منها (Key Revocation/Validation)
الهدف	تحديد متطلبات عملية إلغاء المفاتيح/التحقق منها لضمان الإتلاف التام للمفاتيح وفقًا للقواعد الأمنية المعمول بها.
المخاطر المحتملة	في حال عدم إلغاء مفاتيح التشفير والتحقق منها بما يتماشى مع المتطلبات المحددة، فقد يؤدي ذلك إلى: البيانات المشفرة بسبب فك تشفير المفتاح المخترق وتسربه أو انتهاء صلاحية استخدام المفتاح، ما قد يترتب عليه مخاطر شديدة قد تتسبب بسرقة المعلومات أو الكشف عنها أو الوصول غير المصرح به إليها.
الإجراءات المطلوبة	
1-7	يجب إلغاء المفتاح في الحالات التالية: • يجب إنهاء الاستخدام المصرح به لمفتاح ما قبل نهاية مدة التشفير المحددة لهذا المفتاح. • انتهاء فترة استخدام المفتاح. • اختراق المفتاح.
2-7	يجوز إلغاء المفتاح لأسباب إدارية (مثل: مغادرة مالك المفتاح لـ<اسم الجهة> أو رفع جهاز يحتوي على المفتاح من الخدمة).
3-7	يجب إلغاء المفتاح على أساس طارئ إذا كان هناك سبب وجيه للاعتقاد بأن المفتاح قد كُشف أو تم الوصول إليه بطريقة أخرى من قبل جهة غير مصرح لها.
4-7	يجب إلغاء المفتاح بأسرع وقت ممكن بعد إثبات الحاجة إلى الإلغاء.
5-7	تفعيل قائمة إلغاء الشهادات (CRL) وبروتوكول حالة الشهادة عبر الإنترنت (OCSP) لتجنب الاعتماد على المفاتيح التي انتهت صلاحيتها.
6-7	إشعار الأطراف ذات العلاقة بعملية إلغاء المفتاح باستخدام قوائم إلغاء الشهادات أو بروتوكول حالة الشهادة عبر الإنترنت، على سبيل المثال.
7-7	عند اختراق أو فك تشفير أحد المفاتيح، يجب إشعار جميع الجهات التي تتشارك المفتاح (مثل: باستخدام قائمة المفاتيح المخترقة).

8-7	على <اسم الجهة> التحقق من المفاتيح المستخدمة من خلال التحقق من قوائم/خوادم إلغاء الشهادات أو بروتوكول حالة الشهادة عبر الإنترنت.
9-7	الحصول على ضمان لصلاحية المفاتيح العامة للتأكد من أن المفتاح صحيح حسابياً من خلال إحدى الطرق التالية: ● الحصول على ضمان من مالك المفتاح أو جهة التحقق من المفتاح أو طرف خارجي موثوق. ● التحقق الصريح من المفاتيح العامة من خلال تشفير رسالة باستخدام مفتاح واحد وفك التشفير باستخدام المفتاح الآخر.
8	أرشفة المفاتيح (Key Archive)
الهدف	تحديد متطلبات عملية أرشفة المفاتيح لضمان الأرشفة السليمة للمفاتيح وفقًا للقواعد الأمنية المعمول بها.
المخاطر المحتملة	في حال عدم أرشفة مفاتيح التشفير بما يتماشى مع المتطلبات المحددة، فقد يؤدي ذلك إلى: تسرب بيانات المفتاح وتعرضه للاختراق وتسرب البيانات نتيجة لذلك، ما قد يترتب عليه مخاطر شديدة قد تتسبب بسرقة المعلومات أو الكشف عنها أو الوصول غير المصرح به إليها.
الإجراءات المطلوبة	
1-8	تأمين عملية الأرشفة وضمان السرية للحفاظ على سرية المعلومات المشفرة بالمفاتيح المؤرشفة.
2-8	أرشفة المفاتيح منتهية الصلاحية لضمان إمكانية الوصول إلى البيانات القديمة شريطة أن يكون التشفير الأصلي مدعومًا.
3-8	أن تلتزم أنظمة الأرشفة بفترات الاحتفاظ المحددة وفقًا للوائح ذات الصلة والسياسات والمعايير الداخلية في <اسم الجهة>.
4-8	يجب أن يحتوي أرشيف المفاتيح على المفاتيح والمعلومات المرتبطة بها (أي معلومات المفتاح مثل: معرف المفتاح، والاسم المميز، والملكية، ومستخدمي المفتاح، وتاريخ الإنشاء، وتاريخ انتهاء الصلاحية، وهيئة إصدار الشهادات المعنية لأغراض الاستعادة بعد مدة تشفير المفاتيح.
5-8	ضمان استمرار توفير تدابير الحماية المناسبة من خلال أرشيف المفاتيح بما يتماشى مع المتطلبات الواردة في وثيقة المعايير الوطنية للتشفير لكل مفتاح وأي معلومات أخرى ذات

	صلة في الأرشيف. يجب أن يطبق الأرشيف آلية محكمة للتحكم في الوصول لتقييد الوصول وضمان اقتصاره على الجهات المصرح لها فقط.
6-8	الاحتفاظ بالأرشيف من قبل <اسم الجهة> أو طرف خارجي موثوق.
9	إتلاف المفاتيح (Key Destruction)
الهدف	تحديد متطلبات عملية إتلاف المفاتيح لضمان إتلاف المفاتيح بشكل سليم وفقًا للقواعد الأمنية المعمول بها.
المخاطر المحتملة	في حال عدم إتلاف مفاتيح التشفير بما يتماشى مع المتطلبات المحددة، فقد يؤدي ذلك إلى: احتمالية فك تشفير البيانات من خلال اختراق المفاتيح وتسرب البيانات، ما قد يترتب عليه مخاطر شديدة قد تتسبب بسرقة المعلومات أو الكشف عنها أو الوصول غير المصرح به إليها.
الإجراءات المطلوبة	
1-9	إزالة المفاتيح عند انتهاء فترة صلاحية المفتاح وعندما لا تعود هناك حاجة لأرشفته أو تخزينه من خلال عملية حذف آمنة تمتثل لوثيقة معايير الأمن الوطني للحدّ من احتمالات الاختراق. يجب إزالة المفتاح بالكامل بجميع أحداثه والتأكد من استحالة استعادة ذلك المفتاح.
2-9	إتلاف جميع نسخ المفاتيح السرية (المتماثلة) والمفاتيح العامة والخاصة (غير المتماثلة) بمجرد انتفاء الحاجة إليها (مثل: لأغراض الأرشفة وإعادة الإنشاء) من أجل الحدّ من احتمالية الاختراق.
3-9	إتلاف المفاتيح السرية (المتماثلة) والمفاتيح العامة والخاصة (غير المتماثلة) بما يضمن التخلص من جميع آثار وسجلات المفاتيح بحيث لا يمكن استردادها سواء بوسائل مادية أو إلكترونية.
4-9	إلغاء المفتاح المخترق بأسرع وقت ممكن.
5-9	الاحتفاظ بالمفاتيح العامة أو إتلافها اعتمادًا على الاحتياجات المستقبلية، بالاقتران مع أغراض الأرشفة أو الاستعادة أو المساءلة.
6-9	تطهير أنظمة تخزين الوسائل التي تخزّن المفاتيح بشكل كامل قبل التخلص منها باستخدام عملية تمتثل للمنشور الخاص للمعهد الوطني للمعايير والتكنولوجيا 800-88r1 أو دليل التطهير الكامل لأجهزة التخزين الصادر عن إدارة الأمن المركزي التابعة لوكالة الأمن القومي.

10	المسؤولية عن المفاتيح (Key Accounting)
الهدف	تحديد متطلبات عملية تعيين نطاق المسؤولية عن المفاتيح لضمان تحديد المسؤولية عن المفاتيح بشكل صحيح وفقًا للقواعد الأمنية المعمول بها.
المخاطر المحتملة	في حال عدم تحديد نطاق المسؤولية عن مفاتيح التشفير بما يتماشى مع المتطلبات المحددة، فقد يؤدي ذلك إلى: تعذر استدعاء الشخص المسؤول عن سوء استخدام المفتاح أو اختراق المفتاح، ما قد يترتب عليه مخاطر شديدة قد تتسبب بسرقة المعلومات أو الكشف عنها أو الوصول غير المصرح به إليها.
الإجراءات المطلوبة	
1-10	مراقبة استخدام المفاتيح غير المتماثلة من قبل <الإدارة المعنية بالأمن السيبراني> التابعة ل<اسم الجهة> أو ترشيحها من قبل مالكي/مديري المفاتيح لدى <الإدارة المعنية بالأمن السيبراني> من خلال أدوات مخصصة.
2-10	تحديد نطاق المسؤولية عن المفاتيح، ويجب أن تتضمن عملية تحديد نطاق المسؤولية تعيين الجهات التي تمتلك صلاحيات الوصول إلى مفاتيح التشفير أو التحكم فيها طوال دورة حياتها.
3-10	إبلاغ كل شخص يشارك في إدارة المفاتيح لدى <اسم الجهة> بنطاق مسؤولياتهم بشكل واضح وضمان مساءلتهم عن الالتزام بها.

11	معايير أخرى (Standard controls Other)
الهدف	يجب ضبط إعدادات عملية إدارة المفاتيح وتنفيذها بشكل آمن وتلبية المعايير الأخرى ذات الصلة.
المخاطر المحتملة	قد يترتب على عدم التزام <اسم الجهة> بجميع المعايير والمتطلبات الإلزامية المطبقة ارتفاع احتمالية تعرضها للتهديدات في المجالات التي تغطيها المعايير المذكورة أدناه.
الإجراءات المطلوبة	
1-11	تطبيق المعايير التالية فيما يتعلق بعملية إدارة المفاتيح: 1- المعايير الوطنية للتشفير 2- معيار التشفير

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 عند 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 دوريًا.

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>.