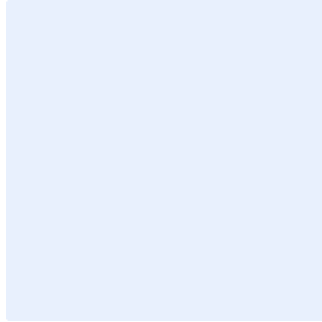


هذا المربع مخصص لأغراض توجيهية. احذف جميع المربعات التوجيهية بعد تعبئة النموذج. يجب تحرير **النود الملونة باللون الأزرق** بصورة مناسبة. ويجب إزالة التظليل الملون بعد إجراء التعديلات.



أدخل شعار الجهة بالضغط على الصورة الموضحة.

## نموذج سياسة مراجعة وتدقيق الأمن السيبراني

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

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

اختر التصنيف

التاريخ:

الإصدار:

المرجع:

اضغط هنا لإضافة نص

اضغط هنا لإضافة نص

اضغط هنا لإضافة نص



## اعتماد الوثيقة

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

## نسخ الوثيقة

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

اختر التصنيف

الإصدار 1.0



## قائمة المحتويات

3	الأهداف
3	نطاق العمل وقابلية التطبيق
3	بنود السياسة
4	الأدوار والمسؤوليات
4	الالتزام بالسياسة

تهدف هذه السياسة إلى تحديد متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير لمراجعة وتدقيق ضوابط الأمن السيبراني لدى **<اسم الجهة>** والتأكد من تطبيقها وأنها تعمل وفقاً للسياسات والإجراءات التنظيمية ل**<اسم الجهة>**، والمتطلبات التشريعية والتنظيمية الوطنية ذات العلاقة، والمتطلبات الدولية المقررة تنظيمياً على **<اسم الجهة>**.

تتبع هذه السياسة المتطلبات التشريعية والتنظيمية الوطنية وأفضل الممارسات الدولية ذات العلاقة، وهي مطلب تشريعي كما هو مذكور في الضابط رقم 1-8-1 من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني.

## نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع ضوابط الأمن السيبراني في **<اسم الجهة>** وتنطبق على جميع العاملين في **<اسم الجهة>**.

## بنود السياسة

### 1- البنود العامة

- 1-1 يجب على **<الإدارة المعنية بالأمن السيبراني>** مراجعة تطبيق ضوابط الأمن السيبراني دورياً، ومراجعة مدى الالتزام بالضوابط الأساسية للأمن السيبراني (ECC:1-2018) وضوابط الأمن السيبراني للأنظمة الحساسة (CSCC-1:2019) الصادرة من الهيئة الوطنية للأمن السيبراني.
- 2-1 يجب مراجعة وتدقيق تطبيق ضوابط الأمن السيبراني دورياً من قبل أطراف مستقلة عن **<الإدارة المعنية بالأمن السيبراني>**، مثل **<الإدارة المعنية بالمراجعة الداخلية>** أو طرف خارجي.
- 3-1 يجب أن تتم مراجعة تطبيق ضوابط الأمن السيبراني للأنظمة الحساسة مرة واحدة كل ثلاث سنوات على الأقل من قبل أطراف مستقلة عن **<الإدارة المعنية بالأمن السيبراني>** من داخل **<اسم الجهة>**.
- 4-1 يجب التأكد من تطبيق ضوابط الأمن السيبراني دورياً، ومرة واحدة سنوياً على الأقل للأنظمة الحساسة للتأكد من مواءمتها مع الضوابط الأساسية للأمن السيبراني (ECC:1-2018) وضوابط الأمن السيبراني للأنظمة الحساسة (CSCC-1:2019).
- 5-1 يجب تحديد إجراءات مراجعة وتدقيق الأمن السيبراني وتوثيقها.
- 6-1 يجب توثيق نتائج مراجعة وتدقيق الأمن السيبراني ومناقشتها مع الإدارات المعنية.
- 7-1 يجب عرض النتائج على اللجنة الإشرافية للأمن السيبراني وصاحب الصلاحية، كما يجب أن تشمل النتائج نطاق المراجعة والتدقيق، والملاحظات المكتشفة، والتوصيات والإجراءات التصحيحية، وتقييم المخاطر وخطة معالجة الملاحظات.
- 8-1 يجب اعتماد جدول المسؤوليات التالي (RACI Chart) في تنفيذ عمليات مراجعة وتدقيق الأمن السيبراني:

اختر التصنيف

الإصدار 1.0

رئيس الجهة	رئيس اللجنة المعنية بالأمن السيبراني بالجهة	رئيس الإدارة المعنية بالأمن السيبراني	الإدارة المعنية بالأمن السيبراني	التدقيق الداخلي	المدقق الخارجي	
I	I	A	R		R	مراجعة الأمن السيبراني
I	A	I	I	R	R	تدقيق الأمن السيبراني
I	A	R	R	C/I	C/I	تنفيذ إجراءات تصحيحية

## 2- متطلبات أخرى

- 1-2 يجب أن تتخذ **الإدارة المعنية بالأمن السيبراني** إجراءات استباقية وتصحيحية خاصة بنتائج المراجعة والتدقيق.
- 2-2 يجب على **الإدارة المعنية بالأمن السيبراني** تحديد العوامل التي أدت إلى هذه الملاحظات وتحليلها ومعرفة أسبابها والحد من تكرارها.
- 3-2 يجب مراجعة سياسة مراجعة وتدقيق الأمن السيبراني سنوياً، وتوثيق التغييرات واعتمادها.

## 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 بالمراجعة الداخلية**.

## الالتزام بالسياسة

- 1- يجب على **رئيس الإدارة المعنية بالأمن السيبراني** ضمان التزام **اسم الجهة** بهذه السياسة دورياً.
- 2- يجب على جميع 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**.

اختر التصنيف

الإصدار 1.0