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 مراجعة وتدقيق الأمن السيبراني

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

* اضغط على مفتاحي "Ctrl" و"H" في الوقت نفسه.
* أضف "<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.

|  |  |
| --- | --- |
| اختر التصنيف | |
| التاريخ: | اضغط هنا لإضافة تاريخ |
| الإصدار: | اضغط هنا لإضافة نص |
| المرجع: | اضغط هنا لإضافة نص |

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

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

نسخ الوثيقة

|  |  |  |  |
| --- | --- | --- | --- |
| النسخة | التاريخ | عُدلَ 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 نص |
|  |  |  |

قائمة المحتويات

[الغرض 4](#_Toc129608074)

[نطاق العمل 4](#_Toc129608075)

[بنود السياسة 4](#_Toc129608076)

[الأدوار والمسؤوليات 5](#_Toc129608077)

[التحديث والمراجعة 6](#_Toc129608078)

[الالتزام بالسياسة 6](#_Toc129608079)

# الغرض

تهدف هذه السياسة إلى تحديد متطلبات الأمن السيبراني المتعلقة بمراجعة 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 المقرة تنظيمياً على <اسم الجهة>.

تهدف هذه السياسة إلى الالتزام بالضوابط والمعايير الصادرة من الهيئة الوطنية للأمن السيبراني والمتطلبات التنظيمية والتشريعية ذات العلاقة.

# [نطاق العمل](#نطاق" \o "يهدف هذا القسم في نموذج السياسة إلى تحديد الأطراف والأشخاص الذين تنطبق عليهم وتحديد مدة فعالية وسيران هذه السياسة والتي قد تمتد إلى ما بعد نهاية العلاقة مع الجهة.)

تغطي هذه السياسة جميع ضوابط الأمن السيبراني في <اسم الجهة> وتنطبق على جميع العاملين (الموظفين والمتعاقدين) في <اسم الجهة>، بما في ذلك الجهات التي تتعامل معها والأطراف الخارجية.

# [بنود السياسة](#بنود" \o "يهدف هذا القسم إلى تحديد جميع المتطلبات والضوابط الأساسية للسياسة؛ بناء على نتائج تقييم المخاطر، ومتطلبات الأعمال، والمتطلبات التنظيمية والتشريعية الخاصة بها.)

1. **البنود العامة**
   1. يجب على >الإدارة المعنية بالأمن السيبراني< في <اسم الجهة> مراجعة وتدقيق تطبيق ضوابط الأمن السيبراني الخاصة ب<اسم الجهة> مرة واحدة سنويًا على الأقل، ومراجعة مدى الالتزام بضوابط الأمن السيبراني الصادرة من الهيئة الوطنية للأمن السيبراني التي تنطبق على <اسم الجهة>.
   2. يجب تحديد إجراءات مراجعة وتدقيق الأمن السيبراني وتوثيقها وتطبيقها.
   3. يجب مراجعة وتدقيق تطبيق ضوابط الأمن السيبراني الخاصة ب<اسم الجهة> دورياً من قبل أطراف مستقلة عن >الإدارة المعنية بالأمن السيبراني<، مثل <الإدارة المعنية بالمراجعة الداخلية> أو طرف خارجي وأن تكون وفق المتطلبات التشريعية والتنظيمية ذات العلاقة.
   4. يجب أن تتم مراجعة تطبيق ضوابط الأمن السيبراني للأنظمة الحساسة مرة واحدة سنويا على الأقل من قبل >الإدارة المعنية بالأمن السيبراني< وكل ثلاث سنوات من قبل أطراف مستقلة عن >الإدارة المعنية بالأمن السيبراني<، مثل <الإدارة المعنية بالمراجعة الداخلية> أو طرف خارجي وأن تكون وفق المتطلبات التشريعية والتنظيمية ذات العلاقة.
   5. يجب على >الإدارة المعنية بالأمن السيبراني< مراجعة تطبيق ضوابط الأمن السيبراني للبيانات (DCC-1:2022) حسب تصنيفها حيث تتم مراجعة الضوابط للبيانات المصنفة (عام ومقيد) مرة واحدة كل 3 سنوات على الأقل، وتتم مراجعة الضوابط للبيانات المصنفة (سري وسري للغاية) مرة واحدة كل سنة على الأقل وأن تكون وفق المتطلبات التشريعية والتنظيمية ذات العلاقة.
   6. يجب أن تتم مراجعة تطبيق ضوابط الأمن السيبراني للبيانات (DCC-1:2022) من قبل أطراف مستقلة عن >الإدارة المعنية بالأمن السيبراني< من داخل >اسم الجهة< حسب المدة المحددة لكل مستوى حيث تتم مراجعة تطبيق الضوابط للبيانات المصنفة (عام ومقيد) مرة واحدة كل 5 سنوات على الأقل وتتم مراجعة تطبيق الضوابط للبيانات المصنفة (سري وسري للغاية) مرة واحدة كل 3 سنوات على الأقل وأن تكون وفق المتطلبات التشريعية والتنظيمية ذات العلاقة.
   7. يجب على >الإدارة المعنية بالأمن السيبراني< في <اسم الجهة> مراجعة تطبيق ضوابط الأمن السيبراني لأنظمة التحكم الصناعي (OT/ICS) (ECC-1:2018) مرة واحدة سنويًا على الأقل.
   8. يجب مراجعة تطبيق ضوابط الأمن السيبراني لأنظمة التحكم الصناعي من قبل أطراف مستقلة عن >الإدارة المعنية بالأمن السيبراني< في <اسم الجهة> مرة واحدة كل ثلاث سنوات على الأقل وأن تكون وفق المتطلبات التشريعية والتنظيمية ذات العلاقة.
   9. يجب توثيق نتائج مراجعة وتدقيق الأمن السيبراني ومناقشتها مع الإدارات المعنية.
   10. 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.
   11. يجب اعتماد جدول المسؤوليات التالي (RACI Chart) في تنفيذ عمليات مراجعة وتدقيق الأمن السيبراني:

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

* 1. يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر والاستخدام الصحيح والفعال لمتطلبات مراجعة وتدقيق متطلبات الأمن السيبراني.

# [الأدوار والمسؤوليات](#الأدوار)

1. **مالك السياسة:** <رئيس الإدارة المعنية بالأمن السيبراني>.
2. **مراجعة السياسة وتحديثها:** <الإدارة المعنية بالأمن السيبراني>.
3. **تنفيذ السياسة وتطبيقها:** <الإدارة المعنية بتقنية المعلومات>.
4. **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](#الالتزام)

1. يجب على <رئيس الإدارة المعنية بالأمن السيبراني> التأكد من التزام <اسم الجهة> بهذه السياسة دورياً.
2. يجب على كافة 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>.