هذا المربع مخصّص لأغراض توجيهية. احذف جميع المربعات التوجيهية بعد تعبئة النموذج. يجب تحرير البنود الملوّنة باللون الأزرق بصورة مناسبة. أما البنود الملوّنة بالأخضر فهي أمثلة يجب حذفها. ويجب إزالة التظليل الملون بعد إجراء التعديلات. قم بإزالة التظليلات الصفراء إذا كانت الجهة لا تنوي إضافة أي جهات فرعية تابعة لها في استراتيجياتها للأمن السيبراني.

أدخل شعار الجهة بالضغط على الصورة الموضحة.

نموذج استراتيجية وخارطة طريق الأمن السيبراني

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 <١,٠>

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	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 <١,٠>

الفهرس

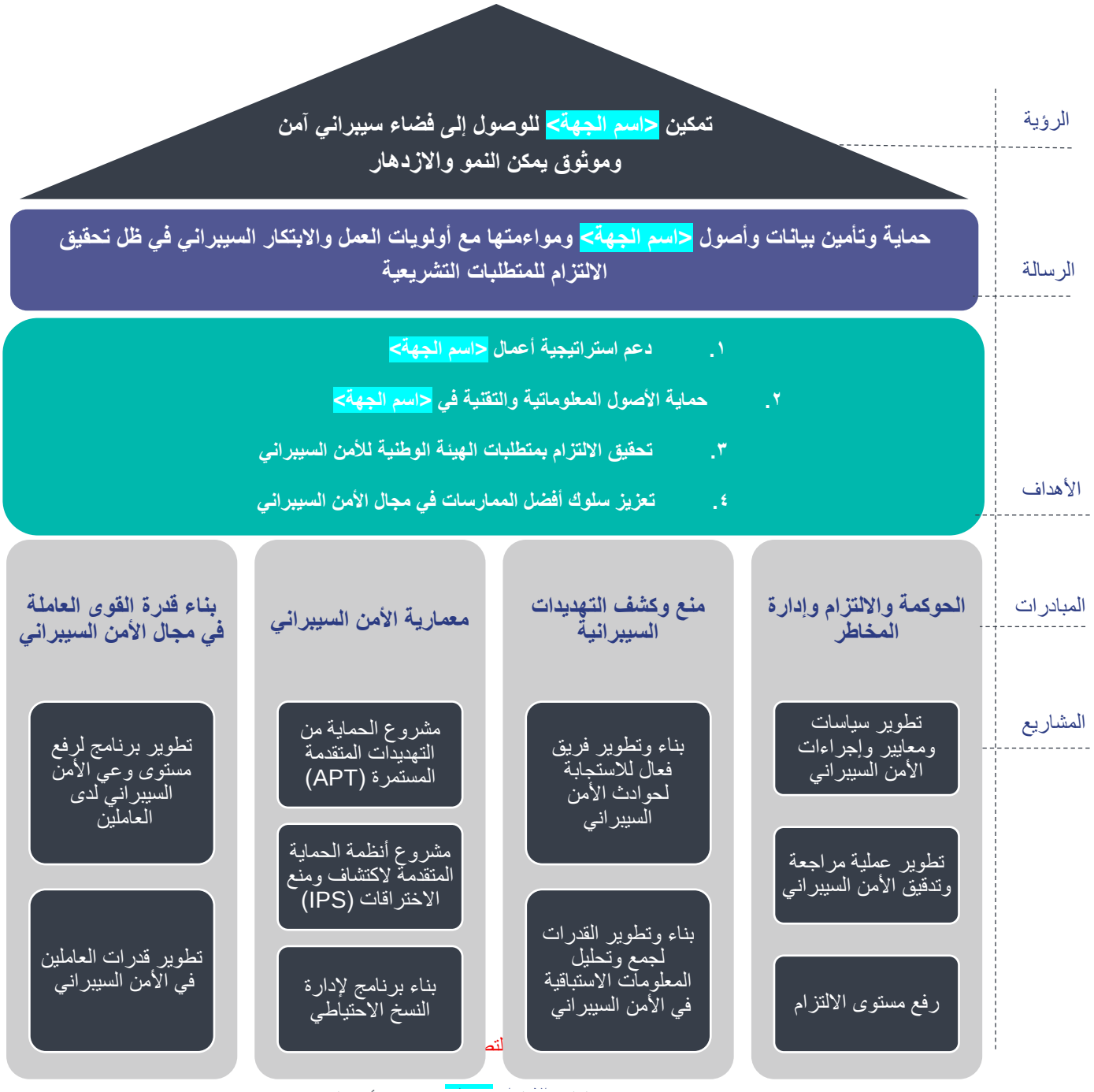
اختر التصنيف

الإصدار <١,٠>

استراتيجية الأمن السيبراني

الملخص التنفيذي

تسعى <اسم الجهة> إلى تطوير قدراتها في مجال الأمن السيبراني، والمحافظة عليه وتعزيزه وحمايتها من المخاطر السيبرانية الداخلية والخارجية، وقد أعدّت <اسم الجهة> هذه الاستراتيجية الخاصة بالأمن السيبراني من أجل مواجهة التهديدات وتقليل المخاطر السيبرانية ودعم استراتيجية أعمال <اسم الجهة> لمدة ثلاث سنوات.



رسم توضيحي ١: الملخص التنفيذي لاستراتيجية الأمن السيبراني

مقدمة

تسعى <اسم الجهة> إلى تطوير قدراتها في مجال الأمن السيبراني بهدف تحسين مستوياته، والمحافظة عليه وتعزيزه في <اسم الجهة> وحمايتها من المخاطر السيبرانية الداخلية والخارجية، وقد أعدّت <اسم الجهة> هذه الاستراتيجية الخاصة بالأمن السيبراني لدعم استراتيجية أعمال <اسم الجهة> ومواجهة التهديدات وتقليل المخاطر السيبرانية.

وتستهدف هذه الاستراتيجية بصورة أساسية كلًا من <رئيس الإدارة المعنية بالأمن السيبراني>، وأعضاء اللجنة الإشرافية للأمن السيبراني، ومشرفي الأمن السيبراني في <اسم الجهة>، وغيرهم من المتخصّصين في هذا المجال. وتقع مسؤولية الأمن السيبراني على عاتق جميع العاملين في <اسم الجهة>، ويشمل ذلك الأطراف الخارجية.

وقد صُمّمت استراتيجية الأمن السيبراني لتقديم التوصيات المتعلّقة بأعمال الأمن السيبراني في <اسم الجهة> بشكل يتوافق مع طبيعة العمل، وذلك لتمكين مبادرات الأعمال، وتقديم رؤية واضحة وموحّدة ونشرها بين كافة إدارات وأقسام <اسم الجهة> والجهات والشركات التابعة لها.

هذه المتطلبات تمت موائمتها مع متطلبات الأمن السيبراني الصادرة من الهيئة الوطنية للأمن السيبراني ويشمل ذلك على سبيل المثال: الضوابط الأساسية للأمن السيبراني (ECC – ١: ٢٠١٨)، وغيرها من المتطلبات التشريعية والتنظيمية ذات العلاقة.

نطاق العمل وقابلية التطبيق

تغطي استراتيجية الأمن السيبراني جميع أعمال <اسم الجهة>، وستحرص <اسم الجهة> بدورها والجهات والشركات التابعة لها على تنفيذها.

وتنطبق هذه الاستراتيجية على الجهات والشركات التالية:

١- <اسم الجهة ١>.
٢- <اسم الجهة ٢>.
٣- ...

وبما أن المبادرات المُحدّدة في هذه الاستراتيجية تنطبق على الجهات والشركات وتؤثّر عليها، فإنه من المقرّر الاتفاق على تنفيذها بالتنسيق مع هذه الجهات.

رؤية الأمن السيبراني (Cybersecurity Vision)

١- تقدم رؤية الأمن السيبراني وصفًا موجزًا للمكانة التي تطمح <اسم الجهة> للوصول إليها من حيث وضع أمنها السيبراني خلال السنوات الثلاث المقبلة، كما تصف الوضع المستهدف مستقبلًا للأمن السيبراني في <اسم الجهة>.

اختر التصنيف

الإصدار <١,٠>

٢- أخذت <الإدارة المعنية بالأمن السيبراني> بالاعتبار الأهداف الخاصة بـ<اسم الجهة> لضمان توافقها مع رؤية الأمن السيبراني.

رؤية الأمن السيبراني

تمكين <اسم الجهة> للوصول إلى فضاء سيبراني آمن وموثوق يمكن النمو والازدهار.

أهداف الأمن السيبراني (Cybersecurity Objectives)

حُدّدت أهداف الأمن السيبراني وفقًا لرؤية الأمن السيبراني ونتائج الوضع الحالي للأمن السيبراني، وهي كالتالي:

١- **دعم استراتيجية أعمال** <اسم الجهة>: ضمان إسهام خطط العمل للأمن السيبراني والأهداف والمبادرات والمشاريع داخل <اسم الجهة> في تحقيق الأهداف والمتطلبات التشريعية والتنظيمية ذات العلاقة.

٢- **حماية الأصول المعلوماتية والتقنية في** <اسم الجهة>: توفير الحلول التقنية اللازمة لحماية الأصول المعلوماتية والتقنية في<اسم الجهة>.

٣- **تعزيز سلوك أفضل الممارسات في مجال الأمن السيبراني:** تطوير العاملين بالمهارات والمؤهلات في مجال الأمن السيبراني، وتعزيز الوعي بالأمن السيبراني من خلال قنوات متعددة، وبناء ثقافة إيجابية للأمن السيبراني.

مبادرات ومشاريع الأمن السيبراني (Cybersecurity Initiatives and Projects)

١- تتضمّن مبادرات الأمن السيبراني جميع المشاريع والبرامج المطلوبة لتنفيذ أهداف استراتيجية الأمن السيبراني، وتُشكَّل هذه المبادرات بناءً على رؤية الأمن السيبراني وأهدافها:

- **الحوكمة والالتزام وإدارة المخاطر:** تشتمل المبادرة على مشاريع وبرامج في الحوكمة والمخاطر والالتزام لتعزيز الأمن السيبراني في <اسم الجهة> وبناء الخطط الاستراتيجية في الأمن السيبراني. ويشمل ذلك على سبيل المثال لا الحصر: مشروع الالتزام بضوابط وإرشادات الهيئة الوطنية للأمن السيبراني والتي تشمل: الضوابط الأساسية للأمن السيبراني، ضوابط الأمن السيبراني للأنظمة الحساسة وغيرها.
- **منع وكشف التهديدات السيبرانية:** تشتمل المبادرة على مشاريع وبرامج تساعد <اسم الجهة> على كشف ومنع التهديدات الداخلية والخارجية. ويشمل ذلك على سبيل المثال لا الحصر: مشروع لشراء وتشغيل الأنظمة الخاصة بكشف ومنع التهديدات الداخلية والخارجية والتي تشمل اكتشاف نقطة النهاية والاستجابة (EDR) أو نظام المعلومات الأمنية وإدارة الأحداث (SIEM) وغيرها.
- **معمارية الأمن السيبراني:** تشتمل المبادرة على مشاريع وبرامج تساعد <اسم الجهة> على زيادة مستوى نضجها في الأمن السيبراني وحماية <اسم الجهة> من المخاطر السيبرانية. ويشمل ذلك على سبيل المثال لا الحصر: بناء وتنفيذ معمارية أمن الشبكات وغيرها.
- **بناء قدرة القوى العاملة في مجال الأمن السيبراني:** تشتمل هذه المبادرة على مشاريع وبرامج تهدف إلى رفع الوعي بالأمن السيبراني وتعزيز العاملين في <الإدارة المعنية بالأمن السيبراني> بالمهارات

والمؤهلات في مجال الأمن السيبراني. ويشمل ذلك على سبيل المثال لا الحصر: مشروع بناء برنامج توعية خاص بالأمن السيبراني المتعلق بالعاملين بالجهة والذي يشمل عدة مواضيع منها التحذير من التصيد بالبريد الإلكتروني ومشاركة المعلومات على وسائل التواصل الاجتماعي.

مؤشرات الأداء الرئيسية (Key Performance Indicators)

لقياس كفاءة الاستراتيجية في تحقيق أهدافها، تم تصميم عدد من مؤشرات الأداء الرئيسية؛ لتقيس مستوى التقدم لكل هدف كما تم تحديد خط أساس ومستهدف سنوي لكل مؤشر؛ وذلك بناء على نتائج دراسة الوضع الراهن والتجارب الدولية وورش العمل مع المختصين والاستشاريين وقد تم ربط المؤشرات بثلاثة نتائج استراتيجية يتم الوصول لها من خلال احتساب المؤشرات بما يحقق الوصول إلى رؤية الاستراتيجية، وتسعى المملكة إلى تحقيقها خلال خمس سنوات، وهذه النتائج الاستراتيجية هي:

١. تقليل المخاطر
٢. تعزيز الثقة
٣. تمكين النمو

وسوف يتضح أثر التنفيذ من خلال الإسهام في النمو، وتقليل المخاطر، وتعزيز الثقة أيضا مع تطور تنفيذ الاستراتيجية، والتزام الجهات الوطنية بالأدوار والمسؤوليات، والأطر والمعايير المناطة بها، وسوف تظهر المخرجات الوطنية تحسنًا كبيرًا على المدى البعيد.

خارطة طريق الأمن السيبراني

مقدمة

تسعى <اسم الجهة> إلى تطوير قدراتها في مجال الأمن السيبراني بهدف تحسين مستوياته، والمحافظة عليه وتعزيزه في <اسم الجهة> وحمايتها من المخاطر السيبرانية الداخلية والخارجية، وقد أعدّت <اسم الجهة> هذه الخارطة الخاصة بالأمن السيبراني لدعم استراتيجية أعمال <اسم الجهة> ومواجهة التهديدات وتقليل المخاطر السيبرانية.

وتهدف هذه الوثيقة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم ١-١-١ من الضوابط الأساسية للأمن السيبراني (ECC-١:٢٠١٨) الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

تغطي خارطة طريق الأمن السيبراني جميع أعمال <اسم الجهة>، وستحرص <اسم الجهة> بدورها والجهات والشركات التابعة لها على تنفيذها.

وتنطبق هذه الخارطة على الجهات والشركات التالية:

٤- <اسم الجهة ١>.
٥- <اسم الجهة ٢>.
٦- ...

وبما أن المبادرات المُحدّدة في هذه الخارطة تنطبق على الجهات والشركات وتؤثّر عليها، فإنه من المقرّر الاتفاق على تنفيذها بالتنسيق مع هذه الجهات.

خارطة طريق الأمن السيبراني (Cybersecurity Roadmap)

١- تحديد خطة عمل لتحقيق أهداف استراتيجية الأمن السيبراني.

٢- تُوفّر الاستراتيجية العناصر الأساسية لخطّة العمل والمكوّنة من مبادرات الأمن السيبراني التي بدورها تُحقّق أهداف الأمن السيبراني في حال تنفيذها (الأهداف مذكورة بالتفصيل في قسم أهداف الأمن السيبراني).

٣- تُصاغ خطّة عمل الاستراتيجية وفقًا للسياسات والإجراءات التنظيمية لـ<اسم الجهة>، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

٤- تتضمّن خطّة عمل الاستراتيجية بنودًا خاصة بالمراقبة ومؤشرات قياس الأداء لتحديد مستوى النجاح، مما يُمكّن من تقديم الملاحظات إلى <رئيس الإدارة المعنية بالأمن السيبراني> واللجنة الإشرافية للأمن السيبراني، ويُتيح ذلك إدخال التعديلات على الخطّة وضمان تنفيذ مبادرات الأمن السيبراني بصورة صحيحة لتحقيق الأهداف.

٥- توضح خارطة طريق الأمن السيبراني طريقة توزيع المبادرات المقرّر تنفيذها على مدى الثلاث سنوات القادمة، إذ تُمنَح الأولوية لمبادرات الأمن السيبراني بناءً على التالي:

٥-١ نتائج تحليل المخاطر وتحليل تأثير الأعمال (BIA) المُوضّحة في قسم تقييم المخاطر وتحليل تأثير الأعمال، مع منح الأولوية للمخاطر العالية.

٥-٢ نتائج حصر الأنظمة الحسّاسة، مع منح الأولوية للمبادرات المتصلة بالأنظمة الحساسة.

خارطة طريق الأمن السيبراني

خارطة طريق الأمن السيبراني.xlsx

قائمة المبادرات والمشاريع

١- أعدّت <اسم الجهة> بيانات تفصيلية للمبادرات والمشاريع المستهدفة في استراتيجية الأمن السيبراني وفقًا لورقة العمل التالية:

بيانات مبادرات ومشاريع الأمن السيبراني

بيانات مبادرات ومشاريع الأمن السيبراني.xlsx

اختر التصنيف

الإصدار <١,٠>

ميزانية الأمن السيبراني (Cybersecurity Budget)

الغرض من ميزانية الأمن السيبراني هو تحديد الميزانية اللازمة لتنفيذ خطّة عمل الأمن السيبراني والمبادرات، والحصول على الاعتمادات اللازمة لتخصيصها من قبل <الإدارة المعنية بالشؤون المالية>.

خصائص الميزانية

١- <الإدارة المعنية بالأمن السيبراني> مسؤولة عن إعداد الميزانية الخاصة بالأمن السيبراني باعتبارها أفضل طريقة لضمان توفير التقنيات والأدوات المتعلقة بالأمن السيبراني، كما يتولّى <رئيس الإدارة المعنية بالأمن السيبراني> مسؤولية تقديم ملخّص لميزانية الأمن السيبراني إلى <صاحب الصلاحية>.

٢- يتم تخصيص ميزانية للأمن السيبراني لتغطي جميع تكاليف خطة عمل الأمن السيبراني، لذلك يجب أن تكون دقيقة ومنطقية وشاملة للمبالغ المتوقع صرفها.

٣- يجب أن تكون ميزانية الأمن السيبراني متوافقة مع السياسات والمتطلبات التشريعية والتنظيمية والأوامر والقرارات ذات العلاقة.

٤- تُحدّد ميزانية الأمن السيبراني بناءً على دورة الميزانية السنوية الخاصة ب<اسم الجهة>.

٥- تخضع ميزانية الأمن السيبراني إلى مراجعة دورية وفقًا للسياسات والإجراءات المعتمدة في <اسم الجهة>.

مكوّنات الميزانية

١- تشتمل ميزانية الأمن السيبراني على المكوّنات التالية:

١-١ ميزانية تشغيل الإدارة المعنية بالأمن السيبراني، وتشمل الآتي:

١-١-١ تكلفة الموارد البشرية.

١-١-٢ تكلفة الخدمات الاستشارية.

١-١-٣ تكلفة الخدمات التقنية.

١-١-٤ تكاليف أخرى.

١-٢ ميزانية مبادرات الأمن السيبراني، وتشمل الآتي:

١-٢-١ تكاليف غير متكرّرة لإنشاء الإدارة المعنية بالأمن السيبراني والعمليات ذات العلاقة لتنفيذ استراتيجية الأمن السيبراني.

١-٢-٢ تكاليف متكرّرة تغطي تدابير الأمن السيبراني (مثل: إدارة الأمن السيبراني، والمراقبة، وإعداد التقارير، والالتزام، وغيرها).

١-٢-٣ تكلفة برامج تطوير المهارات المتخصصة والتدريب اللازم لموظفي الأمن السيبراني مثل الدورات التدريبية والمؤتمرات.

١-٢-٤ تكلفة خدمات الإسناد الخارجي.

اختر التصنيف

الإصدار <١,٠>

حساب ميزانية الأمن السيبراني

١- تم حساب ميزانية الأمن السيبراني الخاصة ب<اسم الجهة> وفقًا لورقة العمل التالية:

حساب ميزانية الأمن السيبراني

٢- ميزانية الأمن السيبراني التي خصّصتها <اسم الجهة> لاستراتيجية الأمن السيبراني التي ستستمر للسنوات الثلاث القادمة هي: <تحدد من قبل الجهة> ريال سعودي.

طلب تقديم العروض (RFPs)

١- أعدّت <اسم الجهة> بيانات تفصيلية لطلب تقديم العروض لاستراتيجية وخارطة طريق الأمن السيبراني وفقًا لنماذج وزارة المالية ومركز تحقيق كفاءة الانفاق التالية على سبيل المثال (لا الحصر) يرجى الدخول على الروابط الموضحة ادناه:

نموذج كراسة (خدمات استشارية)

نموذج كراسة (خدمات تقنية معلومات)

غيرها
(مثل النماذج المقدمة من مركز تحقيق كفاءة الانفاق...الخ)

الأدوار والمسؤوليات

١. **مالك الوثيقة:** <رئيس الإدارة المعنية بالأمن السيبراني>.
٢. **تحديث الوثيقة ومراجعتها:** <الإدارة المعنية بالأمن السيبراني>.
٣. **تنفيذ الوثيقة وتطبيقها:** <الإدارة المعنية بالأمن السيبراني>.
٤. **قياس الالتزام بالوثيقة:** <الإدارة المعنية بالأمن السيبراني>.

اختر التصنيف

الإصدار <١,٠>

التحديث والمراجعة

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