هذا المربع مخصّص لأغراض توجيهية. احذف جميع المربعات التوجيهية بعد تعبئة النموذج. يجب تحرير البنود الملوّنة باللون الأزرق بصورة مناسبة. والبنود الملوّنة باللون الأخضر هي أمثلة يجب حذفها. ويجب إزالة التظليل الملون بعد إجراء التعديلات.

أدخل شعار الجهة بالضغط على الصورة الموضحة.

نموذج برنامج التوعية بالأمن 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

طُوّر هذا النموذج عن طريق الهيئة الوطنية للأمن السيبراني كمثال توضيحي يمكن استخدامه كدليل ومرجع للجهات. يجب 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>

قائمة المحتويات

اختر التصنيف

الإصدار <١,٠>

الغرض

تهدف هذه الوثيقة إلى تحديد متطلبات الأمن السيبراني لإنشاء ومتابعة وتحديث برنامج شامل للتوعية بالأمن السيبراني في إطار برنامج الأمن السيبراني لدى <اسم الجهة>. ويتم تقديم البرنامج في صورة نهج يشمل دورة حياته الكاملة، بدايةً من الإعداد والتنفيذ، مرورًا بمرحلة ما بعد التنفيذ ووصولاً إلى تقييم البرنامج. وتوضح هذه الوثيقة أيضًا كيفية إجراء ما يلي:

- اختيار مواضيع التوعية
- إعداد مواد التوعية
- تقييم فعالية البرنامج

تمت مواءمة متطلبات هذا البرنامج مع متطلبات الأمن السيبراني الصادرة عن الهيئة الوطنية للأمن السيبراني، وتشمل على سبيل المثال لا الحصر: الضوابط الأساسية للأمن السيبراني (ECC – 1: 2018) وغيرها من المتطلبات التشريعية والتنظيمية للأمن السيبراني ذات العلاقة.

نطاق العمل

يشمل نطاق هذه الوثيقة ما يتعين على <اسم الجهة> إجراؤه لتطوير برنامج التوعية بالأمن السيبراني وتنفيذه وتحديثه. ويهدف برنامج التوعية بالأمن السيبراني إلى تقديم المساعدة إلى العديد من الفئات الرئيسية المستهدفة في <اسم الجهة> وتوعيتها، بما في ذلك: الإدارة العليا والعاملين في إدارة تقنية المعلومات وجميع العاملين في <اسم الجهة> (الموظفين والمتعاقدين).

الأدوار والمسؤوليات التفصيلية

١- <رئيس الإدارة المعنية بالأمن السيبراني>

يتولى <رئيس الإدارة المعنية بالأمن السيبراني> الإشراف على العاملين في الجهة ذوي المسؤوليات المهمة المتعلقة بأمن المعلومات. ويجب على <رئيس الإدارة المعنية بالأمن السيبراني> التعاون مع <الإدارة المعنية بالتعلم والتطوير> في <اسم الجهة> من أجل:

- وضع الاستراتيجية العامة لبرنامج التوعية بالأمن السيبراني.
- ضمان فهم الإدارة العليا والعاملين في تقنية المعلومات وقيادة <اسم الجهة> لمفاهيم واستراتيجية برنامج التوعية بالأمن السيبراني، واطلاعهم على التقدم المحرز في تنفيذ البرنامج.
- ضمان توفير التمويل المطلوب لبرنامج التوعية بالأمن السيبراني لدى <اسم الجهة>.
- ضمان تدريب العاملين في <اسم الجهة> ذوي المسؤوليات الأمنية المهمة.
- ضمان تطبيق آليات فعالة للمتابعة وإعداد التقارير.
- تعيين مدير برنامج الأمن السيبراني المسؤول عن تنفيذ البرنامج.

٢- مدير برنامج الأمن السيبراني

يتولى مدير برنامج الأمن السيبراني مسؤوليات هامة في إطار برنامج التوعية؛ ويجب عليهم ما يلي:

- ضمان ارتباط مواد التوعية التي تم إعدادها وملاءمتها للتقنيات القائمة حاليًا وتقديمها في الوقت المناسب إلى الجمهور المستهدف.
- ضمان نشر مواد التوعية بفعالية حتى تصل إلى الجمهور المستهدف.
- ضمان توفير طريقة فعالة للمستخدمين المدراء لتقديم ملاحظاتهم بشأن مواد التوعية وطريقة عرضها.
- ضمان مراجعة مواد التوعية بشكل دوري وتحديثها عند الضرورة.
- المساعدة في وضع استراتيجية المتابعة وإعداد التقارير.

٣- الإدارة

يتحمل المدراء مسؤولية الالتزام بمتطلبات التوعية بالأمن السيبراني للعاملين في إداراتهم؛ ويجب عليهم ما يلي:

- التعاون مع <رئيس الإدارة المعنية بالأمن السيبراني> ومدير برنامج الأمن السيبراني للوفاء بالمسؤوليات المشتركة.
- القيام بدور مالك النظام و/أو مالك البيانات، حيثما ينطبق ذلك.
- دراسة وضع خطط تطوير فردية للمستخدمين المكلفين بأدوار ذات مسؤوليات أمنية مهمة.
- تعزيز التطوير المهني ومنح شهادات الاعتماد للعاملين في برنامج الأمن السيبراني وغيرهم من العاملين أصحاب المسؤوليات الأمنية المهمة.
- ضمان تدريب جميع المستخدمين والمتعاقدين المسؤولين عن إدارة أنظمة <اسم الجهة> والعمل عليها (أي أنظمة الدعم العام والتطبيقات الرئيسية) بالشكل المناسب على كيفية أداء مسؤولياتهم المتعلقة بالأمن السيبراني قبل السماح لهم بالوصول إلى الأنظمة.
- ضمان فهم المستخدمين والمتعاقدين للقواعد المحددة لكل نظام وتطبيق يستخدمونه.
- العمل على تقليل الأخطاء من جانب المستخدمين بسبب غياب الوعي و/أو التدريب.

٤- العاملون في الجهة

يعتبر المستخدمون أكبر فئة مستهدفة في أي جهة وأهم مجموعة يمكنها المساعدة في الحد من الاخطاء غير المقصودة والثغرات الأمنية في تقنيات المعلومات. وقد يشمل المستخدمون الموظفين والمتعاقدين والزوار والضيوف وغيرهم من الأشخاص ذوي العلاقة الذين يحتاجون إلى الوصول إلى الأصول التقنية لدى <اسم الجهة>. ويجب على المستخدمين:

- فهم السياسات والإجراءات الأمنية لدى <اسم الجهة> والالتزام بها.
- حضور التدريب لفهم قواعد سلوكيات التعامل مع الأنظمة والتطبيقات التي يمكنهم الوصول إليها.
- التعاون مع الإدارة لتلبية الاحتياجات التدريبية.
- الإلمام بالإجراءات التي يمكنهم اتخاذها لحماية معلومات <اسم الجهة> على نحو أفضل.

اختيار محتوى التوعية

١- العاملون في تقنية المعلومات:

يجب أن يشمل برنامج التوعية بالأمن السيبراني، على سبيل المثال لا الحصر، المواضيع التالية الموجهة للعاملين في تقنية المعلومات:

- إدارة الأصول
- النسخ الاحتياطي والاسترجاع
- التعافي من الكوارث
- التشفير
- التحصين
- إدارة الهويات وحقوق الوصول
- إدارة التحديثات والإصلاحات
- إدارة الحوادث الأمنية
- إدارة الثغرات الأمنية

٢- الإدارة العليا:

يجب أن يشمل برنامج التوعية بالأمن السيبراني، على سبيل المثال لا الحصر، المواضيع التالية الموجهة لأفراد الإدارة العليا:

- السياسات والمعايير
- مخاطر الأمن السيبراني، بالتركيز على:
  - المشهد العام للتهديدات وتوجهات الأمن السيبراني
  - الأثر المالي
- التدقيقات على الأنظمة والتطبيقات
- المتطلبات التشريعية والتنظيمية
- إدارة الحوادث الأمنية
- استمرارية الأعمال المؤسسية

٣- العاملون في الجهة:

يجب أن يشمل برنامج التوعية بالأمن السيبراني، على سبيل المثال لا الحصر، المواضيع التالية الموجهة للعاملين من الموظفين والمتعاقدين:

- السلامة الأمنية والأخطاء الشائعة
- سياسات الأمن السيبراني:
  - العمل عن بُعد
  - الاستخدام المقبول
  - الوسائط القابلة للإزالة
  - استخدام وسائل التواصل الاجتماعي
  - استخدام الإنترنت والبريد الإلكتروني

اختر التصنيف

الإصدار <١,٠>

- استخدام الأجهزة المحمولة
- هجمات الهندسة الاجتماعية
- حماية البيانات
- كلمات المرور والمصادقة
- الأمن في المنزل
- استخدام الشبكات اللاسلكية العامة

التنفيذ

يجب عدم تنفيذ برنامج التوعية بالأمن السيبراني إلّا بعد:

- وضع استراتيجية لتصميم وتنفيذ برنامج التوعية بالأمن السيبراني.
- الانتهاء من خطة برنامج التوعية المطلوبة لتنفيذ تلك الاستراتيجية.
- إعداد مواد التوعية.
- معالجة المتطلبات المالية أيضًا.

١. **تعميم الخطة**

يجب شرح كيفية تنفيذ البرنامج بشكل وافٍ للإدارة العليا في <اسم الجهة> حتى تقدم الدعم اللازم لتنفيذه وتضمن تخصيص الموارد المطلوبة. ويُقصد بذلك شرح أدوار ومسؤوليات الإدارة والعاملين في الجهة، وكذلك النتائج المتوقعة للبرنامج والفوائد التي ستعود على <اسم الجهة>.

٢. **توفير مواد التوعية**

يجب الإستفادة بشكل فعال من مواد التوعية التي توفر تقنيات تدعم الميزات التالية:

- سهولة الاستخدام (مثل، سهولة الوصول وسهولة التحديث/الصيانة)
- إمكانية التوسع (مثل، يمكن استخدام المواد مع مختلف فئات الجمهور المستهدف مع تنوع أحجامها ومواقعها)
- المساءلة (مثل، تسجيل الإحصائيات بشأن درجة الإنجاز والاستفادة منها)

ومن أكثر الأساليب شيوعًا التي يمكن استخدامها ما يلي:

- التدريب من خلال الفيديوهات التفاعلية
- التدريب عبر الإنترنت
- التدريب عبر جهاز المستخدم، دون الاعتماد على الإنترنت
- جلسات التوعية داخل الموقع بقيادة المدربين
- الملصقات والكتيبات
- شاشات التوقف وخلفيات سطح المكتب

يمكن أن يكون المزج بين الأساليب المختلفة للتوعية في جلسة واحدة من الطرق الفعالة لعرض المواد وجذب اهتمام الجمهور المستهدف.

اختر التصنيف

الإصدار <١,٠>

مرحلة ما بعد التنفيذ

يجب على <الإدارة المعنية بالأمن السيبراني> في <اسم الجهة> دمج الآليات ضمن استراتيجية الأمن السيبراني لضمان الملاءمة المستمرة لبرنامج التوعية بالأمن السيبراني وتوافقه مع الأهداف الكلية. وبالتالي، يجب أن يهتم البرنامج بالتطورات التقنية والتغيرات في البنية التحتية لتقنية المعلومات والتغيرات التنظيمية والتحولات في رسالة الجهة وأولوياتها. ويُعد التحسين المستمر ضروريًا لنجاح برنامج التوعية بالأمن السيبراني.

١. **التقييم والملاحظات**

تعتبر الآليات الرسمية للتقييم وتقديم الملاحظات من العناصر الحيوية في أي برنامج للتوعية والتدريب والتثقيف الأمني. ولا يمكن أن يتم التحسين المستمر دون فهم جيد لأداء البرنامج الحالي. بالإضافة إلى ذلك، يجب تصميم آلية لتقديم الملاحظات من أجل تحقيق الأهداف المحددة من البداية للبرنامج.

يجب إجراء تقييم من أجل تحديد مستوى نضج التوعية والتدريب على الأمن السيبراني في <اسم الجهة>. ولتحقيق ذلك، يمكن ل<اسم الجهة> استخدام نموذج استبيان تقييم الوعي بالأمن السيبراني (الملحق "أ" من هذه الوثيقة).

ويجب أن تشمل استراتيجية تقديم الملاحظات العناصر التالية:

- الجودة
- نطاق العمل
- طريقة النشر (مثل النشر عبر الإنترنت أو داخل الموقع أو خارجه)
- مستوى الصعوبة
- سهولة الاستخدام، ومدة الجلسة
- الصلة
- اقتراحات التعديل

يجب على <اسم الجهة> أيضًا إجراء اختبار دوري للتحقق من فعالية برنامج التوعية بالأمن السيبراني (أي، محاكاة الهجمات، ومكافحة التصيّد الاحتيالي، وغير ذلك)

٢. **عوامل نجاح البرنامج**

من الضروري أن تكون لدى الجميع القدرة والاستعداد لتنفيذ أدوارهم المتعلقة بالأمن السيبراني في <اسم الجهة>. وفيما يلي بعض المؤشرات الرئيسية التي يمكن استخدامها لقياس مستوى دعم البرنامج والقبول به.

- توفير التمويل الكافي لتنفيذ الاستراتيجية المتفق عليها.
- تحديد الأدوار والمسؤوليات بوضوح لتنفيذ الاستراتيجية بفعالية.
- تقديم الدعم من الإدارة التنفيذية/الإدارة العليا.
- استخدام المقاييس.
- مستوى الحضور في جلسات التدريب الإلزامية على الأمن السيبراني.

الملحق "أ"

استبيان تقييم الوعي بالأمن السيبراني

بناء الوعي بالأمن السيبراني	
المبادرات	
1	هل أدركت <اسم الجهة> الحاجة إلى التوعية بتهديدات وثغرات الأمن السيبراني؟
الإجابة	الملاحظات
2	هل الوعي بتهديدات وثغرات الأمن السيبراني يكون في المراحل الأولية فقط من المناقشة في <اسم الجهة>؟
الإجابة	الملاحظات
3	هل وضعت <اسم الجهة> في الاعتبار إشراك الأطراف المعنية ذات العلاقة عند تطوير برنامج التوعية بالأمن السيبراني؟
الإجابة	الملاحظات
4	هل تتوفر الموارد الكافية لد <اسم الجهة> لتنفيذ برنامج التوعية بالأمن السيبراني؟
الإجابة	الملاحظات

5	هل توجد لدى <اسم الجهة> خطة تنفيذ تفصيلية منشورة لبرنامج التوعية بالأمن السيبراني؟
الإجابة	الملاحظات
6	هل طوّرت <اسم الجهة> برنامجًا للتوعية بالأمن السيبراني؟
الإجابة	الملاحظات
7	هل تم التنسيق المشترك لبرنامج التوعية بالأمن السيبراني على مستوى <اسم الجهة>؟
الإجابة	الملاحظات
8	هل توجد منظومة من الآليات والمقاييس مطبقة من البداية لمراجعة برنامج التوعية بالأمن السيبراني في <اسم الجهة>؟
الإجابة	الملاحظات
9	هل يتمتع الموظفون المكلفون بالسلطات والموارد الكافية لتنفيذ إجراءات برنامج التوعية بالأمن السيبراني في <اسم الجهة>؟
الإجابة	الملاحظات
10	هل توجد لدى <اسم الجهة> بوابة للتوعية بالأمن السيبراني من أجل تحسين المهارات والمعارف في مجال الأمن السيبراني؟

اختر التصنيف

الإصدار <١,٠>

الإجابة	الملاحظات
11	هل تشارك <اسم الجهة> في البرامج والدورات والندوات والموارد الإلكترونية للأطراف الأخرى من أجل التوعية بالأمن السيبراني؟
الإجابة	الملاحظات
12	هل توجد لدى <اسم الجهة> عمليات لمراجعة برنامج التوعية بالأمن السيبراني ومقاييس لتقييمه تستند إلى النتائج؟
الإجابة	الملاحظات
رفع مستوى وعي الإدارة التنفيذية	
13	هل توجد لدى <اسم الجهة> برامج لتوعية المدراء التنفيذيين بمسائل الأمن السيبراني؟
الإجابة	الملاحظات
14	هل المدراء التنفيذيون على دراية بمسؤولياتهم تجاه الأطراف المعنية والعملاء والموظفين فيما يتعلق بالأمن السيبراني لدى <اسم الجهة>؟
الإجابة	الملاحظات

15	هل تم إطلاع المدراء التنفيذيين على مسائل الأمن السيبراني العامة التي قد تؤثر على <اسم الجهة>؟
الإجابة	الملاحظات
16	هل المدراء التنفيذيون على دراية بالآثار المحتملة لتلك المسائل والتهديدات على <اسم الجهة>؟
الإجابة	الملاحظات
17	هل تم إطلاع المدراء التنفيذيين بإدارات معينة في <اسم الجهة> (مثل إدارة الشؤون المالية وإدارة الاتصالات) على مخاطر الأمن السيبراني بوجه عام وكيفية تعامل الجهة مع مسائل الأمن السيبراني؟
الإجابة	الملاحظات
18	هل تم إطلاع المدراء التنفيذيين بإدارات معينة في <اسم الجهة> (مثل إدارة الشؤون المالية وإدارة الاتصالات) على التداعيات الاستراتيجية لمخاطر الأمن السيبراني؟
الإجابة	الملاحظات
19	هل يتناول برنامج التوعية بالأمن السيبراني الموجه للمديرين التنفيذيين في <اسم الجهة> مخاطر الأمن السيبراني بوجه عام (مثل، طرق الهجوم الأساسية وكيفية تعامل الجهة مع مسائل الأمن السيبراني)؟
الإجابة	الملاحظات

اختر التصنيف

الإصدار <١,٠>

سياسة التوعية والتدريب	
المبادرات	
20	هل يوجد مدربون على الأمن السيبراني في <اسم الجهة>؟
الإجابة	الملاحظات
21	هل توجد برامج لتأهيل المدربين في <اسم الجهة>؟
الإجابة	الملاحظات
22	هل يتم تقديم دورات لعلوم الحاسب الآلي تشتمل على وحدة عن الأمن في <اسم الجهة>؟
الإجابة	الملاحظات
23	هل يتم تقديم دورات تدريبية متعلقة بالأمن السيبراني للموظفين في <اسم الجهة>؟
الإجابة	الملاحظات
24	هل يستكشف المدربون المؤهلون الحاليون في <اسم الجهة> برامج تأهيل المدربين في مجال الأمن السيبراني؟
الإجابة	الملاحظات

25	هل تُقدم أي دورات تدريبية من أطراف خارجية في المجالات المتعلقة بالأمن السيبراني (مثل، أمن المعلومات وأمن الشبكات والتشفير) في <اسم الجهة>؟
الإجابة	الملاحظات
سياسة التوعية والتدريب	
المبادرات	
26	هل تُقدم أي برامج تدريبية في مجال الأمن السيبراني في <اسم الجهة>؟
الإجابة	الملاحظات
27	هل يتم تقديم التدريب على المسائل المتعلقة بالأمن السيبراني للعاملين في تقنية المعلومات بوجه عام في <اسم الجهة> بحيث يمكنهم الاستجابة للحوادث عند حدوثها؟
الإجابة	الملاحظات
28	هل يتم تقديم التدريب على المسائل المتعلقة بالأمن السيبراني للمتخصصين الأمنيين في <اسم الجهة> بحيث يمكنهم الاستجابة للحوادث عند حدوثها؟
الإجابة	الملاحظات

29	هل تقدم <اسم الجهة> أي شهادات مهنية متعلقة بالأمن السيبراني لموظفيها؟
الإجابة	الملاحظات
30	هل برامج التدريب على الأمن السيبراني لدى <اسم الجهة> منظمة؟
الإجابة	الملاحظات
31	هل تمت مراعاة أيّ من الأطر الوطنية أو الدولية للأمن السيبراني وأفضل الممارسات الدولية المعمول بها عند تصميم دورات التدريب المهني؟
الإجابة	الملاحظات
32	هل يوجد فهم جيد للاحتياجات المتعلقة بالأمن السيبراني لدى <اسم الجهة> (مثل، هل تم توثيق قائمة بمتطلبات التدريب)؟
الإجابة	الملاحظات
33	هل يتم الاعتراف ببرامج التدريب على الأمن السيبراني وتقديمها للموظفين بوجه عام؟
الإجابة	الملاحظات
نقل المعرفة	

اختر التصنيف

الإصدار <١,٠>

34	هل يتم نقل المعرفة بالأمن السيبراني من الموظفين المُدرَّبين إلى الموظفين غير المُدرَّبين في <اسم الجهة> ؟
الإجابة	الملاحظات

الأدوار والمسؤوليات

١- **مالك الوثيقة:** <رئيس الإدارة المعنية بالأمن السيبراني>.

٢- **مراجعة الوثيقة وتحديثها:** <الإدارة المعنية بالأمن السيبراني>.

٣- **تنفيذ الوثيقة وتطبيقها:** <الإدارة المعنية بتقنية المعلومات>.

٤- **قياس الالتزام بالوثيقة:** <الإدارة المعنية بالأمن السيبراني>.

التحديث والمراجعة

يجب على <الإدارة المعنية بالأمن السيبراني> مراجعة البرنامج 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

١- يجب على <رئيس الإدارة المعنية بالأمن السيبراني> التأكد من التزام <اسم الجهة> بهذا البرنامج دوريًا.

٢- يجب على كافة العاملين في <اسم الجهة> الالتزام بهذا البرنامج.

٣- قد يعرض أي انتهاك لهذا البرنامج صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في <اسم الجهة>.

اختر التصنيف

الإصدار <١,٠>