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 قائمة التحقق من متطلبات الأمن السيبراني لمشاريع تقنية المعلومات وإدارة التغيير

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.

اختر التصنيف

الإصدار <١,٠>

.

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 (الهيئة الوطنية للأمن السيبراني) 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 <١,٠>

قائمة المحتويات

الغرض..... ٤
نطاق العمل ٤
الإجراءات المطلوبة..... ٤
الأدوار والمسؤوليات..... ١٠
التحديث والمراجعة..... ١٠
الالتزام بقائمة التحقق..... ١٠

الغرض

تحدد هذه القائمة الحد الأدنى من متطلبات الأمن السيبراني المتعلقة بمشاريع تقنية المعلومات وإدارة التغيير في <اسم الجهة>. حيث أن قدرة <اسم الجهة> على تنفيذ المتطلبات وفقًا لهذه القائمة يساعد في التخفيف من حدة مخاطر الأمن السيبراني في مشاريع تقنية المعلومات وإدارة التغيير وفي الحفاظ على توافر وسلامة وسرية أصول ومعلومات <اسم الجهة>.

تمت مواءمة هذه القائمة مع متطلبات الأمن السيبراني الصادرة عن الهيئة الوطنية للأمن السيبراني بما في ذلك على سبيل المثال لا الحصر الضوابط الأساسية للأمن السيبراني (ECC – ١: ٢٠١٨)، بالإضافة إلى المتطلبات التشريعية والتنظيمية للأمن السيبراني ذات العلاقة.

نطاق العمل

تغطي قائمة التحقق متطلبات الأمن السيبراني المتعلقة بمشاريع تقنية المعلومات وإدارة التغيير لدى <اسم الجهة> وتنطبق على جميع العاملين (الموظفين والمتعاقدين) في <اسم الجهة>.

الإجراءات المطلوبة

يجب تعبئة الجدول التالي من قبل مدير المشروع لدى <اسم الجهة> لتوثيق تنفيذ ضوابط الأمن السيبراني في مشاريع تقنية المعلومات أو إدارة التغيير.

قائمة التحقق من متطلبات الأمن السيبراني لمشاريع تقنية المعلومات وإدارة التغيير										
				نوع التغيير						
الرقم	اسم النشاط	الوصف	إلزامي	المرحلة	تغيير مقرر	المشروع	تغيير في حالات الطوارئ	الحالة	الموعد النهائي للتنفيذ	ملاحظات	الدليل
١	إدارة تحديد الجهات المعنية	تعيين الجهات المعنية ذات العلاقة وإشراكها في المشروع/ التغيير بما في ذلك على سبيل المثال لا الحصر أعضاء الفريق المسؤولين عمّا يلي: • الإشراف الإداري على هذا المشروع • إدارة المشروع • المسائل المتعلقة بالأمن السيبراني في هذا المشروع • الحلول المتأثرة بهذا المشروع • إدارة المخاطر • تنفيذ التغيير	نعم	تحديد الجهات المعنيّة	x	x		اختر حالة.	اختر التاريخ.		

اختر التصنيف

الإصدار <١,٠>

٢	الاحتفاظ بالوثائق	حفظ جميع الوثائق والاتصالات المتعلقة بالمشروع/ التغيير في موقع يمكن الوصول إليه من قبل الموظفين المخولين فقط، ويتم أرشفة جميع البيانات بما يتوافق مع سياسة الاحتفاظ بالبيانات.	نعم	البدء	X	X	X	اختر حالة.	اختر التاريخ.		
٣	تصنيف التغيير	تصنيف التغيير كتغيير مقرر، أو مشروع تقنية المعلومات، أو التغيير في حالات الطوارئ.	نعم	البدء	X	X	X	اختر حالة.	اختر التاريخ.		
٤	تقييم الأثر	تقييم أثر التغيير، إذ يجب أن تكون النتائج هي الدافع لاتخاذ قرار بشأن التنفيذ وتحديد ضوابط الأمن السيبراني ليتم تنفيذها.	نعم	البدء	X	X	X	اختر حالة.	اختر التاريخ.		
٥	تقييم الموردين	إذا تم إشراك مورد خارجي في تنفيذ المشروع، عندئذ يتم تقييمه بما يتوافق مع الإجراءات الداخلية، بما في ذلك على سبيل المثال لا الحصر تقييم مخاطر الأمن السيبراني الخارجية للتحقق من معلومات الأمني.	نعم	البدء		X		اختر حالة.	اختر التاريخ.		

اختر التصنيف

٦	تحليل نمذجة التهديدات	إجراء نمذجة التهديدات في المشروع، مما يتيح تحديد المخاطر والمتطلبات المناسبة.	نعم	البدء		X		اختر حالة.	اختر التاريخ.		
٧	الالتزام التنظيمي/ الداخلي	إجراء تقييم للمتطلبات الخارجية (التشريعية والتنظيمية) والداخلية ومراعاة المتطلبات المستنبطة في تصميم ضوابط الأمن السيبراني.	نعم	البدء		X		اختر حالة.	اختر التاريخ.		
٨	تحديد مخاطر المشروع	إجراء تقييم لمخاطر الأمن السيبراني للمشروع/ التغيير بما يتوافق مع معيار إدارة مخاطر الأمن السيبراني لتحديد الأثر المحتمل على الأعمال في حالة حدوث المخاطر.	نعم	البدء		X		اختر حالة.	اختر التاريخ.		
٩	تحديد المتطلبات الأمنية	تحديد متطلبات الأمن السيبراني، المستخرجة من المتطلبات الوظيفية والأنشطة السابقة (تحليل نمذجة التهديدات، والالتزام التنظيمي/ الداخلي، وتحديد مخاطر التطبيقات).	نعم	البدء	X	X		اختر حالة.	اختر التاريخ.		

١٠	تطوير البرمجيات	في حالة إجراء تطوير برمجيات مخصصة، يتم إعداد "قائمة التحقق من الأمن السيبراني لتطوير البرمجيات" واتباعها.	نعم	التنفيذ		X		اختر حالة.	اختر التاريخ.		
١١	إدارة الأصول	تهيئة جميع المكونات المطورة حديثًا من خلال أداة إدارة الأصول وتم تتبعها لأي تغييرات.	نعم	التنفيذ	X	X		اختر حالة.	اختر التاريخ.		
١٢	الاختبار	اختبار التغيير قبل التنفيذ في بيئة الإنتاج. تضمنت حالات الاختبار تقييمًا لوجود ثغرات متعلقة بالأمن السيبراني. وتم تصميم نطاق العمل وفقًا لمدى التغيير، وتضمن على الأقل فحص الثغرات.	نعم	الإصدار	X	X	X	اختر حالة.	اختر التاريخ.		
١٣	المحاكاة	يتم في بيئة الاختبار محاكاة بيئة الإنتاج إلى أقصى حد ممكن، وتمت مراعاة جميع الفروقات والموافقة عليها.	نعم	الإصدار	X	X	X	اختر حالة.	اختر التاريخ.		

١٤	الموافقة على الإصدار	قيام جميع الجهات المعنية بالموافقة على التغيير قبل طرحه للإنتاج، مؤكدين أنه تم توفير جميع المتطلبات الأساسية، بما في ذلك الاختبار الناجح، ومعالجة المخاطر المحددة.	نعم	الإصدار	X	X		اختر حالة.	اختر التاريخ.		
١٥	الموافقة على التغيير النهائي	قيام جميع الجهات المعنية بالموافقة على التغيير بعد طرحه للإنتاج، مؤكدين على تنفيذ التغيير بنجاح في الإنتاج وتلبية جميع المتطلبات.	نعم	الإصدار	X	X		اختر حالة.	اختر التاريخ.		
١٦	مراقبة تنفيذ التغيير	متابعة إتمام التغيير والتشاور مع الجهات المعنية بشكل منتظم بعد التنفيذ وتم حفظ أدلة التشاور للرجوع إليها مستقبلًا.	نعم	العمليات	X	X	X	اختر حالة.	اختر التاريخ.		
١٧	إعادة تقييم التغيير في حالات الطوارئ	إعادة تقييم التغيير في حالات الطوارئ كتغيير أو مشروع خلال أسرع وقت ممكن، وتمت تلبية المتطلبات الإضافية.	نعم	الإصدار			X	اختر حالة.	اختر التاريخ.		

اختر التصنيف

الإصدار <١,٠>

الأدوار والمسؤوليات

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

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

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

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

التحديث والمراجعة

يجب على <الإدارة المعنية بالأمن السيبراني> مراجعة قائمة التحقق 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 بقائمة التحقق

١- يجب على <رئيس الإدارة المعنية بالأمن السيبراني> التأكد من التزام <اسم الجهة> بقائمة التحقق هذه دوريًا.

٢- يجب على كافة العاملين في <اسم الجهة> الالتزام بقائمة التحقق هذه.

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