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 إدارة حزم التحديثات والإصلاحات

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 "<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.

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	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 تاريخ

قائمة المحتويات

الغرض

تهدف هذه السياسة إلى تحديد متطلبات الأمن السيبراني المتعلقة بإدارة حزم التحديثات والإصلاحات للأنظمة والتطبيقات وقواعد البيانات وأجهزة الشبكة وأجهزة معالجة المعلومات الخاصة ب<اسم الجهة> لتقليل المخاطر السيبرانية وحمايتها من التهديدات الداخلية والخارجية في <اسم الجهة>. هذه المتطلبات تمت موائمتها مع متطلبات الأمن السيبراني الصادرة من الهيئة الوطنية للأمن السيبراني ويشمل ذلك على سبيل المثال لا الحصر: الضوابط الأساسية للأمن السيبراني (ECC – ١: ٢٠١٨)، ضوابط الأمن السيبراني للأنظمة الحساسة (CSCC – ١: ٢٠١٩) وغيرها من المتطلبات التشريعية والتنظيمية ذات العلاقة.

نطاق العمل

تطبق هذه السياسة على جميع الأصول التقنية الخاصة ب<اسم الجهة> بما فيها جميع المكونات التقنية للأنظمة التقنية السحابية (CTS) والأنظمة الحساسة والأنظمة التشغيلية وأنظمة العمل عن بعد والأصول التقنية الخاصة بحسابات التواصل الاجتماعي، وعلى <الإدارة المعنية بالأمن السيبراني> و<الإدارة المعنية بتقنية المعلومات> في <اسم الجهة>.

بنود السياسة

١- البنود العامة

١-١ يجب إدارة حزم التحديثات والإصلاحات (Patch Management) بشكل يضمن حماية الأنظمة والتطبيقات وقواعد البيانات وأجهزة الشبكة وأجهزة معالجة المعلومات الخاصة ب<اسم الجهة> بما فيها جميع المكونات التقنية للأنظمة التقنية السحابية (CTS) والأنظمة الحساسة والأنظمة التشغيلية وأنظمة العمل عن بعد والأصول التقنية الخاصة بحسابات التواصل الاجتماعي.

١-٢ يجب تنزيل حزم التحديثات والإصلاحات من مصادر مرخصة وموثوقة وفقًا للإجراءات المتبعة داخل <اسم الجهة>.

١-٣ يجب استخدام أساليب وأدوات موثوقة وآمنة لإجراء مسح دوري للكشف عن الثغرات وحزم التحديثات ومتابعة تطبيقها.

١-٤ يجب اختبار حزم التحديثات والإصلاحات في البيئة الاختبارية (Test Environment) قبل تثبيتها على الأنظمة والتطبيقات وأجهزة معالجة المعلومات في بيئة الإنتاج (Production Environment)، للتأكد من توافق حزم التحديثات والإصلاحات مع الأنظمة والتطبيقات.

١-٥ يجب وضع خطة للاسترجاع (Rollback Plan) وتطبيقها في حال تأثير حزم التحديثات والإصلاحات سلبًا على أداء الأنظمة أو التطبيقات أو الخدمات.

١-٦ يجب منح الأولوية لحزم التحديثات والإصلاحات التي تعالج الثغرات الأمنية حسب مستوى المخاطر المرتبطة بها.

١-٧ يجب جدولة التحديثات والإصلاحات بما يتماشى مع مراحل الإصدارات البرمجية التي يطرحها المورد.

١-٨ يجب تطبيق التحديثات والإصلاحات على الأصول التقنية على النحو التالي على الأقل:

اختر التصنيف

نوع الأصل	الأنظمة					
	جميع الأنظمة	الأنظمة الحساسة المتصلة بالإنترنت	الأنظمة الحساسة الداخلية	أنظمة العمل عن بعد	أنظمة حسابات التواصل الاجتماعي	أنظمة خدمات الحوسبة السحابية
	معدل تكرار تطبيق التحديثات					
أنظمة التشغيل	شهريًا	شهريًا	شهريًا	شهريًا	شهريًا	شهريًا
قواعد البيانات	ثلاثة أشهر	شهريًا	ثلاثة أشهر	شهريًا	شهريًا	ثلاثة أشهر
أجهزة الشبكة	ثلاثة أشهر	شهريًا	ثلاثة أشهر	شهريًا	شهريًا	ثلاثة أشهر
التطبيقات	ثلاثة أشهر	شهريًا	ثلاثة أشهر	شهريًا	شهريًا	ثلاثة أشهر

١-٩ يجب منع المستخدمين من تعطيل تقنيات حزم التحديثات والإصلاحات أو التأثير عليها بشكل سلبي.

١-١٠ يجب أن تتبع عملية إدارة التحديثات والإصلاحات متطلّبات عملية إدارة التغيير المعتمدة لدى <اسم الجهة>.

١-١١ يجب تطوير واعتماد عملية إدارة التغيير الطارئة (Emergency Change Management) وتطبيق حزم التحديثات والإصلاحات الطارئة وفقًا لها في حال وجود ثغرات أمنية ذات مخاطر عالية.

١-١٢ يجب تنزيل التحديثات والإصلاحات على خادم مركزي (Centralized Patch Management Server) قبل تطبيقها على الأنظمة والتطبيقات وقواعد البيانات وأجهزة الشبكة وأجهزة معالجة المعلومات، ويُستثنى من ذلك حزم التحديثات والإصلاحات التي لا يتوفر لها أدوات آلية مدعومة.

١-١٣ بعد الانتهاء من تطبيق حزم التحديثات والإصلاحات، يجب استخدام أدوات مستقلة وموثوقة للتأكد من أن الثغرات تمت معالجتها بشكل فعّال.

١-١٤ يجب تطوير إجراءات ومعايير خاصة بإدارة حزم التحديثات والإصلاحات بناءً على حاجة العمل.

١-١٥ يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر والاستخدام الصحيح والفعال لمتطلبات إدارة حزم التحديثات والإصلاحات.

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 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

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

٢- يجب على <الإدارة المعنية بالأمن السيبراني> و<الإدارة المعنية بتقنية المعلومات> في <اسم الجهة> الالتزام بهذه السياسة.

٣- قد يعرض أي انتهاك لهذه السياسة صاحب المخالفة، إلى إجراء تأديبي؛ حسب الإجراءات المتبعة في <اسم الجهة>.