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 الثغرات

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.

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	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

اختر التصنيف

الإصدار <١,٠>

قائمة المحتويات

اختر التصنيف

الإصدار <١,٠>

الغرض

تهدف هذه السياسة إلى تحديد متطلبات الأمن السيبراني المتعلقة بضمان اكتشاف الثغرات التقنية في الوقت المناسب ومعالجتها بشكل فعال؛ وذلك لمنع احتمالية استغلال هذه الثغرات من قبل الهجمات السيبرانية أو تقليلها، وكذلك التقليل من الآثار المترتبة على أعمال <اسم الجهة> 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 المعلوماتية والتقنية في <اسم الجهة>، وعلى جميع العاملين (الموظفين والمتعاقدين) في <اسم الجهة>.

بنود السياسة

١- البنود العامة

١-١ يجب فحص وتقييم الثغرات دوريًا من قبل فريق مختص ومؤهل لاكتشاف وتقييم الثغرات التقنية في الوقت المناسب ومعالجتها بشكل فعّال وفقًا للمتطلبات التشريعية والتنظيمية ذات العلاقة على النحو التالي على الأقل:

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 فحص وتقييم الثغرات					
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

اختر التصنيف

الإصدار <١,٠>

* يكون فحص الثغرات شهريًا بينما يكون تقييم الثغرات كل ثلاثة أشهر.

١-٢ يجب تحديد الأنظمة والخدمات والمكونات التقنية التي يجب إجراء فحص الثغرات عليها وذلك وفقًا للمتطلبات التشريعية والتنظيمية ذات العلاقة.

١-٣ يجب استخدام أساليب وأدوات موثوقة ومعتمدة لاكتشاف الثغرات.

١-٤ يجب القيام بفحص واكتشاف الثغرات قبل إطلاق الخدمات أو الأنظمة على الإنترنت أو عند القيام بأي تغيير على البنية التحتية أو الأنظمة وفقًا لسياسة الأمن السيبراني ضمن إدارة المشاريع المعلوماتية والتقنية المعتمدة لدى <اسم الجهة>.

١-٥ يجب تصنيف الثغرات حسب خطورتها، ومعالجتها حسب المخاطر السيبرانية المترتبة عليها وفقًا لمنهجية إدارة المخاطر المعتمدة لدى <اسم الجهة>.

١-٦ في حال تفويض طرف خارجي للقيام بفحص واكتشاف الثغرات نيابة عن <اسم الجهة>، يجب التحقق من تطبيق جميع متطلبات الأمن السيبراني المتعلقة بالأطراف الخارجية وذلك وفقًا لسياسة الأمن السيبراني المتعلّق بالأطراف الخارجية المعتمدة لدى <اسم الجهة> ووفقًا للمتطلبات التشريعية والتنظيمية ذات العلاقة.

١-٧ يجب التواصل والاشتراك مع مصادر أمن سيبراني موثوقة توفر المعلومات الاستباقية (Threat Intelligence)، ومجموعات خاصة ذات اهتمامات مشتركة وخبراء خارجيين في المواضيع المعنية من أجل جمع المعلومات حول التهديدات الجديدة وكيفية الحد من الثغرات المحتملة بالاشتراك مع الهيئة عبر منصة حصين مع ضرورة الحصول على الموافقة من الهيئة الوطنية للأمن السيبراني عند الاشتراك مع المزودين الاخرين .

١-٨ يجب تطوير عمليات لتلقي وتحليل ومعالجة الثغرات التي تم الكشف عنها ل<اسم الجهة> من مصادر داخلية أو خارجية في حال الاشتراك مع مزودي الخدمة لتلقي الاخبار عن أحدث الثغرات.

١-٩ يجب معالجة جميع الثغرات حسب خطورتها وتصنيفها وفقًا لإطار إدارة مخاطر الأمن السيبراني المعتمدة في <اسم الجهة>.

١-١٠ يجب تطوير خطة لإدارة الثغرات الأمنية في <اسم الجهة> على أن يتبعها فريق تقييم الثغرات الداخلي أو الخارجي.

١-١١ يجب تحديد آلية لمعالجة الثغرات بشكل فعّال ومنع أو تقليل احتمالية استغلال هذه الثغرات، وتقليل الآثار الناتجة عن هذه الهجمات على سير الأعمال.

١-١٢ يجب الاحتفاظ بسجلات تقييم الثغرات والتحديثات والتغييرات المرتبطة بها.

١-١٣ يجب تطوير إجراءات ومعايير خاصة بتنفيذ فحص وتقييم الثغرات بناءً على حاجة العمل.

١-١٤ يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر والاستخدام الصحيح والفعال لمتطلبات إدارة الثغرات.

٢- متطلبات معالجة الثغرات

٢-١ بعد الانتهاء من تقييم الثغرات، يجب إعداد تقرير يوضح الثغرات المكتشفة وتصنيفها والتوصيات المقترحة لمعالجتها.

٢-٢ بعد إرسال تقرير تقييم الثغرات ومعالجتها من قبل الأطراف المعنية، يجب إجراء فحص واكتشاف الثغرات المكتشفة مرة أخرى للتأكد من معالجتها.

٢-٣ يجب استخدام حزم التحديثات والإصلاحات من مصادر موثوقة وآمنة ووفقًا لسياسة حزم التحديثات والإصلاحات.

٢-٤ يجب إصلاح وإغلاق الثغرات الحرجة (Critical Vulnerabilities) المكتشفة حديثًا، مع اتباع آليات إدارة التغيير المتبعة لدى <اسم الجهة>.

٢-٥ يجب إدارة الثغرات التي يقوم مقدم خدمات الحوسبة السحابية بالتبليغ عنها ومعالجتها.

٢-٦ يجب وضع خطة للاسترجاع (Rollback Plan) وتطبيقها في حال تأثير حزم التحديثات والإصلاحات سلبًا على أداء الأنظمة أو التطبيقات أو الخدمات.

٢-٧ في حال تعذر إصلاح وإغلاق الثغرة الأمنية لأي سببٍ كان، يجب تطبيق ضوابط أخرى مثل إيقاف تشغيل الخدمة المتعلقة بالثغرة الأمنية، أو توفير ضابط حماية بديل (Compensating Control) مثل التحكم بالوصول عن طريق جدران الحماية وغيرها من الحلول، ومراقبة الثغرة الأمنية للهجمات الفعلية، وإبلاغ فريق الاستجابة للحوادث بهذه الثغرة واحتمالية استغلالها.

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 جميع العاملين في <اسم الجهة> الالتزام بهذه السياسة.

اختر التصنيف

الإصدار <١,٠>

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