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

استبدل <اسم الجهة> باسم الجهة في مجمل صفحات الوثيقة. وللقيام بذلك، اتبع الخطوات التالية:

1. اضغط على مفتاحي "Ctrl" و"H" في الوقت نفسه.
2. أضف "<اسم الجهة>" في مربع البحث عن النص.
3. أدخل الاسم الكامل لجهتك في مربع "استبدال" النص.
4. اضغط على "المزيد" وتأكّد من اختيار "Match case".
5. اضغط على "استبدل الكل".
6. أغلق مربع الحوار.

اختر التصنيف

التاريخ: اضغط هنا لإضافة نص

الإصدار: اضغط هنا لإضافة نص

المرجع: اضغط هنا لإضافة نص

اعتماد الوثيقة

الدور	الاسم	التاريخ	التوقيع
اختر الدور	<أدخل الاسم الكامل للشخص>	اضغط هنا لإضافة نص	<أدخل التوقيع>

نسخ الوثيقة

النسخة	التاريخ	عُدلَ بواسطة	أسباب التعديل
<أدخل رقم النسخة>	اضغط هنا لإضافة نص	<أدخل الاسم الكامل للشخص>	<أدخل وصف التعديل>

اختر التصنيف

الإصدار 1.0

قائمة المحتويات

الأهداف

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير لضمان 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 من خلال التركيز على الأهداف الأساسية للحماية وهي: سرية المعلومات، وسلامتها، وتوافرها.

وتهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم ٢-١٠-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع الأصول المعلوماتية والتقنية في <اسم الجهة>، وتنطبق هذه السياسة على جميع العاملين في <اسم الجهة>.

بنود السياسة

1- المتطلبات العامة

1-1 يجب على <اسم الجهة> إجراء فحص الثغرات (Vulnerabilities Assessment) دورياً، لاكتشاف وتقييم الثغرات التقنية في الوقت المناسب ومعالجتها بشكل فعال.

2-1 تحدد <الإدارة المعنية بالأمن السيبراني> الأنظمة والخدمات والمكونات التقنية التي يجب إجراء فحص الثغرات عليها وذلك وفقاً للمتطلبات التشريعية والتنظيمية ذات العلاقة.

3-1 يجب على <الإدارة المعنية بالأمن السيبراني> التأكد من استخدام أساليب وأدوات موثوقة لاكتشاف الثغرات.

4-1 يجب تطوير واعتماد إجراءات خاصة بتنفيذ فحص واكتشاف الثغرات وفقاً للمتطلبات التشريعية والتنظيمية ذات العلاقة.

5-1 في حال تفويض طرف خارجي للقيام بفحص واكتشاف الثغرات نيابة عن <اسم الجهة>، يجب التحقق من تطبيق جميع متطلبات الأمن السيبراني المتعلقة بالأطراف الخارجية وفقاً لسياسة الأمن السيبراني المتعلّق بالأطراف الخارجية المعتمدة في <اسم الجهة>.

2- متطلبات تقييم الثغرات

2-1 يجب فحص واكتشاف الثغرات قبل نشر الخدمات أو الأنظمة على الإنترنت أو عند القيام بأي تغيير على الأنظمة الحساسة وفقاً لسياسة الأمن السيبراني ضمن إدارة المشاريع المعلوماتية والتقنية.

2-2 يجب تصنيف الثغرات حسب خطورتها، ومعالجتها حسب المخاطر السيبرانية المترتبة عليها وفقاً لمنهجية إدارة المخاطر المعتمدة لدى <اسم الجهة>.

اختر التصنيف

الإصدار 1.0

2-3 يجب على <اسم الجهة> إجراء تقييم الثغرات لجميع الأصول التقنية ومعالجتها دورياً. (ECC-2-10-3-1)

2-4 يجب على <اسم الجهة> إجراء تقييم الثغرات للمكونات التقنية للأنظمة الحساسة الداخلية ومعالجتها كل ثلاثة أشهر؛ على الأقل. (CSCC-2-9-1-3)

2-5 يجب على <اسم الجهة> إجراء تقييم الثغرات للمكونات التقنية للأنظمة الحساسة الخارجية والمتصلة بالإنترنت مرة واحدة شهرياً. (CSCC-2-9-1-2)

3- متطلبات معالجة الثغرات

3-1 بعد الانتهاء من تقييم الثغرات، يجب إعداد تقرير يوضح الثغرات المكتشفة وتصنيفها والتوصيات المقترحة لمعالجتها.

3-2 بعد إرسال تقرير تقييم الثغرات ومعالجتها من قبل الأطراف المعنية، يجب إجراء فحص واكتشاف الثغرات المكتشفة مرة أخرى للتأكد من معالجتها.

3-3 يجب استخدام حزم التحديثات والإصلاحات من مصادر موثوقة وآمنة ووفقاً لسياسة حزم التحديثات والإصلاحات.

3-4 يجب إصلاح وإغلاق الثغرات الحرجة (Critical Vulnerabilities) المكتشفة حديثاً، مع اتباع آليات إدارة التغيير المتبعة لدى <اسم الجهة>. (CSCC-2-9-1-3)

3-5 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.

4- متطلبات أخرى

4-1 يجب على <اسم الجهة> 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 الموجودة. (ECC-2-10-3-5)

4-2 يجب مراجعة تطبيق متطلبات الأمن السيبراني لإدارة الثغرات التقنية لـ<اسم الجهة> دورياً.

4-3 يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر لإدارة الثغرات.

4-4 يجب مراجعة هذه السياسة مرة واحدة في السنة؛ على الأقل.

الأدوار والمسؤوليات

1- **راعي ومالك وثيقة السياسة:** <رئيس الإدارة المعنية بالأمن السيبراني>.

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

3- **تنفيذ السياسة وتطبيقها:** <الإدارة المعنية بتقنية المعلومات> و <الإدارة المعنية بالأمن السيبراني>.

اختر التصنيف

الإصدار 1.0

الالتزام بالسياسة

1- يجب على <رئيس الإدارة المعنية بالأمن السيبراني> ضمان التزام <اسم الجهة> بهذه السياسة بشكل دوري.

2- يجب على كافة العاملين في <اسم الجهة> الالتزام بهذه السياسة.

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