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 حماية تطبيقات الويب

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

1. اضغط على مفتاحي "Ctrl" و"H" بالوقت 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>

قائمة المحتويات

الأهداف

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بحماية تطبيقات الويب الخارجية الخاصة بـ<اسم الجهة>، لتقليل المخاطر السيبرانية 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 ٢-١٥-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع تطبيقات الويب الخارجية الخاصة بـ<اسم الجهة>، وتنطبق هذه السياسة على جميع العاملين في <اسم الجهة>.

بنود السياسة

1 المتطلبات العامة

1-1 يجب أن تتبع تطبيقات الويب الخارجية التي يتم شراؤها أو تطويرها داخلياً مبدأ المعمارية متعددة المستويات (Multi-tier Architecture). (ECC-2-15-3-2)

2-1 يجب استخدام مبدأ المعمارية متعددة المستويات لتطبيقات الويب الخارجية للأنظمة الحساسة على ألا يقل عدد المستويات عن 3 مستويات (3-tier Architecture). (CSCC-2-12-2)

3-1 يجب التأكد من استخدام بروتوكولات الاتصالات الآمنة فقط، مثل بروتوكول نقل النص التشعبي الآمن (HTTPS) وبروتوكول نقل الملفات الآمن (SFTP) وأمن طبقة النقل (TLS) وغيرها. (ECC-2-15-3-3)

4-1 يجب استخدام نظام جدار الحماية لتطبيقات الويب (Web Application Firewall "WAF") لحماية تطبيقات الويب الخارجية من الهجمات الخارجية. (ECC-2-15-3-1)

5-1 يجب تطبيق العزل المنطقي لبيئة التطوير (Development Environment) وبيئة الاختبار (Testing Environment) عن بيئة الإنتاج (Production Environment).

6-1 يجب استخدام تقنيات حماية البيانات والمعلومات في تطبيقات الويب الخارجية ووفقاً لسياسة حماية البيانات والمعلومات وسياسة التصنيف.

7-1 في حال شراء تطبيقات ويب من طرف خارجي، يجب التأكد من التزام المورد بسياسات ومعايير الأمن السيبراني في <اسم الجهة>.

8-1 يجب تطبيق الحد الأدنى على الأقل لمعايير أمن التطبيقات وحمايتها (Ten OWASP Top) لتطبيقات الويب الخارجية للأنظمة الحساسة. (CSCC-2-12-1-2)

2 متطلبات حق الوصول (Access Right)

2-1 يجب استخدام التحقّق من الهوية متعدّد العناصر (Multi-Factor Authentication) لعمليات دخول المستخدمين على تطبيقات الويب الخارجية. (ECC-2-15-3-5)

2-2 يجب توثيق واعتماد معايير أمنية لتطوير تطبيقات الويب، وتشمل كحد أدنى إدارة الجلسات بشكل آمن (Secure Session Management) وموثوقية الجلسات (Authenticity)، وإقفالها (Lockout)، وإنهاء مهلتها (Timeout). (CSCC-2-12-1-1)

2-3 ينبغي أن يقتصر حق الوصول إلى منظومات الإنتاج، وأن يتم التحكم به وفقاً للمسؤوليات الوظيفية.

2-4 يجب نشر سياسة الاستخدام الآمن لجميع مستخدمي تطبيقات الويب الخارجية. (ECC-2-15-3-4)

3 متطلبات تطوير أو شراء تطبيقات الويب

3-1 يجب إجراء تقييم لمخاطر الأمن السيبراني عند التخطيط لتطوير أو شراء تطبيقات الويب وقبل إطلاقها في بيئة الإنتاج ووفقاً لسياسة إدارة مخاطر الأمن السيبراني المعتمدة في <اسم الجهة>.

3-2 قبل استخدام المعلومات المحمية في بيئة الاختبار، يجب الحصول على إذن مسبق من <الإدارة المعنية بالأمن السيبراني> واستخدام ضوابط مشددة لحماية تلك البيانات، مثل: تقنيات مزج البيانات (Data Scrambling) وتقنيات تعتيم البيانات (Data Masking)، وحذفها مباشرة بعد الانتهاء من استخدامها.

3-3 يجب حفظ شفرة المصدر (Source Code) بشكل آمن وتقييد الوصول إليها للمصرح لهم فقط.

3-4 يجب إجراء اختبار الاختراق لتطبيق الويب الخارجي في بيئة الاختبار وتوثيق النتائج والتأكد من معالجة جميع الثغرات قبل إطلاق التطبيق على بيئة الإنتاج.

3-5 يجب إجراء فحص الثغرات للمكونات التقنية لتطبيقات الويب والتأكد من معالجتها بتثبيت حزم التحديثات والإصلاحات المعتمدة لدى <اسم الجهة>.

3-6 يجب اعتماد تطبيقات الويب من قبل اللجنة التقنية الاستشارية للتغيير (CAB) قبل إطلاقها في بيئة الإنتاج.

4 متطلبات أخرى

4-1 يجب مراجعة متطلبات الأمن السيبراني الخاصة بحماية تطبيقات الويب الخارجية دورياً. (ECC-2-15-4)

4-2 يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر لحماية تطبيقات الويب الخارجية.

4-3 تتم 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>.

الالتزام بالسياسة

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

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>.