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

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.

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	عُدل بواسطة	أسباب التعديل
<أدخل رقم النسخة>	اضغط هنا لإضافة نص	<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 نص

اختر التصنيف

الإصدار <١,٠>

قائمة المحتويات

اختر التصنيف

الإصدار <١,٠>

الغرض

تهدف هذه السياسة إلى تحديد متطلبات الأمن السيبراني المتعلقة بحماية تطبيقات الويب الخارجية الخاصة بـ<اسم الجهة>، لتقليل المخاطر السيبرانية وحمايتها من التهديدات الداخلية والخارجية للحفاظ على السرية والموثوقية والتوافر 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 السياسة

تطبق هذه السياسة على جميع تطبيقات الويب الخارجية الخاصة بـ<اسم الجهة>، وعلى جميع العاملين (الموظفين والمتعاقدين) في <اسم الجهة>.

بنود السياسة

١ البنود العامة

١-١ يجب استخدام جدار الحماية لتطبيقات الويب (WAF) لحماية تطبيقات الويب الخارجية من الهجمات الخارجية.

١-٢ يجب أن تتبع تطبيقات الويب الخارجية مبدأ المعمارية متعددة المستويات (Multi-tier Architecture) على ألا يقل عن مستويين (٢-tier Architecture).

١-٣ يجب استخدام مبدأ المعمارية متعددة المستويات لتطبيقات الويب الخارجية للأنظمة الحساسة على ألا يقل عدد المستويات عن ٣ مستويات (٣-tier Architecture).

١-٤ 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.

١-٥ يجب تطبيق العزل المنطقي لبيئة التطوير (Development Environment) وبيئة الاختبار (Testing Environment) عن بيئة الإنتاج (Production Environment).

١-٦ يجب استخدام تقنيات حماية البيانات والمعلومات في تطبيقات الويب الخارجية وذلك وفقًا لسياسة حماية البيانات والمعلومات وسياسة التصنيف المعتمدة لدى <اسم الجهة>.

١-٧ في حال شراء تطبيقات ويب من طرف خارجي، يجب التأكد من التزام المورد بسياسات ومعايير الأمن السيبراني المعتمدة لدى <اسم الجهة>.

١-٨ يجب تطبيق معايير أمن التطبيقات وحمايتها (OWASP Top Ten Web Application Security Risks) في حدها الأدنى لتطبيقات الويب الخارجية للأنظمة الحساسة.

١-٩ يجب تطبيق معايير أمن واجهة برمجة التطبيقات (OWASP Top Ten API Security) في حدها الأدنى لتطبيقات الويب الخارجية للأنظمة الحساسة.

١-١٠ يجب تحديد متطلبات الأمن السيبراني في بناء تطبيقات الويب وتصميمها وتطبيقها بشكل آمن وفعال.

١-١١ يجب ضمان حفظ سجلات الأحداث والتدقيق لتطبيقات الويب في <اسم الجهة> ومراقبتها.

١-١٢ يجب ضمان سلامة بيانات تطبيقات الويب من العبث بها أو فقدانها بالخطأ أو تخريبها، والتأكد من توافرها وقابلية استعادتها عن طريق النسخ الاحتياطية والأرشيف (Backup and Archival).

١-١٣ يجب تحديد متطلبات الأمن السيبراني لتطبيقات الويب المستضافة بالحوسبة السحابية لضمان إعدادها وتثبيتها وتشغيلها بطريقة آمنة.

١-١٤ يجب الحفاظ على توافر تطبيقات الويب الخارجية وحمايتها من هجمات تعطيل الخدمة (Distributed Denial of Service "DDoS" Attacks) على مستوى التطبيقات والشبكة.

١-١٥ يجب تطوير إجراءات ومعايير خاصة بحماية تطبيقات الويب بناءً على حاجة العمل.

١-١٦ يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر والاستخدام الصحيح والفعال لمتطلبات حماية تطبيقات الويب.

٢ متطلبات صلاحية الوصول (Access Right)

٢-١ يجب استخدام التحقّق من الهوية متعدّد العناصر (Multi-Factor Authentication) لعمليات دخول المستخدمين على تطبيقات الويب الخارجية ودخول مسؤولي النظام على تطبيقات الويب الداخلية.

٢-٢ يجب توثيق واعتماد معايير أمنية لتطوير تطبيقات الويب، وتشمل كحد أدنى الإدارة الآمنة للجلسات (Secure Session Management)، بما يتضمن موثوقية الجلسات (Authenticity)، وإقفالها (Lockout)، وإنهاء مهلتها (Timeout).

٢-٣ يجب تقييد صلاحية الوصول إلى منظومات الإنتاج، وأن يتم التحكم بها وفقًا للمسؤوليات الوظيفية.

٢-٤ يجب نشر سياسة الاستخدام الآمن لجميع مستخدمي تطبيقات الويب الخارجية.

٢-٥ يجب استخدام طرق آمنة (hashing function) لحفظ بيانات المستخدم عند الدخول على تطبيقات الويب الخارجية مثل كلمة المرور.

٣ متطلبات مراجعة الإعدادات الأمنية (Secure Configuration)

٣-١ يجب إجراء تقييم لمخاطر الأمن السيبراني عند التخطيط لتطوير أو شراء تطبيقات الويب وقبل إطلاقها في بيئة الإنتاج وفقًا لسياسة إدارة مخاطر الأمن السيبراني المعتمدة لدى <اسم الجهة>.

٣-٢ يجب تحديد الإعدادات الأمنية والتحصين ومراجعتها للتأكد من ضبط إعدادات تطبيقات الويب وتشغيلها بشكل آمن وفعال وتوثيقها.

٣-٣ يجب ضمان سرية بيانات تطبيقات الويب والتأكد من سلامتها وفقًا لسياسة حماية البيانات والمعلومات المعتمدة لدى <اسم الجهة>.

٣-٤ قبل استخدام المعلومات المصنفة 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.

٣-٥ يجب حفظ الشفرة المصدرية (Source Code) بشكل آمن وتقييد الوصول إليها أوتعديلها للمصرح لهم فقط.

٣-٦ يجب إجراء اختبار الاختراق لتطبيق الويب الخارجي في بيئة الاختبار وتوثيق النتائج والتأكد من معالجة جميع الثغرات قبل إطلاق التطبيق على بيئة الإنتاج وفقًا لسياسة اختبار الاختراق المعتمدة لدى <اسم الجهة>.

٣-٧ يجب إجراء فحص الثغرات للمكونات التقنية لتطبيقات الويب والتأكد من معالجتها بتثبيت حزم التحديثات والإصلاحات المعتمدة لدى <اسم الجهة> بشكل دوري.

٣-٨ يجب إجراء اختبارات لتقييم حماية تطبيقات الويب في حال إصدار تطبيق جديد أو رئيسي (New or Major Application Release)، تطبيقات ويب جديدة (Acquired Web Applications)، إصدارات بسيطة (Point Releases)، إصدارات تصحيحية (Patch Releases)، وإصدارات الطوارئ (Emergency Releases).

٣-٩ يجب اعتماد التغييرات على تطبيقات الويب من قبل <اللجنة التقنية الاستشارية للتغيير> (CAB) قبل إطلاقها في بيئة الإنتاج.

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.

اختر التصنيف

الإصدار <١,٠>

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

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