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 دورة حياة تطوير البرمجيات الآمنة

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	عُدِّلَ 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 <1.0>

قائمة المحتويات

الغرض

الغرض من هذه السياسة هو تحديد متطلبات الأمن السيبراني المتعلقة بدورة حياة تطوير البرمجيات الآمنة (SSDLC) لدى <اسم الجهة>. حيث تهدف السياسة إلى وضع البنود المناسبة التي تحكم عملية تطوير الأنظمة والبرمجيات لدى <اسم الجهة> للحد من احتمالية وقوع هجمات الأمن السيبراني بسبب عدم ملائمة التصميمات أو الوظائف. حيث أن دعم الممارسات الجيدة لدورة حياة تطوير البرمجيات الآمنة (SSDLC) ضمن عمليات إدارة مشاريع تقنية المعلومات والتغييرات لدى <اسم الجهة> يساعد في الحد من عدد الثغرات في تصميمات وإعدادات الأنظمة وحزم البرمجيات والتخفيف من آثارها وعلاج الأسباب الأساسية لها.

تمت مواءمة هذه السياسة مع متطلبات الأمن السيبراني الصادرة عن الهيئة الوطنية للأمن السيبراني ويشمل ذلك على سبيل المثال لا الحصر: الضوابط الأساسية للأمن السيبراني (ECC – 1: 2018)، وضوابط الأمن السيبراني للأنظمة الحساسة (CSCC – 1: 2019) وغيرها من المتطلبات التشريعية والتنظيمية ذات العلاقة.

نطاق العمل

تُطبق هذه السياسة على جميع الأنظمة والتطبيقات لدى <اسم الجهة> سواءً تم تصميمها وتطويرها داخليًا أو بالاستعانة بأطراف خارجية، وتسري على جميع العاملين (الموظفين والمتعاقدين) في <اسم الجهة>.

بنود السياسة

1- البنود العامة

1-1 يجب إدارة جميع أنشطة دورة حياة تطوير البرمجيات الآمنة (SSDLC) وفقًا لسياسات المعلومات والأمن السيبراني لدى <اسم الجهة> واللوائح الحكومية ذات العلاقة.

2-1 يجب مراجعة سياسة ومعايير دورة حياة تطوير البرمجيات الآمنة وتعديلها بشكل دوري (حسب الحاجة) مرة واحدة على الأقل سنويًا.

3-1 يجب تطوير وتقديم الدورات والبرامج التدريبية المتعلقة بدورة حياة تطوير البرمجيات الآمنة إلى الموظفين المعنيين.

4-1 يجب وضع خطة لمشروع دورة حياة تطوير البرمجيات الآمنة ومتابعة التقدم في جميع أنشطة تصميم وتطوير وتنفيذ تقنيات المعلومات لدى <اسم الجهة>.

5-1 يجب على <اسم الجهة> تطبيق عملية آمنة وآلية للتحقق من الوظائف المطوّرة أو المحدّثة مؤخرًا واعتمادها ونشرها ضمن أي أنشطة لتطوير البرمجيات.

6-1 يجب تطوير معمارية الحل وأمنه ومراجعتهما في جميع مشاريع تقنية المعلومات.

7-1 يجب تطبيق إعدادات أمن الأنظمة الأساسية على جميع الأنظمة والأجهزة لدى <اسم الجهة>.

8-1 يجب تقييم واجهات المكونات المطلوبة لتطوير المنتج / الميزات قبل دمجها.

1-9 يجب الالتزام بالممارسات الآمنة لترميز البرمجيات في جميع مشاريع تطوير البرمجيات وأن تتم مواءمتها مع أفضل الممارسات المتبعة في القطاع.

1-10 يجب إجراء أنشطة اختبار ضمان الجودة على جميع أنشطة التطوير وتكرارها في المنهجية المعتمدة.

1-11 يجب اختبار البرمجيات المطوّرة قبل استخدامها في بيئة الإنتاج.

1-12 يجب إجراء اختبارات الثغرات الأمنية على جميع الأنظمة والبرمجيات الحساسة في بيئة تقنية المعلومات لدى <اسم الجهة>.

1-13 يجب على <اسم الجهة> وضع خطة مناسبة للتعامل مع جميع الثغرات المتعلقة بالبرمجيات واتخاذ إجراءات التخفيف المطلوبة بناءً على مدى حساسيتها.

1-14 يجب أن تضمن أي خطط لمشاريع تقنية المعلومات استخدام استراتيجيات النشر المصرّح بها والآمنة والقابلة للتتبع.

1-15 يجب أن تخضع أي مشاريع لتقنية المعلومات للمراقبة المستمرة لقياس ومتابعة أدائها.

1-16 يجب أن تخضع جميع البرمجيات والتطبيقات للمراقبة المستمرة عند تصميم وتنفيذ الحلول البرمجية.

1-17 يجب إيقاف جميع الأنظمة والبرمجيات التي تصل إلى نهاية دورة حياتها أو لم تعُد مطلوبة لدى <اسم الجهة> وفقًا للسياسات الأمنية وسياسات التخلص من الوسائط المطبقة لدى <اسم الجهة>.

2- البنود الإضافية لدورة حياة تطوير البرمجيات الآمنة

2-1 يجب إجراء تقييمات للمخاطر الأمنية لجميع الأنظمة والبرمجيات والتطبيقات لدى <اسم الجهة> وفقًا لعمليات إدارة مشاريع تقنية المعلومات وإدارة التغيير والعمليات الأمنية ووفقًا للأنظمة واللوائح ذات العلاقة.

2-2 يجب تحديد التهديدات على مشاريع تطوير الأنظمة والتطبيقات والبرمجيات لدى <اسم الجهة> والتخفيف منها بالشكل المناسب وفقًا للأنظمة واللوائح ذات العلاقة.

2-3 يجب أن تُدمج المتطلبات الأمنية، والتي تشمل تصنيف البيانات وضوابط الوصول، ضمن تصميمات برمجيات الأنظمة أو التطبيقات.

2-4 يجب أن يتم تشغيل الأنظمة والتطبيقات بشكل آمن في بيئة الإنتاج.

2-5 يجب الالتزام بمتطلبات فصل وتقسيم الشبكات بالنسبة لبيئات الأنظمة والتطبيقات لدى <اسم الجهة>.

2-6 يجب استخدام ضوابط حماية البيانات والمعلومات في جميع أنظمة وتطبيقات <اسم الجهة>.

2-7 يجب الالتزام ببروتوكول إدارة الإعدادات والتغيير واتباعه.

2-8 يجب استخدام أداة للتحقق من أمان الشفرة البرمجية لمسح شفرة تطوير البرمجيات وتحديد الثغرات الأمنية في مجموعات البيانات والتطبيقات الحساسة.

9-2 يجب إعداد إجراءات التغيير في حالات الطوارئ وتطبيقها.

10-2 يجب تحديد مشاركة الأطراف الخارجية في أنشطة التطوير وإدارتها بشكل رسمي.

11-2 يجب الالتزام بسياسات ومعايير <اسم الجهة> في جميع مشاريع تقنية المعلومات.

الأدوار والمسؤوليات

1- **مالك 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>.

4- **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

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

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>.