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 قائمة التحقق من متطلبات الأمن السيبراني في تطوير البرمجيات

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.

اختر التصنيف

الإصدار <١,٠>

اعتماد الوثيقة

التوقيع	التاريخ	الاسم	المسمى الوظيفي	الدور
<أدخل التوقيع>	اضغط هنا لإضافة تاريخ	<أدخل الاسم الكامل للموظف>	<أدخل المسمى الوظيفي>	اختر الدور

نسخ الوثيقة

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

جدول المراجعة

تاريخ المراجعة القادمة	التاريخ لأخر مراجعة	معدل المراجعة
اضغط هنا لإضافة تاريخ	اضغط هنا لإضافة تاريخ	<مره واحدة كل سنة>

اختر التصنيف

<الإصدار <١,٠>

قائمة المحتويات

اختر التصنيف

الإصدار <١,٠>

الغرض

تهدف هذه القائمة إلى تحديد متطلبات الأمن السيبراني التي تنطبق على أنشطة تطوير البرمجيات لدى <اسم الجهة>. حيث أن قدرة <اسم الجهة> على تنفيذ المتطلبات وفقًا لهذه القائمة يساعد في تطوير برمجيات آمنة وإصدارها للمستخدمين النهائيين بشكل سليم وفي الحفاظ على توافر أصول ومعلومات <اسم الجهة> وسلامتها وسريتها.

تمت مواءمة هذه المتطلبات مع متطلبات الأمن السيبراني الصادرة من الهيئة الوطنية للأمن السيبراني ويشمل ذلك على سبيل المثال لا الحصر: الضوابط الأساسية للأمن السيبراني (ECC – ١: ٢٠١٨) وغيرها من المتطلبات التشريعية والتنظيمية ذات العلاقة.

نطاق العمل

تطبّق قائمة التحقق هذه على متطلبات الأمن السيبراني في تطوير البرمجيات لدى <اسم الجهة>، وعلى جميع العاملين (الموظفين والمتعاقدين) في <اسم الجهة>.

اختر التصنيف

المتطلبات

ينبغي لـ<اسم الجهة> تعبئة الجدول التالي لتوثيق تطبيق متطلبات الأمن السيبراني في عملية تطوير البرمجيات. ويحتوي الملحق (أ) على وصف لكل عمود في هذه القائمة.

قائمة التحقق من متطلبات الأمن السيبراني في تطوير البرمجيات								
الرقم	النشاط	الوصف	إلزامي	المرحلة	الحالة	الموعد النهائي للتنفيذ	الملاحظات	الأدلّة
١	تسجيل أصول البرمجيات	إعداد مستودع مركزي واستخدامه لتخزين جميع المعلومات المتعلقة بالمشروع.	نعم	الخطة	اختَر الحالة.	اختَر التاريخ.		
٢	حزمة أدوات التطوير	وضع حل مركزي لتتبّع الشفرة البرمجية المصدرية ومعالجة الأدوات وإصدارها ونشرها للسماح بالنشر الآلي في البيئة ونشر ضوابط الأمن السيبراني.	نعم	الخطة	اختَر الحالة.	اختَر التاريخ.		

اختر التصنيف

الإصدار <١,٠>

	قائمة التحقق من متطلبات الأمن السيبراني في تطوير البرمجيات							
الرقم	النشاط	الوصف	إلزامي	المرحلة	الحالة	الموعد النهائي للتنفيذ	الملاحظات	الأدلّة
٣	تحليل نمذجة التهديدات	إجراء نمذجة التهديدات للتطبيق، مما يتيح تحديد المخاطر والمتطلبات المناسبة.	نعم	الخطة	اختَر الحالة.	اختَر التاريخ.		
٤	الالتزام التنظيمي/ الداخلي	إجراء تقييم للمتطلبات الخارجية (التشريعية والتنظيمية) والداخلية ومراعاة المتطلبات المستنبطة في تصميم ضوابط الأمن السيبراني.	نعم	الخطة	اختَر الحالة.	اختَر التاريخ.		
٥	تحديد سمات مخاطر التطبيق	إجراء تقييم لمخاطر الأمن السيبراني للتطبيق بما يتوافق مع معيار إدارة مخاطر الأمن السيبراني لتحديد الأثر المحتمل على الأعمال في	نعم	الخطة	اختَر الحالة.	اختَر التاريخ.		

اختر التصنيف

الإصدار <١,٠>

	قائمة التحقق من متطلبات الأمن السيبراني في تطوير البرمجيات							
الرقم	النشاط	الوصف	إلزامي	المرحلة	الحالة	الموعد النهائي للتنفيذ	الملاحظات	الأدلّة
		حالة حدوث المخاطر.						
٦	تحديد المتطلبات الأمنية	تحديد متطلبات الأمن السيبراني، المستخرجة من المتطلبات الوظيفية والأنشطة السابقة (تحليل نمذجة التهديدات، والالتزام التنظيمي/ الداخلي، وتحديد مخاطر التطبيقات).	نعم	الخطة	اختَر الحالة.	اختَر التاريخ.		

	قائمة التحقق من متطلبات الأمن السيبراني في تطوير البرمجيات						
الرقم	النشاط	الوصف	إلزامي	المرحلة	الحالة	الموعد النهائي للتنفيذ	الملاحظات	الأدلّة
٧	تحديد المجموعات والأدوار	تحديد الأدوار والمسؤوليات قبل أنشطة التطوير لضمان مبدأ الحد الأدنى من الصلاحيات والامتيازات. أُخذت العوامل التالية بعين الاعتبار: - نوع البيئة - الوصول إلى أدوات التطوير وخطوط التكامل المستمر/التنفيذ المستمر - حساسية البيانات المستخدمة للتطوير	نعم	الحوكمة	اختَر الحالة.	اختَر التاريخ.		
٨	تحديد المسؤول عن الأمن	تحديد وسيط بين إدارة الأمن السيبراني وفرق التطوير لضمان التواصل حول المتطلبات وتبادل المعرفة بالإضافة إلى حل المشاكل التي تنشأ خلال عملية	نعم	الحوكمة	اختَر الحالة.	اختَر التاريخ.		

اختر التصنيف

الإصدار <١,٠>

	قائمة التحقق من متطلبات الأمن السيبراني في تطوير البرمجيات							
الرقم	النشاط	الوصف	إلزامي	المرحلة	الحالة	الموعد النهائي للتنفيذ	الملاحظات	الأدلّة
		التطوير.						
٩	إدارة المشاكل	استخدام مستودع مركزي للمشاكل المحددة خلال عملية التطوير، ويكون قادرًا على استيعاب البنود التالية وتتبعها: - المتطلبات غير المستوفاة - أوجه الضعف الأمني المحددة خلال الاختبارات - الملاحظات الأخرى المرتبطة بالأمن السيبراني	لا	الحوكمة	اختَر الحالة.	اختَر التاريخ.		

اختر التصنيف

الإصدار <١,٠>

	قائمة التحقق من متطلبات الأمن السيبراني في تطوير البرمجيات							
الرقم	النشاط	الوصف	إلزامي	المرحلة	الحالة	الموعد النهائي للتنفيذ	الملاحظات	الأدلّة
١٠	تحديد بوابات الأمن	تحديد نقاط تحقق إلزامية والمتطلبات المرتبطة بها لإجراءات عملية التطوير. تُساعد نقاط التحكّم هذه على تحديد ما إذا كانت الضوابط الأمنية المطبّقة تُعالج مخاطر الأمن السيبراني بكفاءة.	نعم	الحوكمة	اختَر الحالة.	اختَر التاريخ.		
١١	الفصل بين البيئات	عند الحد الأدنى من التطوير، تم إعداد بيئات الاختبار والإنتاج. مُنح وصول المطوّر إلى بيئة الإنتاج لفترة محدّدة فقط وتحت الإشراف.	نعم	الحوكمة	اختَر الحالة.	اختَر التاريخ.		
١٢	تنقية بيانات الاختبار	تعقيم البيانات المستخدمة للاختبار المستخلصة من بيانات الإنتاج وأُستبدلت البيانات الحساسة بمحتوى	نعم	الحوكمة	اختَر الحالة.	اختَر التاريخ.		

اختر التصنيف

الإصدار <١,٠>

	قائمة التحقق من متطلبات الأمن السيبراني في تطوير البرمجيات						
الرقم	النشاط	الوصف	إلزامي	المرحلة	الحالة	الموعد النهائي للتنفيذ	الملاحظات	الأدلّة
		عشوائي.						
١٣	اعتماد مكوّنات الأطراف الخارجية	التأكد من أنه تم تقييم فريق الأمن السيبراني جميع مكوّنات الأطراف الخارجية بالفعل وجرى اعتمادها للاستخدام في عملية التطوير. شمل نطاق التقييم التحقّق من المرونة ضد هجمات الأمن السيبراني ونموذج الترخيص ومتطلبات الامتثال والمتطلبات التنظيمية.	نعم	الحوكمة	اختَر الحالة.	اختَر التاريخ.		
١٤	تحديد اتفاقية مستوى	تحديد اتفاقية مستوى الخدمة لمعالجة المشاكل المحددة خلال عملية التطوير وأنه تم	نعم	الحوكمة	اختَر الحالة.	اختَر التاريخ.		

اختر التصنيف

الإصدار <١,٠>

	قائمة التحقق من متطلبات الأمن السيبراني في تطوير البرمجيات						
الرقم	النشاط	الوصف	إلزامي	المرحلة	الحالة	الموعد النهائي للتنفيذ	الملاحظات	الأدلّة
	الخدمة	تتبعها خلال العملية.						
١٥	إدارة المقاييس	اتباع المقاييس المجمعة خلال عملية التطوير والتأكد من إجراء المعالجة النهائية في حالات رصد أي انحرافات عن اتفاقيات مستوى الخدمة.	نعم	الحوكمة	اختَر الحالة.	اختَر التاريخ.		
١٦	تدريب الفرق	تدريب فرق التطوير وغيرها من الموظفين المشاركين في العملية والتأكد من أن لديهم معرفة محدثة مرتبطة بمخاطر الأمن السيبراني في تطوير البرمجيات بالإضافة إلى الأنشطة المرتبطة بها التي تُنفّذ في الجهة.	نعم	الحوكمة	اختَر الحالة.	اختَر التاريخ.		

اختر التصنيف

الإصدار <١,٠>

	قائمة التحقق من متطلبات الأمن السيبراني في تطوير البرمجيات						
الرقم	النشاط	الوصف	إلزامي	المرحلة	الحالة	الموعد النهائي للتنفيذ	الملاحظات	الأدلّة
١٧	إرشادات التطوير الآمن	إعداد إرشادات حول الاستخدام الآمن للتقنيات المستخدمة في عملية التطوير وتحديثها واستخدمها من قبل الفريق.	نعم	الشفرة	اختَر الحالة.	اختَر التاريخ.		
١٨	التحليل الساكن لبيئة التطوير المتكاملة	إجراء تكامل أدوات تحرير النصوص البرمجية المستخدمة للتطوير مع حلول تُجري تحليلًا ساكنًا للامتثال بالمقارنة بإرشادات الأمن السيبراني. أُستخدمت نتائج ذلك التحليل لتحديد ملاءمة جودة النصوص البرمجية من منظور الأمن السيبراني لإدخالها في مستودع مركزي.	لا	الشفرة	اختَر الحالة.	اختَر التاريخ.		

اختر التصنيف

الإصدار <١,٠>

قائمة التحقق من متطلبات الأمن السيبراني في تطوير البرمجيات								
الرقم	النشاط	الوصف	إلزامي	المرحلة	الحالة	الموعد النهائي للتنفيذ	الملاحظات	الأدلّة
١٩	الاختبار الساكن لأمن التطبيق	إجراء اختبارات آلية لأمن التطبيق بناءً على تقييم المخاطر، وحدّدت تلك الاختبارات تصنيف التطبيق. جرى تتبّع النتائج ومعالجتها وفقًا لاتفاقيات مستوى الخدمة المتفق عليها، وأُجري قبل الفحص ضبط دقيق لإعدادات أداة الفحص لضمان مراجعة البرمجية الأساسي بأكمله بحثًا عن أي عيوب أمنية.	لا	الاختبار	اختَر الحالة.	اختَر التاريخ.		
٢٠	تحليل تكوين البرمجيات	إجراء تحليل آلي لتكوين البرمجيات لتحديد ما إذا كانت جميع المكوّنات المستخدمة لبناء التطبيق خالية من الثغرات ومستخدمة بطريقة مناسبة.	لا	الاختبار	اختَر الحالة.	اختَر التاريخ.		

اختر التصنيف

الإصدار <١,٠>

	قائمة التحقق من متطلبات الأمن السيبراني في تطوير البرمجيات							
الرقم	**النشاط**	**الوصف**	**إلزامي**	**المرحلة**	**الحالة**	**الموعد النهائي للتنفيذ**	**الملاحظات**	**الأدلّة**
٢١	مراجعة الإعدادات	إجراء تقييم آلي لمعايير إعدادات المكونات المستخدمة في بيئات التطوير والإنتاج بالمقارنة بأدلّة التحصين الحالية المعتمدة لكل تقنية، بما يشمل ما يلي دون حصر: - البيئة الأمنية - أنظمة التشغيل - قواعد البيانات - الأدوات الوسيطة - الحاويات - مقدّمي الخدمة الخارجيين - الموارد السحابية	نعم	الاختبار	اختَر الحالة.	اختَر التاريخ.		

اختر التصنيف

الإصدار <١,٠>

قائمة التحقق من متطلبات الأمن السيبراني في تطوير البرمجيات								
الرقم	النشاط	الوصف	إلزامي	المرحلة	الحالة	الموعد النهائي للتنفيذ	الملاحظات	الأدلّة
٢٢	الاختبار الديناميكي لأمن التطبيق	إجراء اختبارات آلية لأمن التطبيق بناءً على تقييم المخاطر، وحدّدت تلك الاختبارات تصنيف التطبيق. جرى تتبّع النتائج ومعالجتها وفقًا لاتفاقيات مستوى الخدمة المتفق عليها، وأُجري قبل الفحص ضبط دقيق لإعدادات أداة الفحص لضمان مراجعة الكود الأساسي بأكمله بحثًا عن أي عيوب أمنية (بما في ذلك إعدادات التحقق من الهوية والتصاريح).	لا	الاختبار	اختَر الحالة.	اختَر التاريخ.		

اختر التصنيف

الإصدار <١,٠>

	قائمة التحقق من متطلبات الأمن السيبراني في تطوير البرمجيات						
الرقم	النشاط	الوصف	إلزامي	المرحلة	الحالة	الموعد النهائي للتنفيذ	الملاحظات	الأدلّة
٢٣	اختبار الاختراق	إجراء اختبارات يدوية لأمن التطبيق بناءً على تقييم المخاطر، وحدّدت تلك الاختبارات تصنيف التطبيق. جرى تتبّع النتائج ومعالجتها وفقًا لاتفاقيات مستوى الخدمة المتفق عليها، وأُجري قبل الفحص ضبط دقيق لإعدادات أداة الفحص لضمان مراجعة البرمجية الأساسي بأكمله بحثًا عن أي عيوب أمنية (بما في ذلك إعدادات التحقق من الهوية والتصاريح).	لا	الاختبار	اختَر الحالة.	اختَر التاريخ.		

اختر التصنيف

الإصدار <١,٠>

	قائمة التحقق من متطلبات الأمن السيبراني في تطوير البرمجيات							
الرقم	النشاط	الوصف	إلزامي	المرحلة	الحالة	الموعد النهائي للتنفيذ	الملاحظات	الأدلّة
٢٤	المراقبة الأمنية	مراقبة التطبيقات المنشورة في بيئة الإنتاج بحثًا عن أي حوادث أمنية وأنماط معروفة وأي حالات غير طبيعية قد تُشير إلى وجود هجمات حديثة. شملت المراقبة أحداث التطبيق والنظام والأدوات الوسيطة والسحابة. جرى تحديث إجراءات الاستجابة للحوادث ودليل التطبيق بما يشمل التطبيقات المنشورة حديثًا.	نعم	التشغيل	اختَر الحالة.	اختَر التاريخ.		
٢٥	أمن النقاط الطرفية	استيفاء النقاط الطرفية المستخدمة في بيئة تنفيذ التطبيق متطلبات التحصين لدى <اسم الجهة>.	نعم	أمن النقاط الطرفية	اختَر الحالة.	اختَر التاريخ.		

اختر التصنيف

الإصدار <١,٠>

	قائمة التحقق من متطلبات الأمن السيبراني في تطوير البرمجيات							
الرقم	النشاط	الوصف	إلزامي	المرحلة	الحالة	الموعد النهائي للتنفيذ	الملاحظات	الأدلّة
٢٦	استمرارية الأعمال	تقييم التطبيق من منظور استمرارية الأعمال لضمان تحديث العمليات والضوابط لتشمل المكوّنات المنشورة حديثًا.	نعم	أمن البنى التحتية	اختَر الحالة.	اختَر التاريخ.		
٢٧	إدارة الأصول	تهيئة جميع المكوّنات المنشورة حديثًا من خلال نظام إدارة الأصول وتتبعها لتحديد أي تغيرات.	نعم	أمن البنى التحتية	اختَر الحالة.	اختَر التاريخ.		
٢٨	إدارة الإعدادات	تتبّع إعدادات جميع المكوّنات لتحديد أي تغيّرات غير مصرّح بها وتخزين كامل مسار الاعتماد تماشيًا مع إجراءات إدارة التغيير في الجهة.	نعم	أمن البنى التحتية	اختَر الحالة.	اختَر التاريخ.		

اختر التصنيف

الإصدار <١,٠>

	قائمة التحقق من متطلبات الأمن السيبراني في تطوير البرمجيات							
الرقم	النشاط	الوصف	إلزامي	المرحلة	الحالة	الموعد النهائي للتنفيذ	الملاحظات	الأدلّة
٢٩	إدارة الثغرات	شمول نطاق مسح الثغرات المنتظم مكوّنات التطبيق وجرى التعامل مع الملاحظات الناتجة باستخدام الإجراءات المحدّدة بالفعل في إطار سياسة إدارة الثغرات في <اسم الجهة>.	نعم	التشغيل	اختَر الحالة.	اختَر التاريخ.		
٣٠	التكامل مع الخدمات الأمنية	تكامل بيئة الإنتاج مع الخدمات الأمنية المتاحة (حسب التصنيف)، بما في ذلك دون حصر: - نظام منع/اكتشاف التسلل - جدار الحماية لتطبيقات الويب - نظام الكشف عن تهديدات النقاط الطرفية والاستجابة لها - نظام إدارة المعلومات الأمنية والأدلّة	نعم	التشغيل	اختَر الحالة.	اختَر التاريخ.		

اختر التصنيف

	قائمة التحقق من متطلبات الأمن السيبراني في تطوير البرمجيات						
الرقم	النشاط	الوصف	إلزامي	المرحلة	الحالة	الموعد النهائي للتنفيذ	الملاحظات	الأدلّة
٣١	إدارة الأسرار	تدوير معايير الإعدادات شاملة القيم الحساسة (أي مفاتيح لبيانات الاعتماد والشهادات ومفاتيح التراخيص وما إلى ذلك) وتعديلها عن تلك المستخدمة في التطوير. جرى تخزين الأسرار بطريقة آمنة باستخدام الآليات المتاحة في المنصة. حُدّدت عمليات لضمان تدوير الأسرار دوريًا والتخلّص منها بأمان.	نعم	التشغيل	اختَر الحالة.	اختَر التاريخ.		
٣٢	معلومات التهديدات الاستباقية	شمول أنشطة معلومات التهديدات الاستباقية المنتظمة التطبيق وطُبّقت التغييرات اللازمة على التطبيق وبيئات التنفيذ استجابةً للتهديدات الناشئة.	نعم	التشغيل	اختَر الحالة.	اختَر التاريخ.		

اختر التصنيف

الإصدار <١,٠>

الأدوار والمسؤوليات

١- **مالك قائمة التحقق**: <رئيس الإدارة المعنية بالأمن السيبراني>

٢- **مراجعة قائمة التحقق وتحديثها:** <الإدارة المعنية بالأمن السيبراني>

٣- **تنفيذ قائمة التحقق وتطبيقها:** <الإدارة المعنية بتقنية المعلومات>

٤- **قياس الالتزام بالقائمة المرجعية**: <الإدارة المعنية بالأمن السيبراني>

التحديث والمراجعة

يجب على <الإدارة المعنية بالأمن السيبراني> مراجعة قائمة التحقق سنويًا على الأقل أو في حال حدوث تغييرات في السياسات أو الإجراءات التنظيمية في <اسم الجهة> أو المتطلبات التشريعية والتنظيمية ذات العلاقة.

الالتزام بقائمة التحقق

١- يجب على <رئيس الإدارة المعنية بالأمن السيبراني> التأكد من التزام <اسم الجهة> بقائمة التحقق هذه باستمرار.

٢- يجب على كافة العاملين في <اسم الجهة> الالتزام بقائمة التحقق.

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

الملحق (أ) - وصف أسماء أعمدة قائمة التحقق

الوصف التوضيحي	
اسم العمود	الوصف
الرقم	رقم التعريف المخصّص للنشاط
النشاط	اسم النشاط الذي ينبغي استكماله
الوصف	وصف النشاط الذي ينبغي استكماله
إلزامي	هل الضابط المحدّد مطلوب أو يُمكن الاستغناء عنه شريطة أن يكون غير قابل للتطبيق ويُوافق الفريق الأمني على ذلك.
المرحلة	المرحلة المحددة للنشاط لاستكماله
الحالة	معلومات حول حالة تنفيذ الضابط، والحالات المحتملة هي ما يلي: • منجز • قيد التنفيذ • لا ينطبق
الموعد النهائي للتنفيذ	التاريخ الذي ينبغي تنفيذ الضابط بحلوله وتغيير الحالة إلى "منجز" أو "لا ينطبق"
الملاحظات	ملاحظات إضافية حول حالة تنفيذ الضابط
الأدلّة	معلومات حول طريقة التعامل مع المتطلّب - لقطة شاشة أو رابط للتوثيق