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 معيار حماية تطبيقات الويب

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.

اختر التصنيف

التاريخ: اضغط هنا لإضافة تاريخ

الإصدار: اضغط هنا لإضافة نص

المرجع: اضغط هنا لإضافة نص

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	عُدلَ 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 <١,٠>

قائمة المحتويات

الغرض

يهدف هذا المعيار إلى تحديد متطلبات الأمن السيبراني التفصيلية المتعلقة بحماية تطبيقات الويب الخارجية الخاصة ب<اسم الجهة> لتقليل المخاطر السيبرانية وحمايتها من التهديدات الداخلية والخارجية في <اسم الجهة>. هذه المتطلبات تمت موائمتها مع سياسة حماية تطبيقات الويب ومتطلبات 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.

النطاق

يطبق هذا المعيار على جميع تطبيقات الويب الخارجية الخاصة ب<اسم الجهة>، وعلى جميع العاملين (الموظفين والمتعاقدين) في <اسم الجهة>.

المعايير

١	إدارة هويات الدخول
الهدف	ضمان حماية تطبيقات الويب من الوصول غير المصرح به.
المخاطر المحتملة	يترتب على الوصول غير المصرّح به لتطبيقات الويب مخاطر كبيرة قد تؤدي إلى تسرب أو سرقة المعلومات، وقد تساعد هذه المعلومات في تنفيذ المزيد من الهجمات السيبرانية ضد البنية التحتية ل<اسم الجهة>.
الإجراءات المطلوبة	
١-١	تطبيق الوصول الآمن وإدارة هويات الدخول لتطبيقات الويب الخارجية بما يتوافق مع المعايير التقنية والأمنية المذكورة في معيار إدارة الصلاحيات والهويات المعتمد في <اسم الجهة> لمقاومة الهجمات السيبرانية.
١-٢	التأكد من وجود إدارة آمنة للجلسات (Secure Session Management)، بحيث تشمل موثوقية الجلسات (Authenticity)، إقفالها (Lockout)، وإنهاء مهلتها (Timeout).
٢	هندسة تطبيقات الويب
الهدف	تحديد متطلبات الأمن السيبراني في بناء تطبيقات الويب وتصميمها وتطبيقها بشكل آمن وفعال.

المخاطر المحتملة	قد يسبب البناء العشوائي لتطبيقات الويب مخاطر أمنية حساسة يمكن استغلالها في الهجمات السيبرانية التي قد تؤثر على أعمال <اسم الجهة>.
الإجراءات المطلوبة	
٢-١	حماية تطبيقات الويب الخارجية للأنظمة الحساسة من خلال استخدام مبدأ المعمارية ذات المستويات المتعددة (Multi-tier Architecture) على أن لا يقل عدد المستويات عن ٣، أو معمارية الخدمات الصغيرة المحمية بجدار حماية ثنائي الطبقة، وتحديدًا، إدراج **خادم الويب** في منطقة الإنترنت المحايدة، و**خوادم تطبيقات الويب** في منطقة الإنتاج، و**خوادم قواعد البيانات** في المنطقة الموثوقة أو منطقة قاعدة البيانات.
٢-٢	تطبيق العزل المادي أو المنطقي لتطبيقات الويب الحساسة عن التطبيقات أو الأنظمة الأخرى. فعلى سبيل المثال، يمكن تحقيق العزل المادي من خلال استضافة تطبيقات الويب في بيئة مادية منفصلة ومختلفة تمامًا، في حين يمكن تحقيق العزل المنطقي من خلال إدراج تطبيقات الويب في مناطق منفصلة داخل الشبكة دون السماح بالوصول إليها من أي منطقة أخرى.
٢-٣	عزل تطبيقات الويب الخاصة بالإنتاج منطقيًا عن بيئة الاختبار وبيئة التطوير باستخدام محددات الشبكة عن طريق ضبط إعدادات قوائم التحكّم بالوصول (ACL) والسياسات الأمنية على جدران الحماية.
٢-٤	تقييد الوصول عبر الشبكة لتطبيقات الويب وحصره بمنطقة خوادم الويب، ومنطقة خوادم تطبيقات الويب، ومنطقة الإدارة.
٢-٥	تثبيت جدار الحماية لتطبيقات الويب (WAF) على خوادم تطبيقات الويب للتحقق من حركة البيانات الواردة والمصادقة عليها، وتسجيل أي حركة بيانات غير مصرح بها وحجبها، حيث تعمل أجهزة جدار الحماية لتطبيقات الويب (WAF) على كشف هجمات الويب أو هجمات التطبيقات على الخدمات الخارجية وتطبيقات الويب أو حجبها. (بالإضافة إلى ذلك، إعداد جدار الحماية لتطبيقات الويب (WAF) لتمكين خاصية التحكم ببروتوكول الإنترنت وخصائص الموقع الجغرافي لبروتوكول الإنترنت من أجل حجب بروتوكولات الإنترنت المحظورة ودول معينة).
٢-٦	إعداد جدار الحماية لتطبيقات الويب (WAF) للحد من أعلى المخاطر الشائعة التي تستهدف تطبيقات الويب الصادرة عن المشروع المفتوح لأمن تطبيقات الويب (OWASP Top Ten Web Application Security) على تطبيقات الويب الحساسة وفقًا للمعايير والإجراءات ذات العلاقة في <اسم الجهة>.
٢-٧	تطبيق معايير أمن واجهة برمجة التطبيقات للحد من أعلى المخاطر الشائعة التي تستهدفها (OWASP Top Ten API Security) في حدها الأدنى لتطبيقات الويب الخارجية للأنظمة الحساسة.

٢-٨	ضبط إعدادات نظام منع الاختراق (IPS) وجدار الحماية لتطبيقات الويب (WAF) لإتاحة التواقيع التي تطابق سلوك وبروتوكولات تطبيقات الويب (مثل Oracle OHS، وIIS، وApache، وSQL، وXML، وغيرها).
٢-٩	ضبط إعدادات تقنيات الحماية من البرمجيات الضارة وأنظمة الحماية من التهديدات المتقدمة والمستمرة على سبيل المثال للتحقق من كافة عمليات نقل الملفات المرتبطة بتطبيقات الويب بحثًا عن أي ملفات خبيثة وفقًا لسياسة ومعيار الحماية من البرمجيات الضارة المعتمدين في <اسم الجهة>.
٢-١٠	ضبط إعدادات تقنيات وأنظمة حماية تطبيقات الويب لتتبع نموذجًا أمنيًا إيجابيًا أو نموذج السماح بقائمة محددة من التطبيقات، وذلك من خلال السماح بأنواع محددة من الملفات، وبروتوكولات ومنافذ محددة، وتطبيقات ويب محددة من المستوى ٧، ومتغيرات تطبيقات ويب محددة، مع منع جميع التطبيقات والملفات التي لم يتم ضبط إعداداتها.
٢-١١	استخدام تطبيقات ويب وبروتوكولات اتصالات آمنة مثل بروتوكول نقل النص التشعبي الآمن (HTTPS) وبروتوكول نقل الملفات الآمن (SFTP) وبروتوكول أمن طبقة النقل (TLS) ونحوها.
٣	**مراجعة الإعدادات والتحصين**
الهدف	تحديد الإعدادات والتحصين ومراجعتها للتأكد من ضبط إعدادات تطبيقات الويب وتشغيلها بشكل آمن وفعال.
المخاطر المحتملة	قد يؤدي عدم الدقة في ضبط إعدادات تطبيقات الويب ومكوناتها التقنية إلى ظهور ثغرات أمنية يمكن استغلالها لشن هجمات سيبرانية أو التأثير على سير الأعمال في <اسم الجهة>.
الإجراءات المطلوبة	
٣-١	تطبيق مراجعة الإعدادات والتحصين لتطبيقات الويب الخارجية بما يتوافق مع المعايير التقنية والأمنية المذكورة في معيار إعدادات الحماية والتحصين المعتمد في <اسم الجهة> لمقاومة الهجمات السيبرانية.
٣-٢	إجراء اختبارات دورية لتقييم حماية تطبيقات الويب مثل اختبار أمن التطبيقات الثابت (SAST) واختبار أمن التطبيقات الديناميكي (DAST).
٣-٣	إيقاف أو تعطيل الوظائف والخدمات وملفات الإعدادات غير الضرورية أو غير المستخدمة.

٣-٤	حجب إمكانية الوصول إلى الملفات والمجلدات المشاركة عبر الشبكة غير الضرورية أو غير اللازمة.
٣-٥	حماية الشفرة المصدرية وتحصينها.
٣-٦	إنشاء نسخ أو قوالب آمنة لكافة تطبيقات الويب بناءً على المعايير الأمنية المعتمدة. وإعادة نسخ تطبيقات الويب باستخدام أحد قوالب النسخ في حال تعرضها لانتهاك أمني.
٣-٧	تخزين النسخ في بيئة آمنة على خوادم مؤمنة والتحقق منها باستخدام أدوات مراقبة سلامة المعلومات دوريًا.
٤	توافر المعلومات
الهدف	الحفاظ على توافر تطبيقات الويب الخارجية وحمايتها من هجمات حجب الخدمة (DDoS Attacks) وتعطل الخدمة العرضي.
المخاطر المحتملة	إذا لم يتم توفير أنظمة الحماية من هجمات حجب الخدمة وتعطل البنية التحتية، قد تكون تطبيقات الويب هدفًا لهجمات حجب الخدمة، مما قد يسبب انقطاعًا دائمًا في الخدمات أو يؤثر على كفاءة تطبيق الويب.
الإجراءات المطلوبة	
٤-١	استخدام مبدأ معمارية تطبيقات الويب التوزيعية الذي يعمل على توزيع نقاط التعطل الحاسمة.
٤-٢	توفير تقنيات توزيع الجهد (Load Balancer) مثل تقنيات توزيع حركة البيانات والاتصالات.
٤-٣	تطبيق آليات تكرار البيانات (Data Replication) على تطبيقات الويب في مواقع التعافي من الكوارث أو المواقع البديلة (Secondary Data Center).
٤-٤	توفير نسخة مطابقة لبيئة إنتاج تطبيقات الويب للأنظمة الحساسة في موقع التعافي من الكوارث.
٤-٥	فيما يتعلق بتطبيقات الويب التي تستضيفها أطراف خارجية، يجب أن تتضمن بنود اتفاقية مستوى الخدمة مستوى مقبول من توافر تطبيقات الويب والخدمات المقدمة من خلالها، وذلك وفقًا لسياسة الأمن السيبراني المتعلق بالأطراف الخارجية المعتمدة في <اسم الجهة>.

٦-٤	ضبط إعدادات إعادة توجيه حركة بيانات تطبيقات الويب تلقائيًا أو يدويًا لموقع النسخ الاحتياطية أو التعافي من الكوارث في حال تعطل بيئة الإنتاج.
٥	التشفير
الهدف	ضمان سرية بيانات تطبيقات الويب والتأكد من سلامتها.
المخاطر المحتملة	في حال عدم استخدام تقنيات التشفير والتحقق من سلامة المعلومات، يمكن أن تتعرض المعلومات المحمية وبيانات تطبيقات الويب إلى الكشف أو التلاعب بها أو الوصول غير المصرح به.
الإجراءات المطلوبة	
٥-١	تطبيق التشفير لتطبيقات الويب الخارجية بما يتوافق مع المعايير التقنية والأمنية المذكورة في معيار التشفير المعتمد في <اسم الجهة> والمتطلبات التشريعية والتنظيمية ذات العلاقة لمقاومة الهجمات السيبرانية.
٥-٢	استخدام تقنيات التشفير للاتصالات بين الخوادم وأجهزة المستخدمين في تطبيقات الويب (End-to-End Encryption).
٥-٣	توفير شهادات تشفير تطبيقات الويب من جهة إصدار شهادات موثوقة ومعتمدة وفقًا للمتطلبات التنظيمية والتشريعية ذات العلاقة والتأكّد من تجديدها بشكل دوري.
٥-٤	استخدام تقنيات التشفير غير التماثلي القائم على شهادات التشفير (الخاص/العام) لكافة تطبيقات الويب العامة والخارجية، وذلك وفقًا لمعيار التشفير المعتمد في <اسم الجهة>.
٥-٥	تفعيل وظائف التشفير وإدارة شهادات التشفير على جدار الحماية لتطبيقات الويب للسيطرة بشكل أكبر على الهجمات والتهديدات.
٥-٦	تخزين مفاتيح تشفير تطبيقات الويب في مكان ملائم وآمن وفقًا للسياسات والإجراءات ذات العلاقة في <اسم الجهة>.
٦	تسجيل الأحداث وسجل التدقيق
الهدف	ضمان حفظ سجلات الأحداث لتطبيقات الويب في <اسم الجهة> ومراقبتها.
المخاطر المحتملة	يؤدي عدم حفظ ومراقبة سجلات الأحداث لتطبيقات الويب في <اسم الجهة> إلى صعوبة الكشف عن حوادث وتهديدات الأمن السيبراني وغيرها، وقد يتسبب بمضاعفة الأضرار التي قد تلحق بالتطبيقات.

الإجراءات المطلوبة	
٦-١	تفعيل تسجيل الأحداث وسجلات التدقيق لتطبيقات الويب الخارجية بما يتوافق مع المعايير التقنية الأمنية المذكورة في معيار إدارة سجلات الأحداث ومراقبة الأمن السيبراني المعتمد لدى <اسم الجهة> لمقاومة الهجمات السيبرانية.
٧	النسخ الاحتياطي والأرشفة
الهدف	ضمان سلامة بيانات تطبيقات الويب من العبث أو فقدانها بالخطأ أو تخريبها، والتأكد من توافرها وقابلية استعادتها.
المخاطر المحتملة	في حال حذف بيانات تطبيقات الويب أو العبث بها أو فقدانها بالخطأ أو تخريبها أو تعرّضها لهجوم إلكتروني، لن تتمكّن <اسم الجهة> من استرداد البيانات مما سيؤثّر على أنشطة أعمالها الاعتيادية.
الإجراءات المطلوبة	
٧-١	تطبيق النسخ الاحتياطي والأرشفة لتطبيقات الويب بما يتوافق مع المعايير التقنية والأمنية المذكورة في معيار إدارة النسخ الاحتياطية والتعافي من الكوارث المعتمد في <اسم الجهة> لمقاومة الهجمات السيبرانية.
٧-٢	عمل نسخ احتياطية كاملة لتطبيقات الويب وترقيمها تسلسليًا وتحديد تاريخها ووقتها وفهرستها وفقًا لسياسة إدارة النسخ الاحتياطية المعتمدة في <اسم الجهة>. وينبغي أن تشمل النسخ الاحتياطية على الأقل النسخ الاحتياطية لإعدادات تطبيقات الويب وبيانات ومعلومات تطبيقات الويب المخزنة.
٨	تطبيقات الويب الحديثة والسحابية الأصلية
الهدف	تحديد متطلبات الأمن السيبراني لتطبيقات الويب المستضافة بالحوسبة السحابية لضمان إعدادها وتثبيتها وتشغيلها بطريقة آمنة.
المخاطر المحتملة	قد يؤدي استخدام خدمة الحوسبة السحابية لتشغيل تطبيقات الويب بدون وضع معايير أمنية وتطبيق متطلبات الأمن السيبراني إلى ظهور ثغرات أمنية شائعة يمكن استغلالها لشن هجمات سيبرانية أو التأثير على كفاءة أعمال <اسم الجهة>.
الإجراءات المطلوبة	
٨-١	يجب تطوير واعتماد منهجية التطوير الآمن وفقًا لعملية "DevSecOps".
٨-٢	تطوير نظام التكامل المستمر/التثبيت المستمر (CI/CD) الآمن وتطبيقه باتباع أفضل الممارسات.

٨-٣	تنصيب منصة أمن الحاويات من مورد موثوق لإدارة أمن الحاويات وضمان حماية نظام الحاويات.
٨-٤	تنصيب حزم التحديثات والإصلاحات دوريًا.
٨-٥	توفير حلول إدارة المعلومات الحساسة وذلك من أجل إدارة المعلومات الحساسة والمفاتيح والشهادات ومنع تخزين المعلومات الحساسة في الحاويات.
٨-٦	استخدام نسخ الحاويات من مصادر موثوقة أو معتمدة.
٨-٧	عزل البنية التحتية الخاصة بالحاويات.
٨-٨	استخدام كشف الثغرات التلقائي لفحص الحاويات قبل وبعد تثبيتها في بيئة الإنتاج.
٨-٩	توفير تقنيات وأدوات المراقبة للتأكد من سلامة تطبيقات الويب وتوافرها وكفاءتها باستمرار.

الأدوار والمسؤوليات

١- **مالك المعيار:** <رئيس الإدارة المعنية بالأمن السيبراني>.

٢- **مراجعة المعيار وتحديثه:** <الإدارة المعنية بالأمن السيبراني>.

٣- **تنفيذ المعيار وتطبيقه:** <الإدارة المعنية بتقنية المعلومات> و <الإدارة المعنية بالأمن السيبراني>.

٤- **قياس الالتزام بالمعيار:** <الإدارة المعنية بالأمن السيبراني>.

التحديث والمراجعة

يجب على <الإدارة المعنية بالأمن السيبراني> مراجعة المعيار سنويًا على الأقل أو في حال حدوث تغييرات تقنية جوهرية في البنية التحتية أو في حال حدوث تغييرات في السياسات أو الإجراءات التنظيمية في <اسم الجهة> أو المتطلبات التشريعية والتنظيمية ذات العلاقة.

الالتزام بالمعيار

١- يجب على <رئيس الإدارة المعنية بالأمن السيبراني> التأكد من التزام <اسم الجهة> بهذا المعيار دوريًا.

٢- يجب على جميع العاملين في <اسم الجهة> الالتزام بهذا المعيار.

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