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:

1. اضغط على مفتاحي "Ctrl" و"H" في الوقت 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 هذا المعيار 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.

ويهدف هذا المعيار إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهو مطلب تشريعي في الضابط رقم ١-١٥-٢ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

يغطي هذا المعيار جميع تطبيقات الويب الخارجية الخاصة بـ<اسم الجهة>، وينطبق على جميع العاملين في <اسم الجهة>.

المعايير

1	إدارة هويات الدخول (Access Management)
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 لـ<اسم الجهة>.
الإجراءات المطلوبة	
1-1	استخدام مبدأ الحد الأدنى من الصلاحيات والامتيازات "Principle of Least Privilege" الذي يمنح المستخدمين الحد الأدنى من صلاحيات الوصول إلى تطبيقات الويب الخارجية. Security Principle of Least Privilege shall be applied to provide users with least privileged access permissions to external web applications.
2-1	حصر الوصول إلى المكونات التقنية الخاصة بالويب وتطبيقات الويب حسب الأدوار الوظيفية (مثل: مشرفو النظام، ومسؤولو دعم التطبيقات، وغيرها) وذلك باستخدام الحسابات الفردية لتلك الأدوار فقط. بالإضافة إلى ذلك، استخدام قوائم التحكم بالوصول

	إلى الشبكة (ACL) التي تعتمد على عناوين بروتوكولات الإنترنت (IP Address) الخاصة بأجهزة المستخدمين. Access to web applications and technical equipment shall be restricted to the required job roles (e.g., system administrator, deployment engineer, developer, etc.) by using the individual accounts for these roles only. In addition, network Access-Control Lists (ACLs) which use the IPs of users' workstations shall be used only.
3-1	إيقاف أو حذف الحسابات الافتراضية غير المستخدمة. Non-interactive or unused default and virtual accounts shall be removed or disabled.
4-1	إلى جانب ضرورة إدخال اسم المستخدم وكلمة المرور، إلزام المستخدم باستعمال التحقّق من الهوية متعدّد العناصر باستخدام آليات أخرى للتحقّق من الهوية مثل الخصائص الحيوية والمفاتيح المادية وكلمات المرور المؤقتة والبطاقات الذكية وشهادات التشفير، وغيرها. Besides a user/password combination, users shall be required to implement multi-factor authentication using a different authentication mechanism such as biometrics, hardware keys, one-time passwords, smart cards, certificates, etc.
5-1	استخدام كلمة مرور معقدة للدخول إلى تطبيقات الويب وفقاً لسياسة إدارة هويات الدخول والصلاحيات في <اسم الجهة>. Complex passwords shall be used for web applications, in accordance with <entity name>'s Identity and Access Management Policy.
6-1	ضبط إعدادات تطبيقات الويب الخاصة بالأنظمة الحساسة من خلال تحديد وقت انتهاء مهلة الجلسة وإقفالها عند عدم الاستخدام (على سبيل المثال، لمدة 5 دقائق). Session timeout and session idle lockout on web applications shall be configured for critical systems (e.g., 5 minutes).
2	هندسة تطبيقات الويب (Web Application Architecture)

اختر التصنيف

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	
1-2	تنفيذ البنية التحتية لتطبيقات الويب للأنظمة الحساسة باستخدام مبدأ البنية متعددة الطبقات (3 مستويات على الأقل)، أو معمارية الخدمات الصغيرة المحمية بجدار حماية ثنائي الطبقة. وتحديداً، 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. Web applications for critical systems infrastructure following at least 3-tier security architecture or micro-services architecture protected by a dual layer of firewalls shall be implemented. More specifically, **webservers** shall be placed in the Internet DMZ, **web application servers** shall be placed in the Production Zone, and **database servers** shall be placed in the Trusted/Database zone.
2-2	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 تماماً، في حين يمكن تحقيق العزل المنطقي من خلال إدراج تطبيقات الويب في مناطق منفصلة داخل الشبكة دون السماح بالوصول إليها من أي منطقة أخرى. Logical or physical isolation of critical web applications from other web applications or systems shall be implemented. For example, physical isolation can be achieved by hosting web applications in a completely different separate physical environment, while logical isolation can be achieved by implementing web applications in a separate zone inside the network without allowing access from any other zone.
3-2	عزل تطبيقات الويب الخاصة بالإنتاج منطقياً عن بيئة الاختبار وبيئة التطوير باستخدام محددات الشبكة عن طريق ضبط إعدادات قوائم التحكّم بالوصول (ACL) والسياسات الأمنية على جدران الحماية. Production web applications shall be logically isolated from test and development environments using network

restrictions by configuring Access-Control Lists (ACLs) and security policies on firewalls.	
تقييد الوصول عبر الشبكة لتطبيقات الويب وحصره بمنطقة خوادم الويب، ومنطقة خوادم تطبيقات الويب، ومنطقة الإدارة. Network access to web applications shall be restricted to web servers zones, web applications server zones and management server zone.	4-2
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). A Web Application Firewall (WAF) shall be deployed in front of all web application servers to verify and validate the traffic going to the server. Since WAF devices detect or block web-based and application-based attacks on external-facing services and web applications, any unauthorized traffic shall be blocked and logged. (Additionally, WAF shall be configured to enable IP the intelligence feature and IP geo-location features in order to block blacklisted IPs and specific countries).	5-2
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) على تطبيقات الويب الحساسة وفقاً للمعايير والإجراءات ذات العلاقة في <اسم الجهة>. Configure WAF to mitigate the Open Web Application Security Project (OWASP Top Ten) web applications security risks for critical web applications as per <entity name>'s relevant standards.	6-2
ضبط إعدادات نظام الحماية المتقدمة لاكتشاف ومنع الاختراقات (IPS) وجدار الحماية لتطبيقات الويب (WAF) لإتاحة التواقيع التي تطابق سلوك وبروتوكولات	7-2

	تطبيقات الويب (مثل Oracle OHS، وIIS، وApache، وSQL، وXML، وغيرها). IPS and WAF shall be configured to enable signatures that match the web application behavior and protocols (e.g., Oracle OHS, IIS, Apache, SQL, XML, etc.).
8-2	ضبط إعدادات تقنيات الحماية من البرمجيات الضارة وأنظمة الحماية من التهديدات المتقدمة المستمرة للتحقق من كافة عمليات نقل الملفات المرتبطة بتطبيقات الويب بحثاً عن أي ملفات خبيثة وفقاً لسياسة ومعيار الحماية من البرمجيات الضارة المعتمدين في <اسم الجهة>. Malware protection solution and APT systems shall be configured to check all file transfer operations related to web applications for malicious files as per <entity name>'s Malware Protection Policy and Standard.
9-2	ضبط إعدادات تقنيات وأنظمة حماية تطبيقات الويب لتتبع نموذجاً أمنياً إيجابياً أو نموذج السماح بقائمة محددة من التطبيقات، وذلك من خلال السماح بأنواع محددة من عمليات نقل الملفات، وبروتوكولات ومنافذ محددة، وتطبيقات ويب محددة من المستوى 7، ومتغيرات تطبيقات ويب محددة، وحجب جميع التطبيقات والملفات التي لم يتم ضبط إعداداتها. Web application security solutions and systems shall be configured to follow a positive security model or whitelisting model by allowing only specific file types for transfer, specific protocols and ports, specific layer 7 web applications and specific web application parameters, and denying all files and applications that are not configured.
10-2	استخدام تطبيقات ويب وبروتوكولات اتصالات آمنة مثل بروتوكول نقل النص التشعبي الآمن (HTTPS) وبروتوكول نقل الملفات الآمن (SFTP) وبروتوكول أمن طبقة النقل (TLS) وغيرها. Secure web applications and communication protocols, such HTTPS, SFTP and TLS, shall be used.
3	مراجعة الإعدادات والتحصين (Secure Configuration and Hardening)
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	
1-3	يجب إجراء اختبارات أمنية دورية (مثل تقييم الثغرات الأمنية واختبار الاختراق) وفقاً لسياسات إدارة الثغرات الأمنية واختبار الاختراق المعتمدة في <اسم الجهة>. Regular security testing (such as vulnerability assessments and penetration testing) shall be performed in accordance with <entity name>'s Vulnerability Management and Penetration Testing Policies.
2-3	إجراء اختبارات دورية لتقييم حماية تطبيقات الويب مثل اختبار أمن التطبيقات الثابت (SAST) واختبار أمن التطبيقات الديناميكي (DAST). Web application security assessments, including Static Application Security Testing (SAST) and Dynamic Application Security Testing (DAST), shall be performed regularly.
3-3	تنصيب حزم التحديثات والإصلاحات على تطبيقات الويب ومكوناتها التقنية بانتظام وفقاً لسياسة إدارة التحديثات والإصلاحات المعتمدة في <اسم الجهة>. Web applications shall be regularly patched and updated in accordance with <entity name>'s Patch Management Policy.
4-3	إيقاف الوظائف والخدمات وملفات الإعدادات غير الضرورية أو غير المستخدمة أو تعطيلها. Unnecessary/unrequired services, functionalities and configuration files shall be removed or disabled.
5-3	حجب إمكانية الوصول إلى الملفات والمجلدات المشاركة عبر الشبكة غير الضرورية أو غير اللازمة. Access to unnecessary/unrequired network shared files and directories shall be blocked.
6-3	حماية الشفرة المصدرية وتحصينها. Application source code shall be secured and hardened.

7-3	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. Secure web application images or templates shall be created for all web applications based on the approved configuration standards. Any web application server that becomes compromised shall be reimaged using one of these image templates.
8-3	تخزين النسخ في بيئة آمنة على خوادم مؤمنة والتحقق منها باستخدام أدوات مراقبة سلامة المعلومات دورياً. Images shall be stored in a secure environment on securely configured servers, and shall be regularly validated using integrity monitoring tools.
9-3	يجب مزامنة توقيت تطبيقات الويب من مصادر الوقت المعتمدة من قبل <اسم الجهة>. Web applications shall be configured to synchronize time to <entity name>'s approved time sources.
4	توافر المعلومات (Availability)
الهدف	الحفاظ على توافر تطبيقات الويب الخارجية وحمايتها من هجمات حجب الخدمة (DoS Attacks) وتعطل الخدمة العرضي.
المخاطر المحتملة	إذا لم يتم توفير أنظمة الحماية من هجمات حجب الخدمة وتعطل البنية التحتية، قد تكون تطبيقات الويب هدفاً لهجمات حجب الخدمة، مما قد يسبب انقطاعاً دائماً في الخدمات أو يؤثر على كفاءة تطبيق الويب.
الإجراءات المطلوبة	
1-4	استخدام مبدأ معمارية تطبيقات الويب التوزيعية الذي يعمل على توزيع نقاط التعطل الحاسمة. A web application architecture that eliminates the existence of single points of failure shall be deploy and implemented.
2-4	توفير تقنيات توزيع الجهد (Load Balancer) مثل تقنيات توزيع حركة البيانات والاتصالات.

	Load balancing mechanisms, such as those offered by an application load balancer device, shall be deployed.
3-4	تطبيق آليات تكرار البيانات (Data Replication) على تطبيقات الويب في مواقع التعافي من الكوارث أو المواقع البديلة (Secondary Data Center). Web application data replication mechanisms shall be implemented on Disaster Recovery (DR) or secondary sites.
4-4	توفير نسخة مطابقة لبيئة إنتاج تطبيقات الويب للأنظمة الحساسة في موقع التعافي من الكوارث. An exact replica of critical web application production environment shall be deployed on the Disaster Recovery (DR) site.
5-4	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، وفقاً لسياسة الأمن السيبراني المتعلق بالأطراف الخارجية المعتمدة في <اسم الجهة>. For web applications hosted by third parties, the Service Level Agreement (SLA) shall maintain an acceptable level of web application and services availability in accordance with <entity name>'s Third Party Cybersecurity Policy.
6-4	ضبط إعدادات إعادة توجيه حركة بيانات تطبيقات الويب تلقائياً أو يدوياً لموقع النسخ الاحتياطية أو التعافي من الكوارث في حال تعطل بيئة الإنتاج. Automated or manual web application traffic redirection to the backup or Disaster Recovery (DR) site shall be configured in case of production environment failure.
5	التشفير (Cryptography)
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.

اختر التصنيف

الإجراءات المطلوبة	
1-5	تطبيق تقنيات التشفير مثل أمن طبقة النقل (Transport Layer Security) والشبكات الخاصة الافتراضية (Virtual Private Networks) لحماية تقنيات التحقّق من الهوية (Authentication)، إلى جانب استخدام أحدث بروتوكولات التشفير وخوارزميات التشفير المدعومة (Cipher Suite) وفقاً لمعيار التشفير المعتمد في <اسم الجهة>. Encryption technologies, such as Transport Layer Security (TLS) and Virtual Private Networks (VPN), shall be implemented to protect authentication mechanisms during transmission. In addition, recommended next generation encryption protocols and cipher suites shall be used as per <entity name>'s Cryptography Standard.
2-5	ضبط إعدادات تطبيقات الويب وتمكينها من استخدام بروتوكولات آمنة للتشفير حيثما أمكن، مثل بروتوكول نقل النص التشعبي الآمن (HTTPS) وبروتوكول النقل الآمن (FTP) عبر أمن طبقة النقل (TLS) وغيرها. Web application protocols shall be configured to use encryption wherever applicable (e.g., HTTPS, FTP over TLS, etc.).
3-5	توفير تقنيات التشفير للاتصالات بين الخوادم وأجهزة المستخدمين في تطبيقات الويب (End-to-End Encryption). End-to-end encryption for web applications client/server communications shall be implemented.
4-5	تقييد استخدام بروتوكولات النقل الآمن (SSHv2) وبروتوكول التحكم بسطح المكتب عن بعد (RDP) عن طريق تقنيات التشفير مثل أمن طبقة النقل (TLS). The use of secure encrypted management protocols such as Secure Shell (SSH) v2 and Remote Desktop Protocol (RDP) over TLS shall be restricted.
5-5	استخدام تقنيات التشفير غير التماثلي القائم على شهادات التشفير (الخاص/العام) لكافة تطبيقات الويب العامة والخارجية وفقاً لمعيار التشفير المعتمد في <اسم الجهة>. Certificate based asymmetric (private/public) cryptography shall be used for all public external web applications as per <entity name>'s Cryptography Standard.

6-5	شراء شهادات تشفير تطبيقات الويب من جهة إصدار شهادات موثوقة ومعتمدة وفقاً للمتطلبات التنظيمية والتشريعية ذات العلاقة والتأكّد من تجديدها بشكل دوري. Web application certificates shall be purchased from a trusted CA compliance source and periodically renewed in accordance with the related laws and regulations.
7-5	تثبيت وظائف التشفير وإدارة شهادات التشفير على جدار الحماية لتطبيقات الويب للسيطرة بشكل أكبر على الهجمات والتهديدات. Encryption functionalities and certificate management shall be offloaded on the web application firewall to provide more visibility into threats and attacks.
8-5	تخزين مفاتيح تشفير تطبيقات الويب في مكان ملائم وآمن وفقاً للسياسات والإجراءات ذات العلاقة في <اسم الجهة>. Web applications cryptographic keys shall be stored in a secure vault and physically secure locations as per <entity name>'s relevant policies and procedures.
6	تسجيل الأحداث وسجل التدقيق (Event and Audit Logging)
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	
1-6	تفعيل جميع سجلات الأحداث (سجلات التدقيق والسجلات المتعلقة بالأمن السيبراني) لجميع تطبيقات الويب ومكوناتها التقنية. All levels of logging as well as audit trail and security logs shall be enabled on all web application and technical components.
2-6	جمع سجلات الأحداث الخاصة بالأمن السيبراني في نظام تسجيل مركزي (SIEM) وفقاً لسياسة ومعيار إدارة سجلات الأحداث ومراقبة الأمن السيبراني المعتمدين في <اسم الجهة>.

	Server logging and audit trail shall be configured to be forwarded to a centralized logging system as per <entity name>'s Cybersecurity Event Logs and Monitoring Management Policy and Standard.
7	النسخ الاحتياطي والأرشفة (Backup and Archival)
الهدف	ضمان سلامة بيانات تطبيقات الويب من العبث بها 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	
1-7	عمل نسخ احتياطية كاملة لتطبيقات الويب وترقيمها تسلسلياً وتحديد تاريخها ووقتها وفهرستها وفقاً 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. Full backups for web applications shall be performed, serialized, time-dated and indexed in accordance with <entity name>'s Backup and Recovery Management Policy. The backups must include at minimum web applications' configuration backups, and the stored data and information of web applications.
2-7	تشفير النسخ الاحتياطية لتطبيقات الويب الخاصة بـ<اسم الجهة>. <Entity name>'s web applications backups shall be encrypted.
3-7	تخزين النسخ الاحتياطية من تطبيقات الويب للأنظمة الحساسة الخاصة <باسم الجهة> على الأقل في موقعين ماديين ومعزولين مادياً عن بعضهما البعض. Backups of <entity name>'s web applications for critical systems shall be stored in at least two geographically distinct protected off-sites.
4-7	اختبار إمكانية استرجاع النسخة الاحتياطية كل ثلاثة أشهر أو وفقاً للسياسات والإجراءات ذات العلاقة في <اسم الجهة>.

	Backup recovery test shall be conducted every quarter or in accordance with <entity name>'s relevant policies and procedures.
5-7	استخدام تقنيات توثيق وسلامة النسخ الاحتياطي لضمان نسخ بيانات تطبيقات الويب وأرشفتها بطريقة صحيحة. Backup verification and integrity mechanisms shall be employed to ensure that web application data is correctly backed up and archived.
6-7	أرشفة النسخ الاحتياطية لتطبيقات الويب الخاصة بـ<اسم الجهة> في موقع تخزين معزول مادياً ومنطقياً ووفقاً للسياسات والإجراءات ذات العلاقة في <اسم الجهة>. <Entity name>'s web applications backups shall be archived in an offsite storage for a retention period as per <entity name>'s relevant policies and procedures.
8	تطبيقات الويب الحديثة والسحابية الأصلية (Modernized and Cloud Native Web Applications)
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	
1-8	تطوير منهجية التطوير الآمن وفقاً لآلية "DevSecOps". A DevSecOps methodology and process shall be developed and adopted.
2-8	تطوير نظام التكامل المستمر/التثبيت المستمر (CI/CD) الآمن وتطبيقه باتباع أفضل الممارسات. A secure Continuous Integration/Continuous Deployment (CI/CD) pipeline shall be developed and implemented following best practices.

3-8	تنصيب منصة أمن الحاويات من مورد موثوق لإدارة أمن الحاويات وضمان حماية نظام الحاويات. A container security platform shall be deployed from a trusted vendor to manage container security and ensure that the container system is safe.
4-8	تنصيب حزم التحديثات والإصلاحات دورياً. Security patches shall be regularly deployed.
5-8	توفير حلول إدارة المعلومات الحساسة وذلك من أجل إدارة المعلومات الحساسة والمفاتيح والشهادات ومنع تخزين المعلومات الحساسة في الحاويات. Critical information management mechanisms shall be implemented to manage Confidential information, keys and certifications, and prevent storing confidential information in containers.
6-8	استخدام نسخ الحاويات من مصادر موثوقة أو معتمدة. Container images from trusted or approved sources shall be used.
7-8	عزل البنية التحتية الخاصة بالحاويات. Containers' infrastructure shall be isolated.
8-8	استخدام كشف الثغرات التلقائي لفحص الحاويات قبل وبعد تثبيتها في بيئة الإنتاج. Automated vulnerability detection shall be used to scan containers before and after their deployment into the production environment.
9-8	توفير تقنيات وأدوات المراقبة للتأكد من سلامة تطبيقات الويب وتوافرها وكفاءتها باستمرار. Monitoring tools shall be deployed to regularly monitor applications' health, availability and efficiency.

الأدوار والمسؤوليات

1- **راعي ومالك وثيقة المعيار:** <رئيس الإدارة المعنية بالأمن السيبراني>.

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

3- **تنفيذ المعيار وتطبيقه:** <الإدارة المعنية بتقنية المعلومات>.

الالتزام بالمعيار

1- يجب على <رئيس الإدارة المعنية بالأمن السيبراني> ضمان التزام <اسم الجهة> بهذا المعيار باستمرار.

2- يجب على كافة العاملين في <اسم الجهة> الالتزام بهذا المعيار.

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