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 أمن الخوادم

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	عُدّل بواسطة	أسباب التعديل
<أدخل رقم النسخة>	اضغط هنا لإضافة نص	<أدخل الاسم الكامل للشخص>	<أدخل وصف التعديل>

اختر التصنيف

الإصدار 1.0

قائمة المحتويات

الأهداف

الغرض من هذا المعيار هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بإدارة الخوادم 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 ٢-٣-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

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

المعايير

1	الوصول الآمن (Secure Access)
الهدف	ضمان حماية الخوادم ووظائفها من الوصول غير المصرح به.
المخاطر المحتملة	ينطوي الوصول غير المصرّح به إلى الخوادم على مخاطر عالية قد تؤدي إلى تسريب البيانات أو سرقتها أو تعطيل الخدمات أو انتهاكات أمنية تسمح لمنفذيها باستخدامها لشن المزيد من الهجمات السيبرانية ضد <اسم الجهة> وبنيتها التحتية.
الضوابط	
1-1	استخدام مبدأ الحماية الذي يمنح مشرفي ومُشغّلي الخوادم الحد الأدنى من صلاحيات الوصول إلى مختلف أنواع أنظمة البريد الإلكتروني. Least-privilege security principle shall be used to provide access to different types of email systems to server administrators and operators.
2-1	حصر الوصول إلى الخوادم على مشرفي الخوادم فقط وذلك من خلال منح حق الوصول لحسابات المشرفين المختلفين وبروتوكول الإنترنت لأجهزة المستخدمين باستخدام قوائم التحكم بالوصول (ACLs). Access on servers shall be restricted to server administrators by only allowing access to administrators' individual accounts

and workstation IPs using network Access Control Lists (ACLs).	
إيقاف أو تغيير الحسابات الافتراضية أو غير التفاعلية أو غير اللازمة. Default/non-interactive/unneeded accounts shall be disabled or renamed.	3-1
إلى جانب ضرورة إدخال اسم المستخدم وكلمة المرور، إلزام المستخدم باستعمال آليات أخرى للتحقّق من الهوية مثل السمات الحيوية، والمفاتيح المادية، وكلمات المرور المؤقتة، والبطاقات الذكية، وشهادات التشفير، وغيرها. In addition to a user/password combination, users shall be required to use other authentication mechanisms such as biometrics, hardware keys, one-time passwords, smart cards, certificates, etc.	4-1
إعداد متطلبات تعقيد كلمة المرور الخاصة بالخادم وفقاً لسياسة إدارة هويات الدخول والصلاحيات في <اسم الجهة>. Server password complexity requirements shall be configured in accordance with <entity name>'s Identity and Access Management Policy.	5-1
تطبيق تقنيات التشفير مثل «أمن طبقة النقل» (Transport Layer Security) و«الشبكات الخاصة الافتراضية» (Virtual Private Networks) لحماية آليات التحقّق من الهوية أثناء إرسال الرسائل. واستخدام أحدث بروتوكولات التشفير وخوارزميات التشفير المدعومة (Cipher Suite) المُوصى بها. للمزيد من التفاصيل، يُرجى الرجوع إلى معيار 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. For more details, refer to <entity name>'s Cryptography Standard.	6-1
تطبيق نظام إدارة الصلاحيات الهامة والحسّاسة (PAM) لمنح حق الوصول المؤقت إلى الخوادم القائم على نوع الجلسة المطلوبة.	7-1

A Privilege Access Management (PAM) system shall be implemented to enforce session-based temporary access to servers based on request.	
ضبط وإعداد وقت انتهاء الجلسة وحد إغلاق الجلسة عند عدم الاستخدام وفقاً لسياسات الأمن السيبراني في <اسم الجهة>. Session timeout and session idle lockout shall be configured in accordance with <entity name>'s cybersecurity polices.	8-1
ضبط وإعداد كلمات مرور مُحمِّل تشغيل (Bootloader) نظام الإدخال/الإخراج الأساسي (BIOS). BIOS bootloader passwords shall be configured.	9-1
إلزام مشرفي ومُشغّلي الخوادم باستخدام آلية التحقّق من الهوية متعدّد العناصر للوصول إلى الخوادم الحساسة. Server administrators and operators shall be required to use multi-factor authentication to access critical servers.	10-1
تقييد وصول المشرفين والمشغلين إلى الخوادم الحساسة وحصره على أجهزة الحاسب ذات الصلاحيات والامتيازات الهامة والحساسة (PAWs). Access to critical servers shall be restricted by administrators and operators to be provided through Privileged Access Workstations (PAW) only.	11-1
تقييد الوصول إلى الخوادم وحصره على المشرفين والمشغلين وذلك عن طريق خوادم الوصول إلى المناطق الآمنة (Jump Servers) أو إدارة الصلاحيات الهامة والحسّاسة (PAM). 1-12-1 استخدام خوادم منفصلة للوصول إلى المناطق الآمنة (Jump Servers) لمشرفي ومستخدمي النظام. 2-12-1 استخدام التحقّق من الهوية متعدّد العناصر من أجل الوصول عبر خوادم الوصول إلى المناطق الآمنة (Jump Server) المستخدمة من قبل مشرفي النظام وذلك من خلال تطبيق قوائم التحكم بالوصول (ACLs). 3-12-1 تقييد الوصول إلى خوادم الوصول إلى المناطق الآمنة (Jump Servers) وحصره على المشرفين والمشغلين المصرح لهم فقط. 4-12-1 تقييد الوصول إلى الشبكة وحصره على خوادم الوصول إلى المناطق الآمنة (Jump Servers) من خلال تطبيق قوائم التحكم بالوصول (ACLs).	12-1

	5-12-1 وضع خوادم الوصول إلى المناطق الآمنة (Jump Servers) في منطقة إدارة الشبكة. 6-12-1 إلغاء تفعيل خاصية الوصول إلى الإنترنت على خوادم الوصول إلى المناطق الآمنة (Jump Servers). 7-12-1 إلغاء تفعيل الخدمات الخطرة وغير اللازمة (مثل إرسال رسائل البريد الإلكتروني واستلامها) على خوادم الوصول إلى المناطق الآمنة (Jump Servers). 8-12-1 تفعيل جميع مستويات التسجيل إضافةً إلى سجل التدقيق والسجلات الأمنية محلياً وعلى نظام تسجيل أحداث مركزي. Access to servers shall be restricted by administrators and operators and shall only be provided through a jump server or PAM. 1-12-1 A separate jump server shall be used for system administrators and users. 1-12-2 The use of multi-factor authentication shall be required for the access of jump servers used by system administrators by implementing ACLs. 1-12-3 Access to jump servers shall be restricted to the accounts of authorized administrators and operators only. 1-12-4 Network access shall be restricted to jump servers by implementing ACLs. 1-12-5 Jump servers shall be placed in the network management zone. 1-12-6 Internet access on jump servers shall be disabled. 1-12-7 Unnecessary and risky services (such as sending and receiving emails) shall be disabled on jump servers. 1-12-8 All levels of logging, as well as audit trail and security logs, shall be enabled locally and to a centralized event logging system.
2	مراجعة الإعدادات والتحصين (Secure Hardening Configuration)
الهدف	تحديد متطلبات الأمن الأساسية للخوادم لضمان تصميم الخوادم وإعدادها وتشغيلها بطريقة آمنة.

المخاطر المحتملة	يعتبر الإعداد الخاطئ للخوادم والتصميم الضعيف من الثغرات الأمنية الشائعة التي يمكن استغلالها لتهديد سرية وسلامة وتوافر بيانات <اسم الجهة> وسير عملها.
الضوابط	
1-2	إجراء اختبارات أمنية دورية (مثل تقييم الثغرات الأمنية واختبار الاختراق) وفقاً لسياسة إدارة الثغرات الأمنية المتّبعة في <اسم الجهة>. Regular security testing (such as vulnerability assessments and penetration testing) shall be performed in accordance with <entity name>'s Vulnerability Management Policy.
2-2	إجراء التحديثات والإصلاحات على الخوادم بانتظام وفقاً لسياسة إدارة التحديثات والإصلاحات في <اسم الجهة> لضمان تحديث جميع أنظمة التشغيل وبرمجيات التطبيقات على الخوادم. Servers shall be regularly patched and updated in accordance with <entity name>'s Patch Management Policy to ensure that all servers' OSs and application software are up-to-date.
3-2	حذف أو إلغاء تفعيل التطبيقات والخدمات غير الضرورية أو غير اللازمة من الخوادم مثل خدمات الطباعة، وبروتوكول تل نت (telnet)، وغيره. Unnecessary/unrequired applications and services on servers, such as printing services, telnet, etc., shall be removed or disabled.
4-2	استخدام مبدأ الحماية الذي يمنح مشرفي ومُشغّلي الخوادم الحد الأدنى من صلاحيات الوصول إلى مختلف أنواع الأنظمة. Least-privilege security principle shall be used to provide access to different types of systems to server administrators and operators.
5-2	حصر الوصول إلى الشبكة بمناطق الخوادم ومناطق إدارة الخوادم. Network access shall be restricted to server zones and server management zones.
6-2	حذف أو إلغاء تفعيل خصائص نظام التشغيل والتطبيق وملفات الإعدادات غير الضرورية أو غير اللازمة.

Unnecessary/unrequired OS and application features and configuration files shall be removed/disabled.	
حجب إمكانية الوصول إلى مجلدات الشبكة والملفات غير الضرورية أو غير اللازمة. Access to unnecessary/unrequired network and file directories shall be blocked	7-2
استخدام ضوابط الأجهزة وحجب الوصول إلى وسائط التخزين القابلة للإزالة. Hardware controls shall be used and access to removable media shall be blocked.	8-2
إنشاء البنية التحتية للخوادم تبعاً لبنية متعدّدة الطبقات محمية باستخدام جدران حماية ذات طبقة مزدوجة. وإدراج خادم ويب في منطقة الإنترنت المحايدة، وخوادم التطبيقات في منطقة الإنتاج، وخوادم قواعد البيانات في المنطقة الموثوقة أو منطقة قاعدة البيانات. Server's infrastructure shall be implemented following N-tier architecture protected by a dual layer of firewalls. Specifically, webservers shall be placed in the Internet DMZ, Application Servers shall be placed in the Production Zone, and Database Servers shall be placed in the Trusted/Database zone.	9-2
العزل المادي أو المنطقي لخوادم الأنظمة الحساسة عن الخوادم أو الأنظمة الأخرى. فعلى سبيل المثال، يمكن تحقيق العزل المادي من خلال استضافة الخوادم في بيئة مادية منفصلة ومختلفة تماماً، ويمكن تحقيق العزل المنطقي من خلال تطبيق الخوادم في مناطق منفصلة داخل الشبكة دون السماح بالوصول إليها من أي منطقة أخرى. Critical system servers shall be logically and physically isolated from other servers or systems. For example, physical isolation can be achieved by hosting the servers in a completely different separate physical environment, while logical isolation is achieved by implementing servers in a separate zone inside the network without allowing access from any other zone.	10-2
ضبط إعدادات وتحصين الخوادم بما في ذلك التحصين على مستوى التطبيقات وقاعدة البيانات ونظام التشغيل. Server configuration hardening shall be configured, including application, database, and operating system level hardening.	11-2
إنشاء نسخ أو قوالب آمنة لكافة الخوادم بناءً على معايير الإعدادات المعتمدة، وإعادة نسخ الخوادم باستخدام أحد قوالب نسخ الخوادم في حال تعرضها لانتهاك أمني.	12-2

	Secure server images or templates shall be created for all servers based on the approved configuration standards. Any server or system that becomes compromised shall be reimaged using one of these server image templates.
13-2	تخزين نسخ الخوادم في بيئة آمنة على خوادم معدة بصورة آمنة والتحقق بانتظام من هذه النسخ باستخدام أدوات مراقبة سلامة المعلومات. Server images shall be stored in a secure environment on securely configured servers and shall be regularly validated using integrity monitoring tools.
14-2	تطبيق الفصل المنطقي أو المادي للخوادم بين بيئات الإنتاج والتطوير والاختبار. Logical or physical segregation for servers among production, development and testing environments shall be implemented.
3	النسخ الاحتياطي والأرشفة (Backup and Archiving)
الهدف	ضمان سلامة بيانات الخوادم وتوافرها وقابلية استعادتها والتأكد من عدم العبث بها أو فقدانها بالخطأ أو تخريبها.
المخاطر المحتملة	في حال حذف بيانات الخوادم أو فقدانها بالخطأ أو العبث بها أو تخريبها أو تعرّضها إلى هجوم إلكتروني، لن تتمكّن <اسم الجهة> من استرداد البيانات مما سيؤثّر على أنشطة أعمالها الاعتيادية.
الضوابط	
1-3	عمل نسخة احتياطية كاملة للخوادم وفقاً لسياسة إدارة النسخ الاحتياطية المعتمدة في <اسم الجهة>. يجب أن تشمل النسخ الاحتياطية على الأقل نسخاً احتياطية لنظام تشغيل الخوادم، ونسخاً احتياطية لإعدادات التطبيقات، ونسخاً احتياطية لإعدادات قواعد البيانات، وقواعد البيانات والمعلومات المخزنة. Full backup for server shall be performed in accordance with <entity name>'s Backup and Recovery Management Policy. Backups must include, at minimum, servers operating system backup, applications configuration backup, database configuration backup, and stored databases and information.
2-3	تشفير النسخ الاحتياطية للخوادم في <اسم الجهة>. <Entity name>'s server backups shall be encrypted.

3-3	إضافة ترتيب تسلسلي للنسخ الاحتياطية عن الخوادم الخاصة <بالجهة> وتسجيل وقتها وتاريخها وجدولتها. <Entity name>'s server backups shall be serialized, time-dated and indexed.
4-3	تخزين النسخ الاحتياطية عن الخوادم الخاصة بـ<اسم الجهة> في موقعين خارجيين محميّين منفصلين على الأقل. <Entity name>'s server backups shall be stored in at least two geographically distinct protected off-sites.
5-3	اختبار إمكانية استرجاع النسخة الاحتياطية كل ثلاثة أشهر وفقاً لسياسة إدارة النسخ الاحتياطية المعتمدة في <اسم الجهة>. Backup recovery shall be regularly tested every quarter or in accordance with <entity name>'s Backup and Recovery Management Policy.
6-3	تطبيق آليات توثيق النسخ الاحتياطية وسلامتها لضمان نسخ بيانات أجهزة المستخدمين أو أرشفتها بطريقة صحيحة. Backup verification and integrity mechanisms shall be implemented to ensure that data is being correctly backed up or archived.
7-3	أرشفة النسخ الاحتياطية لخوادم <اسم الجهة> في موقع تخزين غير مرتبط بالشبكة طوال فترة التخزين المعتمدة وفقاً لسياسة إدارة النسخ الاحتياطية في <اسم الجهة>. <Entity name>'s server backups shall be archived in an offsite storage location for the entire approved retention period and as per <entity name>'s Backup and Recovery Management Policy.
4	حماية الخوادم (Server Protection)
الهدف	ضمان حماية الخوادم من الفيروسات والبرمجيات الضارة والتهديدات المتقدّمة المستمرة والهجمات غير المعروفة مسبقاً وأي نوع آخر من الهجمات الخبيثة.
المخاطر المحتملة	يمكن أن تؤدي الهجمات الخبيثة الناجحة على الخوادم إلى تعريض <اسم الجهة> لاختراق أمني أو وصول غير مصرح به أو الكشف عن البيانات في حال تركت الخوادم دون حماية.

الضوابط	
1-4	ضبط وإعداد حد إغلاق نظام التشغيل ووظائف التطبيقات عن طريق الحد الأدنى من الصلاحيات والامتيازات المطلوب للتشغيل في الظروف الاعتيادية، مثل إلغاء تفعيل تغيير وقت النظام يدوياً، والإغلاق/إعادة التشغيل، وتعديل ملفات النظام، وإنشاء/تعديل/حذف الملفات، وغيرها. OS and application functionality lockout shall be configured with the least privilege required to operate in normal conditions. For example, changing system time manually, shutting down/restarting, editing system files, creating/modifying/deleting files, etc., shall be disabled.
2-4	تطبيق خاصية السماح بقائمة محددة من التطبيقات على الخوادم لتمكين عمل تطبيقات وبرمجيات محددة فقط وفقاً للحاجة. Application whitelisting shall be enabled on servers to allow only specific applications and software to run based on need.
3-4	إعداد أنظمة السماح بقائمة محددة من التطبيقات بحيث لا يمكن للمستخدمين إلغاء تفعيل الأنظمة باستثناء مديري النظام عند أدائهم لمهام إدارية معينة تقتضي إلغاء تفعيل السماح بقائمة محددة من التطبيقات مؤقتاً. Application whitelisting agents shall be configured so that users cannot disable the agents with the exception of administrators when performing specific administrative tasks that would require disabling application whitelisting temporarily.
4-4	تعريف الملفات التنفيذية المعتمدة (exe, com, pif, وغيرها) ومكتبات البرمجيات (dll, ocx, وغيرها) والنصوص (ps1, bat, vbs, وغيرها) وبرامج التثبيت (msi, msp, وغيرها). A list of approved executables (exe, com, pif, etc.), software libraries (dll, ocx, etc.), scripts (ps1, bat, vbs, etc.), and installers (msi, msp, etc.) shall be defined.
5-4	تطبيق خاصية السماح بقائمة محددة من التطبيقات لاستخدام قواعد التجزئة المشفرة أو قواعد شهادات الناشر أو قواعد المسار للسماح باستخدام التطبيقات أو منعها.

Application whitelisting shall be implemented to use cryptographic hash rules, publisher certificate rules or path rules to allow or restrict the use of applications.	
ضبط وإعداد مجلدات التطبيقات وفقاً لتصاريح نظام الملفات لمنع أي تعديل غير مصرح به على المجلد أو تصاريح الملفات. Application folders shall be configured with file system permissions to prevent unauthorized modification of folder and file permissions.	6-4
تمكين وظيفة الحماية على الخوادم لاستخدامها في إجراءات الحد من المخاطر على نظام التشغيل وإجراءات الحد من المخاطر لتطبيقات معينة. Exploit protection functionality shall be enabled on servers with both operating system mitigation measures and application-specific mitigation measures.	7-4
تطبيق نظام الحماية المتقدمة لاكتشاف ومنع الاختراقات في المستضيف (Host-based Intrusion Prevention System "HIPS") على جميع الخوادم. Host-based Intrusion Prevention System (HIPS) shall be implemented on all servers.	8-4
تطبيق جدار حماية من البرمجيات المستضافة على جميع الخوادم. Software host firewall shall be implemented on all servers.	9-4
تطبيق برامج مكافحة الفيروسات على جميع الخوادم. Antivirus shall be implemented on all servers.	10-4
تطبيق حماية النهاية الطرفية (Endpoint Protection) على جميع الخوادم. Endpoint protection shall be implemented on all servers.	11-4
تطبيق برامج الحماية من التهديدات المتقدمة المستمرة (APT) على جميع الخوادم. Advanced Persistent Threat agents shall be implemented on all servers.	12-4
تطبيق برمجيات التحكم بأجهزة النهاية الطرفية على كافة الخوادم لمنع الاستخدام غير المصرح به للأجهزة.	13-4

	Endpoint device control software shall be implemented on all servers to prevent the use of unauthorized devices.
14-4	تطبيق منع تسّرب البيانات (DLP) عند الضرورة. Data Leakage Prevention (DLP) shall be implemented where required.
15-4	تطبيق جميع المتطلبات بموجب سياسة الحماية من البرمجيات الضارة المعتمدة في <اسم الجهة>. All requirements under <entity name>'s Malware Protection Policy shall be implemented.
5	تسجيل الأحداث وسجل التدقيق (Event and Audit Logging)
الهدف	ضمان الحفاظ على سريّة بيانات الخوادم والتأكّد من سلامتها وموثوقيتها لحمايتها من الوصول غير المصرّح به والكشف عن المعلومات الحسّاسة.
المخاطر المحتملة	إمكانية التأكّد من سلامة البيانات وموثوقيتها على الخوادم لحماية <اسم الجهة> من الهجمات الخبيثة والكشف عن المعلومات المهمّة والحسّاسة والوصول غير المصرّح به.
الضوابط	
1-5	ضبط وإعداد سجل الخوادم وسجل التدقيق ليتم ترحيلها إلى نظام تسجيل مركزي وفقاً لسياسة ومعيار إدارة سجلات الأحداث ومراقبة الأمن السيبراني 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.
2-5	إعداد الخوادم ليتزامن وقتها مع ثلاثة خوادم زمنية إضافية على الأقل في غضون أجزاء من الثانية بطريقة ممكنة تقنياً مما يسمح باتساق الأختام الزمنية في السجلات. Servers shall be configured to synchronize time to at least three redundant central time servers within milliseconds where technically possible so that timestamps in logs are consistent.
3-5	ضبط إعدادات الخوادم ذات الخطورة العالية التي تعتمد عادةً على التسجيل المركزي لحفظ سجلات أنظمة التشغيل في حال تعطّل اتصال الشبكة.

	High risk servers that normally rely on centralized logging shall be configured to maintain local logs in the event that network connectivity fails.
6	التشفير (Cryptography)
الهدف	ضمان الحفاظ على سريّة بيانات الخوادم والتأكّد من سلامتها وموثوقيتها لحمايتها من الوصول غير المصرّح به والكشف عن المعلومات الحسّاسة.
المخاطر المحتملة	إمكانية التأكّد من سلامة البيانات وموثوقيتها على الخوادم لحماية <اسم الجهة> من الهجمات الخبيثة والكشف عن المعلومات المهمّة والحسّاسة والوصول غير المصرّح به.
الضوابط	
1-6	تطبيق تقنيات التشفير مثل «أمن طبقة النقل» (Transport Layer Security) و«الشبكات الخاصة الافتراضية» (Virtual Private Networks) لحماية آليات التحقّق من الهوية أثناء إرسال الرسائل. واستخدام أحدث بروتوكولات التشفير وخوارزميات التشفير المدعومة (Cipher Suite) المُوصى بها. لمزيد من التفاصيل، يُرجى الرجوع إلى معيار 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. For more details, refer to <entity name>'s Cryptography Standard.
2-6	تشفير وسائط التخزين في الخوادم بما في ذلك الأقراص الصلبة، ووسائط التخزين الملحقة بالشبكة (NAS)، ووسائط التخزين المتصلة بشبكة التخزين (SAN)، أو أي نوع آخر من وسائط التخزين المتصلة. Servers storage media shall be configured, including hard disks, Network Attached Storage (NAS), Storage Area Network (SAN) connected storage, or any other type of connected storage.
3-6	استخدام بروتوكول إدارة الخوادم الذي يدعم التشفير أو يقوم بضبط إعدادات التشفير لبروتوكولات إدارة الخوادم، مثل بروتوكول النفاذ إلى الدليل البسيط (LDAP) على أمن طبقة النقل (TLS)، والنسخة الثالثة من بروتوكول إدارة الشبكة البسيط (SNMPv3) لغايات المصادقة والخصوصية، وبروتوكول كيربيروس (Kerberos) مع أمن طبقة النقل (TLS)، وسجل النظام المشفر، وغيرها.

	Server management protocol that supports encryption or configures encryption for server management protocols, such as LDAP over TLS, SNMPv3 with authentication and privacy, Kerberos with TLS, encrypted syslog, etc., shall be used.
4-6	إعداد التشفير لتطبيقات الخوادم وبروتوكولات الاتصال بقواعد البيانات، مثل بروتوكول نقل النص التشعبي الآمن (HTTPS)، وواجهة برمجة التطبيقات الآمنة (API)، وتشفير البيانات الشفاف (TDE)، أو برنامج (SQL) على أمن طبقة النقل (TLS)، وبروتوكول نقل الملفات الآمن (SFTP)، وبروتوكول النقل الآمن (SSHv2)، وغيرها. Encryption for server application and database communication protocols, such as HTTPS, Secure API, TDE or SQL with TLS, SFTP, SSHv2, etc., shall be configured.
7	أمن البيئة الافتراضية (Virtual Security)
الهدف	تحديد المتطلبات الهامة للخوادم الموجودة في البيئة الافتراضية لضمان تصميم الخوادم الافتراضية وإعدادها وتشغيلها بطريقة آمنة.
المخاطر المحتملة	يعتبر الإعداد الخاطئ والتصميم الضعيف للبيئة الافتراضية والافتقار إلى الأنظمة الافتراضية الآمنة من الثغرات الأمنية التي يمكن استغلالها لتهديد سرية وسلامة وتوافر بيانات <اسم الجهة> وسير عملها.
الضوابط	
1-7	إعداد وضبط الحدود لكافة أشكال استخدام مصادر البيئة الافتراضية الموجودة على الخوادم. Limits for all server VM resources use shall be configured.
2-7	تطبيق حل إعدادات الخوادم الافتراضية مركزي. A centralized server VM configuration solution shall be implemented.
3-7	فصل الأجهزة الطرفية غير المستخدمة في بيئة الأنظمة الافتراضية لكافة الخوادم. Unused peripheral devices in the virtualization environment shall be disconnected for all servers.
4-7	تطبيق وإعداد جدار الحماية وخصائص منع التسلل والاختراق للحركة بين الخوادم الافتراضية حتى لو كانت موجودة في نفس الخادم أو المستضيف المادي (الحركة بين الخوادم "East-West traffic").

Firewalling and intrusion inspection and prevention features shall be implemented and configured for traffic between virtual servers even within the same physical server or host (East-West traffic).	
إعداد شبكات محلية افتراضية (VLANs) للاتصال بين الخادم المستضيف والخادم الضيف بصورة تختلف عن الاتصالات بين الخوادم الافتراضية. Separate VLANs for communication between host and guest server VMs shall be configured to be different than server VM to server VM communication.	5-7
إعداد متحكم منفصل بواجهة شبكة (NIC) في جميع الخوادم الافتراضية للإدارة المتصلة بشبكة افتراضية محلية مستقلة للإدارة. A separate NIC shall be configured on all server VMs for management connected to a separate out-of-band management VLAN.	6-7
إعداد بروتوكولات الإنترنت الثابتة على الخوادم الافتراضية. Static IPs shall be configured on server VMs.	7-7
استخدام البروتوكولات الإدارية التي تدعم التشفير مثل أمن طبقة النقل (TLS)، وبروتوكول النقل الآمن (SSH)، وبروتوكول نقل النص التشعبي الآمن (HTTPS)، وغيرها. Management protocols that support encryption, such as TLS, SSH, HTTPS, etc., shall be utilized.	8-7
تقييد إدارة بيئة الأنظمة الافتراضية وحصرها على المشرفين المعنيين فقط. تشمل إدارة الأنظمة الافتراضية: • إنشاء الخوادم الافتراضية وتثبيتها وبدء تشغيلها ونقلها وإغلاقها وإزالتها. • إعداد وتغيير المتحكم بواجهة الشبكة (NIC) والشبكة المحلية الافتراضية (VLAN) ومفتاح التحويل الافتراضي (Vswitch). • إدارة الخوادم الافتراضية وإعدادات الوصول. Virtualization environment management shall be restricted to respective administrators only. Virtualization management includes: • VM creation, deployment, initialization, migration, shutdown, or deletion.	9-7

	• NIC, VLAN and Vswitch configuration and change. • VM administration and access configuration
10-7	عمل نسخة احتياطية على الخوادم الافتراضية وفقاً لسياسة إدارة النسخ الاحتياطية المعتمدة في <اسم الجهة>. Regular VM backup shall be performed in accordance with <entity name>'s Backup and Recovery Management Policy.
11-7	إلغاء تفعيل مشاركة الملفات بين البيئات الافتراضية للخوادم والمستضيف. File sharing between host and server VMs shall be disabled.
12-7	تطبيق وإعداد نظام أمان ذو طبقة مزدوجة للبيئة الافتراضية وعزل بيئة الإنتاج عن بيئات الاختبار الافتراضية. Layer-2 security shall be configured for the virtual environment, and production environment shall be separated from VMs test environments.
13-7	إعداد شعارات التحذير والتصريح على خوادم المضيف والضيف لإنذار الأشخاص غير المصرح لهم من الاستخدام غير السليم للخادم. Warning and authorization banners shall be configured on both host and guest servers to warn unauthorized users who improperly use a server.
14-7	تسجيل جميع الأنشطة المتعلقة بالأجهزة الافتراضية بما في ذلك الإنشاء والنشر والترحيل والحذف. All activities related to virtual machines, including creation, deployment, migration and deletion, shall be logged.
8	إدارة الخوادم (Central Management)
الهدف	تحديد المتطلبات الأمنية لإدارة الخوادم لضمان إدارة وتشغيل الخوادم بطريقة آمنة وضمان تطبيق وتنفيذ جميع المتطلبات الأمنية.
المخاطر المحتملة	يؤدي الافتقار إلى الإدارة الآمنة وعدم تطبيق المتطلبات الأمنية على الخوادم إلى زيادة احتمالية التعرض للهجمات ووجود الثغرات ونقاط الضعف في بيئة <اسم الجهة>، حيث يمكن استغلال هذه الثغرات في الهجمات أو الاختراقات الخبيثة التي تعرض الخوادم والبيانات في <اسم الجهة> إلى انتهاكات أمنية.

الضوابط	
1-8	إعداد خادم الإدارة المركزية أو خادم النطاق ليطبق سياسات الإعدادات والتحصين المعتمدة في <اسم الجهة> على جميع الخوادم. Central management server or domain server shall be configured to enforce <entity name>'s Configuration and Hardening policies on all servers.
2-8	تثبيت أدوات إدارة إعدادات النظام التي تقوم تلقائياً بتنفيذ وإعادة تثبيت إعدادات الضبط والتهيئة للأنظمة في فترات زمنية محددة ومنتظمة. System configuration management tools that automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals shall be deployed.
3-8	تطبيق نظام مراقبة الإعدادات المتوافقة مع بروتوكول أتمتة محتوى الأمن (Security Content Automation Protocol "SCAP") للتأكد من عناصر الإعدادات الأمنية كافة وجدولة الاستثناءات المعتمدة والإبلاغ عن حدوث أي تغييرات غير مصرّح بها. Configuration monitoring system compliant with Security Content Automation Protocol (SCAP) shall be implemented to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.

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 دورياً.

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>.