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 أمن الخوادم

استبدل <اسم الجهة> باسم الجهة في مجمل صفحات الوثيقة.
وللقيام بذلك، اتبع الخطوات التالية:

1. اضغط على مفتاحي "Ctrl" و"H" بالوقت 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>

قائمة المحتويات

الأهداف

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بالخوادم (Servers) الخاصة بـ<اسم الجهة> لتقليل المخاطر السيبرانية وحمايتها من التهديدات الداخلية والخارجية من خلال التركيز على الأهداف الأساسية للحماية وهي: سرية المعلومات، وسلامتها، وتوافرها.

وتهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي 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

تغطي هذه السياسة جميع الخوادم الخاصة بـ<اسم الجهة>، وتنطبق على جميع العاملين في <اسم الجهة>.

بنود السياسة

1- البنود العامة

1-1 يجب تحديد جميع الخوادم الخاصة بـ<اسم الجهة> وتوثيقها، والتأكد من أن برمجيات الخوادم محدثة ومعتمدة.

2-1 يجب تطوير وتطبيق معايير تقنية أمنية (Technical Security Standards) للخوادم المستخدمة داخل <اسم الجهة> باستخدام أفضل المعايير الدولية.

3-1 يجب ضبط إعدادات الخوادم وفقاً للمعايير التقنية الأمنية المعتمدة قبل تشغيل الخوادم في بيئة الإنتاج.

4-1 يجب توفير الحماية اللازمة لجميع الخوادم للسيطرة على مخاطر الأمن السيبراني ذات العلاقة.

5-1 يجب عمل نسخ احتياطية منتظمة للخوادم وفقاً لسياسة إدارة النسخ الاحتياطية المعتمدة في <اسم الجهة> لضمان إمكانية استعادتها في حال تعرّضها لتلف أو حادث غير مقصود. (توصي الهيئة بعمل نسخ احتياطية يومياً للأنظمة الحساسة).

6-1 يجب تحديث برمجيات الخوادم بما في ذلك أنظمة التشغيل وبرامج التطبيقات وتزويدها بأحدث حزم التحديثات والإصلاحات الأمنية وفقاً لسياسة إدارة التحديثات والإصلاحات المعتمدة في <اسم الجهة>.

2- إعدادات الخوادم

1-2 يجب اعتماد صورة (Image) لإعدادات وتحصين أنظمة تشغيل الخوادم الخاصة بـ<اسم الجهة> وحفظها في مكان آمن وفقاً للمعايير التقنية الأمنية المعتمدة.

2-2 يجب استخدام صورة (Image) معتمدة لتثبيت أنظمة تشغيل الخوادم أو تحديثها.

3-2 يجب اعتماد إعدادات وتحصين الخوادم، ومراجعتها وتحديثها دورياً، وكل ستة أشهر على الأقل بالنسبة لخوادم الأنظمة الحساسة (CSCC-6-1-3-2).

3- الوصول والإدارة

1-3 يجب تقييد الوصول إلى الخوادم الخاصة بـ<اسم الجهة> بحيث يكون الوصول متاحاً للمستخدمين المصرح لهم وعند الحاجة فقط.

2-3 يجب تقييد الدخول إلى الخوادم وحصره على حسابات مشرفي الأنظمة ومراجعة الحسابات والصلاحيات الممنوحة للمشرفين بشكل دوري.

3-3 يجب تقييد الوصول إلى الخوادم الخاصة بالأنظمة الحساسة وحصره على الفريق التقني ذي الصلاحيات الهامة وذلك عن طريق أجهزة حاسب (Workstations)، كما يجب عزل هذه الأجهزة في شبكة خاصة لإدارة الأنظمة (Management Network)، ومنع ارتباطها بأي شبكة أو خدمة أخرى (مثل خدمة البريد الإلكتروني والإنترنت).

4-3 يجب استخدام التحقق من الهوية متعدد العناصر (Multi-Factor Authentication) للدخول إلى الخوادم الخاصة بالأنظمة الحساسة (CSCC-3-1-2-2).

5-3 يجب إيقاف الحسابات المصنعية والافتراضية أو تغييرها، وإيقاف الخدمات غير المستخدمة، ومنافذ الشبكة غير المستخدمة في نظام التشغيل (Operating System).

6-3 يجب حماية البيانات المخزنة على الخوادم وتشفيرها بالتوافق مع ضوابط التشفير المعتمدة بناءً على تصنيفها وحسب المتطلبات التشريعية والتنظيمية ذات العلاقة. (ECC-2-8-3-3).

4- حماية الخوادم

1-4 يجب أن تُمنَع الخوادم غير المحدّثة أو غير الموثوقة من الاتصال بشبكة <اسم الجهة> ووضعها في شبكة معزولة لأخذ التحديثات اللازمة لتقليل المخاطر السيبرانية ذات العلاقة والتي قد تؤدي إلى الوصول غير المصرّح به أو دخول البرمجيات الضارة أو تسرّب البيانات.

2-4 يجب استخدام تقنيات وآليات الحماية الحديثة والمتقدمة للحماية من الفيروسات (Virus) والبرامج والأنشطة المشبوهة والبرمجيات الضارة (Malware) وإدارتها بشكل آمن.

3-4 يجب السماح فقط بقائمة محددة من ملفات التشغيل (Whitelisting) للتطبيقات والبرامج للعمل على الخوادم الخاصة بالأنظمة الحساسة (CSCC-2-3-1-1).

4-4 يجب تقييد استخدام وسائط التخزين الخارجية على الخوادم، ويجب الحصول على إذن مسبق من <الإدارة المعنية بالأمن السيبراني> قبل استخدامها، والتأكد من استخدامها بشكل آمن.

5-4 يجب تثبيت الخوادم في المنطقة المناسبة من مخطط/هيكل الشبكة حسب المتطلبات التشغيلية والتشريعية لها لضمان إدارتها وتطبيق الحماية اللازمة عليها بشكل فعّال.

5- المتطلبات التشغيلية لإدارة الخوادم

1-5 يجب إدارة الخوادم مركزياً في <اسم الجهة> لكشف المخاطر بصورة أسرع، وتسهيل إدارة ومراقبة الخوادم مثل تقييد الوصول وتثبيت حزم التحديثات وغيرها.

2-5 يجب توفير الحماية اللازمة للخوادم التي تعمل في بيئة الأنظمة الافتراضية (Virtual Environment) وإدارتها بشكل آمن حسب تقييم المخاطر.

اختر التصنيف

متاح

3-5 يجب ضبط إعدادات الخوادم وتفعيل إرسال سجلات الأحداث إلى نظام السجلات والمراقبة (SIEM) وفقاً لسياسة إدارة سجلات الأحداث ومراقبة الأمن السيبراني.

4-5 يجب مزامنة توقيت جميع الخوادم مركزياً (Clock Synchronization) من مصدر دقيق وموثوق ومعتمد.

5-5 يجب توفير المتطلبات اللازمة لتشغيل الخوادم بشكل آمن وملائم، مثل توفير بيئة مناسبة وآمنة وتقييد الوصول المادي إلى منطقة الخوادم للعاملين المصرح لهم فقط ومراقبته.

6-5 يجب على <الإدارة المعنية بتقنية المعلومات> مراقبة مكونات الخوادم التشغيلية والتأكد من فعالية أدائها، وتوافرها، وتوفير سعة تخزينية مناسبة، ونحو ذلك.

6- إدارة الثغرات واختبار الاختراق

1-6 يجب فحص الخوادم واكتشاف الثغرات الموجودة فيها ومعالجتها بناءً على تصنيف الثغرات المكتشفة والمخاطر السيبرانية المترتبة عليها دورياً، ومرة واحدة شهرياً على الأقل بالنسبة لخوادم الأنظمة الحساسة (CSCC-2-9-1-2).

2-6 يجب تنفيذ عمليات اختبار الاختراق على الخوادم دورياً، وكل ثلاثة أشهر على الأقل على خوادم الأنظمة الحساسة (CSCC-2-10-2).

3-6 يجب تثبيت حزم التحديثات والإصلاحات الأمنية لمعالجة الثغرات ورفع مستوى كفاءة الخوادم وأمنها، حسب سياسة إدارة التحديثات والإصلاحات.

7- الحماية المادية والبيئية للخوادم

1-7 يجب رصد ومراقبة الدخول والخروج من مرافق <اسم الجهة>، على سبيل المثال الأبواب والأقفال.

2-7 يجب رصد ومراقبة العوامل البيئية كالتدفئة وتكييف الهواء والدخان وأجهزة إنذار الحريق وأنظمة إخماد الحرائق.

3-7 يجب الالتزام بوضع الضوابط الأمنية المادية المناسبة (مثل كاميرات المراقبة داخل وخارج مركز بيانات <اسم الجهة>، وحراس الأمن، وتأمين الكابلات، وغيرها).

8- متطلبات أخرى

1-8 يجب استخدام مؤشر قياس الأداء (Key Performance Indicator "KPI") لضمان التطوير المستمر لحماية الخوادم.

2-8 يجب مراجعة متطلبات الأمن السيبراني الخاصة بإدارة الخوادم سنوياً على الأقل، أو في حال حدوث تغييرات في المتطلبات التشريعية أو التنظيمية أو المعايير ذات العلاقة.

الأدوار والمسؤوليات

1- **راعي ومالك وثيقة 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>.

الالتزام بالسياسة

1- يجب على <رئيس الإدارة المعنية بالأمن السيبراني> ضمان التزام <اسم الجهة> بهذه السياسة دورياً.

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>.