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

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 "<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.

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	عُدِّلَ 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

قائمة المحتويات

الغرض

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

تمت موائمة هذه السياسة مع الضوابط والمعايير الصادرة من الهيئة الوطنية للأمن السيبراني والمتطلبات التنظيمية والتشريعية ذات العلاقة.

نطاق العمل

تغطي هذه السياسة جميع الأصول التقنية والمعلوماتية (شاملة الخوادم) الخاصة ب<اسم الجهة>، وتنطبق على جميع العاملين (الموظفين والمتعاقدين) في <اسم الجهة>.

بنود السياسة

١- البنود العامة

١-١ يجب تحديد وتوثيق جميع الخوادم الخاصة ب<اسم الجهة>، وتسجيلها تحت إدارة فريق تشغيلي معين مسؤول عن العمليات التشغيلية والأمنية وفقًا لسياسات <اسم الجهة> والمتطلبات التشريعية والتنظيمية ذات العلاقة.

١-٢ يجب تطوير وتوثيق واعتماد ومراجعة المعايير التقنية الأمنية (Technical Security Standards) للخوادم المستخدمة داخل <اسم الجهة>، وفقًا لأفضل الممارسات الدولية والسياسات والإجراءات التنظيمية المعتمدة لدى <اسم الجهة>، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

١-٣ يجب ضبط إعدادات الخوادم وفقًا للمعايير التقنية الأمنية المعتمدة قبل تشغيل الخوادم في البيئة التشغيلية

١-٤ يجب عمل نسخ احتياطية منتظمة للخوادم وفقًا لسياسة إدارة النسخ الاحتياطية المعتمدة لدى <اسم الجهة> لضمان إمكانية استعادتها في حال تعرّضها لتلف أو حادث غير مقصود.

١-٥ يجب استخدام التقنيات الأمنية اللازمة وتعطيل وإعادة استخدام الخوادم التي تحوي معلومات مصنفة بشكل آمن وفقًا للسياسات والمتطلبات التشريعية والتنظيمية ذات العلاقة.

١-٦ يجب تحديث برمجيات الخوادم بما في ذلك أنظمة التشغيل وبرامج التطبيقات وتزويدها بأحدث حزم التحديثات والإصلاحات الأمنية وفقًا لسياسة إدارة التحديثات والإصلاحات المعتمدة في <اسم الجهة>.

١-٧ يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر والاستخدام الصحيح والفعال لمتطلبات حماية الخوادم.

٢- إعدادات الخوادم

٢-١ يجب تطبيق متطلبات الإعدادات والتحصين المعتمدة لدى <اسم الجهة>.

٢-٢ يجب تعطيل الخوادم والتطبيقات غير المستخدمة وفقًا للمعايير التقنية الأمنية المعتمدة.

٢-٣ يجب اعتماد إعدادات وتحصين الخوادم، ومراجعتها وتحديثها <سنويًا>، وتطبيق ذلك كل ستة أشهر على الأقل بالنسبة لخوادم الأنظمة الحساسة.

٢-٤ يجب تغيير كلمات المرور الثابتة للخوادم وفقًا للمعايير التقنية الأمنية المعتمدة لدى <اسم الجهة>.

٣- الوصول والإدارة

٣-١ يجب تقييد الوصول إلى الخوادم الخاصة ب<اسم الجهة> بحيث يكون الوصول متاحًا للمستخدمين المصرح لهم وعند الحاجة فقط.

٣-٢ يجب تقييد الدخول إلى الخوادم والأنظمة الحساسة وحصره على حسابات مشرفي الأنظمة ومراجعة الحسابات والصلاحيات الممنوحة للمشرفين بشكل دوري وفقًا لسياسة إدارة هويات الدخول والصلاحيات المعتمدة لدى <اسم الجهة>.

٣-٣ يجب تقييد الوصول إلى الخوادم الخاصة بالأنظمة الحساسة وحصره على الفريق التقني ذو الصلاحيات الهامة وذلك عن طريق أجهزة حاسب (Workstations) فقط وعدم استخدام أجهزة محمولة، كما يجب عزل هذه الأجهزة في شبكة خاصة لإدارة الأنظمة (Management Network)، ومنع ارتباطها بأي شبكة أو خدمة أخرى (مثل خدمة البريد الإلكتروني والإنترنت).

٣-٤ يجب استخدام التحقق من الهوية متعدد العناصر (Multi-Factor Authentication) للدخول إلى الخوادم الخاصة بالأنظمة الحساسة.

٣-٥ يجب إيقاف الحسابات المصنعية والافتراضية (Default Accounts) أو تغييرها، وإيقاف الخدمات غير المستخدمة، ومنافذ الشبكة غير المستخدمة في نظام التشغيل (Operating System) على جميع الخوادم.

٣-٦ يجب حماية البيانات المخزنة على الخوادم وتشفيرها بالتوافق مع سياسة التشفير المعتمدة لدى <اسم الجهة> بناءً على تصنيفها وفقاً للمتطلبات التشريعية والتنظيمية ذات العلاقة.

٤- حماية الخوادم

٤-١ يجب تحديث 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.

٤-٢ يجب استخدام تقنيات وآليات الحماية الحديثة والمتقدمة على جميع الخوادم للحماية من الفيروسات (Virus) والبرامج والأنشطة المشبوهة والبرمجيات الضارة (Malware) وغير المعروفة (Zero-Day) وإدارتها بشكل آمن.

٤-٣ يجب السماح فقط بقائمة محددة من ملفات التشغيل (Whitelisting) للتطبيقات والبرامج للعمل على الخوادم الخاصة بالأنظمة الحساسة.

٤-٤ 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.

٤-٥ يجب تثبيت الخوادم في المنطقة المناسبة من مخطط/هيكل الشبكة حسب المتطلبات التشغيلية والتشريعية لها لضمان إدارتها وتطبيق الحماية اللازمة عليها بشكل فعّال.

٥- المتطلبات التشغيلية لإدارة الخوادم

٥-١ يجب إدارة الخوادم مركزيًا في <اسم الجهة> لكشف المخاطر بصورة أسرع، وتسهيل إدارة ومراقبة الخوادم مثل تقييد الوصول وتثبيت حزم التحديثات وغيرها.

٥-٢ يجب توفير الحماية اللازمة للخوادم التي تعمل في بيئة الأنظمة الافتراضية (Virtual Environment) وإدارتها بشكل آمن بناءً على تقييم المخاطر السيبرانية.

٥-٣ يجب ضبط إعدادات الخوادم وتفعيل إرسال سجلات الأحداث إلى نظام السجلات والمراقبة (SIEM) وفقًا لسياسة إدارة سجلات الأحداث ومراقبة الأمن السيبراني المعتمدة لدى <اسم الجهة>.

٥-٤ يجب مزامنة التوقيت (Clock Synchronization) مركزيًا لجميع الخوادم ومن مصدر دقيق وموثوق ومعتمد.

٥-٥ 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.

٥-٦ يجب على <الإدارة المعنية بتقنية المعلومات> مراقبة الخوادم التشغيلية والتأكد من فعالية أدائها، وتوافرها، وتوفير سعة تخزينية مناسبة، ونحو ذلك.

٦- إدارة الثغرات واختبار الاختراق

٦-١ يجب فحص الخوادم واكتشاف الثغرات عليها ومعالجتها بناءً على تصنيفها والمخاطر السيبرانية المترتبة عليها دوريًا وفقًا لسياسة إدارة الثغرات المعتمدة لدى <اسم الجهة> والمتطلبات التشريعية والتنظيمية ذات العلاقة.

٦-٢ يجب تنفيذ عمليات اختبار الاختراق على الخوادم دوريًا، وفقًا لسياسة اختبار الاختراق المعتمدة لدى <اسم الجهة>.

٦-٣ يجب تثبيت حزم التحديثات والإصلاحات الأمنية لمعالجة الثغرات ورفع مستوى كفاءة الخوادم وأمنها، وفقًا لسياسة إدارة التحديثات والإصلاحات المعتمدة لدى <اسم الجهة>.

٧- الحماية المادية والبيئية للخوادم

٧-١ يجب رصد ومراقبة الدخول والخروج من مرافق الخوادم داخل <اسم الجهة>، على سبيل المثال الأبواب والأقفال، أنظمة المراقبة الحديثة.

٧-٢ يجب رصد ومراقبة العوامل البيئية للخوادم كالتدفئة وتكييف الهواء والدخان وأجهزة إنذار الحريق وأنظمة إخماد الحرائق.

٧-٣ يجب تطبيق العزل المادي للخوادم وشبكات الأنظمة الحساسة في بيئة مقيدة الوصول وفقًا للسياسات والمتطلبات التنظيمية التشريعية ذات العلاقة.

٧-٤ يجب الالتزام بوضع الضوابط الأمنية المادية المناسبة (مثل كاميرات المراقبة داخل وخارج مركز بيانات <اسم الجهة>، وحراس الأمن، وتأمين الكابلات، وغيرها).

الأدوار والمسؤوليات

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

٢- **مراجعة السياسة وتحديثها:** <الإدارة المعنية بالأمن السيبراني>.

٣- **تنفيذ السياسة وتطبيقها:** <الإدارة المعنية بتقنية المعلومات> و<الإدارة المعنية بالأمن السيبراني>.

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

التحديث والمراجعة

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

الالتزام بالسياسة

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

٢- يجب على كافة العاملين في <اسم الجهة> الالتزام بهذه السياسة.

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