هذا المربع مخصّص لأغراض توجيهية. احذف جميع المربعات التوجيهية بعد تعبئة النموذج. يجب تحرير البنود الملوّنة باللون الأزرق بصورة مناسبة. والبنود الملونة باللون الأخضر هي أمثلة يجب حذفها. ويجب حذف التظليل الملون بعد إجراء التعديلات.

أدخل شعار الجهة بالضغط على الصورة الموضحة.

نموذج سياسة إدارة الأصول

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.

اختر التصنيف

الإصدار <١,٠>

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

اختر التصنيف

الإصدار <١,٠>

قائمة المحتويات

اختر التصنيف

الإصدار <١,٠>

الغرض

الغرض من هذه السياسة هو تحديد متطلبات الأمن السيبراني المتعلقة بإدارة الأصول الخاصة بأنظمة وبيانات ومعلومات <اسم الجهة> لتقليل المخاطر السيبرانية الناتجة عن التهديدات الداخلية والخارجية وذلك لتحقيق الأهداف الرئيسية للحماية وهي: سرية المعلومات، وسلامة أنظمة المعلومات، وتوافرها.

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

نطاق العمل

تطبق هذه السياسة على جميع الأصول المعلوماتية الخاصة ب<اسم الجهة> (مثل الأصول المادية والبيانات وتطبيقات الاعمال والبرمجيات والأصول التقنية)، وعلى جميع العاملين (الموظفين والمتعاقدين) في <اسم الجهة>.

بنود السياسة

١ البنود العامة

١-١ يجب حصر جميع الأصول المعلوماتية والتقنية الخاصة ب<اسم الجهة>.

١-٢ يجب حفظ جميع الأصول المعلوماتية والتقنية في <اسم الجهة> في قائمة جرد للأصول وتحديثها سنويًا على الأقل أو عند امتلاك أو تغيير أي أصل معلوماتي.

١-٣ يجب تعيين مالك لكل أصل من الأصول في <اسم الجهة>، بحيث يتولى المالك مسؤولية إعداد قائمة جرد الأصول والحفاظ عليها والتأكد من دقتها.

١-٤ يجب ضبط جميع الأصول في <اسم الجهة> وفقًا لسياسة الإعدادات والتحصين الخاصة ب<اسم الجهة>.

١-٥ يجب ضبط جميع الأصول وفقًا للإجراءات والمعايير والإرشادات المنشورة الخاصة بإعدادات الأصول لدى <اسم الجهة>.

١-٦ يجب أن يقرأ جميع مستخدمي وملاك الأصول سياسة الاستخدام المقبول للأصول المعتمدة من <اسم الجهة> والإقرار بها قبل منحهم حق الوصول إلى الأصل.

١-٧ قد تؤدي أي مخالفة لسياسة الإستخدام المقبول الخاصة ب<اسم الجهة> إلى اتخاذ إجراءات تأديبية بحق الشخص أو الأشخاص المخالفين للسياسة. وقد تشمل الإجراءات التأديبية الفصل أو إنهاء خدمات الشخص من <اسم الجهة>.

١-٨ يجب إشراك ملاك الأصول في دورة حياة إدارة الأصول للأنظمة الحساسة ومكوناتها.

١-٩ يجب استخدام مؤشرات الأداء الرئيسية (KPI) لضمان التحسين المستمر لمتطلبات الأمن السيبراني الخاصة بإدارة الأصول.

اختر التصنيف

الإصدار <١,٠>

٢ تعريف الأصول

٢-١ يجب تصنيف الأصول إلى الأنواع التالية:

٢-١-١ الأصول ذات المعلومات المصنفة، التي تحتوي على معلومات مصنفة بحسب مستوى تصنيف المعلومات مثل "سري للغاية" و"سري" (على النحو المحدد في معيار تصنيف الأصول في <اسم الجهة>).

٢-١-٢ معدات تقنية المعلومات، مثل الخوادم، وأجهزة الحاسوب المحمول، والأجهزة المحمولة، جدار الحماية، ومُوجّهات الإنترنت اللاسلكية (Wi-Fi routers) ومكثفات الشبكة الافتراضية الخاصة (VPN concentrators)، وغيرها.

٢-١-٣ البرمجيات والأنظمة، مثل:

٢-١-٣-١ تطبيقات الأعمال مثل إدارة علاقات العملاء، والتخطيط للموارد المؤسسية، وقواعد البيانات ومنصات التعاون.

٢-١-٣-٢ البرمجيات والأدوات مثل أنظمة التشغيل، وبرمجيات المحاكاة الافتراضية وبرمجيات الإنتاج.

٢-١-٣-٣ الوثائق المتعلقة بالأنظمة الحساسة.

٢-١-٣-٤ أنظمة العمل عن بُعد والأصول المرتبطة بها.

٢-١-٤ حسابات مواقع التواصل الاجتماعي والأصول المرتبطة بها.

٢-١-٥ الأطراف الخارجية والموردون والأصول المرتبطة بهم.

٢-١-٦ مقدمو خدمات الحوسبة السحابية، ومقدمو خدمات الاستضافة والحوسبة السحابية، والخدمات المُدارة والأصول المرتبطة بهم.

٣ ملكية الأصول

٣-١ بالإضافة إلى ما تم ذكره في البنود العامة أعلاه، يتولى مالك الأصل مسؤولية ما يلي:

٣-١-١ فهم وتحديد وإدارة مخاطر المعلومات خلال دورة حياة المعلومات.

٣-١-٢ تحديد متطلبات الأعمال (بما في ذلك الأمن السيبراني) واعتمادها.

٣-١-٣ تحديد تأثير الأمن السيبراني على التقنيات التشغيلية.

٣-١-٤ تعزيز الوعي بالأمن السيبراني والسلوكيات الأمنية الإيجابية.

٣-١-٥ تحديد الأولويات والميزانيات وتخصيص الموارد.

٣-١-٦ التأكد من حماية المعلومات والأنظمة بما يتوافق مع ضوابط الأمن السيبراني ذات العلاقة في الجهة.

٣-١-٧ الموافقة على إجراء التغييرات على الأصول التي يديرها.

٣-١-٨ دعم عمليات مراجعة وتدقيق الأمن السيبراني.

اختر التصنيف

الإصدار <١,٠>

٢-٣ يجب أن يتلقى ملاك الأصول التدريبات لتمكينهم من تأدية أدوارهم ومسؤولياتهم.

٣-٣ يجب أن يتولى ملاك الأصول المادية وتطبيقات الأعمال والبرمجيات مسؤولية الأمور التالية على سبيل المثال لا الحصر:

١-٣-٣ إنشاء الإعدادات الأمنية، والحصول على الموافقات والاعتمادات، ونشر الإعدادات للعمليات والإجراءات والمعايير والإرشادات.

٢-٣-٣ تطبيق الإعدادات الأمنية.

٣-٣-٣ مراجعة الإعدادات الأمنية مرة واحدة سنويًا على الأقل. وإذا كانت التغييرات مطلوبة، يجب على المسؤولين تحديث الإعدادات الأمنية، وتحديث العمليات والإجراءات والمعايير والإرشادات، والتأكد من تطبيق التغييرات باستخدام سياسة إدارة التغيير في <اسم الجهة>.

٤ قائمة جرد الأصول

٤-١ يجب إعداد قائمة جرد الأصول لكل نوع من أنواع الأصول وفقًا للبند ٢-١ من هذه السياسة.

٤-٢ يجب إعداد قائمة جرد الأصول بصيغة إلكترونية. ويمكن استخدام قائمة جرد الأصول بأحد الأمثلة التالية: قاعدة بيانات إدارة الإعدادات (Configuration Management Database "CMDB")، أو برمجيات إدارة الأصول (asset management software)، أو أداة إدارة الأصول المتخصصة (specialized asset management tool)، أو جداول البيانات (spreadsheet)، أو قاعدة البيانات (database).

٤-٣ يجب إعداد قائمة جرد الأصول لجميع خدمات الحوسبة السحابية وأصول تقنية المعلومات المتعلقة بخدمات الحوسبة السحابية.

٤-٤ يجب إعداد قائمة جرد الأصول للأنظمة الحساسة وحسابات التواصل الاجتماعي بما في ذلك جميع المكونات المعلوماتية والتقنية.

٤-٥ يجب تحديث قوائم جرد الأصول بشكل دوري أو عند حدوث أي تغيير.

٥ تصنيف وترميز الأصول

٥-١ يجب تصنيف وترميز جميع أصول <اسم الجهة> والتعامل معها وفقًا لسياسات <اسم الجهة> والمتطلبات التشريعية والتنظيمية.

٥-٢ يجب ترميز الأصول المادية (الشبكات، وتقنية المعلومات، وغيرها) برموز ملصقة تمنع التلاعب والعبث ويكتب عليها التعريف المميز للأصل.

٥-٣ يجب ترميز المعلومات سواءً أكانت بصيغة رقمية أو ورقية وفقًا لمعيار تصنيف الأصول في <اسم الجهة>.

٦ التخلص الآمن

٦-١ يجب التخلص من الأصول المملوكة ل<اسم الجهة> بطريقة آمنة ومعتمدة وفقًا للمتطلبات التشريعية والتنظيمية ذات العلاقة.

اختر التصنيف

الإصدار <١,٠>

٦-٢ يجب تشكيل لجنة للتخلص من الأصول، بحيث تشرف على جميع الأنشطة المتعلقة بالتخلص من الأصول.

٦-٣ يجب أن تتألف اللجنة من مالك الأصول وممثل عن <الإدارة المعنية بالأمن السيبراني>.

٦-٤ يجب تحديد واعتماد وتنفيذ إجراءات التخلص الآمن من الأجهزة، والأقراص القابلة للإزالة، وأجهزة التخزين (USB)، والبرمجيات، والسجلات الورقية وغيرها.

٦-٥ يجب مسح المعلومات المصنفة في الأصول بشكل آمن قبل التخلص منها.

٦-٦ يجب تسجيل أنشطة التخلص وتوقيعها من قبل لجنة التخلص من الأصول.

٦-٧ يجب أن يتضمن سجل التخلص من الأصول جميع المعلومات حول الأصول التي تم التخلص منها وفقًا لمعايير إدارة الأصول في <اسم الجهة>، على أن تشمل معلومات الأصول التي تم التخلص منها، على سبيل المثال لا الحصر، التاريخ ونوع الأصول والكمية والترميز أو الرقم التعريفي والتصنيف ومسؤول الأصول وطريقة التخلص 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 جميع 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>.

اختر التصنيف

الإصدار <١,٠>