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 الاستخدام المقبول للأصول

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 "<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".

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

اختر التصنيف

الإصدار <١,٠>

قائمة المحتويات

اختر التصنيف

الإصدار <١,٠>

الغرض

الغرض من هذه السياسة هو تحديد متطلبات الاستخدام المقبول في <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 المعلوماتية والتقنية الخاصة ب<اسم الجهة>، وتنطبق على جميع العاملين (الموظفين والمتعاقدين) لدى <اسم الجهة>.

بنود السياسة

١- البنود العامة

١-١ يجب اتباع متطلبات الأمن السيبراني في السياسات والمعايير والإجراءات المعتمدة لدى <اسم الجهة>.

٢-١ يجب حماية البيانات، والأصول (الأجهزة أو المعلومات أو البرامج) والتعامل معها حسب حساسيتها وتصنيفها، وفقًا لسياسة حماية البيانات المعتمدة لدى <اسم الجهة> وضمان سرية البيانات وسلامتها وتوافرها.

٣-١ يجب عدم ترك المطبوعات على الطابعة المشتركة دون رقابة.

٤-١ يجب حفظ وسائط التخزين الخارجية بشكل آمن وملائم، مثل التأكد من ضبط درجة الحرارة بدرجة معينة، وحفظها في مكان معزول وآمن.

٥-١ يمنع الإفصاح عن أي معلومات تخص <اسم الجهة>، بما في ذلك المعلومات المتعلقة بالأنظمة والشبكات لأي جهة أو طرف غير مصرح له سواءً كان ذلك داخليًا أو خارجيًا.

٦-١ يُمنع نشر معلومات تخص <اسم الجهة> عبر وسائل الإعلام، وشبكات التواصل الاجتماعي دون تصريح من صاحب الصلاحية.

٧-١ يُمنع استخدام أنظمة <اسم الجهة> وأصولها بغرض تحقيق منفعة وأعمال شخصية، أو تحقيق أي غرض لا يتعلق بنشاط وأعمال <اسم الجهة>.

٨-١ يُمنع ربط الأجهزة الشخصية بالشبكات، والأنظمة الخاصة ب<اسم الجهة> دون الحصول على تصريح مسبق من <الإدارة المعنية بالأمن السيبراني>، وبما يتوافق مع سياسة أمن أجهزة المستخدمين والأجهزة المحمولة والأجهزة الشخصية المعتمدة لدى <اسم الجهة>.

٩-١ يُمنع القيام بأي أنشطة تهدف إلى تجاوز أنظمة الحماية الخاصة ب<اسم الجهة>، بما في ذلك برامج مكافحة الفيروسات، وجدار الحماية، والبرمجيات الضارة دون الحصول على تصريح مسبق، وبما يتوافق مع الإجراءات المعتمدة لدى <اسم الجهة>.

١-١٠ تحتفظ <الإدارة المعنية بالأمن السيبراني> بحقها في مراقبة الأنظمة والشبكات والأجهزة الشخصية المتعلقة بالعمل، ومراجعتها دوريًا لمراقبة الالتزام بسياسات ومعايير الأمن السيبراني المعتمدة لدى <اسم الجهة>.

١-١١ يجب أن تكون البطاقة التعريفية للموظف أو الزوار بارزة في جميع مرافق <اسم الجهة>.

١-١٢ يجب تبليغ <الإدارة المعنية بالأمن السيبراني> في حال فقدان المعلومات الخاصة بـ<اسم الجهة> أو سرقتها أو تسريبها.

١-١٣ يجب متابعة قواعد الاستخدام المقبول للمعلومات والأصول المرتبطة بأنظمة معالجة المعلومات.

١-١٤ يجب على جميع الموظفين والعاملين في <اسم الجهة> إرجاع جميع الملفات والمستندات والمعلومات والأصول التي في حوزتهم عند إنهاء عملهم أو عقدهم أو اتفاقهم.

١-١٥ يمنع نقل الأصول خارج مواقعها بدون إذن مسبق من الإدارات المعنية.

١-١٦ يجب حماية الأصول التي تكون خارج المواقع مع مراعاة المخاطر المختلفة للعمل خارج مباني <اسم الجهة>.

١-١٧ يجب حضور الجلسات واللقاءات والمحتويات الخاصة بحملات التوعية الأمنية التي تقدمها <اسم الجهة> والالتزام بها.

١-١٨ يجب على جميع العاملين توقيع إقرار الموافقة على الاستخدام المقبول للأصول المعتمدة لدى <اسم الجهة>.

١-١٩ يجب على جميع العاملين الموافقة والإقرار على قواعد السلوك وسياسة الاستخدام المقبول عند أي مراجعة أو تحديث عليها.

١-٢٠ يجب أن يكون الوصول إلى أصول <اسم الجهة> وفقًا للمسؤوليات والأدوار المطلوبة لأداء المهام فقط.

١-٢١ يجب تنبيه مشرفي الأصول التقنية حول تصحيحات الأمن السيبراني التي يجب تطبيقها وفقًا لسياسة إدارة حزم التحديثات والإصلاحات المعتمدة لدى <اسم الجهة>.

١-٢٢ يجب على ملاك الأصول مراجعة صلاحيات وصول المستخدمين على فترات محددة ومنتظمة.

١-٢٣ يجب تبليغ <الإدارة المعنية بالأمن السيبراني> عند الاشتباه بأي نشاط قد يتسبب بضرر على <اسم الجهة> أو أصولها مثل: وجود مواقع مشبوهة، الاشتباه بوجود مخاطر سيبرانية أو الاشتباه بمحتوى بريد الكتروني قد يتسبب بضرر لـ<اسم الجهة>.

١-٢٤ في حال عدم الالتزام بأحد البنود يجب على <اسم الجهة> تقديم مبررات وذكر أسباب عدم الالتزام.

١-٢٥ يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر والاستخدام الصحيح والفعال لمتطلبات حماية الأصول المعلوماتية والتقنية الخاصة بـ <اسم الجهة>.

٢- حماية أجهزة الحاسب الآلي

٢-١ يمنع استخدام وسائط التخزين الخارجية دون الحصول على تصريح مسبق من <الإدارة المعنية بالأمن السيبراني>، وعند الاستخدام يجب تشفير البيانات المخزنة عليها وفقًا لمعيار التشفير المعتمد لدى <اسم الجهة>.

٢-٢ يجب تأمين الأجهزة قبل مغادرة المكتب وذلك بقفل الشاشة، أو تسجيل الخروج (Sign out or Lock)، سواءً كانت المغادرة لفترة قصيرة أو عند انتهاء ساعات العمل.

٢-٣ يُمنع استخدام أو تثبيت أجهزة أو أدوات أو تطبيقات غير معتمدة من <اسم الجهة> على جهاز الحاسب الآلي دون الحصول على إذن مسبق من <الإدارة المعنية بتقنية المعلومات>.

٣- الاستخدام المقبول للإنترنت والبرمجيات

٣-١ يجب التعامل بحذر مع الرسائل الأمنية التي قد تظهر خلال تصفح شبكة الإنترنت أو الشبكات الداخلية وعدم التفاعل معها إلا بالتواصل مع <الإدارة المعنية بالأمن السيبراني>.

٣-٢ يُمنع انتهاك حقوق أي شخص، أو شركة محمية بحقوق النشر، أو براءة الاختراع، أو أي ملكية فكرية أخرى، أو قوانين أو لوائح مماثلة؛ بما في ذلك، على سبيل المثال لا الحصر، تثبيت برامج غير مصرح بها أو غير قانونية لأي غرض من أغراض العمل، أو استخدام وسائط تخزين خارجية بدون أخذ الموافقة من <اسم الجهة>.

٣-٣ يجب استخدام متصفح آمن ومصرح به للوصول إلى الشبكة الداخلية أو شبكة الإنترنت.

٣-٤ يُمنع استخدام التقنيات التي تسمح بتجاوز الخادم الوكيل (Proxy) أو جدار الحماية (Firewall) للوصول إلى شبكة الإنترنت.

٣-٥ يُمنع تحميل البرمجيات والأدوات أو تثبيتها على أصول <اسم الجهة> دون الحصول على تصريح مسبق من <الإدارة المعنية بالأمن السيبراني>.

٣-٦ يُمنع استخدام شبكة الإنترنت في غير أغراض العمل، بما في ذلك تحميل الوسائط والملفات واستخدام برمجيات مشاركة الملفات دون الحصول على تصريح مسبق من <الإدارة المعنية بالأمن السيبراني>.

٣-٧ يُمنع إجراء أي فحص أمني لغرض اكتشاف الثغرات الأمنية، ويشمل ذلك إجراء اختبار الاختراقات، أو مراقبة شبكات <اسم الجهة> وأنظمتها، أو الشبكات والأنظمة الخاصة بالجهات الخارجية دون الحصول على تصريح مسبق من <الإدارة المعنية بالأمن السيبراني>.

٤- الاستخدام المقبول للبريد الإلكتروني

٤-١ يُمنع استخدام البريد الإلكتروني أو الهاتف أو الفاكس الإلكتروني في غير أغراض العمل، ويكون الاستخدام فقط بما يتوافق مع سياسات الأمن السيبراني ومعاييره المعتمدة لدى <اسم الجهة>.

٤-٢ يُمنع تداول رسائل تتضمن محتوى غير لائق أو غير مقبول، بما في ذلك الرسائل المتداولة مع الأطراف الداخلية والخارجية.

٤-٣ يجب استخدام تقنيات التشفير عند إرسال معلومات حساسة عن طريق البريد الإلكتروني أو أنظمة الاتصالات وفقًا لسياسة حماية البيانات المعتمدة لدى <اسم الجهة>.

٤-٤ يجب عدم تسجيل عنوان البريد الإلكتروني الخاص ب<اسم الجهة> في أي موقع ليس له علاقة بالعمل.

٤-٥ تحتفظ <اسم الجهة> بحقها في كشف محتويات رسائل البريد الإلكتروني بعد الحصول على التصاريح اللازمة من صاحب الصلاحية و<الإدارة المعنية بالأمن السيبراني> وفقًا للإجراءات والتنظيمات ذات العلاقة المعتمدة لدى <اسم الجهة>.

٤-٦ يُمنع فتح رسائل البريد الإلكتروني والمرفقات المشبوهة أو غير المتوقعة حتى وإن كانت تبدو من مصادر موثوقة.

٥- الاجتماعات المرئية والاتصالات القائمة على شبكة الإنترنت

٥-١ يُمنع استخدام أدوات أو برمجيات غير مصرح بها لإجراء اتصالات أو عقد اجتماعات مرئية تتعلق بالعمل.

٥-٢ يُمنع إجراء اتصالات أو عقد اجتماعات مرئية لا تتعلق بالعمل دون الحصول على تصريح مسبق باستخدام أدوات أو برمجيات خاصة ب<اسم الجهة>.

٥-٣ يُمنع عقد اجتماعات تتعلق بالعمل في أماكن عامة لخطورة تسريب معلومات مصنفة.

٦- استخدام كلمات المرور

٦-١ يجب اختيار كلمات مرور آمنة، والمحافظة على كلمات المرور الخاصة بأنظمة <اسم الجهة> وأصولها وفقًا لسياسة إدارة هويات الدخول والصلاحيات في <اسم الجهة>. كما يجب اختيار كلمات مرور مختلفة عن كلمات مرور الحسابات الشخصية، مثل حسابات البريد الشخصي ومواقع التواصل الاجتماعي.

٦-٢ يُمنع مشاركة كلمة المرور عبر أي وسيلة كانت، بما في ذلك المراسلات الإلكترونية، والاتصالات الصوتية، والكتابة الورقية. كما يجب على جميع المستخدمين عدم الكشف عن كلمة المرور لأي طرف آخر بما في ذلك زملاء العمل وموظفو <الإدارة المعنية بتقنية المعلومات> وإبلاغ <الإدارة المعنية بالأمن السيبراني> فورًا في حال وقوع ذلك.

٦-٣ يجب تغيير كلمة المرور بشكل دوري وفقًا لمتطلبات سياسة كلمة المرور أو عند الحصول على كلمة مرور جديدة من قبل مسؤول النظام.

٦-٤ يمنع استخدام كلمات مرور مستخدمة من قبل أو متعارف عليها، بالإضافة إلى عدم مشاركة كلمة المرور الخاصة بالمستخدم لأي شخص إطلاقًا.

٧- استخدام المكتب

٧-١ يجب الالتزام بسياسة المكتب الآمن والنظيف المعتمدة لدى <اسم الجهة>، والتأكد من خلو سطح المكتب وشاشة العرض من المعلومات المصنفة والحساسة وفقًا للتصنيفات المعتمدة لدى <اسم الجهة>.

٧-٢ يُمنع ترك أي معلومات مصنفة أو حساسة بالنسبة ل<اسم الجهة> في أماكن يسهل الوصول إليها، أو الاطلاع عليها من قبل أشخاص غير مصرح لهم.

٧-٣ يمنع ترك أبواب المكتب والخزانات التي تحتوي على معلومات مصنفة وحساسة مفتوحة.

٨- الحوسبة السحابية

٨-١ يجب تصنيف البيانات قبل استضافتها لدى مقدمي خدمات الحوسبة السحابية والاستضافة، وإعادتها للجهة (بصيغة قابلة للاستخدام) عند إنتهاء الخدمة.

٨-٢ يجب فصل البيئة الخاصة بـ<اسم الجهة> (وخصوصًا الخوادم الافتراضية)عن غيرها من البيئات التابعة لجهات أخرى في خدمات الحوسبة السحابية.

٨-٣ يجب أن يكون موقع استضافة وتخزين معلومات <اسم الجهة> داخل المملكة، وأن يكون التخزين وفقًا للمتطلبات التشريعية والتنظيمية ذات العلاقة.

٨-٤ يجب أن تغطي متطلبات الأمن السيبراني الخاصة بحماية بيانات ومعلومات المشتركين في الحوسبة السحابية وفقاً للمتطلبات التشريعية والتنظيمية ذات العلاقة، بحد أدنى ما يلي:

٨-٥-١ وجود ضمانات للقدرة على حذف البيانات بطرق آمنة عند الانتهاء من العلاقة مع مقدم الخدمة (Exit Strategy).

٨-٥-٢ استخدام وسائل آمنة لتصدير ونقل البيانات والبنية التحتية الافتراضية.

الأدوار والمسؤوليات

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

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

٣- **تنفيذ السياسة وتطبيقها:** <الإدارة المعنية بالموارد البشرية>.

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 يُعرّض أي انتهاك لهذه السياسة صاحب المخالفة إلى إجراء تأديبي؛ حسب الإجراءات المُتبعة في <اسم الجهة>.