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 أجهزة المستخدمين والأجهزة المحمولة والأجهزة الشخصية

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".
- 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

اختر التصنيف

الإصدار <١,٠>

قائمة المحتويات

الغرض

الغرض من هذه السياسة هو تحديد متطلبات الأمن السيبراني المتعلقة باستخدام أجهزة المستخدمين (Workstations)، والأجهزة المحمولة (Mobile Devices)، والأجهزة الشخصية للعاملين (Bring Your Own Device "BYOD") 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 أجهزة المستخدمين والأجهزة المحمولة والأجهزة الشخصية للعاملين في <اسم الجهة>، وتنطبق على جميع العاملين (الموظفين والمتعاقدين) في <اسم الجهة>.

بنود السياسة

١- البنود العامة

١-١ يجب حماية البيانات والمعلومات المُخزّنة في أجهزة المستخدمين والأجهزة المحمولة والأجهزة الشخصية (BYOD) حسب تصنيفها باستخدام الضوابط الأمنية المناسبة لتقييد الوصول إلى هذه المعلومات، ومنع العاملين غير المصرّح لهم من الوصول لها أو الاطلاع عليها.

١-٢ يجب تحديث برمجيات أجهزة المستخدمين والأجهزة المحمولة والأجهزة الشخصية (BYOD)، بما في ذلك أنظمة التشغيل والبرامج والتطبيقات، وتزويدها بأحدث حزم التحديثات والإصلاحات وذلك وفقًا لسياسة إدارة التحديثات والإصلاحات المعتمدة في <اسم الجهة>.

١-٣ يجب تطبيق ضوابط الإعدادات والتحصين (Configuration and Hardening) لأجهزة المستخدمين والأجهزة المحمولة والأجهزة الشخصية (BYOD) وفقًا للمعايير التقنية الأمنية المعتمدة لدى <اسم الجهة>.

١-٤ يجب عدم منح العاملين صلاحيات هامة وحساسة (Privileged Access) على أنظمة <اسم الجهة> باستخدام الأجهزة المحمولة والأجهزة الشخصية (BYOD)، ويجب منح الصلاحيات وفقًا لمبدأ الحد الأدنى من الصلاحيات والامتيازات (Principle of Least Privilege).

١-٥ يجب حذف أو إعادة تسمية حسابات المستخدم الافتراضية في أنظمة التشغيل والتطبيقات.

١-٦ يجب مزامنة التوقيت (Clock Synchronization) مركزيًا ومن مصدر دقيق وموثوق لجميع أجهزة المستخدمين والأجهزة المحمولة والأجهزة الشخصية (BYOD).

١-٧ يجب تزويد أجهزة المستخدمين والأجهزة المحمولة برسالة نصيّة (Banner) لإتاحة الاستخدام المصرّح به.

١-٨ يجب السماح فقط بقائمة محددة من التطبيقات (Whitelisting) للعمل على أجهزة المستخدمين والأجهزة المحمولة.

١-٩ يجب استخدام تقنية منع تسرّب البيانات (Data Leakage Prevention) واستخدام أنظمة مراقبة البيانات لضمان حماية البيانات على أجهزة المستخدمين والأجهزة المحمولة.

١-١٠ يجب تشفير وسائط وأقراص التخزين الخاصة بأجهزة المستخدمين والأجهزة المحمولة الهامة والحساسة والتي لها صلاحيات متقدمة وصلاحيات وصول للأنظمة الحساسة تشفيرًا كاملًا (Full Disk Encryption) وفقًا لمعيار التشفير المعتمد لدى <اسم الجهة>.

١-١١ يجب تقييد استخدام وسائط التخزين الخارجية وفق إجراءات معتمدة لدى <اسم الجهة> بعد الحصول على إذن مسبق من <الإدارة المعنية بالأمن السيبراني>.

١-١٢ يجب إدارة الأجهزة المحمولة والأجهزة الشخصية (BYOD) مركزيًا باستخدام نظام إدارة الأجهزة المحمولة (Mobile Device Management "MDM").

١-١٣ يجب عدم السماح لأجهزة المستخدمين والأجهزة المحمولة والأجهزة الشخصية (BYOD) المزوّدة ببرمجيات غير محدثة أو منتهية الصلاحية (بما في ذلك أنظمة التشغيل والبرامج والتطبيقات) بالاتصال بشبكة <اسم الجهة> لمنع التهديدات الأمنية الناشئة عن البرمجيات منتهية الصلاحية غير المحمية بحزم التحديثات والإصلاحات.

١-١٤ يجب منع أجهزة المستخدمين والأجهزة المحمولة والأجهزة الشخصية (BYOD) غير المزوّدة بأحدث برمجيات الحماية من الاتصال بشبكة <اسم الجهة> لتجنب حدوث المخاطر السيبرانية التي تؤدي إلى الوصول غير المصرّح به أو دخول البرمجيات الضارة أو تسرّب البيانات. وتتضمّن برمجيات الحماية برامج إلزامية، مثل: برامج الحماية من الفيروسات والبرامج والأنشطة المشبوهة والبرمجيات الضارة (Malware)، وجدار الحماية للمستضيف (Host-Based Firewall)، وأنظمة الحماية المتقدمة لاكتشاف ومنع الاختراقات في المستضيف (Host-based Intrusion Detection/Prevention)

١-١٥ يجب تحديد الانحرافات عن سلوك المستخدمين المقبول، وتقييم مستوى المخاطر، وتطوير و/أو توصية التدابير المضادة المناسبة للتخفيف منها.

١-١٦ يجب ضبط إعدادات أجهزة المستخدمين والأجهزة المحمولة غير المستخدمة بحيث تعرض شاشة توقّف محمية بكلمة مرور في حال عدم استخدام الجهاز (Session Timeout) لمدة <٥ دقائق>.

١-١٧ يجب إدارة حسابات أجهزة المستخدمين والأجهزة المحمولة مركزيًا من خلال خادم الدليل النشط (Directory Active) الخاص بنطاق <اسم الجهة> أو نظام إداري مركزي.

١-١٨ يجب تنفيذ سياسات النطاق المناسبة (Group Policy) في <اسم الجهة> وتطبيقها على جميع أجهزة المستخدمين والأجهزة المحمولة لضمان ضبط الإعدادات والتحصين والتزام <اسم الجهة> بالضوابط التنظيمية والأمنية وتثبيت الإعدادات البرمجية اللازمة.

١-١٩ يجب إجراء نسخ احتياطي دوري للبيانات المخزّنة على أجهزة المستخدمين والأجهزة المحمولة، وذلك وفقًا لسياسة النسخ الاحتياطية المعتمدة في <اسم الجهة>.

١-٢٠ يجب توفير واستخدام التقنيات التي تُمكّن من حذف البيانات عن بعد والمُخزّنة على الأجهزة المحمولة والأجهزة الشخصية (BYOD) في الحالات التالية:

اختر التصنيف

١-٢١-١ فقدان الجهاز المحمول أو سرقته.

١-٢١-٢ انتهاء أو إنهاء العلاقة الوظيفية بين المستخدم و<اسم الجهة>.

١-٢١-٣ انتهاء صلاحية الاستخدام وتسليم الجهاز المحمول للإدارة المعنية <اسم الجهة>.

١-٢١ يجب حامية أنظمة العمل عن بعد وأجهزة المعلومات الخاصة بها، من خلال:

١-٢١-١ تطبيق الإدارة الآمنة للجلسات (Secure Session Management) ويشمل موثوقية الجلسات (Authenticity)، وإقفالها (Lockout)، وإنهاء مهلتها (Timeout).

١-٢١-٢ تطبيق حزم التحديثات، والإصلاحات الأمنية لأنظمة العمل عن بعد، مرة واحدة شهريا على الأقل.

١-٢١-٣ مراجعة إعدادات الحماية لأنظمة العمل عن بعد والتحصين مرة واحدة كل سنة على الأقل.

١-٢١-٤ تقييد تفعيل الخصائص والخدمات في أنظمة العمل عن بعد حسب الحاجة، على أن يتم تحليل المخاطر السيبرانية المحتملة في حال الحاجة لتفعيلها.

١-٢٢ يجب تنظيم حملات توعية بالطرق الآمنة لاستخدام الأجهزة المحمولة والأجهزة الشخصية (BYOD) ومسؤوليات المستخدمين تجاهها وفقًا لسياسة الاستخدام المقبول المعتمدة لدى <اسم الجهة> وإجراء جلسات توعية مخصصة للمستخدمين ذوي الصلاحيات الهامة والحساسة.

١-٢٣ يجب تطوير إجراءات ومعايير خاصة بأمن أجهزة المستخدمين والأجهزة المحمولة والأجهزة الشخصية بناء على حاجة العمل.

١-٢٤ يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر والاستخدام الصحيح والفعال لمتطلبات حماية أجهزة المستخدمين والأجهزة المحمولة والأجهزة الشخصية.

٢- متطلبات الأمن السيبراني لأمن أجهزة المستخدمين

٢-١ يجب تخصيص أجهزة المستخدمين للعاملين في الوظائف التقنية، ذات الصلاحيات الهامة والحساسة، على أن تكون معزولة في شبكة خاصة لإدارة الأنظمة (Management Network) وعلى ألا ترتبط بأي شبكة أو خدمة أخرى.

٢-٢ يجب ضبط إعدادات أجهزة المستخدمين الهامة والحساسة (PAWs) ذات صلاحيات متقدمة لإرسال السجلات إلى نظام التسجيل والمراقبة المركزي الخاص ب<اسم الجهة> وفقًا لسياسة إدارة سجلات الأحداث ومراقبة الأمن السيبراني المعتمدة لدى <اسم الجهة>، مع منع إمكانية تغيير الإعدادات عن طريق المستخدم.

٢-٣ يجب تأمين أجهزة المستخدمين ماديًا داخل مباني <اسم الجهة> وتسجيل عمليات الخروج والدخول وذلك بعد الحصول على الموافقات اللازمة وفقًا لسياسة الأمن المادي المعتمدة لدى <اسم الجهة>.

٢-٤ يجب ضمان حماية أجهزة المستخدمين من الفيروسات والبرمجيات الضارة والتهديدات المتقدّمة والمستمرة والهجمات غير المعروفة مسبقًا وأي نوع آخر من الهجمات الخبيثة من خلال تقنيات حماية الأجهزة الطرفية (Endpoint Protection Software).

٢-٥ يجب ضمان سلامة بيانات أجهزة المستخدمين من العبث بها أو فقدانها بالخطأ أو تخريبها والتأكد من توافرها وإمكانية استعادتها.

اختر التصنيف

٢-٦ يجب تطبيق جميع الضوابط الأمنية اللازمة عند إزالة من بيانات أجهزة المستخدمين وخصوصًا الأجهزة المتصلة بالخدمات السحابية وفقًا لسياسة حماية البيانات والمعلومات المعتمدة لدى <اسم الجهة>.

٢-٧ يجب إدارة حزم التحديثات والإصلاحات مرة واحدة على الأقل كل شهر للأجهزة المستخدمة لإدارة الأنظمة الحساسة الخارجية والمتصلة بالإنترنت ومرة واحدة على الأقل كل ثلاثة أشهر للأجهزة المستخدمة لإدارة الأنظمة الحساسة الداخلية، وفقًا لسياسة إدارة التغيير المعتمدة لدى <اسم الجهة>.

٢-٨ يجب مراجعة إعدادات الأجهزة المستخدمة لإدارة الأنظمة الحساسة وتحصيناتها مرة واحدة كل ستة أشهر على الأقل.

٣- متطلبات الأمن السيبراني لأمن الأجهزة المحمولة

٣-١ يجب تقييد وصول الأجهزة المحمولة إلى الأنظمة الحساسة إلا لفترة مؤقتة فقط، وذلك بعد إجراء تقييم المخاطر وأخذ الموافقات اللازمة من <الإدارة المعنية بالأمن السيبراني>.

٣-٢ يجب تقييد وصول المستخدمين غير المصرّح لهم (Device Access Locking) إلى الأجهزة غير المراقبة و/أو المفقودة و/أو المسروقة.

٣-٣ يجب ضمان سلامة المعلومات المخزنة على الأجهزة المحمولة (Device Contents Integrity).

٣-٤ يجب ضمان تحديث وضبط نظام التشغيل والتطبيقات المثبّتة على الأجهزة المحمولة بطريقة مناسبة قبل استخدامه (Device OS and Applications Security) وفقًا للمعايير التقنية المعتمدة لدى <اسم الجهة>.

٣-٥ يجب تطبيق حزم التحديثات والإصلاحات الأمنية لجميع الأجهزة المحمولة مرة واحدة شهريًا على الأقل.

٣-٦ يجب فصل وتشفير البيانات والمعلومات الخاصة ب<اسم الجهة> المخزنة على الأجهزة المحمولة.

٤- متطلبات الأمن السيبراني لأمن الأجهزة الشخصية (BYOD)

٤-١ في حال استخدام أجهزة العاملين الشخصية لأغراض العمل، يجب أن يكون ذلك مدعومًا باتفاقيات موثقة مع العاملين وضوابط أمنية تقنية لحماية بيانات ومعلومات <اسم الجهة>.

٤-٢ يجب فصل وتشفير البيانات والمعلومات الخاصة ب<اسم الجهة> المخزنة على الأجهزة الشخصية (BYOD).

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>.

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

اختر التصنيف

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>.