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 معيار أمن الأجهزة المحمولة

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

طُوّر 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 ٤
نطاق العمل..... ٤
المعايير ٤
الأدوار والمسؤوليات ٨
التحديث والمراجعة ٨
الالتزام بالمعيار ٨

اختر التصنيف

الإصدار <١,٠>

الغرض

يهدف هذا المعيار إلى تحديد متطلبات الأمن السيبراني التفصيلية لحماية الأجهزة المحمولة (Mobile Devices) الخاصة ب<اسم الجهة> والأجهزة الشخصية للعاملين (Bring Your Own Device "BYOD") وذلك لتحقيق الغرض الأساسي وهو تقليل المخاطر السيبرانية الناتجة عن التهديدات الداخلية والخارجية في <اسم الجهة>. هذه المتطلبات تمت موائمتها مع سياسة أمن أجهزة المستخدمين والأجهزة المحمولة والأجهزة الشخصية ومتطلبات الأمن السيبراني الصادرة من الهيئة الوطنية للأمن السيبراني ويشمل ذلك على سبيل المثال لا الحصر: الضوابط الأساسية للأمن السيبراني (ECC – ١: ٢٠١٨)، ضوابط الأمن السيبراني للأنظمة الحساسة (CSCC – ١: ٢٠١٩) وغيرها من المتطلبات التشريعية والتنظيمية ذات العلاقة.

نطاق العمل

يطبق هذا المعيار على جميع الأجهزة المحمولة (Mobile Devices) في <اسم الجهة>، وعلى جميع الأجهزة الشخصية للعاملين (BYOD)، وعلى جميع العاملين (الموظفين والمتعاقدين) في <اسم الجهة>.

المعايير

١	منع الوصول إلى الجهاز
الهدف	ضمان عدم وصول المستخدمين غير المصرّح لهم إلى الأجهزة غير المراقبة و/أو المفقودة و/أو المسروقة.
المخاطر المحتملة	في حال الوصول غير مصرّح به إلى جهاز محمول تملكه <اسم الجهة> ويحتوي على بيانات خاصة ب<اسم الجهة> أو منح صلاحيات هامة للدخول إلى بيئة تقنية المعلومات الخاصة ب<اسم الجهة>، فقد يؤثّر أي اختراق محتمل متعلّق بالعمل في الإدارة حسب شدّة الحادث.
الإجراءات المطلوبة	
١-١	إعداد رموز مرور (Passcodes) معقّدة لقفل الأجهزة تتكون من أحرف كبيرة وأحرف صغيرة، أرقام ورموز، ويجب منع استخدام رموز المرور السهلة المكوّنة من أحرف أو أرقام متتالية أو متسلسلة (مثل: ٠٠٠٠، أو ١٢٣٤، أو ٩٨٧٦، إلخ)، كما يُنصَح باستخدام رموز مرور مكوّنة من مجموعات إضافية من الأحرف أو الأرقام أو استخدام رموز مرور طويلة.
١-٢	إضافة عنصر تحقّق (Factor of Authentication) آخر لقفل الجهاز (كاستخدام تقنية التعرّف على الوجه، أو نمط التمرير السريع على الشاشة "Swiping Pattern"، أو بصمة الأصبع، كلمة المرور لمرة واحدة (OTP) ، وغيرها) إن سمحت خصائص الجهاز المحمول بذلك.
١-٣	تغيير رمز المرور لقفل الجهاز المحمول دورياً، أو كل ثلاثة أشهر على الأقل.

١-٤	منع المستخدمين من تعديل أو إلغاء آلية القفل الآمن للجهاز.
١-٥	يجب ضبط آليات القفل التلقائي للجهاز عندما لا يكون الجهاز قيد الاستعمال لمدة لا تزيد عن ٩٠ ثانية أو وفقًا لمتطلبات <اسم الجهة>.
٢	سلامة المعلومات المخزنة في الجهاز المحمول
الهدف	تطبيق آلية قياسية لمنع إجراء تعديلات غير مقصودة أو ضارة على محتويات البيانات المُخزّنة في الجهاز.
المخاطر المحتملة	في حال تعرّض البيانات المُخزّنة في الجهاز للعبث أو التلف أو التعديل، فإنه لا يمكن اعتبار الجهاز أو البيانات المخزنة بعد ذلك من الأصول الموثوقة التي يُسمَح باستخدامها داخل بيئة تقنية المعلومات الخاصة ب<اسم الجهة>.
الإجراءات المطلوبة	
٢-١	تفعيل التشفير الكامل لمحتويات الجهاز إن كان الجهاز المحمول يدعم هذا الخيار.
٢-٢	تفعيل وتطبيق خاصية فصل البيانات بين المعلومات الشخصية والبيانات الخاصة ب<اسم الجهة>، وذلك في الأجهزة الشخصية للعاملين (BYOD) إن كانت تدعم هذه الخاصية. كما يجب تشفير البيانات بعد فصلها.
٢-٣	ضبط وإعداد كلمات مرور مُحمِّل التشغيل (Bootloader) لنظام الإدخال/الإخراج الأساسي (BIOS).
٢-٤	تفعيل إغلاق مُحمِّل التشغيل (Bootloader) إن كان الجهاز المحمول يدعم هذا الخيار.
٢-٥	ضبط وتطبيق التشفير على أي من وسائط التخزين القابلة للإزالة (مثل: بطاقات التخزين الآمنة "SD Cards" أو وسائط التخزين الخارجية "USB") التي تصل إليها الأجهزة المحمولة.
٢-٦	ضبط إعدادات الجهاز لإجراء قفل تلقائي بعد القيام بخمس محاولات خاطئة لإدخال رمز المرور، وإجراء مسح تلقائي للبيانات بعد القيام بعشر محاولات خاطئة لإدخال رمز المرور أو وفقاً لعدد المحاولات التي يدعمها نظام تشغيل الجهاز.
٢-٧	تفعيل إمكانية مسح البيانات عن بُعد من الأجهزة المفقودة أو المسروقة.
٢-٨	منع المستخدمين من تعديل أو إلغاء آلية إغلاق مُحمِّل التشغيل (Bootloader).

٢-٩	منع إجراء أي عملية تجاوز للقيود التي تفرضها الشركات المصنّعة للجهاز (مثل Rooting أو Jailbreaking) على أي جهاز محمول، ومنع استخدام الأجهزة التي تم إجراء هاتين العمليتين عليها داخل بيئة تقنية المعلومات الخاصة ب<اسم الجهة>.
٣	أمن نظام تشغيل وتطبيقات الجهاز
الهدف	ضمان تحديث وضبط نظام التشغيل والتطبيقات المثبّتة في الجهاز المحمول بطريقة مناسبة قبل استخدامه.
المخاطر المحتملة	تثبيت التطبيقات الغير مصرح بها أو عدم تحديث أنظمة التشغيل والتطبيقات الخاصة بالأجهزة المحمولة يزيد من احتمالية وجود برمجيات ضارة قد تؤثر على البيئة التقنية الخاصة ب<اسم الجهة>.
الإجراءات المطلوبة	
١-٣	إتاحة تثبيت التطبيقات المقدّمة فقط من الجهة أو المتاجر المعتمدة الخاصة بالمورّد.
٢-٣	تقييد الصلاحيات الممنوحة للتطبيقات المثبّتة على الجهاز المحمول بحيث تُطبّق مبدأ الحدّ الأدنى من الصلاحيات.
٣-٣	تعطيل الكاميرا والميكروفون بشكل افتراضي وتحديد التطبيقات المصرح لها باستخدامها حسب حاجة العمل.
٤-٣	التأكّد من التواقيع الرقمية للتطبيقات قبل تثبيتها.
٥-٣	التأكّد من تزويد الجهاز المحمول بأحدث نسخة رسمية من إصدار/نسخة نظام التشغيل من خلال مورّد الجهاز. وإذا تعذّر تزويد أي جهاز بنسخة أحدث من نظام التشغيل، وتوقّف المورّد عن تقديم حزم الإصلاحات والتحديثات الأمنية للجهاز في العامين الماضيين، يجب عندها التوقف عن استخدام الجهاز واستبداله.
٦-٣	تطبيق نظام مراقبة الإعدادات المتوافقة مع بروتوكول أتمتة محتوى الأمن (Security Content Automation Protocol) لتدقيق عناصر الإعدادات الأمنية كافة والتأكّد منها في الأجهزة المحمولة وجدولة الاستثناءات المعتمدة والإبلاغ عن حدوث أي تغييرات غير مصرّح بها..
٧-٣	منع المستخدمين من تعديل أو إلغاء أي إعدادات أمنية للجهاز المحمول.
٨-٣	تعطيل أو إزالة الحسابات الافتراضية، وتقييد الوصول إلى الحسابات ذات الصلاحية العالية على الأجهزة المحمولة بالتوافق مع سياسة إدارة هويات الوصول والصلاحيات.
٩-٣	تطوير المعايير الأمنية الأساسية للأجهزة المحمولة وتنفيذها ومراقبتها دورياً.

٣-١٠	إجراء نسخ احتياطي كامل ومنتظم للبيانات المخزنة على الأجهزة المحمولة وفقاً لسياسة النسخ الاحتياطية الخاصة ب<اسم الجهة>.
٣-١١	إجراء التحديثات والإصلاحات على أجهزة المستخدمين المحمولة بشكل منتظم وفقاً لسياسة أمن أجهزة المستخدمين وسياسة إدارة التحديثات والإصلاحات في <اسم الجهة> لضمان تحديث جميع أنظمة التشغيل وبرمجيات التطبيقات على أجهزة المستخدمين المحمولة.
٣-١٢	استخدام عناصر التحكم في الأجهزة وحظر الوصول إلى الوسائط القابلة للإزالة عند الضرورة أو وفقاً لسياسة الاستخدام المقبول في <اسم الجهة>.
٣-١٣	تثبيت برمجيات التحكم بأجهزة المستخدمين المحمولة على كافة الأجهزة لمنع الاستخدام غير المصرح به لأدوات اتصال الشبكة (Wi-Fi, Bluetooth, etc.) والأجهزة الطرفية.
٣-١٤	تعطيل كافة خصائص تبادل البيانات أو الملفات مثل (Airdrop, NFC, Bluetooth .(.etc
٣-١٥	تثبيت برمجيات الحماية على أجهزة المستخدمين المحمولة بما في ذلك مضاد الفيروسات، والبرامج التي تسمح لقائمة محددة فقط من التطبيقات، وبرامج منع تسرب المعلومات والبيانات على كافة الأجهزة المحمولة.
٣-١٦	استخدام خاصية العلامة المائية (Watermark) على شاشة المستخدمين.
٣-١٧	تطبيق الإعدادات الأمنية والتحصين لأجهزة المستخدمين بما في ذلك التحصين على مستوى البرمجيات وأنظمة التشغيل وفقاً لسياسة الإعدادات والتحصين في <اسم الجهة>.
٤	معايير أخرى
الهدف	تطبيق جميع المعايير والمتطلبات الأمنية للأجهزة المحمولة لضمان أعلى مستويات الحماية.
المخاطر المحتملة	عدم تطبيق جميع المعايير والمتطلبات الأمنية يعرض <اسم الجهة> إلى زيادة في المخاطر الأمنية للأجهزة المحمولة.
الإجراءات المطلوبة	
٤-١	تطبيق المعايير التالية: ١- معيار التعافي من الكوارث والنسخ الاحتياطية ٢- معيار تسجيل الأحداث وسجل التدقيق ٣- معيار الحماية من البرمجيات الضارة ٤- معيار التشفير ٥- معيار الإعدادات والتحصين

الأدوار والمسؤوليات

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

٢- **مراجعة المعيار وتحديثه:** <الإدارة المعنية بالأمن السيبراني>.

٣- **تنفيذ المعيار وتطبيقه:** <الإدارة المعنية بتقنية المعلومات> و< الإدارة المعنية بالأمن السيبراني>.

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

التحديث والمراجعة

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

الالتزام بالمعيار

١- يجب على <رئيس الإدارة المعنية بالأمن السيبراني> التأكد من التزام <اسم الجهة> بهذا المعيار دورياً.

٢- يجب على جميع العاملين في <اسم الجهة> الالتزام بهذا المعيار.

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