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 نص

الإصدار: اضغط هنا لإضافة نص

المرجع: اضغط هنا لإضافة نص

استبدل <اسم الجهة> باسم الجهة في مجمل صفحات الوثيقة.
وللقيام بذلك، اتبع الخطوات التالية:

1. اضغط على مفتاحي "Ctrl" و"H" في الوقت نفسه.
2. أضف "<اسم الجهة>" في مربع البحث عن النص.
3. أدخل الاسم الكامل لجهتك في مربع "استبدال" النص.
4. اضغط على "المزيد" وتأكّد من اختيار "Match case".
5. اضغط على "استبدل الكل".
6. أغلق مربع الحوار.

اعتماد الوثيقة

الدور	الاسم	التاريخ	التوقيع
اختر الدور	<أدخل الاسم الكامل للشخص>	اضغط هنا لإضافة نص	<أدخل التوقيع>

نسخ الوثيقة

النسخة	التاريخ	عُدّل بواسطة	أسباب التعديل
<أدخل رقم النسخة>	اضغط هنا لإضافة نص	<أدخل الاسم الكامل للشخص>	<أدخل وصف التعديل>

قائمة المحتويات

الأهداف

يهدف هذا المعيار إلى توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير لتقليل المخاطر الناتجة عن استخدام أجهزة <اسم الجهة> المحمولة (Mobile Devices) والأجهزة الشخصية للعاملين (مبدأ "Bring Your Own Device "BYOD) وحمايتها من التهديدات الداخلية والخارجية من خلال التركيز على الأهداف الأساسية للحماية وهي: سرية المعلومات، وسلامتها، وتوافرها.

يتبع هذا المعيار المتطلبات التشريعية والتنظيمية الوطنية وأفضل الممارسات الدولية ذات العلاقة، وهو متطلب تشريعي في الضابط رقم ١-٣-٣ والضابط رقم ٢-٦-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل

يغطي هذا المعيار أنظمة إدارة الأجهزة المحمولة في <اسم الجهة>، وينطبق على الأجهزة المحمولة (Devices Mobile) الخاصة بـ<اسم الجهة> والأجهزة الشخصية للعاملين (BYOD).

المعايير

1	منع الوصول إلى الجهاز (Device Access Locking)
الهدف	ضمان عدم وصول المستخدمين غير المصرّح لهم إلى الأجهزة غير المراقبة و/أو المفقودة و/أو المسروقة.
المخاطر المحتملة	في حال منح حق وصول غير مصرّح به إلى جهاز محمول تملكه <اسم الجهة> ويحتوي على بيانات خاصة بـ<اسم الجهة> أو منح صلاحيات هامة للدخول إلى بيئة تقنية المعلومات الخاصة بـ<اسم الجهة>، فقد يؤثّر أي اختراق محتمل متعلّق بالعمل في الإدارة حسب شدّة الحادث.
الإجراءات المطلوبة	
1-1	إعداد رموز مرور (Passcodes) معقّدة لقفل الأجهزة. ويُنصَح بشدة عدم استخدام رموز المرور السهلة المكوّنة من أحرف أو أرقام متتالية أو متسلسلة (مثل: 0000، أو 1234، أو 9876)، كما يُنصَح باستخدام رموز مرور مكوّنة من مجموعات إضافية من الأحرف أو الأرقام أو استخدام رموز مرور طويلة. Passcodes consisting of complex characters shall be set up. Simple passcodes consisting of consecutive or sequential characters) e.g., 0000, 1234, 9876, etc.) are strongly discouraged. Passcodes consisting of additional character sets or greater lengths are recommended.

2-1	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، وغيرها) إن سمحت خصائص الجهاز المحمول بذلك. If the mobile device allows for it, an additional factor of authentication to lock the device (e.g., facial recognition, swiping pattern, fingerprint, etc.) shall be implemented.
3-1	تغيير رمز المرور لقفل الجهاز المحمول دورياً، أو كل ثلاثة أشهر على الأقل. The passcode for the mobile device shall be changed periodically or at least every three months.
4-1	منع المستخدمين من تعديل أو إلغاء آلية القفل الآمن للجهاز. Users shall be prohibited from modifying or disabling security locking mechanisms.
5-1	يجب ضبط آليات القفل التلقائي للجهاز عندما لا يكون الجهاز قيد الاستعمال لمدة لا تزيد عن 90 ثانية أو وفقًا لمتطلبات <اسم الجهة>. The device auto-lock mechanism shall be set to lock the device when it is idle and not being used for no more than 90 seconds or as per <entity name>'s requirements.
2	سلامة المعلومات المخزنة في الجهاز المحمول (Device Contents Integrity)
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 بعد ذلك من الأصول الموثوقة التي يُسمَح باستخدامها داخل بيئة تقنية المعلومات الخاصة بـ<اسم الجهة>.
الإجراءات المطلوبة	
1-2	تفعيل التشفير الكامل لمحتويات الجهاز إن كان الجهاز المحمول يدعم هذا الخيار. If the mobile device supports it, full device contents encryption shall be enabled.
2-2	تفعيل وتطبيق خاصية فصل البيانات بين المعلومات الشخصية والبيانات الخاصة بـ<اسم الجهة>، وذلك في الأجهزة الشخصية للعاملين (مبدأ BYOD) إن كانت تدعم هذه الخاصية. كما يجب تشفير البيانات بعد فصلها.

If supported by personal mobile devices (BYOD), data segregation between personal information and data owned by the <entity name> shall be enabled and enforced. Additionally, segregated data shall be encrypted.	
ضبط وإعداد كلمات مرور مُحمِّل التشغيل (Bootloader) لنظام الإدخال/الإخراج الأساسي (BIOS). BIOS bootloader passwords shall be configured.	3-2
تفعيل إغلاق «مُحمِّل تشغيل» (Bootloader) إن كان الجهاز المحمول يدعم هذا الخيار. If the mobile device supports it, locking Bootloader shall be enabled.	4-2
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. Encryption shall be configured and enforced on any removable storage (e.g., SD cards or USB) that can be accessed by mobile devices.	5-2
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. The device shall be set up to perform automatic lockout after five failed passcode entry attempts, and to perform data wiping after ten failed passcode entry attempts or as supported by the device operating system.	6-2
تفعيل إمكانية مسح البيانات عن بُعد من الأجهزة المفقودة أو المسروقة. Wiping data remotely from lost/stolen devices shall be enabled.	7-2
منع المستخدمين من تعديل أو إلغاء آلية إغلاق «مُحمِّل التشغيل» (Bootloader). Modifying or disabling Bootloader locking by users shall be prohibited.	8-2

9-2	منع إجراء أي عمليات تجاوز القيود 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 بـ<اسم الجهة>. Rooting or jailbreaking a mobile device shall be prohibited, and the use of rooted or jailbroken devices within <entity name>'s IT environment shall also be prohibited.
3	أمن نظام تشغيل وتطبيقات الجهاز (Device OS and Applications Security)
الهدف	ضمان تحديث وضبط نظام التشغيل والتطبيقات المثبّتة في الجهاز المحمول بطريقة مناسبة قبل استخدامه.
المخاطر المحتملة	عدم الكشف عن استخدام التطبيقات غير المصرّح بها أو الملغيّة أو غير المزوّدة بالتحديثات والإصلاحات أو البرمجيات الضارة سيمنع <اسم الجهة> من مراقبة الاستخدام الآمن للأجهزة المحمولة.
الإجراءات المطلوبة	
1-3	إتاحة تثبيت التطبيقات المقدّمة فقط من المتاجر المعتمدة الخاصة بالمورّد أو الجهة. Application installation shall be allowed only from Vendor/Entity approved stores.
2-3	تقييد الأذونات الممنوحة للتطبيقات المثبّتة على الجهاز المحمول بحيث تُطبّق المبدأ الأساسي القائم على الحدّ الأدنى من الصلاحيات. The permissions assigned to applications installed on a mobile device shall be restricted, and the principle of Least Privilege shall be applied.
3-3	تعطيل الكاميرا والميكروفون بشكل افتراضي وتحديد التطبيقات المصرح لها باستخدامها حسب حاجة العمل. Camera and Microphone shall be disabled by default and access to them should be allowed based on need.
4-3	التأكّد من التواقيع الرقمية للتطبيقات قبل تثبيتها. Application digital signatures shall be verified before installation.
5-3	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.

The mobile device shall be updated to last Operating Systems (OS) versions/releases provided by the device vendor. If a device cannot be further updated to a newer OS, and the vendor has not provided security patches for the device in the last two years, the mobile device shall be decommissioned and replaced.	
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. Security Content Automation Protocol (SCAP) shall be utilized to audit and verify all security configuration elements within the mobile devices, catalog approved exceptions, and report any unauthorized changes.	6-3
منع المستخدمين من تعديل أو إلغاء أي إعدادات أمنية للجهاز المحمول. Users shall not be able to modify or remove any secure configurations on the mobile device.	7-3
تعطيل أو إزالة الحسابات الافتراضية، وتقييد الوصول إلى الحسابات ذات الصلاحية العالية على الأجهزة المحمولة بالتوافق مع سياسة إدارة هويات الوصول والصلاحيات. Disabling or removal of virtual accounts, and limiting access to accounts with high privilege based on Identity and Access Management Policy.	8-3
تطوير المعايير الأمنية الأساسية للأجهزة المحمولة وتنفيذها ومراقبتها دورياً. A Minimum-Security Baseline for mobile devices shall be developed, implemented and regularly monitored.	9-3
إجراء نسخ احتياطي كامل ومنتظم للبيانات المخزنة على الأجهزة المحمولة وفقاً لسياسة النسخ الاحتياطية الخاصة بـ<اسم الجهة>. A regular full backup of data stored on the mobile devices shall be performed as per <entity name>'s Backup Policy.	10-3
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.	11-3

Mobile devices shall be regularly patched and updated as per <entity name>'s Workstation and Mobile Device Security Policy and Patch Management Policy to ensure that all OS and application software is up-to-date.	
استخدام عناصر التحكم في الأجهزة وحظر الوصول إلى الوسائط القابلة للإزالة عند الضرورة أو وفقاً لسياسة الاستخدام المقبول في <اسم الجهة>. Hardware controls shall be implemented and access to removable media shall be blocked where necessary or as per <entity name>'s Acceptable Use Policy.	12-3
تثبيت برمجيات التحكم بأجهزة المستخدمين المحمولة على كافة الأجهزة لمنع الاستخدام غير المصرح به لأدوات اتصال الشبكة (Wi-Fi, Bluetooth, etc.) والأجهزة الطرفية. Device control software shall be implemented on all mobile devices to prevent unauthorized use of network communication tools (Wi-Fi, Bluetooth, etc.) or peripheral devices.	13-3
تعطيل كافة خصائص تبادل البيانات أو الملفات مثل (Airdrop, NFC, Bluetooth etc.) Disabling all information and file sharing features such s (Airdrop, NFC, and Bluetooth, etc.).	14-3
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. Protection software including antivirus, antimalware, application whitelisting and data leakage prevention software shall be installed on all mobile devices.	15-3
تطبيق الإعدادات والتحصين لأجهزة المستخدمين بما في ذلك التحصين على مستوى البرمجيات وأنظمة التشغيل وفقاً لسياسة الإعدادات والتحصين في <اسم الجهة>. Workstation configuration hardening, including software and operating system level hardening, shall be implemented in accordance with <entity name>'s Secure Configuration and Hardening Policy.	16-3

الأدوار والمسؤوليات

1- **راعي ومالك وثيقة المعيار:** <رئيس الإدارة المعنية بالأمن السيبراني>.

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

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

الالتزام بالمعيار

1- يجب على <رئيس الإدارة المعنية بالأمن السيبراني> ضمان التزام <اسم الجهة> بهذا المعيار دورياً.

2- يجب على كافة العاملين في <اسم الجهة> الالتزام بهذا المعيار.

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