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 أجهزة المستخدمين

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.

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	عُدلَ بواسطة	تفاصيل الإصدار
<أدخل رقم النسخة>	اضغط هنا لإضافة تاريخ	<أدخل الاسم الكامل للموظف>	<أدخل تفاصيل الإصدار>

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

يهدف هذا المعيار إلى تحديد متطلبات الأمن السيبراني التفصيلية المتعلقة بإدارة أجهزة المستخدمين (Workstations) الخاصة بـ<اسم الجهة> لتقليل المخاطر السيبرانية وحمايتها من 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.

النطاق

يطبق هذا المعيار على جميع أجهزة المستخدمين المكتبية الخاصة بـ<اسم الجهة>، وعلى جميع العاملين (الموظفين والمتعاقدين) في <اسم الجهة>.

المعايير

١	الوصول الآمن
الهدف	ضمان حماية أجهزة المستخدمين ووظائفها من الوصول غير المصرح به.
المخاطر المحتملة	ينطوي على الوصول غير المصرّح به إلى أجهزة المستخدمين مخاطر كبيرة قد تؤدي إلى سرقة المعلومات ووقوع انتهاكات أمنية تُمكن منفذيها من شن المزيد من الهجمات الضارة ضد موظفي <اسم الجهة> وبنيتها التحتية أو ضد أي هدف خارجي آخر.
الإجراءات المطلوبة	
١-١	تطبيق الوصول الآمن وإدارة هويات الدخول لأجهزة المستخدمين بما يتوافق مع المعايير التقنية والأمنية المذكورة في معيار إدارة الصلاحيات والهويات المعتمد لدى <اسم الجهة> لمقاومة الهجمات السيبرانية.
١-٢	تقييد الوصول إلى أجهزة المستخدمين وحصره على حساب المستخدم للجهاز.
١-٣	إلى جانب استخدام تركيبة اسم المستخدم/كلمة المرور، إلزام المستخدم باستخدام آليات المصادقة أو التحقّق من الهوية متعدّد العناصر (MFA)، مثل الخصائص الحيوية والمفاتيح المادية وكلمات المرور المؤقتة والبطاقات الذكية وشهادات التشفير وغيرها، على أجهزة المستخدمين في البيئات فائقة الحماية مثل مركز العمليات الأمنية (SOC).

١-٤	ضبط وإعداد كلمات مرور مُحمِّل التشغيل (Bootloader) لنظام الإدخال/الإخراج الأساسي (BIOS).
١-٥	تقييد الوصول المادي إلى أجهزة المستخدمين على العاملين المصرح لهم فقط.
١-٦	حماية أجهزة المستخدمين من خلال قفل الشاشة أو تسجيل الخروج (screen lock or logout) قبل مغادرة مساحة العمل لمنع الوصل الغير مصرح به.
١-٧	ضبط إعدادات أجهزة المستخدمين بحيث تعرض شاشة توقّف (screen saver) محمية بكلمة مرور في حال عدم استخدام الجهاز (Session Timeout) لمدة <٥ دقائق> لضمان حماية محطات العمل التي تركت بشكل غير آمنة.
١-٨	استخدام طبقات شاشة لدعم الخصوصية أو استخدام حواجز مادية أخرى للحد من تعرض البيانات للاطلاع غير المصرح به.
١-٩	الخروج من التطبيقات قيد التشغيل وإغلاق المستندات المفتوحة عند مغادرة المكتب.
١-١٠	التأكد من وصول أجهزة المستخدمين الآمن للشبكة اللاسلكية وفقًا لمعيار أمن الشبكة اللاسلكية المعتمد لدى <اسم الجهة>.
٢	**مراجعة الإعدادات والتحصين**
الهدف	تحديد متطلبات الأمن السيبراني الحساسة لأجهزة المستخدمين لضمان تصميم أجهزة المستخدمين وإعدادها وتشغيلها بطريقة آمنة.
المخاطر المحتملة	يمكن أن يؤدي الإعداد الخاطئ والتصميم غير الآمن لأجهزة المستخدمين إلى ثغرات أمنية يمكن استغلالها لتهديد سرية وسلامة وتوافر بيانات <اسم الجهة> وسير عملها.
الإجراءات المطلوبة	
٢-١	تطبيق مراجعة الإعدادات والتحصين لأجهزة المستخدمين بما يتوافق مع المعايير التقنية والأمنية المذكورة في معيار إعدادات الحماية والتحصين المعتمد في <اسم الجهة> لمقاومة الهجمات السيبرانية.
٢-٢	حذف التطبيقات والخدمات غير الضرورية أو غير اللازمة أو إلغاء تفعيلها على أجهزة المستخدمين مثل بروتوكول تل نت (Telnet)، ولوحة المفاتيح باللمس، والسجل عن بعد (إذا لم يكن ضروريًا)، وغيرها.
٢-٣	إنشاء نسخ وقوالب آمنة لأجهزة المستخدمين بناءً على معايير الإعدادات المعتمدة ووفقًا لسياسة الإعدادات والتحصين المعتمدة لدى <اسم الجهة> وإعادة نسخ الأجهزة باستخدام أحد قوالب نسخ أجهزة المستخدمين في حال تعرضها لانتهاك أمني.

٢-٤	تخزين نسخ أجهزة المستخدمين في بيئة آمنة على أو بيئة تخزين معدة بصورة آمنة وغير مرتبطة بالشبكة والتحقق بانتظام من هذه النسخ باستخدام أدوات مراقبة سلامة المعلومات.
٢-٥	منع تنزيل برامج غير مصرح بها على أجهزة المستخدمين.
٢-٦	استخدام خاصية العلامة المائية (Watermark) على أجهزة المستخدمين.
٣	برمجيات حماية الأجهزة الطرفية
الهدف	ضمان حماية أجهزة المستخدمين من الفيروسات والبرمجيات الضارة والتهديدات المتقدّمة المستمرة والهجمات غير المعروفة مسبقًا وأي نوع آخر من الهجمات الخبيثة.
المخاطر المحتملة	يمكن أن تؤدي الهجمات الخبيثة الناجحة على أجهزة المستخدمين إلى تعريض <اسم الجهة> لاختراق أمني أو الوصول غير المصرح به أو الكشف عن بياناتها في حال تركت أجهزة المستخدمين دون حماية.
الإجراءات المطلوبة	
٣-١	منع إنشاء/تعديل/حذف إعدادات نظام التشغيل وبرامج حماية الأجهزة الطرفية، مثل إلغاء تفعيل تغيير وقت النظام يدويًا، وتعديل ملفات النظام، وإنشاء الملفات أو تعديلها أو حذفها، وغيره.
٣-٢	تطبيق خاصية السماح بقائمة محددة من التطبيقات على أجهزة المستخدمين لتمكين عمل تطبيقات وبرمجيات محددة فقط وفقًا للحاجة.
٣-٣	تطبيق خاصية السماح بقائمة محددة من التطبيقات واستخدام ميزتين لتحديد التطبيق، بما في ذلك على سبيل المثال لا الحصر، قواعد التجزئة المشفرة أو قواعد شهادات الناشر أو قواعد المسار للسماح باستخدام التطبيقات أو منعها.
٣-٤	ضبط إعدادات أنظمة السماح بقائمة محددة من التطبيقات بحيث لا يمكن للمستخدمين إلغاء تفعيل الأنظمة باستثناء المديرين عند أدائهم لمهام إدارية معينة تقتضي إلغاء تفعيل السماح بقائمة محددة من التطبيقات مؤقتًا.
٣-٥	فيما يخص خاصية السماح بقائمة محددة من التطبيقات، يجب تعريف الملفات التنفيذية المعتمدة (exe, com, pif, وغيرها) ومكتبات البرمجيات (dll, ocx, وغيرها) والنصوص (ps١, bat, vbs, وغيرها) وبرامج التثبيت (msi, msp, وغيرها) من أجل تنفيذ الملفات من القائمة المعتمدة فقط.
٣-٦	تطبيق نظام الحماية المتقدمة لاكتشاف ومنع الاختراقات في المستضيف (Host-based Intrusion Prevention System "HIPS") على جميع أجهزة المستخدمين.

اختر التصنيف

الإصدار <١,٠>

٣-٧	تطبيق جدار حماية من البرمجيات المستضافة على جميع أجهزة المستخدمين.
٣-٨	تطبيق برامج مكافحة الفيروسات على جميع أجهزة المستخدمين.
٣-٩	تطبيق برامج مكافحة البرامج الضارة على جميع أجهزة المستخدمين.
٣-١٠	تطبيق برامج الحماية من التهديدات المتقدمة المستمرة (APT) على جميع أجهزة المستخدمين.
٣-١١	تطبيق برامج اكتشاف أجهزة النهاية الطرفية والاستجابة لها على جميع أجهزة المستخدمين.
٣-١٢	تطبيق برمجيات التحكم بأجهزة النهاية الطرفية على كافة أجهزة المستخدمين لمنع أي دخول من أجهزة خارجية غير مصرحة.
٣-١٣	تطبيق منع تسّرب البيانات (DLP) حيثما كان ذلك لازمًا وفقًا للسياسات والإجراءات ذات العلاقة في <اسم الجهة>.
٤	**التشفير**
الهدف	ضمان الحفاظ على سريّة بيانات المستخدمين والتأكّد من سلامتها وموثوقيتها لحمايتها من الوصول غير المصرّح به والكشف عن المعلومات الحسّاسة.
المخاطر المحتملة	قد يؤدي عدم وجود التقنيات الأمنية المناسبة لضمان تشفير بيانات أجهزة المستخدمين إلى تعرض بيانات <اسم الجهة> لمخاطر سيبرانية عالية نتيجة الوصول غير المصرح به إلى هذه البيانات.
الإجراءات المطلوبة	
٤-١	تطبيق التشفير لأجهزة المستخدمين بما يتوافق مع المعايير التقنية والأمنية المذكورة في معيار التشفير المعتمد لدى <اسم الجهة> للحد من محاولات الاطلاع غير المصرح به.
٤-٢	تشفير وسائط التخزين في أجهزة المستخدمين بما في ذلك الأقراص الصلبة وفقًا للسياسات والإجراءات ذات العلاقة في <اسم الجهة>.
٤-٣	استخدام بروتوكول إدارة أجهزة المستخدمين الذي يدعم التشفير أو يقوم بضبط إعدادات التشفير لبروتوكولات إدارة أجهزة المستخدمين مثل: بروتوكول النفاذ إلى الدليل البسيط (LDAP) على أمن طبقة النقل (TLS)، والنسخة الثالثة من بروتوكول إدارة الشبكة

	البسيط (SNMPv٣) لغايات المصادقة والخصوصية، وبروتوكول كيربيروس (Kerberos) مع أمن طبقة النقل (TLS)، وسجل النظام (syslog)، وغيرها.
٥	الإدارة المركزية
الهدف	تحديد المتطلبات الأمنية لإدارة أجهزة المستخدمين لضمان تشغيل أجهزة المستخدمين وإداراتها مركزيًا وبطريقة آمنة وضمان تطبيق جميع المتطلبات الأمنية وتنفيذها.
المخاطر المحتملة	يؤدي الافتقار إلى الإدارة الآمنة وعدم تطبيق المتطلبات الأمنية على أجهزة المستخدمين إلى زيادة احتمالية التعرض للهجمات، ويزيد من فرص وجود ثغرات ونقاط ضعف في بيئة <اسم الجهة> يمكن استغلالها في الهجمات أو الاختراقات الخبيثة، مما يعرض أجهزة المستخدمين والبيانات في <اسم الجهة> إلى انتهاكات أمنية.
الإجراءات المطلوبة	
٥-١	ضبط إعدادات خادم الإدارة المركزية أو خادم النطاق ليطبق سياسة أمن الخوادم في <اسم الجهة> على جميع أجهزة المستخدمين.
٥-٢	تثبيت أدوات إدارة إعدادات النظام التي تنفذ إعدادات الضبط والتهيئة لأجهزة المستخدمين وتعيد تثبيتها تلقائيًا في فترات زمنية محددة ومنتظمة. للمزيد من التفاصيل، يرجى الرجوع إلى سياسة الإعدادات والتحصين في <اسم الجهة>.
٥-٣	تطبيق نظام مراقبة الإعدادات المتوافقة مع بروتوكول أتمتة محتوى الأمن (Security Content Automation Protocol "SCAP") للتأكد من عناصر الإعدادات الأمنية كافة وجدولة الاستثناءات المعتمدة والإبلاغ عن حدوث أي تغييرات غير مصرّح بها.
٦	أجهزة المستخدمين ذات الصلاحيات والامتيازات الهامة والحساسة (Privileged Access Workstations “PAW”)
الهدف	تحديد المتطلبات الأمنية الإضافية لحماية أجهزة المستخدمين ذات الصلاحيات والامتيازات الهامة والحساسة (PAWs) المستخدمة في الوصول إلى الأنظمة ومناطق الشبكة الهامة.
المخاطر المحتملة	يمكن أن تؤدي الهجمات الخبيثة الناجحة على أجهزة المستخدمين ذات الصلاحيات الهامة والحساسة إلى تعريض <اسم الجهة> لاختراقات خطيرة وانتهاكات أمنية لأهم أصولها الحساسة مما يؤدي إلى أضرار جسيمة.
الإجراءات المطلوبة	

٦-١	فرض استخدام التحقّق من الهوية متعدّد العناصر من أجل الوصول إلى أجهزة المستخدمين ذات الصلاحيات والامتيازات الهامة والحساسة (PAW) التي يستخدمها مديرو النظام.
٦-٢	تقييد الوصول إلى أجهزة المستخدمين ذات الصلاحيات والامتيازات الهامة والحساسة (PAW) وحصره على المشرفين والمشغلين المصرح لهم فقط.
٦-٣	وضع أجهزة المستخدمين ذات الصلاحيات والامتيازات الهامة والحساسة (PAW) في منطقة الإدارة في الشبكة.
٦-٤	تشفير جميع أنواع الحركة المنقولة من أو إلى أجهزة المستخدمين ذات الصلاحيات والامتيازات الهامة والحساسة (PAW) بما في ذلك حركة الوصول الإداري والتحكم (مثل بروتوكول النقل الآمن "SSH"، وبروتوكول التحكم بسطح المكتب عن بعد "RDP")، وحركة البيانات باستخدام آليات التشفير (مثل أمن طبقة النقل "TLS") وفقًا لمعيار التشفير المعتمد في <اسم الجهة>.
٦-٥	إلغاء تفعيل خاصية الوصول إلى الإنترنت على أجهزة المستخدمين ذات الصلاحيات والامتيازات الهامة والحساسة (PAW).
٦-٦	إلغاء تفعيل الخدمات غير الأساسية أو اللازمة (مثل إرسال رسائل البريد الإلكتروني واستلامها) على أجهزة المستخدمين ذات الصلاحيات والامتيازات الهامة والحساسة (PAW).
٦-٧	تفعيل جميع مستويات التسجيل، إلى جانب سجل التدقيق والسجلات الأمنية، محليًا وعلى نظام تسجيل أحداث مركزي.
٧	معايير أخرى
الهدف	تطبيق جميع المعايير والمتطلبات الأمنية لأجهزة المستخدمين لضمان أعلى مستويات الحماية.
المخاطر المحتملة	عدم تطبيق جميع المعايير والمتطلبات الأمنية يعرض <اسم الجهة> إلى زيادة في المخاطر الأمنية التي تهدد أجهزة المستخدمين.
الإجراءات المطلوبة	
٧-١	تطبيق المعايير التالية ذات الصلة بأجهزة المستخدمين: ١. معيار إدارة سجلات الأحداث ومراقبة الأمن السيبراني ٢. معيار الأمن السيبراني في إدارة النسخ الاحتياطية ٣. معيار الأمن المادي

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 دوريًا.

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>.