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

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.

اختر التصنيف

التاريخ: اضغط هنا لإضافة نص

الإصدار: اضغط هنا لإضافة نص

المرجع: اضغط هنا لإضافة نص

# 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

الغرض من هذا المعيار هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بإدارة أجهزة المستخدمين (Workstations) الخاصة بـ<اسم الجهة> لتقليل المخاطر السيبرانية وحمايتها من التهديدات الداخلية والخارجية من خلال التركيز على الأهداف الأساسية للحماية وهي: سرية المعلومات، وسلامتها، وتوافرها.

ويهدف هذا المعيار إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهو مطلب تشريعي في الضابط رقم ٢-٣-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة عن الهيئة الوطنية للأمن السيبراني.

## نطاق العمل وقابلية التطبيق

يغطي هذا المعيار جميع أجهزة المستخدمين المكتبية الخاصة بـ<اسم الجهة>، وينطبق على جميع العاملين في <اسم الجهة>.

## المعايير

| 1 | الوصول الآمن (Secure Access) |
|---|---|
| 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 | |
| 1-1 | تقييد الوصول إلى أجهزة المستخدمين وحصره على حساب المستخدم للجهاز.<br>Access to workstations shall be limited to the accounts of the individual users of the workstations only. |
| 2-1 | تطبيق مبدأ الحد الأدنى من الصلاحيات والامتيازات عند منح الصلاحيات على أجهزة المستخدمين.<br>Least Privilege principle shall be applied to provide access to users' workstations. |
| 3-1 | إلغاء أو إعادة تسمية الحسابات الافتراضية أو غير التفاعلية أو غير اللازمة. |

| | |
|---|---|
| Default/non-interactive/unneeded accounts shall be disabled or renamed. | |
| 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).<br>In addition to a user/password combination, users shall be required to use other authentication mechanisms or Multi-Factor Authentication (MFA), such as biometrics, hardware keys, one-time passwords, smart cards, certificates, etc., on workstations of highly protected environment, such as Security Operations Center (SOC). | 4-1 |
| إعداد متطلبات تعقيد كلمة المرور الخاصة بجهاز المستخدم وفقاً لسياسة إدارة هويات الدخول والصلاحيات في <اسم الجهة>.<br>Workstation password complexity requirements shall be configured in accordance with <entity name>'s Identity and Access Management Policy. | 5-1 |
| ضبط وإعداد حد الإغلاق بعد عدد معين من محاولات تسجيل الدخول غير الناجحة وانتهاء وقت الجلسة وتسجيل الخروج في حال عدم الاستخدام بالنسبة لحالات الوصول المحلية والوصول إلى النطاقات وفقاً لسياسة إدارة هويات الدخول والصلاحيات في <اسم الجهة>.<br>Login attempts lockout, session timeout and session idle logout for local access and domain access shall be configured in accordance with <entity name>'s Identity and Access Management Policy. | 6-1 |
| ضبط وإعداد كلمات مرور مُحمِّل التشغيل (Bootloader) لنظام الإدخال/الإخراج الأساسي (BIOS).<br>BIOS bootloader passwords shall be configured. | 7-1 |
| مراجعة الإعدادات والتحصين (Secure Hardening Configuration) | 2 |

| | |
|---|---|
| الهدف | تحديد متطلبات الأمن الأساسية 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 | |
| 1-2 | إجراء اختبارات أمنية منتظمة (مثل تقييم الثغرات الأمنية واختبار الاختراق) وفقاً لسياسة إدارة الثغرات الأمنية المتّبعة في <اسم الجهة>.<br>Regular security testing (such as vulnerability assessments and penetration testing) shall be conducted in accordance with <entity name>'s Vulnerability Management Policy. |
| 2-2 | إجراء التحديثات والإصلاحات على أجهزة المستخدمين بانتظام وفقاً لسياسة أمن أجهزة المستخدمين وسياسة إدارة التحديثات والإصلاحات في <اسم الجهة> لضمان تحديث جميع أنظمة التشغيل وبرمجيات التطبيقات على أجهزة المستخدمين.<br>Workstations shall be regularly patched and updated in accordance with <entity name>'s Workstation Security Policy and Patch Management Policy to ensure that all workstation Operating Systems (OS) and application software are up-to-date. |
| 3-2 | 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 ضرورياً)، وغيرها.<br>Unnecessary/unrequired applications and services, such as Telnet Protocol, touch keyboard, remote registry (if not needed), etc., shall be removed/disabled on workstations. |
| 4-2 | حذف/تعطيل خصائص نظام التشغيل والتطبيق وملفات الإعدادات غير الضرورية أو غير اللازمة أو إلغاء تفعيلها.<br>Unnecessary/unrequired OS and application features and configuration files shall be removed/disabled. |
| 5-2 | حجب إمكانية الوصول إلى أدلة الشبكة والملفات غير الضرورية أو غير اللازمة.<br>Access to unnecessary/unrequired network and file directories shall be blocked. |

| | |
|---|---|
| 6-2 | استخدام الضوابط المادية وحظر الوصول إلى الوسائط القابلة للإزالة عند الضرورة أو وفقاً لسياسة الاستخدام المقبول في <اسم الجهة>.<br>Hardware controls shall be used and access to removable media shall be blocked where necessary or as per <entity name>'s Acceptable Usage Policy. |
| 7-2 | تطبيق الإعدادات والتحصين لأجهزة المستخدمين بما في ذلك التحصين على مستوى البرمجيات وأنظمة التشغيل وفقاً لسياسة الإعدادات والتحصين في <اسم الجهة>.<br>Workstation configuration hardening, including software and operating system level hardening, shall be implemented in accordance with <entity name>'s Secure Configuration and Hardening Policy. |
| 8-2 | إنشاء نسخ وقوالب آمنة لأجهزة المستخدمين بناءً على معايير الإعدادات المعتمدة ووفقاً لسياسة الإعدادات والتحصين في <اسم الجهة>. وإعادة نسخ الأجهزة باستخدام أحد قوالب نسخ أجهزة المستخدمين في حال تعرضها لانتهاك أمني.<br>Secure workstation images or templates shall be created for all workstations based on the approved configuration standards and as per <entity name>'s Secure Configuration and Hardening Policy. Compromised workstations shall be reimaged using one of the workstation image templates. |
| 9-2 | تخزين نسخ أجهزة المستخدمين في بيئة آمنة على نسخ احتياطية أو بيئة تخزين معدة بصورة آمنة وغير مرتبطة بالشبكة والتحقق بانتظام من هذه النسخ باستخدام أدوات مراقبة سلامة المعلومات.<br>Workstation images shall be stored in a secure environment on securely configured offline backups or storage environment, and they shall be validated regularly using integrity monitoring tools. |
| 3 | النسخ الاحتياطي والأرشفة (Backup and Archiving) |
| الهدف | ضمان سلامة بيانات أجهزة المستخدمين من العبث بها أو فقدانها بالخطأ أو تخريبها والتأكد من توافرها وإمكانية استعادتها. |
| المخاطر المحتملة | في حال حذف بيانات أجهزة المستخدمين بالخطأ أو العبث بها أو فقدانها أو تخريبها أو تعرّضها لهجوم إلكتروني، لن تتمكّن <اسم الجهة> من استعادة البيانات، مما سيؤثّر في أنشطة أعمالها الاعتيادية. |

| | الإجراءات المطلوبة |
|---|---|
| 1-3 | عمل نسخ احتياطية كاملة وتزايدية لأجهزة المستخدمين وفقاً لسياسة إدارة النسخ الاحتياطي المعتمدة في <اسم الجهة>. ويجب أن تشمل النسخ الاحتياطية على الأقل نسخاً احتياطية لنظام تشغيل أجهزة المستخدمين، ونسخاً احتياطية لإعدادات البرمجيات، ونسخاً احتياطية للبيانات.<br><br>Full and incremental backup of workstations shall be performed in accordance with <entity name>'s Backup and Recovery Management Policy. The backups must include, at minimum, workstations operating system backups, software configuration backups, and data backups. |
| 2-3 | تخزين النسخ الاحتياطية لثلاث فترات متتالية بما في ذلك الفترة الحالية. فعلى سبيل المثال، إذا تم عمل النسخ الاحتياطية شهرياً، يجب تخزين النسخ الاحتياطية للشهر الحالي ولشهرين سابقين فقط.<br><br>Three generations of backups shall be stored including the backups for the current period. For example, if backup is performed monthly, backups of the current month and the two previous months shall be stored only. |
| 3-3 | تشفير النسخ الاحتياطية لأجهزة المستخدمين الخاصة بـ<اسم الجهة>.<br><br><Entity name>'s workstation backups shall be encrypted. |
| 4-3 | ترتيب النسخ الاحتياطية الخاصة بأجهزة مستخدمي <اسم الجهة> تسلسلياً وتسجيل وقتها وتاريخها وجدولتها.<br><br><Entity name>'s workstation backups shall be serialized, time-dated and indexed. |
| 5-3 | اختبار إمكانية استرجاع النسخة الاحتياطية كل ثلاثة أشهر وفقاً لسياسة إدارة النسخ الاحتياطي المعتمدة في <اسم الجهة>.<br><br>Backup recovery shall be tested every quarter or as per <entity name>'s Backup and Recovery Management Policy. |
| 6-3 | تطبيق آليات توثيق النسخ الاحتياطي وسلامتها لضمان نسخ بيانات أجهزة المستخدمين أو أرشفتها بطريقة صحيحة. |

| | |
|---|---|
| | Backup verification and integrity mechanisms shall be employed to ensure that data is being correctly backed up or archived. |
| 4 | برمجيات حماية الأجهزة الطرفية (Endpoint Protection Software) |
| الهدف | ضمان حماية أجهزة المستخدمين من الفيروسات والبرمجيات الضارة والتهديدات المتقدّمة المستمرة والهجمات غير المعروفة مسبقاً 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 | |
| 1-4 | ضبط وإعداد حد إغلاق نظام التشغيل ووظائف التطبيقات عن طريق الحد الأدنى من الصلاحيات والامتيازات المطلوبة للتشغيل في الظروف الاعتيادية، مثل إلغاء تفعيل تغيير وقت النظام يدوياً، وتعديل ملفات النظام، وإنشاء الملفات أو تعديلها أو حذفها، وغيره.<br>OS and application functionality lockout shall be configured with the least privilege required to operate in normal conditions. For example, changing system time manually, editing system files, creating/modifying/deleting files, etc., shall be disabled. |
| 2-4 | تطبيق خاصية السماح بقائمة محددة من التطبيقات على أجهزة المستخدمين لتمكين عمل تطبيقات وبرمجيات محددة فقط وفقاً للحاجة.<br>Application whitelisting shall be implemented on workstations to allow only specific applications and software to run based on need. |
| 3-4 | تطبيق خاصية السماح بقائمة محددة من التطبيقات لاستخدام خاصيتين لتحديد التطبيق، بما في ذلك على سبيل المثال وليس الحصر، قواعد التجزئة المشفرة أو قواعد شهادات الناشر أو قواعد المسار للسماح باستخدام التطبيقات أو منعها.<br>Application whitelisting shall be implemented to use two features of identifying the application, including but not limited to cryptographic hash rules, publisher certificate rules or path rules to allow or restrict the use of applications. |

| | |
|---|---|
| 4-4 | 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 مؤقتاً.<br>Application whitelisting agents shall be configured so that users cannot disable the agents with the exception of administrators when performing specific administrative tasks that require disabling application whitelisting temporarily. |
| 5-4 | فيما يخص خاصية السماح بقائمة محددة من التطبيقات، يجب تعريف الملفات التنفيذية المعتمدة (exe, com, pif, وغيرها) ومكتبات البرمجيات (dll, ocx, وغيرها) والنصوص (ps1, bat, vbs, وغيرها) وبرامج التثبيت (msi, msp, وغيرها) من أجل تنفيذ الملفات من القائمة المعتمدة فقط.<br>For application whitelisting, a list of approved executable files (exe, com, pif, etc.), software libraries (dll, ocx, etc.), scripts (ps1, bat, vbs, etc.), and installers (msi, msp, etc.) shall be defined to allow files from the approved list to be executed only. |
| 6-4 | تطبيق نظام الحماية المتقدمة لاكتشاف ومنع الاختراقات في المستضيف (Host-based Intrusion Prevention System "HIPS") على جميع أجهزة المستخدمين.<br>Host-based Intrusion Prevention System (HIPS) shall be implemented on all workstations. |
| 7-4 | تطبيق جدار حماية من البرمجيات المستضافة على جميع أجهزة المستخدمين.<br>Software host firewall shall be implemented on all workstations. |
| 8-4 | تطبيق برامج مكافحة الفيروسات على جميع أجهزة المستخدمين.<br>Antivirus shall be implemented on all workstations. |
| 9-4 | تطبيق برامج مكافحة البرامج الضارة على جميع أجهزة المستخدمين.<br>Antimalware shall be implemented on all workstations. |
| 10-4 | تطبيق برامج الحماية من التهديدات المتقدمة المستمرة (APT) على جميع أجهزة المستخدمين. |

| | |
|---|---|
| | Host Advanced Persistent Threat (APT) agents shall be implemented on all workstations. |
| 11-4 | تطبيق برامج اكتشاف أجهزة النهاية الطرفية والاستجابة لها على جميع أجهزة المستخدمين.<br>Endpoint Detection and Response shall be implemented on all workstations. |
| 12-4 | تطبيق برمجيات التحكم بأجهزة النهاية الطرفية على كافة أجهزة المستخدمين لمنع أي دخول من أجهزة خارجية غير مصرحة.<br>Endpoint Device Control software shall be implemented on all workstations to prevent the use of unauthorized peripheral devices. |
| 13-4 | تطبيق منع تسّرب البيانات (DLP) حيثما كان ذلك لازماً وفقاً للسياسات والإجراءات ذات العلاقة في <اسم الجهة>.<br>Data Leakage Prevention (DLP) shall be implemented where deemed necessary by <entity name>'s relevant policies and procedures. |
| 5 | تسجيل الأحداث وسجل التدقيق (Event and Audit Logging) |
| الهدف | التأكّد من توثيق وتسجيل الأحداث الأمنية والأنشطة غير المصرّح بها التي تشهدها أجهزة المستخدمين. |
| المخاطر المحتملة | قد يؤدي عدم تفعيل وتسجيل الأحداث الأساسية التي تُنفذ في أجهزة المستخدمين والتي حدّدتها متطلّبات الضابط إلى صعوبة اكتشاف ومنع الهجمات السيبرانية، أو إساءة استخدام الصلاحيات الهامة والحساسة، مما قد يؤثّر على أعمال <اسم الجهة>. |
| الإجراءات المطلوبة | |
| 1-5 | ضبط وإعداد سجل أجهزة المستخدمين وسجل التدقيق ليتم ترحيلهما إلى نظام تسجيل مركزي وفقاً لسياسة ومعيار إدارة سجلات الأحداث ومراقبة الأمن السيبراني في <اسم الجهة>.<br>Workstation logging and audit trail shall be configured to be forwarded to a centralized logging system as per <entity name>'s Cybersecurity Event Logs and Monitoring Management Policy and Standard. |

| | |
|---|---|
| 2-5 | إعداد أجهزة المستخدمين ليتزامن توقيتها مع توقيت ثلاثة أجهزة تزامن مركزية على الأقل مما يسمح بتزامن توقيت سجلات الأحداث.<br>Workstations shall be configured to synchronize clock to at least three redundant central time workstations to ensure that timestamps in logs are consistent. |
| 3-5 | ضبط إعدادات أجهزة المستخدمين وذلك بحفظ سجلات الأحداث المحلية، وسجلات التدقيق والسجلات الأمنية، بحيث تشمل جميع مستويات السجلات.<br>Local logging, as well as audit trail and security logs, shall be configured with all levels of logging. |
| 6 | التشفير (Cryptography) |
| 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 | |
| 1-6 | تطبيق تقنيات التشفير مثل أمن طبقة النقل (TLS) والشبكات الخاصة الافتراضية (VPN) لحماية آليات التحقّق من الهوية أثناء إرسال الرسائل، واستخدام أحدث بروتوكولات التشفير وخوارزميات التشفير المدعومة (Cipher Suite) المُوصى بها. للمزيد من التفاصيل، يُرجى الرجوع إلى معيار التشفير المعتمد في <اسم الجهة>.<br>Encryption technologies, such as Transport Layer Security (TLS) and Virtual Private Network (VPN), shall be implemented to protect authentication mechanisms during transmission. In addition, recommended next generation encryption protocols and cipher suites shall be used. For more details, refer to <entity name>'s Cryptography Standard. |
| 2-6 | تشفير وسائط التخزين في أجهزة المستخدمين بما في ذلك الأقراص الصلبة حيثما كان ذلك ضرورياً وفقاً للسياسات والإجراءات ذات العلاقة في <اسم الجهة>.<br>Workstations storage media, including hard disks, shall be encrypted where deemed necessary by <entity name>'s relevant policies and procedures. |

| | |
|---|---|
| 3-6 | 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 (SNMPv3) لغايات المصادقة والخصوصية، وبروتوكول كيربيروس (Kerberos) مع أمن طبقة النقل (TLS)، وسجل النظام المشفر، وغيرها.<br><br>Workstation management protocol that supports or configures encryption for workstation management protocols, such as LDAP over TLS, SNMPv3 with authentication and privacy, Kerberos with TLS, encrypted syslog, etc., shall be used. |
| 7 | الإدارة المركزية (Central Management) |
| الهدف | تحديد المتطلبات الأمنية لإدارة أجهزة المستخدمين لضمان تشغيل أجهزة المستخدمين وإداراتها مركزياً 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 | |
| 1-7 | ضبط إعدادات خادم الإدارة المركزية أو خادم النطاق ليطبق سياسة أمن الخوادم في <اسم الجهة> على جميع أجهزة المستخدمين.<br><br>The central management server or domain server shall be configured to enforce <entity name>'s policies on all workstations. |
| 2-7 | تثبيت أدوات إدارة إعدادات النظام التي تنفذ إعدادات الضبط والتهيئة لأجهزة المستخدمين وتعيد تثبيتها تلقائياً في فترات زمنية محددة ومنتظمة. للمزيد من التفاصيل، يرجى الرجوع إلى سياسة الإعدادات والتحصين في <اسم الجهة>.<br><br>System configuration management tools that automatically enforce and redeploy configuration settings to workstations at regularly scheduled intervals shall be deployed. For more details, refer to the <entity name>'s Secure Configuration and Hardening Policy. |
| 3-7 | 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.<br>A Security Content Automation Protocol (SCAP) compliant configuration monitoring system shall be implemented to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur. |
| 8 | أجهزة المستخدمين ذات الصلاحيات والامتيازات الهامة والحساسة<br>(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 | |
| 1-8 | فرض استخدام التحقّق من الهوية متعدّد العناصر من أجل الوصول إلى أجهزة المستخدمين ذات الصلاحيات والامتيازات الهامة والحساسة (PAW) التي يستخدمها مديرو النظام.<br>Use of multi-factor authentication shall be required for accessing PAWs used by system administrators. |
| 2-8 | تقييد الوصول إلى أجهزة المستخدمين ذات الصلاحيات والامتيازات الهامة والحساسة (PAW) وحصره على المشرفين والمشغلين المصرح لهم فقط.<br>Access to PAWs shall be restricted to only authorized administrators and operators. |
| 3-8 | وضع أجهزة المستخدمين ذات الصلاحيات والامتيازات الهامة والحساسة (PAW) في منطقة الإدارة في الشبكة.<br>PAWs shall be placed in the network management zone. |
| 4-8 | 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") وفقاً لمعيار التشفير المعتمد في <اسم الجهة>.<br>All traffic transmitted to or out of PAWs, including administrative access and control traffic (such as Secure Shell "SSH" and Remote Desktop Protocol "RDP"), and data traffic using cryptographic mechanisms (such as Transport Layer Security "TLS"), shall be encrypted as per <entity name>'s Cryptography Standard. |
| 5-8 | إلغاء تفعيل خاصية الوصول إلى الإنترنت على أجهزة المستخدمين ذات الصلاحيات والامتيازات الهامة والحساسة (PAW).<br>Internet access on PAWs shall be disabled. |
| 6-8 | إلغاء تفعيل الخدمات الخطرة وغير اللازمة (مثل إرسال رسائل البريد الإلكتروني واستلامها) على أجهزة المستخدمين ذات الصلاحيات والامتيازات الهامة والحساسة (PAW).<br>Unnecessary and risky services (such as sending and receiving emails) shall be disabled on PAWs. |
| 7-8 | تفعيل جميع مستويات التسجيل، إلى جانب سجل التدقيق والسجلات الأمنية، محلياً وعلى نظام تسجيل أحداث مركزي.<br>All levels of logging, as well as audit trail and security logs, shall be enabled locally and to a centralized event logging system. |

## 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>.

## 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>.