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 إدارة سجلات الأحداث ومراقبة الأمن السيبراني

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

يهدف هذا المعيار إلى توفير متطلبات الأمن السيبراني التقنية المبنية على أفضل الممارسات والمعايير لإدارة سجلات الأحداث ومراقبة الأمن السيبراني والعمل على حماية <اسم الجهة> من التهديدات الداخلية والخارجية.

يتبع هذا المعيار المتطلبات التشريعية والتنظيمية الوطنية وأفضل الممارسات الدولية ذات العلاقة، وهو متطلب تشريعي في الضابط رقم ١-٣-٣ والضابط رقم ٢-١٢-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل

يغطي هذا المعيار جميع تقنيات إدارة سجلات الأحداث ومراقبة الأمن السيبراني (SIEM) في <اسم الجهة>، وينطبق على جميع العاملين في <اسم الجهة>.

المعايير

1	صيغة السجل (Log Format)
الهدف	استخدام صيغة قياسية ومتسقة للسجل تشتمل على جميع المعلومات المطلوبة.
المخاطر المحتملة	قد يصعب الربط بين عدة سجلات مختلفة إذا تم حفظها بصورة غير متسقة، وهذا يؤدي إلى زيادة المخاطر الناتجة عن المعلومات الخاطئة، وبالتالي يُعقِّد التعامل مع الأحداث الأمنية وحلها.
الإجراءات المطلوبة	
1-1	يجب أن تشتمل صيغة سجل الأحداث على المعلومات التالية: 1-1-1 **نوع سجل الأحداث:** مثل النظام، والأمن، والتدقيق، والنقطة الأساسية (Kernel)، والتصريح، والبريد، وغيرها. 1-1-2 **موقع** الحدث أو مصدر السجل ونظامه. 1-1-3 **تاريخ** سجل الحدث **وختمه الزمني.** 1-1-4 **حالة الحدث:** مثل ناجح، أو فاشل، أو نشط، أو غير نشط، أو مسموح، أو مرفوض، أو غيره. 1-1-5 **مستوى خطورة الحدث:** مثل طارئ، أو تنبيه، أو حرج، أو خطأ، أو تحذير، أو إشعار معلوماتي، أو إشعار تصحيحي. 1-1-6 **رسالة الحدث:** رسالة فعلية من الحدث. Events log format shall include:

	1-1-1 **Event Log Type:** Such as System, Security, Audit, Kernel, Authorization, Mail, etc. 1-1-2 **Location** of the event or source/system of the log. 1-1-3 **Date** and **Timestamp** of the event log. 1-1-4 **Event Status:** Success, Failure, Up, Down, Allow, Deny, etc. 1-1-5 **Event Severity:** Emergency, Alert, Critical, Error, Warning, Notice, Informational, etc. 1-1-6 **Event Message:** Actual message of the event.
2-1	إدراج تفاصيل إضافية في السجلات حيثما ينطبق ذلك، مثل: المستخدم وعنوان الإنترنت ومنفذ المصدر، وعنوان ومنفذ الوجهة، وعناصر أخرى مفيدة. Additional details shall be included in logs wherever applicable, such as user, source address/port, destination address/port, and other useful elements.
2	الأختام الزمنية (Timestamps) - الخوادم الزمنية المتزامنة الإضافية (Redundant Time Servers Synchronized)
الهدف	استخدام نظام زمني ثابت للأصول المعلوماتية والتقنية الداخلية.
المخاطر المحتملة	قد يصعب المقارنة بين مجموعتين مختلفتين من السجلات إذا تم حفظها بصورة غير متسقة، ويؤدي ذلك إلى زيادة المخاطر الناتجة عن المعلومات الخاطئة وبالتالي يُعقِّد التعامل مع الأحداث الأمنية وحلها.
الإجراءات المطلوبة	
1-2	تزامن الأصل المعلوماتي والتقني مع ثلاثة خوادم زمنية إضافية على الأقل في غضون أجزاء من الثانية. The information and technology asset shall be synchronized to at least three redundant central time servers within milliseconds.
3	تسجيل الأحداث (Event Logging)
الهدف	التأكّد من توثيق وتسجيل الأحداث السيبرانية والأنشطة غير المصرّح بها التي تشهدها البيئة.

المخاطر المحتملة	من الضروري تسجيل بعض الأحداث الأساسية التي تُنفذ في البيئة، وإذا تعذّر على <اسم الجهة> تسجيل الأحداث التي حدّدتها متطلّبات الضابط، فسيؤدي ذلك إلى زيادة المخاطر الناتجة عن الأحداث غير المُحدّدة وغير المصرّح بها المحتمل حدوثها في البيئة، والتي قد تؤثّر على أعمال الجهة بناءً على مستوى خطورة الحدث.
الإجراءات المطلوبة	
1-3	تسجيل جميع الأحداث المُحدّدة في متطلّبات هذا الضابط والتي تشمل: 1-1-3 محاولات الدخول الناجحة. 2-1-3 محاولات الدخول غير الناجحة، بالإضافة إلى تحديد ما إذا كانت محاولة الدخول قد تضمّنت إدخال كلمة مرور خاطئة. 3-1-3 جميع عمليات تسجيل الخروج. 4-1-3 الإضافات والمحذوفات والتعديلات على حسابات وصلاحيات المستخدم. 5-1-3 تغيير المستخدم لهويته خلال فترة زمنية معيّنة على الإنترنت. 6-1-3 محاولات لتنفيذ مهام غير مصرّح بها. 7-1-3 أنشطة الحسابات التي تملك صلاحيات هامة وحسّاسة. 8-1-3 إجراء تعديلات على إعدادات النظام (محدّدات النظام). 9-1-3 حق الوصول لقراءة أو تعديل معلومات سريّة للغاية التي يُحتمل تعرّضها للسرقة. 10-1-3 تسريب مواد متعلّقة بمعلومات سريّة للغاية خارج <اسم الجهة>. 11-1-3 الأحداث المتعلقة بالاتصالات الواردة والصادرة والتي تتضمّن أنشطة غير عادية أو غير مصرّح بها بما في ذلك وجود برامج ضارة (رموز البرامج الخبيثة "Malicious Code" وبرامج التجسّس "Spyware" والبرامج الدعائية "Adware"). 12-1-3 الإضافات والمحذوفات والتعديلات على معايير سجل الأمن والتدقيق. 13-1-3 الأخطاء (أي المشاكل التقنية في الأصول المعلوماتية والتقنية) التي قد تحدث نتيجة حادث أمني. 14-1-3 تشغيل الأنشطة أو إيقافها عن طريق خدمة معيّنة. 15-1-3 تعطّل النظام أو إعادة تشغيله. 16-1-3 تغيير كلمة المرور. 17-1-3 تفعيل جميع السجلات للأنظمة الحسّاسة.

	All the events specified under these control requirements shall be logged: 3-1-1 Successful login attempts. 3-1-2 Unsuccessful login attempts, along with the identification of whether the login attempt involved an invalid password. 3-1-3 All logoffs. 3-1-4 Additions, deletions and modifications to user accounts/privileges. 3-1-5 Users switching IDs during an online session. 3-1-6 Attempts to perform unauthorized functions. 3-1-7 Activities performed by privileged accounts. 3-1-8 Modifications to system settings (parameters). 3-1-9 Read or write access to protected information, where there is a potential for theft of that information. 3-1-10 Exfiltration of materials related to protected information outside <entity name>. 3-1-11 Detections in inbound and outbound communications for unusual or unauthorized activities including the detection of malware (such as malicious code, spyware, and adware). 3-1-12 Additions, deletions and modifications to security/audit log parameters. 3-1-13 Faults (technical problems in information and technology assets) that could potentially be attributed to a security event. 3-1-14 Activation or deactivation of activities by a specific service. 3-1-15 System crashes or restarts. 3-1-16 Password changes. 3-1-17 Enablement of all critical systems logs.
4	مصادر الأحداث (Event Sources)
الهدف	التأكّد من مراقبة جميع سجلات الأحداث المتعلّقة بالأصول المعلوماتية والتقنية الخاصة بـ<اسم الجهة> لكشف أي نشاط غير مصرّح به في الشبكة والذي قد يتسبب بحدث أمني.
المخاطر المحتملة	إن عدم التمكّن من كشف أي نشاط غير مصرّح به سيمنع <اسم الجهة> من التعامل بطريقة مناسبة مع الأحداث المشبوهة قبل أن تتفاقم وتصبح أكثر خطورة.

اختر التصنيف

الإجراءات المطلوبة	
1-4	تهيئة مصادر سجل الأحداث وأنظمة تسجيل الدخول لنقل السجلات عبر بروتوكولات موثوقة وشائعة الاستخدام لنقل سجل الأحداث، مثل: (Syslog)، و(Windows Instrumentation Interface)، و(SNMP Traps)، وغيرها. The event log sources and logging systems shall be configured to transport logs over reliable and commonly used event log transport protocols such as syslog, Windows Instrumentation Interface (WMI), SNMP traps, etc.
2-4	جمع كافة سجلات الأحداث من المصادر المُحدّدة ضمن هذا المطلب: 1-2-4 الأنظمة بما فيها أنظمة التشغيل وقواعد البيانات ووسائط التخزين والشبكات والتطبيقات، التي تغطي أحداث النظام وسجلات الأمن والتدقيق. 2-2-4 الأنظمة الحسّاسة بما فيها أنظمة التشغيل وقواعد البيانات ووسائط التخزين والشبكات والتطبيقات، التي تغطي أحداث النظام وسجلات الأمن والتدقيق. 3-2-4 أحداث الحسابات ذات الصلاحيات الهامة والحسّاسة. 4-2-4 الأحداث الخاصة بالتصفّح والاتصال بالإنترنت والشبكة اللاسلكية. 5-2-4 الأحداث الناتجة عن نقل البيانات إلى وسائط تخزين خارجية. 6-2-4 سجلات الأحداث الصادرة من تقنيات إدارة تغييرات الملفات (File Monitoring Integrity). 7-2-4 سجلات الأحداث المُولّدة من تغييرات إعدادات النظام وتحديثات وإصلاحات النظام والتغييرات على التطبيقات. 8-2-4 أنشطة مشبوهة مثل الأنشطة التي يكتشفها نظام منع الاختراقات (Prevention System Intrusion). 9-2-4 أحداث تُولّدها الحلول الأمنية بما فيها البرامج المضادة للبرمجيات الخبيثة (Antivirus, Antimalware, Advanced Persistent Threat "APT") وتقنيات الوصول عن بُعد (Remote-Access Technologies) (مثل: الشبكة الافتراضية الخاصة " Virtual Private Network")، ووسطاء الويب (Web Proxies)، وبرنامج إدارة الثغرات، ونظام منع الاختراقات في المستضيف (Host Intrusion System Prevention)، وخوادم التحقّق من الهوية (Authentication Servers)، وغيرها. 10-2-4 أحداث تُولّدها أجهزة حماية الشبكة بما في ذلك جدران الحماية والمُوجّهات (Routers) ومديري حركة الشبكة (Traffic Managers)، وغيرها.

اختر التصنيف

4-2-11 أحداث تُولّدها البيئة الافتراضية وأدواتها وبنيتها التحتية الأساسية. 4-2-12 تفعيل تسجيل الاستفسارات (Query Logging) في نظام أسماء النطاقات (Domain Name System) حيثما أمكن ذلك من الناحية التقنية. 4-2-13 سجلات الأحداث التي تُولّدها أنظمة التحكّم الصناعي (Industrial Systems Control). All event logs shall be collected from the sources specified under this requirement: 4-2-1 Systems, including Operating Systems, Databases, Storage, Networks, Applications, etc., covering system events and security/audit logs. 4-2-2 Critical Systems, including Operating Systems, Databases, Storage, Networks, Applications, etc., covering system events and security/audit logs. 4-2-3 Events of privileged accounts. 4-2-4 Logs generated in the events of Internet browsing, Internet connections and Wi-Fi connections. 4-2-5 Events generating from data transfer to external storage. 4-2-6 File Integrity Monitoring (FIM) event logs. 4-2-7 Event logs generated from system configuration changes, system updates and patches, and application changes. 4-2-8 Abnormal activities such as those detected by Intrusion Prevention System (IPS). 4-2-9 Events generated by security solutions including Antimalware, Remote-Access Technologies (such as Virtual Private Network VPN), Web Proxies, Vulnerability Management Software, Host Intrusion Prevention System (HIPS), Authentication Servers, etc. 4-2-10 Events generated by perimeter devices including firewalls, routers, traffic managers, etc.	

	4-2-11 Events generated by virtualization environments and their underlying tools and infrastructure. 4-2-12 Enable Domain Name System (DNS) query logging wherever technically applicable. 4-2-13 Event logs generated by Industrial Control Systems (ICS).
5	مراقبة الأحداث (Events Monitoring)
الهدف	كشف أي نشاط غير مصرّح به في الشبكة والذي قد يسبب حدث أمني.
المخاطر المحتملة	إن عدم التمكّن من كشف أي نشاط غير مصرّح به في الشبكة يمنع الجهة من التعامل بالطريقة المناسبة مع الأحداث المشبوهة قبل أن تتفاقم وتصبح أكثر خطورة.
الإجراءات المطلوبة	
1-5	يجب مراجعة تنبيهات الأحداث الأمنية الناتجة عن جدران الحماية يومياً للكشف عن أي محاولات وصول غير مصرح بها أو سلوك غير عادي. وتستطيع <اسم الجهة> مراقبة التنبيهات الصادرة عن جدران الحماية على سبيل المثال من خلال مراقبة السجلات يومياً أو من خلال مراقبة جوانب النظام الأخرى مثل أنماط محاولة الوصول، وخصائص الوصول، وغيرها من الإجراءات. Security event alerts generated from firewalls shall be reviewed on a daily basis to detect any unauthorized access attempts or unusual behavior. <Entity name> can monitor alerts from firewalls, for example, by observing logs daily or by observing other system aspects such as access attempt patterns, characteristics of access, etc.
2-5	تفعيل مراقبة الشبكة اللاسلكية وذلك لكشف نقاط الوصول اللاسلكية غير المصرّح بها. وقد تتجاوز الإشارات اللاسلكية حدود النطاق الخاضع للمراقبة، وعلى ذلك تتخذ الجهات خطوة استباقية للبحث عن الاتصالات اللاسلكية غير المصرّح بها، بما في ذلك إجراء عمليات مسح مكثّفة عن نقاط الوصول اللاسلكية غير المصرّح بها، وهذه العمليات المسحية لا تقتصر فقط على الأصول التي تحتوي على أصول معلوماتية وتقنية، بل تشمل كذلك المناطق الواقعة خارج مبانيها عند الضرورة، وذلك للتحقّق من عدم اتصال نقاط الوصول اللاسلكية غير المصرّح بها بالأنظمة. Wireless network monitoring shall be enabled to detect unauthorized wireless access points. Wireless signals may radiate beyond the confines of organization-controlled facilities. Organizations shall proactively search for

unauthorized wireless connections including performing thorough scans for unauthorized wireless access points. Scans shall not be limited to those areas within facilities containing information and technology assets, but also shall include areas outside facilities as needed to verify that unauthorized wireless access points are not connected to the systems.	
تطبيق آليات مراقبة المستضيف (Host-based Monitoring Mechanisms) على النهايات الطرفية للأصول المعلوماتية والتقنية ذات الخطورة العالية. وتشمل مكوّنات الأصول المعلوماتية والتقنية التي يُمكن تطبيق آليات مراقبة المستضيف عليها الخوادم وأجهزة المستخدمين والأجهزة المحمولة. Host-based monitoring mechanisms shall be implemented on endpoint system components for high-risk information and technology assets. Information and technology asset components where host-based monitoring can be implemented include servers, workstations, and mobile devices.	3-5
تطبيق آليات المراقبة القائمة على ملف تعريف الملف والسلوك (Signature-based and Behavior-based Code)، مثل البرامج المضادة للفيروسات وتقنية كشف النهايات الطرفية والاستجابة لها (Endpoint Detection and Response) وأدوات كشف التهديدات المتقدمة المستمرة (APT Tools) على الأصول المعلوماتية والتقنية لكشف رمز البرامج الخبيثة. Signature-based and behavior-based code monitoring mechanisms (such as Antivirus, EDR, and APT tools) shall be implemented on information and technology assets to detect malicious code.	4-5
ضمان مواصلة تحديث آليات المراقبة القائمة على ملفات التعريف والسلوك بشكل مستمر. Signature-based and behavior-based code monitoring mechanisms shall be kept current with all available signatures or indicators.	5-5
تُنشَر أجهزة المراقبة لمتابعة الاتصالات على المكوّنات الخارجية للنظام (مثل: محيط النظام) وعلى المكوّنات الداخلية الرئيسية (مثل: الواجهات المنطقية والمادية داخل الأصول المعلوماتية والتقنية) لاكتشاف العيوب واكتشاف التسريب المخفي للمعلومات وتتبع أنواع محدّدة من الأنشطة التي تهم <اسم الجهة>. على سبيل المثال: الأجزاء الشبكية حيث تقع الأنظمة التي يُمكن الوصول إليها من الإنترنت.	6-5

اختر التصنيف

	Monitoring devices shall be deployed to monitor communications at the external boundary of the system (e.g., *system perimeter*) and at key internal boundaries *(e.g., logical/physical interfaces within the information and technology asset*) to discover anomalies, detect covert exfiltration of information and track specific types of transactions of interest to <entity name>. For example, *Network segments* where systems that are accessible from the Internet are located.
7-5	تطبيق أدوات المراقبة للكشف عن مؤشرات الهجمات المنفّذة ضد الأصول المعلوماتية والتقنية الخاصة بـ<اسم الجهة> والتي تؤدي إلى حجب *الخدمة*. Monitoring tools shall be employed to detect indicators of *denial of service* attacks against <entity name>'s information and technology assets and infrastructure.
6	التنبيه بالأحداث (Event Alerting)
الهدف	التأكّد من تفعيل وضبط خاصية التنبيه بالأحداث وإبلاغ العاملين المعنيين في <اسم الجهة> بشأنها ليتمكّنوا من التعامل مع أي حادث أمني بأكبر قدر من الفاعلية.
المخاطر المحتملة	قد يؤدي عدم ضبط خاصية التنبيه بالأحداث في أنظمة التسجيل إلى التعامل مع الأحداث الأمنية بطريقة خاطئة أو حتّى عدم التعامل معها كلياً.
الإجراءات المطلوبة	
1-6	إصدار التنبيهات للأصول المعلوماتية والتقنية عند وقوع أحداث المراقبة الأمنية المحدّدة مسبقاً و/أو عند استيفاء مستويات المؤشرات المتعلّقة بأي نشاط ضار محتمل. Alerts for information and technology assets shall be generated when previously defined security monitoring events occur and/or thresholds for indications of potentially malicious activity are met.
2-6	ضبط وسائل التنبيه لإبلاغ العاملين المعنيين، بما في ذلك البريد الإلكتروني والرسائل النصية القصيرة وأنظمة شاشات المراقبة، وغيرها. Alerting methods, including email, SMS, video wall systems, etc., shall be configured to notify the appropriate personnel.
7	مستويات التنبيه (Alert Threshold)
الهدف	اتباع نهج مُوثّق بشأن الحالات التي ينبغي تشغيل التنبيهات فيها.

المخاطر المحتملة	قد يؤدي عدم توثيق نطاق التنبيهات والغرض منها إلى عدم تهيئتها بالشكل المناسب، وقد تمر الأحداث الضارة المحتملة دون أن يلاحظها أحد.
الإجراءات المطلوبة	
1-7	تحديد وتوثيق المستويات المحدّدة للتنبيه عن أحداث مراقبة الأمن، ومراجعة مستوى التنبيه وتحديثه دورياً لمواكبة الهجمات الأمنية المستجدة. Specific thresholds for alerting on security monitoring events shall be identified and documented. Thresholds shall be periodically revised and updated to stay current with trending security attacks.
8	التنبيه بالأحداث الناتجة عن جدار الحماية (Firewall Event Alerting)
الهدف	إبلاغ العاملين المعنيين المؤهلين للتعامل مع الأحداث الأمنية المحتملة والناتجة عن جدران الحماية.
المخاطر المحتملة	إن لم يتم إبلاغ العاملين المعنيين بالأحداث الناتجة عن جدار الحماية، فإن <اسم الجهة> لن تكون على دراية بالمحاولات الخبيثة المحتملة غير المصرّح بها للاتصال بالشبكة، وبالتالي إذا تمكّن هذا النشاط من اختراق جدار الحماية، ستتعرّض أعمال <اسم الجهة> لمخاطر ضارة ناتجة عن الحادث الأمني.
الإجراءات المطلوبة	
1-8	ضبط التنبيهات أو أدوات المراقبة لتنويه العاملين المعنيين بالأحداث المتعلّقة بالأمن والناتجة عن جدار الحماية. Alarms or monitoring tools shall be configured to alert the appropriate personnel of security-related events originating from the firewall.
9	التنبيه بالأحداث الناتجة عن التطبيقات (Application Event Alerting)
الهدف	التأكّد من توثيق وتسجيل الأحداث الأمنية والأنشطة غير المصرّح بها التي تشهدها البيئة.
المخاطر المحتملة	من الضروري تسجيل بعض الأحداث المحورية المتعلّقة بالتطبيقات الخاصة بـ<اسم الجهة>، فإذا تعذّر على <اسم الجهة> تسجيل الحوادث المتعلّقة بالتطبيق والتي حدّدتها متطلّبات الضابط، سيؤدي ذلك إلى زيادة المخاطر الناتجة عن الحوادث الأمنية غير المُحدّدة وغير المصرّح بها المحتمل حدوثها في التطبيق، والتي قد تؤثّر على أعمال الجهة بناءً على مستوى خطورة الحادث.

الإجراءات المطلوبة	
1-9	تسجيل جميع طلبات العميل واستجابات الخادم. All client requests and server responses shall be logged.
2-9	تسجيل جميع معلومات الحساب (مثل: محاولات التحقّق الناجحة وغير الناجحة والتغييرات على الحساب). All account information (e.g., successful and failed authentication attempts and account changes) shall be logged.
3-9	تسجيل جميع المعلومات المتعلّقة بالاستخدام (مثل: عدد الأنشطة التي تحدث في فترة معيّنة). All usage information (e.g., the number of transactions occurring in a certain period) shall be logged.
4-9	تسجيل جميع الإجراءات التشغيلية المهمّة (مثل: تشغيل وإغلاق التطبيقات وأعطال التطبيقات والتغييرات على إعدادات التطبيقات). All significant operational actions (e.g., application startup and shutdown, application failures, and application configuration changes) shall be logged.
10	مراقبة البرمجيات الضارة في الاتصالات (Malware in Communication Monitoring)
الهدف	تحديد وجود البرمجيات الضارة (مثل: رمز البرامج الخبيثة وبرامج التجسّس والإعلانات المتسلّلة) في اتصالات <اسم الجهة> قبل أن تتسبّب بأي ضرر.
المخاطر المحتملة	إذا لم يتم كشف أي استخدام غير مصرّح به للأنشطة بما في ذلك وجود البرمجيات الضارة، لن تكون <اسم الجهة> على دراية بوجود البرمجيات الضارة قبل أن تنتشر، مما يعرّض عملها لخطر هجوم أمني واسع النطاق.
الإجراءات المطلوبة	
1-10	مراقبة الاتصالات الواردة والصادرة الخاصة بـ<اسم الجهة> (مثل: رسائل البريد الإلكتروني والملفات المرفقة وعمليات التحميل) لضمان خلوها من البرمجيات الضارة (مثل: البرمجيات الضارة وبرامج التجسّس والبرامج الدعائية). Inbound and outbound <entity name>'s communications (such as *emails, file attachments, downloads*) shall be monitored for malware (such as *malicious code, spyware and adware*).

11	تحليلات مراجعة سجل الأحداث (Event Log Review Analytics)
الهدف	يُمكن أن يسهم تحليل السجل ونظام إدارة سجلات الأحداث ومراقبة الأمن السيبراني (SIEM) في اكتشاف الأنشطة المشبوهة وتعزيز قدرات الاستجابة لحوادث الأمن السيبراني وكشف الهجمات التي تجاوزت الأنظمة الأمنية الأخرى.
المخاطر المحتملة	إن عدم التمكّن من كشف أحداث وحوادث الأمن السيبراني سيزيد من المخاطر الناتجة عن عدم ملاحظة الهجمات السيبرانية مما يؤدي إلى انتهاك الأصول المعلوماتية والتقنية الخاصة بـ<اسم الجهة>.
الإجراءات المطلوبة	
1-11	إرسال جميع الأحداث إلى نظام إدارة سجلات الأحداث ومراقبة الأمن السيبراني من أجل إدارة السجلات وتحليل محتواها وعلاقتها ببعضها والتنبيه عليها. All event logs shall be forwarded to a centralized log analytics or Security Information and Event Management (SIEM) system for log correlation, analysis and alerting.
2-11	إجراء مراجعة دورية لسجلات الأحداث لمراقبة السلوكيات والأحداث المشبوهة واكتشافها. Regular review on SIEM shall be performed to monitor and detect abnormal behavior and anomalies.
3-11	ضبط نظام إدارة سجلات الأحداث ومراقبة الأمن السيبراني دورياً لتحديد الأحداث القابلة للتطبيق وتقليل الأحداث الناتجة عنها بطريقة أفضل. SIEM system shall be tuned on a regular basis to better identify actionable events and decrease event noise.
4-11	مراجعة سجلات الأحداث والتنبيهات دورياً باستخدام أساليب يدوية وتقنيات آلية. Event logs and alerts shall be periodically reviewed, using manual and automated techniques.
5-11	الكشف عن الأحداث غير المصرّح بها والمتعلّقة بالأصول المعلوماتية والتقنية. Significant unauthorized activity related to information and technology assets shall be detected.
6-11	كشف سوء استخدام حسابات المستخدم ذات الصلاحيات الهامة والحسّاسة. Misuse of privileged user accounts shall be detected.

12	تحويل السجل وتحليله (Log Conversion and Parsing)
الهدف	التأكّد من مراقبة جميع سجلات الأحداث المتعلّقة بالأصول المعلوماتية والتقنية الخاصة بـ<اسم الجهة> لكشف أي نشاط غير مصرّح به في الشبكة والذي قد يسبب حدثاً أمنياً.
المخاطر المحتملة	من الضروري تسجيل بعض الأحداث المحورية التي تُنفذ في البيئة، فإذا تعذّر على <اسم الجهة> تسجيل الأحداث التي حدّدتها متطلّبات الضابط، سيؤدي ذلك إلى زيادة المخاطر الناتجة عن الأحداث غير المُحدّدة وغير المصرّح بها المحتمل حدوثها في البيئة، والتي قد تؤثّر على أعمال الجهة بناءً على مستوى خطورة الحادث.
الإجراءات المطلوبة	
1-12	استخدام أدوات لتحويل السجلات غير المدعومة من نظام التسجيل الخاص بـ<اسم الجهة> إلى صيغة قياسية أو مدعومة للسجل. Log conversion utilities shall be used to convert logs unsupported by <entity name>'s logging system to a standard or supported log format.
2-12	تطبيق برنامج تسجيل مزوّد بآليات التحليل لاسترجاع السجلات من الأنظمة غير المدعومة بطريقة مناسبة. Logging software with parsing mechanisms shall be implemented to retrieve logs properly from unsupported systems.
13	المراقبة المستمرة (Continuous Monitoring)
الهدف	تفعيل المراقبة المستمرة لجميع سجلات الأصول المعلوماتية والتقنية للكشف عن الأنشطة الخبيثة والحفاظ على فاعلية المراقبة مع الوقت.
المخاطر المحتملة	إذا لم تضع الجهة خطّة مراقبة لهذه الأنشطة وتوثّقها، فقد يرتفع خطر عدم وجود مراقبة مخصصة أو كافية لهذا الغرض، مما يزيد من مخاطر عدم الكشف عن الأنشطة الخبيثة.
الإجراءات المطلوبة	
1-13	تطوير وإعداد خطّة للمراقبة المستمرة (والتي تشمل على سبيل المثال: الجوانب التي يجب مراقبتها في نطاق العمل، وآلية المراقبة، واختبار فاعلية المراقبة) للأصول المعلوماتية والتقنية وتحديثها عند الحاجة. A plan for the continuous monitoring (which includes monitoring scope, frequency, and effectiveness testing) of the

	information and technology assets shall be developed and configured, and it shall be updated if needed.
14	أمن نظام التسجيل (Logging System Security)
الهدف	ضمان حماية وأمن البنية التحتية الأساسية لنظام التسجيل بما في ذلك محرّكات جمع سجلات الأحداث وتجميعها وربطها.
المخاطر المحتملة	من الممكن أن يؤدي عدم اتخاذ أي إجراء لحماية البنية التحتية لنظام التسجيل في <اسم الجهة> إلى استفادة المهاجمين من نقاط الضعف الكامنة في أنظمة التسجيل واستغلال ثغراتها للوصول غير مصرّح به إلى شبكة <اسم الجهة> وبياناتها.
الإجراءات المطلوبة	
1-14	إجراء اختبارات أمنية دورية (مثل: تقييم الثغرات الأمنية واختبار الاختراق) وفقاً لسياسة إدارة الثغرات الأمنية المتّبعة في <اسم الجهة>. Regular security testing (such as vulnerability assessments and penetration testing) shall be performed as per <entity name>'s Vulnerability Management Policy.
2-14	تنفيذ إصلاحات وتحديثات دورية على أنظمة التسجيل وفقاً لسياسة إدارة التحديثات والإصلاحات المتّبعة في <اسم الجهة>، وضمان تحديث جميع الأنظمة. Logging systems shall be regularly patched and updated as per <entity name>'s Patch Management Policy, and all systems shall be up-to-date.
3-14	حذف أو إلغاء تفعيل التطبيقات والخدمات غير الضرورية أو غير اللازمة من أنظمة التسجيل (مثل: خدمات الطباعة وبروتوكول تل نت "Telnet"، وغيرها). Unnecessary/unrequired applications and services on logging systems (e.g., *printing services, telnet, etc.*) shall be removed/disabled.
4-14	ضبط وتحصين أنظمة التسجيل بما في ذلك التطبيقات وقاعدة البيانات والتحصين على مستوى نظام التشغيل. يُرجى الرجوع إلى معيار أمن الخادم ومعيار أمن قاعدة البيانات المعتمدين في <اسم الجهة>. Logging systems hardening, including *application, database, and operating system level hardening,* shall be configured. Refer to <entity name>'s Server Security Standard and Database Security Standard.

5-14	تقييد الوصول لأنظمة التسجيل وحصره على مديري نظام التسجيل فقط. Access on logging systems shall be restricted to logging system administrators only.
6-14	حذف أو إلغاء تفعيل الحسابات الافتراضية أو غير التفاعلية أو غير اللازمة. Default/non-interactive/unneeded accounts shall be removed/disabled.
7-14	إلزام مشرفي ومُشغّلي أنظمة التسجيل باستخدام آلية التحقّق من الهوية متعدّد العناصر للوصول إلى أنظمة التسجيل. Logging systems administrators and operators shall be obliged to use multi-factor authentication to access the logging systems.
8-14	استخدام مبدأ الحد الأدنى من الصلاحيات والامتيازات الذي يمنح مديري ومُشغّلي أنظمة التسجيل امتيازات الوصول إلى مختلف أنواع أنظمة التسجيل. The least-privilege security principle shall be used to provide logging system administrators and operators with access to different types of logging systems.
9-14	تقييد الوصول لأنظمة التسجيل من خلال المنطقة الإدارية أو الشبكة المحلية الافتراضية الإدارية (Management VLAN) فقط. Access to logging systems shall be restricted to management zone or management VLAN only.
10-14	حذف أو إلغاء تفعيل خصائص نظام التسجيل وملفات الإعدادات غير الضرورية أو غير اللازمة. Unnecessary/unrequired logging system features and configuration files shall be removed/disabled.
11-14	حجب إمكانية الوصول إلى الملفات المشتركة عبر الشبكة والملفات غير الضرورية أو غير اللازمة. Access to unnecessary/unrequired network and file directories shall be blocked.
12-14	استخدام ضوابط الأجهزة وحجب الوصول إلى وسائط التخزين القابلة للإزالة.

	Hardware controls shall be used and access to removable media shall be blocked.
13-14	تثبيت برامج أنظمة تسجيل الأحداث على خوادم مخصصة لها. Logging systems software shall be installed on dedicated servers.
14-14	استخدام محرّك لجمع الأحداث في كل منطقة من مناطق بنية الشبكة، والسماح فقط لهذه المحرّكات بالتواصل مع نظام التسجيل المركزي أو أنظمة تجميع السجلات، على أن تتوفر في المناطق التالية على الأقل: 1-14-14 وضع محرّك لجمع الأحداث في *المنطقة المحايدة (DMZ)*. 2-14-14 وضع محرّك لجمع الأحداث في *منطقة قاعدة البيانات*. 3-14-14 وضع محرّك لجمع الأحداث في *منطقة التطبيقات*. 4-14-14 وضع محرّك لجمع الأحداث في *منطقة خدمات المؤسسة*. 5-14-14 وضع محرّك لجمع الأحداث في *منطقة المستخدم*. 6-14-14 وضع محرّك لجمع الأحداث في *منطقة الإدارة*. A log collector shall be implemented in each zone in the network architecture, and only these collectors shall be allowed to communicate with the centralized logging system or logging aggregation systems. A log collector shall be placed, at a minimum, in the following zones: 14-14-1 Place a log collector in the *DMZ*. 14-14-2 Place a log collector in the *database zone*. 14-14-3 Place a log collector in the *application zone*. 14-14-4 Place a log collector in the *corporate services zone*. 14-14-5 Place a log collector in the *user zone*. 14-14-6 Place a log collector in the *management zone.*
15	اختبار ومراجعة نظام المراقبة (Monitoring System Testing and Review)
الهدف	الحفاظ على القدرات التشغيلية والفاعلية في الكشف عن المحاولات غير المصرّح بها للوصول إلى الأصول المعلوماتية والتقنية.

المخاطر المحتملة	إذا لم تنجح أنظمة المراقبة في الكشف عن الأنشطة غير المصرّح بها، فإن ذلك سيزيد من احتمالية عدم ملاحظة النشاط الخبيث، والذي قد يؤدي إلى وقوع حادث أمني خطير.
الإجراءات المطلوبة	
1-15	إجراء مراجعات واختبارات على أدوات المراقبة الأمنية الخاصة بـ<اسم الجهة> عن طريق أفراد مصرّح لهم بذلك للتأكّد من الالتزام بسياسة إدارة سجلات الأحداث ومراقبة الأمن السيبراني المعتمدة في <اسم الجهة> ونجاحها في تلبية أهداف المراقبة. Reviews and tests shall be performed by authorized individuals on <entity name>'s security monitoring tools to validate that they comply with <entity name>'s Cybersecurity Event Logs and Monitoring Management Policy and successfully meet the monitoring objectives.
16	الاحتفاظ بسجلات الأحداث (Retaining Event Logs)
الهدف	تجنّب حذف سجلات الأحداث الأمنية خلال الفترة التي يُمكن أن تُستخدَم خلالها.
المخاطر المحتملة	إذا حُذِفَت سجلات الأحداث الأمنية قبل تدقيقها أو التحقيق فيها، لن تتمكّن <اسم الجهة> من حماية أو فحص الأنشطة التي حدثت في الأصول المعلوماتية والتقنية الخاصة بها.
الإجراءات المطلوبة	
1-16	القيام بالنسخ الاحتياطي للسجلات دورياً ووفقاً لسياسة إدارة النسخ الاحتياطية المعتمدة في <اسم الجهة>. Periodic backup of logs shall be performed as per <entity name>’s Backup and Recovery Management Policy.
2-16	الاحتفاظ بسجلات الأحداث لمدة 12 شهراً على الأقل، ولمدة 18 شهراً بالنسبة للأصول الحسّاسة كحد أدنى أو لفترة أطول، وفقاً لسياسة الأمن السيبراني المعتمدة في <اسم الجهة>. Event logs shall be retained for at least twelve (12) months for all assets, and at least eighteen (18) months for critical assets, or for a longer period, as per <entity name>’s Cybersecurity Policy.
3-16	تقييد أرشفة وحذف سجلات الأحداث وحصره على المستخدمين المصرّح لهم وذلك فقط بعد انتهاء المدّة الزمنية المحدّدة للاحتفاظ بالسجلات، والسماح للمديرين المعنيين بالأصول المعلوماتية والتقنية بإجراء عملية أرشفة سجلات الأحداث وحذفها.

	The archival and deletion of event logs shall be restricted to authorized users and only after the expiration of the retention period. Appropriate information and technology asset administrators shall be authorized to carry out event log archival and deletion.
4-16	اختبار إمكانية استعادة واسترجاع النسخ الاحتياطية دورياً وفقاً لسياسة إدارة النسخ الاحتياطية المعتمدة في <اسم الجهة>. Backup retrieval and recovery shall be regularly tested as per <entity name>'s Backup and Recovery Management Policy.
17	توفير عملية بديلة لتسجيل الأحداث (Alternate Logging Capability)
الهدف	تمكين <اسم الجهة> من مواصلة تسجيل الأنشطة المتعلّقة بالأحداث الأمنية الحسّاسة حتّى في حال تعطّل الوسيلة الأساسية لتسجيل الأحداث (مثل: التسجيل المركزي).
المخاطر المحتملة	إذا تعطّلت وسيلة تسجيل الأحداث الأساسية المتعلّقة بأصل عالي الخطورة ولم تتوفّر عملية تسجيل بديلة، فإنه قد يتعذّر إنشاء سجل تدقيق أو تحديد النشاط الخبيث وذلك لعدم وجود سجلات يُمكن أن تستخدمها <اسم الجهة> للقيام بإجراءات المراقبة والتحقيق، علماً بأن الأصول الأعلى خطورة تؤثّر بشكل أكبر على أعمال الجهة في حال وقوع حادث أمني معيّن.
الإجراءات المطلوبة	
1-17	ضبط الأنظمة الحساسة، بالإضافة إلى إرسال السجلات إلى نظام تسجيل أحداث مركزي، لتحفظ سجلات الأحداث على أجهزتها في حال تعطّل الاتصال بالشبكة. In addition to sending logs to a centralized logging system, high risk information and technology assets shall be configured to maintain local logs in the event of network connectivity failure
18	توافر سجل الأحداث (Event Log Availability)
الهدف	ضمان استمرارية تشغيل وسيلة تسجيل الأحداث وقابلية استخدامها للأصول المعلوماتية والتقنية الحسّاسة.
المخاطر المحتملة	إذا لم تتوفّر وسيلة تسجيل الأحداث، فإن ذلك سيزيد من احتمالية عدم ملاحظة النشاط الخبيث وعدم القدرة على إجراء تحقيق بشأن الحادث والذي قد يؤدي إلى وقوع حادث أمني خطير.
الإجراءات المطلوبة	

1-18	ضبط الأصول المعلوماتية والتقنية الخاصة بـ<اسم الجهة> والتي تحتوي على معلومات **محمية**، أو معلومات مصنفة من خلال تقييم إدارة المخاطر على أنها تتطلب تسجيل أحداثها، لإرسال الأحداث الخاصة بها بشكلٍ دائم. <Entity name>'s information and technology assets with **protected** information, or designated through risk management assessment as requiring event logs, shall be configured to generate event logs at all times.
2-18	إعداد أنظمة تسجيل إضافية متعدّدة مزوّدة بقدرات توفير الخدمة على مدار الساعة ودون انقطاع. Multiple redundant logging systems with failover capabilities shall be configured.
19	تصنيف السجلات (Log Classification)
الهدف	يجب حماية جميع سجلات أحداث الأمن السيبراني بطريقة آمنة.
المخاطر المحتملة	إذا طبّقت السجلات ضوابط مُخصّصة لبيانات ذات تصنيف أدنى على الرغم من احتواء هذه السجلات على بيانات مُصنّفة بأنها **سريّة للغاية**، فستكون هذه البيانات أكثر عرضة لخطر انتهاكها لأن الضوابط المحدّدة لحمايتها تعتبر أقل صرامة.
الإجراءات المطلوبة	
1-19	التعامل مع أنظمة التسجيل المركزي باعتبار أنها تحتوي بحدٍّ أدنى على بيانات **سرية** و**مقيدة** خاصة بـ<اسم الجهة> وأنها ملتزمة بجميع الضوابط ذات العلاقة بسريّة المعلومات. Centralized logging solutions shall be treated as if they contain, at a minimum, <entity name>'s **Secret** and **Restricted** data, and as if they comply with all relevant confidentiality controls.
2-19	بالنسبة إلى أي سجل للتطبيقات أو للأنشطة يحتوي على بيانات مُصنّفة على أنها **سرية للغاية**، يجب فرض الضوابط المطلوبة لهذا النوع من البيانات. For any application log or transaction record(s) that contains data classified as **Top Secret**, the controls required for that classification of data shall be enforced.
20	أمن السجلات وسلامتها (Log Integrity and Security)

الهدف	اعتماد آلية قادرة على كشف التعديلات على سجلات الأحداث الأمنية للتأكد من الاحتفاظ بها في حالتها الأصلية.
المخاطر المحتملة	إذا كان من الممكن تعديل سجلات الأحداث الأمنية دون وجود أي وسيلة لكشف هذا التعديل، فيمكن للمستخدم أن يُخفي نشاطه الخبيث داخل الأصل المعلوماتي والتقني. وفي هذه الحالة، إذا أُجري تحقيق بناءً على الأنشطة الضارة التي قام بها المستخدم، فلن يكون هناك دليل لمحاكمة المستخدم، ولن تُوجّه <اسم الجهة> ادعاءات مبرّرة بحق المستخدم ذي النوايا الضارة أو الخبيثة. كما أنه في حال انتهاك سلامة السجلات، فإنها قد تعتبر غير مقبولة في إجراءات المحكمة.
الإجراءات المطلوبة	
1-20	الحفاظ على سلامة السجل الأصلي، وتوفير آليات لحماية سلامة السجل بما فيها *ضابط تقييد الوصول ومستودعات البيانات المحظورة*، وغيرها. Original log integrity shall be maintained. Mechanisms to protect log integrity can include *strict access control*, *restricted data repositories*, etc.
2-20	تطبيق وسائل لتشفير السجلات في حالتي الإرسال والتخزين، مثل أمن طبقة النقل (Transport Layer Security)، واستخدام أحدث بروتوكولات التشفير وخوارزميات التشفير المدعومة (Cipher Suite) المُوصى بها (مثل: التشفير بمجموعة suite B). يُرجى الرجوع إلى معيار التشفير المعتمد في <اسم الجهة>. Methods to encrypt logs during transmission and at rest shall be implemented, such as Transport Layer Security (TLS). Recommended next generation encryption protocols and cipher suites (such as suite B cryptography) shall be used. Refer to <entity name>'s Cryptography Standard.
3-20	تطبيق وسائل يُمكنها كشف التعديلات على السجلات في حالتي الإرسال والتخزين مثل خوارزميتي دالة التجزئة (Hashing) واختزال الرسالة (Message Digest) التشفيريتين، وذلك بالإضافة إلى آليات لكشف التعديل أو محاولات التعديل التي تعتمد على أساليب معيّنة مثل تقليل حجم السجل وتغيير دالة تجزئة الملف ووصول العمليات من غير النظام (مثل: كافة العمليات لكتابة واختزال السجلات باستثناء الآلية منها). يُرجى الرجوع إلى معيار التشفير المعتمد في <اسم الجهة> للاطلاع على متطلّبات السلامة والتجزئة. Methods that can detect modification of logs during transmission and at rest, such as hashing and message digest algorithms, shall be implemented. Mechanisms to detect modification or attempts of modification can rely on certain triggers such as reduction in log size, change in file hash,

	access by non-system processes (e.g., everything except automated processes for writing and digesting logs). Refer to <entity name>'s Cryptography Standard for integrity and hashing requirements.
4-20	تقييد الوصول إلى ملفات السجل ووسائط تخزين السجلات على نظام التسجيل فقط. ومنح المديرين حق الوصول إلى السجلات لأغراض استكشاف الأخطاء وإصلاحها في الفترة المخصّصة للصيانة فقط. Access to log files and logs storage shall be restricted to the logging system only. Access to logs shall be provided to administrators for troubleshooting purposes only during the troubleshooting or maintenance period.
5-20	ضبط إعدادات التحكّم بمعدل إرسال السجلات (Log Rate Limiting) لمنع تعرّض نظام التسجيل إلى هجمات حجب الخدمة، وضبط مستواه عند حد معقول. Rate limiting shall be configured to prevent *denial of service* attacks for the logging system. Additionally, it shall be configured to a reasonable threshold.
21	موارد تسجيل الأحداث (Logging Resources)
الهدف	تجنّب فقدان السجلات جرّاء استبدال البيانات المُخزّنة على وسائط التخزين.
المخاطر المحتملة	إن عدم التمكّن من توفير مساحة كافية لتخزين أقصى حدّ ممكن من السجلات قد يؤدي إلى استبدال المعلومات المُخزّنة في السجل وفقدان بيانات قيّمة ومهمّة خاصة بـ<اسم الجهة>. وفي هذه الحالة، من الممكن أن تُحذَف السجلات الحسّاسة بالكامل ولن تتمكّن <اسم الجهة> من الاعتماد على هذه السجلات في حال توجيه دعوى قضائية أو إجراء تحقيق معيّن، وهذا الأمر قد يؤثّر على أعمالها.
الإجراءات المطلوبة	
1-21	توفير موارد كافية (مثل: موارد النظام ووسائط تخزين البيانات ونطاق الشبكة) لاستيعاب أنشطة التسجيل المحدّدة. ويجب أن تحتوي أجهزة تخزين السجلات على سعة تخزين كافية لجمع السجلات. Sufficient resources (e.g., *system resources, data storage, and network bandwidth*) shall be provided to accommodate prescribed logging activities. Log storage devices shall have sufficient log storage for collecting logs.

22	التغييرات على إعدادات التسجيل (Logging Configuration Changes)
الهدف	الحد من إمكانية إجراء أي تغييرات غير مصرّح بها أو ضارة على عملية تسجيل الأحداث الجاري تنفيذها في مكوّنات النظام.
المخاطر المحتملة	إذا لم تُفرَض أي قيود على المسؤول عن إدخال التغييرات على إعدادات السجل ومكان وموعد إجرائها، فإنه يُمكن أن يقوم مُستخدم خبيث بإيقاف التسجيل على الأجهزة الحسّاسة لتنفيذ هجوم غير ملحوظ.
الإجراءات المطلوبة	
1-22	تقييد إمكانية تغيير إعدادات سجل الأحداث الأمنية، بما فيها نطاق العمل وآلية المراقبة، وحصرها على المستخدمين المصرّح لهم فقط. Security event log configuration changes, including scope and monitoring frequency, shall be restricted to authorized users.
23	استخدام أجهزة المراقبة (Use of Monitoring Devices)
الهدف	منع الكشف عن البيانات الحسّاسة والتأثير على شبكة <اسم الجهة> (مثل: استنزاف موارد الشبكة أو استخدام أدوات ضارة/خبيثة في البيئة).
المخاطر المحتملة	إذا لم تصرّح الإدارة المعنية بالأمن السيبراني في <اسم الجهة> ولم تسمح لموظفين معيّنين باستخدام أدوات أو أجهزة المراقبة والفحص، من الممكن أن تُستخدَم إحدى الأدوات بطريقة تضر البيئة وتزيد خطر انتهاك البيانات أو وقوع حادث أمني.
الإجراءات المطلوبة	
1-23	تقييد استخدام أجهزة أو أدوات المراقبة والفحص على المستخدمين المصرّح لهم. The use of monitoring and scanning devices or tools shall be limited to authorized users.
2-23	تصنيف نتائج جميع أنشطة المراقبة والفحص ضمن المعلومات السريّة بحدٍّ أدنى. The results of all monitoring and scanning activities shall be classified as Confidential, at minimum.

الأدوار والمسؤوليات

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

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

اختر التصنيف

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>.