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 حوادث وتهديدات 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

متاح

اعتماد الوثيقة

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

نسخ الوثيقة

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

قائمة المحتويات

الأهداف 3
نطاق العمل وقابلية التطبيق 3
المعايير 3
الأدوار والمسؤوليات 23
الالتزام بالمعيار 23

الأهداف

الغرض من هذا المعيار هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بإدارة حوادث وتهديدات الأمن السيبراني 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 ١-١٣-٢ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

يغطي هذا المعيار كافة الأصول المعلوماتية والتقنية الخاصة بـ<اسم الجهة>، وينطبق على جميع العاملين في <اسم الجهة>.

المعايير

1	خطط الاستجابة للحوادث (Incident Response Plans)
الهدف	ضمان التطبيق الملائم لمنهجية بشكل رسمي ومركز ومتناسق وتشكيل خارطة الطريق لتنفيذ عمليات الاستجابة للحوادث في <اسم الجهة> في حال التعرض لهجوم يستهدف البيانات الشخصية وبيانات العمل.
المخاطر المحتملة	في حال عدم وضع خطة استجابة للحوادث وتطبيقها في <اسم الجهة>، قد تواجه <اسم الجهة> المخاطر المحتملة التالية: • الإخفاق في الاستجابة بشكل مُمنهج (أي باتباع منهجية شاملة في التعامل مع الحوادث) للحوادث التي قد تؤدي إلى إتلاف المعلومات أو سرقتها أو الوصول غير المصرح به إليها أو الإفصاح عنها مما يمكن أن يؤدي إلى انقطاع الخدمات. • عدم القدرة على التعامل بكفاءة مع الحوادث التي يمكن أن تؤدي إلى مخاطر قد تؤثر على سمعة <اسم الجهة>. • عدم الاستفادة من المعلومات أثناء التعامل مع الحوادث من أجل التحضير بشكل أفضل للتعامل مع الحوادث المستقبلية وتوفير حماية أعلى للأنظمة والبيانات. • اتباع منهجية ضعيفة في التعامل مع القضايا القانونية التي قد تنشأ خلال الحوادث وتهديدات الأمن السيبراني.

الإجراءات المطلوبة	
1-1	تطوير خطة تلبي متطلبات الأعمال الخاصة بـ<اسم الجهة>، وترتبط بالمهام والحجم والهيكلية والوظائف الخاصة بـ<اسم الجهة>، وتحدد الموارد اللازمة والدعم الإداري المطلوب. A plan that meets <entity name>'s unique business requirements, which relates to <entity name>'s mission, size, structure, and functions, and lays out the necessary resources and management support, shall be developed.
2-1	تتضمن خطة الاستجابة للحوادث العناصر التالية: • المهام. • الأهداف الاستراتيجية. • موافقة الإدارة العليا. • منهجية <اسم الجهة> للاستجابة للحوادث. • كيفية تواصل فريق الاستجابة للحوادث مع باقي الإدارات المعنية (داخلياً) والجهات الأخرى (خارجياً). • المقاييس الرئيسية لقدرات الاستجابة للحوادث وفاعليتها. • خارطة طريق لتطوير قدرات الاستجابة للحوادث. • مدى ملائمة قدرات الاستجابة للحوادث للجهة. The following elements shall be included in the incident response plan: • Mission • Strategic goals • Senior management approval • Organizational approach to incident response • How the incident response team communicates with the rest of the organization (internally) and with other organizations (externally) • Metrics for measuring the incident response capability and its effectiveness • Incident response maturity roadmap

• How the incident response capability fits into the overall large organization	
تحديد عاملين إداريين، إضافة إلى من ينوبهم عند الحاجة، لتوفير الدعم اللازم في عمليات التعامل مع الحوادث من خلال تولي الأدوار الرئيسية لاتخاذ القرارات. Management personnel, as well as backups, who will support the incident handling process by acting in key decision-making roles, shall be designated.	3-1
دراسة العوامل ذات العلاقة عند اختيار هيكلية فريق الاستجابة للحوادث في سياق احتياجات الجهة والموارد المتوفرة. ومن أمثلة هيكلية فريق الاستجابة للحوادث التالي: • الفريق المركزي للاستجابة للحوادث والذي يتألف من فريق واحد يتعامل مع الحوادث في كافة أقسام <اسم الجهة>. • الفرق الموزعة للاستجابة للحوادث والتي تتألف من العديد من فرق الاستجابة للحوادث، حيث يكون كل فريق منها مسؤولاً عن شريحة منطقية أو مادية معينة في <اسم الجهة>. All relevant factors shall be considered during the selection of an incident response team structure, in the context of the organization's needs and available resources. Examples of incident response structures are: • Central Incident Response Team (CIRT), which consists of a single team who handles incidents throughout the <entity name>. • Distributed Incident Response Teams (DIRT), which consist of multiple incident response teams, each responsible for a particular logical or physical segment of the <entity name>.	4-1
تحديد هيكلية فريق الاستجابة للحوادث الذي يجب أن يكون متوفراً لمساعدة أي فرد يكتشف أو يشتبه بوقوع حادثة لها علاقة بـ<اسم الجهة>. The structure of the incident response team, who shall be available to provide assistance to those who discover or suspect that an incident involving <entity name> has occurred, shall be determined.	5-1

6-1	اختيار الأفراد الذين يملكون المهارات الفنية والخبرة والكفاءة المطلوبة للعمل في فريق الاستجابة للحوادث وتمكينه من القيام بأنشطة الاستجابة للحوادث إلى جانب الأنشطة التالية: • كشف الاختراقات: يتوقع من الفريق تحليل الحوادث بسرعة ودقة بناءً على المعرفة المكتسبة من تقنيات كشف الاختراقات. • تقديم الاستشارات: يمكن أن يقدم الفريق الاستشارات لـ<اسم الجهة> فيما يتعلق بالثغرات والتهديدات الجديدة. وعادةً ما تكون الاستشارات مطلوبة عند ظهور تهديدات جديدة مثل الأحداث السياسية البارزة. • رفع مستوى الوعي والتوعية: أن يكون المستخدمون والعاملون الفنيون على اطلاع بكيفية كشف الحوادث والإبلاغ عنها والاستجابة لها. ويمكن تحقيق هذا من خلال وسائل مختلفة مثل ورشات العمل والمواقع الإلكترونية والنشرات الإخبارية والملصقات. • مشاركة المعلومات: يشارك فريق الاستجابة للحوادث عادة في مجموعات مشاركة المعلومات. Individuals with appropriate skills shall be selected to be members in the incident response team. Such individuals shall have the required expertise and proficiency to assist the team in performing not only incident response activities, but also: • Intrusion Detection: the team is expected to analyze incidents more quickly and accurately, based on the knowledge it gains from intrusion detection technologies. • Advisory Distribution: the team may issue advisories within the <entity name> regarding new vulnerabilities and threats. Advisories are often needed when new threats are emerging, such as a high-profile political event. • Education and Awareness: it is highly recommended that the users and technical staff are aware of how to detect, report, and respond to incidents. This can be achieved through many means: workshops, websites, newsletters and posters.

	• Information Sharing: incident response teams often participate in information sharing groups.
7-1	إدراج التفاصيل في التحليل الأولي عند وقوع حادثة أمنية وذلك لتحديد نطاقها. وتشمل هذه التفاصيل الشبكات أو الأنظمة أو التطبيقات المتأثرة، والمتسبب بالحادثة، وكيفية وقوعها (مثل الأدوات أو طرق الهجوم المستخدمة والثغرات المستغلة). كما يجب أخذ ما يلي بعين الاعتبار عند إجراء التحليل الأولي: • تحديد خصائص الشبكات والأنظمة التي تم قياس خصائص النشاط المتوقع فيها بحيث يكون من السهل تحديد التغييرات. • فهم السلوكيات الطبيعية. • استخدام سجل مركزي وصياغة سياسة الاحتفاظ بالسجلات. • ربط الأحداث مع بعضها البعض. • الحفاظ على تزامن ساعات المستضيف. • الحفاظ على قاعدة معرفية بالمعلومات واستخدامها. • تشغيل برامج التلصص على المعلومات لجمع معلومات إضافية. • وضع مصفوفة تشخيص للعاملين الأقل خبرة. Upon the occurrence of an incident, the incident details shall be included in the initial analysis to determine its scope. Such details shall include the affected networks, systems, or applications; who or what caused the incident; and how the incident occurred (e.g., what tools or attack methods are being used, what vulnerabilities are being exploited, etc.). When performing an initial analysis, the following shall be considered: • Profiling of networks and systems in which the characteristics of expected activity is measured so that changes to it can be more easily identified • Understanding normal behaviors • Using a centralized logging and creating a log retention policy • Performing event correlation • Keeping all host clocks synchronized • Maintaining and using a knowledge base of information

	• Running packet sniffers to collect additional data • Creating a diagnosis matrix for less experienced staff
8-1	تحديد أولويات الأنشطة اللاحقة، مثل احتواء الحادثة والتحليل العميق لتأثيرات الحادثة، وذلك بناءً على نتائج التحليل الأولي. Subsequent activities, such as incident containment and deeper analysis of the incident impact, shall be prioritized based on the results of the initial analysis.
9-1	توثيق وتسجيل كافة الحقائق المتعلقة بالحادثة عن طريق السجل أو أجهزة الكمبيوتر المحمولة أو التسجيلات الصوتية أو الكاميرات الرقمية. All facts regarding an incident shall be documented and recorded through logbook, laptops, audio recorders or digital cameras.
10-1	توثيق وتسجيل توقيت كل خطوة تم اتخاذها من وقت اكتشاف الحادثة وحتى وقت معالجتها، وتأريخ كل وثيقة تتعلق بالحادثة والتوقيع عليها من قبل الجهة المعنية بالتعامل مع الحوادث. The time for every step taken from the minute the incident was detected to its final resolution shall be documented and recorded. Additionally, every document regarding the incident shall be dated and signed by the incident handler.
11-1	الاحتفاظ بسجلات حول حالة الحادثة باستخدام تطبيق أو قاعدة بيانات مثل نظام تتبع المشكلات، على أن تتضمن هذه السجلات ما يلي: • ملخص الحادثة. • المؤشرات المتعلقة بالحادثة (أي الدلائل التي تشير إلى وقوع الحادثة أو احتمالية وقوعها في المستقبل). • الإجراءات المتخذة من قبل جميع جهات التعامل مع الحوادث فيما يخص الحادثة. • تسلسل العهدة، إن كان مطبقاً. • تقييمات الأثر المتعلقة بالحادثة. • معلومات الاتصال بالأطراف الأخرى المعنية (مثل الجهات المسؤولة عن النظام، أو مشرفي النظام، أو الموردين). • قائمة بالأدلة التي تم جمعها خلال التحقيق في الحادثة.

	• آراء وتعليقات الجهات المعنية بالتعامل مع الحوادث. • الخطوات اللاحقة التي سيتم اتخاذها. Records regarding the status of incidents shall be maintained using an application or a database, such as an issue tracking system. Those records shall include the following: • Summary of the incident • Indicators related to the incident (i.e., a sign that an incident may have occurred or may occur) • Actions taken by all incident handlers on this incident • Chain of custody, if applicable • Impact assessments related to the incident • Contact information of relevant parties (e.g., system owners, system administrators, or vendors) • A list of evidence gathered during the incident investigation • Comments from incident handlers • Next steps to be taken
12-1	وضع معيار لعملية المراجعة المطلوبة من الإدارة العليا لتحديد إمكانية إفصاح <اسم الجهة> عن أي معلومات تتعلق بالحادثة الأمنية (مثل الجهة التي أبلغت عن الحادثة/المسببات والأنظمة المتأثرة) إلى أطراف خارجية (باستثناء الهيئة الوطنية للأمن السيبراني). A standard for the review process required by the upper management shall be created to determine whether or not <entity name> can disclose any information regarding the security incident (such as incident reporter/incident causes and affected systems) to external parties (except NCA).
13-1	حماية بيانات الحادثة وتقييد الوصول إليها إلى جانب تشفير المراسلات المتعلقة بالحادثة (مثل رسائل البريد الإلكتروني). Incident data shall be protected and access to it shall be restricted. Additionally, communications with regards to the incident (e.g., emails) shall be encrypted.

2	تصنيف الحوادث وتحديد أولوياتها (Incidents Classification and Prioritization)
الهدف	ضمان الاستجابة الفعالة والملائمة للحوادث بناءً على تقدير أثرها على الأعمال.
المخاطر المحتملة	في حالات الحوادث، يؤدي عدم تحديد الأولويات بصورة صحيحة إلى تسمية غير واضحة لحوادث أمن الشبكات وتنبيهاته ومشكلاته، مما ينتج عنه تأخير في الاستجابة للحوادث الطارئة، وعدم القدرة على تحديد الحوادث التي يمكن التعامل معها باعتبارها غير طارئة أو التنبيهات التي يمكن تجاهلها (مؤشرات سلبية خاطئة)، إلى جانب سوء تقدير نوع الاستجابة المناسب لحوادث وتنبيهات ومشكلات معينة.
الإجراءات المطلوبة	
1-2	تحديد أولويات الاستجابة لكل حادثة بناءً على تقدير أثرها على الأعمال والجهود المطلوبة للتعافي منها. ويجب أخذ العوامل التالية بعين الاعتبار عند دراسة أثر الحادثة: • الأثر الوظيفي للحادثة: تؤثر الحوادث التي تستهدف أنظمة تقنية المعلومات عادة على وظائف الأعمال التي تقدمها تلك الأنظمة، مما يؤثر سلباً على مستخدميها. يتضمن الجدول أ أمثلة على فئات الآثار الوظيفية يمكن لـ<اسم الجهة> استخدامها لتقييم حوادثها. • الأثر المعلوماتي للحادثة: يمكن أن تؤثر الحوادث على سرية معلومات <اسم الجهة> وسلامتها وتوافرها. يتضمن الجدول ب أمثلة على فئات الآثار المعلوماتية المحتملة تصف مقدار الانتهاك الأمني الذي تعرضت له المعلومات خلال الحادثة. • إمكانية التعافي من الحادثة: يحدد حجم الحادثة ونوع الموارد المتأثرة بالحادثة مقدار الوقت والموارد المطلوبة للتعافي منها. يحتوي الجدول ج على فئات الجهد المطلوب للتعافي من الحوادث، وتعكس هذه الفئات مستوى الموارد المطلوبة للتعافي ونوعها. Response to each incident shall be prioritized based on the estimated business impact caused by that incident and the estimated efforts required to recover from it. The following factors shall be considered when determining the impact of an incident: • Functional Impact: incidents targeting IT systems typically impact the business functionality that those systems provide, which negatively affects the users of those systems. Table A provides examples of

	functional impact categories that an organization might use for rating its own incidents. • Information Impact: incidents may affect the confidentiality, integrity, and availability of <entity name>'s information. Table B provides examples of possible information impact categories that describe the extent of information compromise caused by an incident. • Recoverability: the incident scope and the type of resources it affects determine the amount of time and resources required for recovery. Table C provides recoverability effort categories that reflect the resources level and type required to recover from an incident.
2-2	تصنيف جميع الحوادث بناءً على مستوى الحدة (الجدول د). Incidents shall be classified based on severity level (Table D).
3-2	إجراء الأنشطة التالية عند محاولة تحديد المستضيف المسؤول عن هجوم الأمن السيبراني: • التحقق من عنوان بروتوكول الإنترنت للمستضيف المهاجم. • البحث عن المستضيف المهاجم عن طريق محركات البحث. • استخدام قاعدة بيانات الحوادث. • مراقبة قنوات الاتصالات المحتملة التي يستخدمها المهاجم. The following activities shall be conducted when attempting to identify an attacking host: • Validating the attacking host's IP address • Searching for the attacking host on search engines • Using incidents database • Monitoring attacker's possible communication channels

4-2	تحديد إجراء التصعيد في الحالات التي لا يستجيب فيها فريق الاستجابة للحوادث للحادثة ضمن الإطار الزمني المحدد. An escalation procedure shall be established for the instances in which the incident response team does not respond to an incident within the designated timeframe.
3	الإبلاغ عن الحوادث (Incident Reporting)
الهدف	ضمان الالتزام التام بأنظمة الهيئة الوطنية للأمن السيبراني أو بما تصدره، وتعزيز جهود <اسم الجهة> من خلال توفير حلقة وصل للتعامل مع الحوادث. وتقوم الهيئة الوطنية للأمن السيبراني، إضافة إلى الجهات الأخرى، بتحليل المعلومات التي تقدمها <اسم الجهة> لتحديد توجهات الهجمات ومؤشراتها. ويمكن تمييز هذه التوجهات بشكل أدق عند مراجعة بيانات العديد من الجهات مقارنة بمراجعة بيانات جهة واحدة.
المخاطر المحتملة	يعتبر الإخفاق في إبلاغ الهيئة الوطنية للأمن السيبراني عن الحوادث نوعاً من عدم الالتزام بالمتطلبات الرسمية التي حددتها الهيئة الوطنية للأمن السيبراني، والتي تتمحور رسالتها حول مراقبة التزام الجهات باستمرار بهدف دعم الدور الهام للأمن السيبراني. ونظراً إلى أنه يتوجب على جميع الجهات الوطنية تطبيق كافة الإجراءات اللازمة لضمان الالتزام المستمر بالضوابط الأساسية للأمن السيبراني وفقاً للبند 3 من المادة 10 من تكليف الهيئة الوطنية للأمن السيبراني، ووفقاً للأمر السامي الكريم رقم 57231 بتاريخ 1439/11/10، فإن الإخفاق في الإبلاغ عن الحوادث يمكن أن يؤدي إلى عقوبات بحق <اسم الجهة>.
الإجراءات المطلوبة	
1-3	تحديد جهة اتصال رئيسية واحتياطية مع الهيئة الوطنية للأمن السيبراني، والإبلاغ عن كافة الحوادث التي تتوافق مع سياسة إدارة حوادث وتهديدات الأمن السيبراني في <اسم الجهة>. A primary and secondary Point of Contact (PoC) with NCA shall be designated, and all incidents consistent with <entity name>'s Incident Response Policy shall be reported.
2-3	تحديد طرق وقنوات الاتصال المطلوبة لإطلاع <اسم الجهة> والجهات المعنية الخارجية، مثل الهيئة الوطنية للأمن السيبراني، على آخر المستجدات. The communication methods and channels required to provide status updates to <entity name> and external stakeholders, such as NCA, shall be determined.

3-3	وضع سياسة تحدد المدة الزمنية التي يجب على مشرفي النظام وأفراد فريق العمل الآخرين إبلاغ فريق الاستجابة للحوادث عن الأحداث الشاذة خلالها، وآليات الإبلاغ (بما في ذلك قنوات الإبلاغ مثل رقم الهاتف و/أو عنوان البريد الإلكتروني)، ونوع المعلومات التي يجب إدراجها عند الإبلاغ عن الحوادث. A policy which states the maximum time during which system administrators and other workforce members must report anomalous events to the incident response team shall be developed. The mechanisms for such reporting (including the reporting channels such as phone number and/or email address), and the type of information that should be included in the incident notification shall be included in the policy as well.
4-3	وضع خطط تدريبية وسيناريوهات استجابة للحوادث وتطبيقها من أجل اختبار قنوات الاتصال التي تستخدمها فرق الاستجابة للحوادث، وتقييم مهارات اتخاذ القرار لديهم إلى جانب قدراتهم الفنية وذلك بهدف زيادة الوعي والمرونة في الاستجابة للتهديدات. Routine incident response exercises and scenarios shall be planned and conducted to test the communication channels used by the incident response team, in addition to its decision-making skills and technical capabilities to increase awareness and improve agility in responding to real-world threats.
5-3	تحديد أطر زمنية معينة والالتزام بها عند إبلاغ الهيئة الوطنية للأمن السيبراني عن حوادث الأمن السيبراني. Specified timeframes shall be determined and adhered to when reporting incidents to NCA.
4	خطة التعافي من الحوادث واستمرارية الأعمال (Incident Recovery and (Business Continuity Plan
الهدف	ضمان تعافي واستعادة عمل الأنظمة بشكل طبيعي، واستعادة وظائف المستضيف المتأثر وبياناته، وإلغاء إجراءات الاحتواء المؤقت (في الحوادث المرتبطة بالبرمجيات الضارة)، وضمان توافق إجراءات وسياسات الاستجابة للحوادث وعمليات استمرارية الأعمال، مما يخدم رسالة <اسم الجهة> وأهدافها العامة.
المخاطر المحتملة	يمكن أن يؤدي الإخفاق في تطبيق إجراءات خطة التعافي واستمرارية الأعمال بشكل ملائم إلى تكرار الهجمات في المستقبل مما قد يضر بسمعة <اسم الجهة> وعلامتها

	التجارية، وعملياتها وعلاقاتها مع العملاء والموردين، بالإضافة إلى الآثار القانونية والمالية المصاحبة.
الإجراءات المطلوبة	
1-4	إصدار بلاغ باستجابة لحادثة أمنية وإسنادها إلى فريق الاستجابة للحوادث عند الإبلاغ عن حادثة أمنية. An incident response ticket shall be assigned to the incident response team the moment a security incident is reported.
2-4	القيام بالأنشطة اللازمة لاستعادة الأنظمة المتأثرة، وتشمل هذه الأنشطة على سبيل المثال لا الحصر ما يلي: • استعادة الأنظمة من النسخ الاحتياطية السليمة. • إعادة بناء الأنظمة من الصفر. • استبدال الملفات التي تعرضت لانتهاكات أمنية بنسخ سليمة. • تثبيت التحديثات والإصلاحات. • تغيير كلمات المرور وتشديد أمن محيط الشبكة (مثل مجموعة قواعد جدار الحماية، وقوائم التحكم بالوصول إلى مُوجّه الحدود). Necessary activities shall be taken to restore the affected systems. Such activities shall include, but shall not be limited to, the following: • Restoring systems from clean backups • Rebuilding systems from scratch • Replacing compromised files with clean versions • Installing patches • Changing passwords, and tightening network perimeter security (e.g., firewall rulesets, boundary router access control lists, etc.).
3-4	ضمان معالجة حادثة الأمن السيبراني وتصحيحها ضمن الأطر الزمنية المحددة، وفي حال عدم القدرة على ذلك، يجب على فريق الاستجابة للحوادث تصعيد الحادثة وفقاً لتصنيف الحوادث الأمنية وقواعد وإجراءات تصعيد الحوادث المعتمدة في <الإدارة المعنية بالأمن السيبراني>. Cybersecurity incidents shall be resolved and corrected within the pre-defined timeframes, otherwise, the incident

response team shall escalate the incident as per the classification of security incidents and incidents escalation rules and procedures at the <cybersecurity organization>.	
تخصيص الميزانية والموارد اللازمة للتعافي من حوادث الأمن السيبراني، حيث تكون <اسم الجهة> هي المسؤولة عن توفير التمويل الكافي لـ<الإدارة المعنية بالأمن السيبراني>، والتي تستخدمه بدورها من أجل التقليل من الأضرار والتعافي من الحوادث. The budget and resources required to recover from a cybersecurity incident shall be allocated. <Entity name> shall be held responsible for providing sufficient fund to the <cybersecurity organization>, which will in turn utilize it to minimize the damage and ultimately, recover from the incident.	4-4
في بعض الحالات، يجب أن تدرس الجهات المعنية بالتعامل مع الحوادث الجهد المطلوب للتعافي فعلياً من الحادثة، وتقارن هذا الجهد بالقيمة الناتجة عن جهود التعافي، وأي متطلبات مرتبطة بالتعامل مع الحوادث. In some cases, incident handlers shall consider the effort necessary to actually recover from an incident and carefully weigh that against the value the recovery effort will create and any requirements related to incident handling.	5-4
تخزين تفاصيل حوادث الأمن السيبراني التي تقع (مثل نوع الحادثة وفئتها، والمستخدمين الذين أبلغوا عنها، والخدمات والأصول والمعلومات المتأثرة بها، وكيفية اكتشافها، وأي وثائق مساندة) وحفظها ومراجعتها دورياً. Details regarding cybersecurity incidents (e.g., incident type and category, incident reporters, affected services/assets/information, incident detection method, and any other supporting documents) shall be stored, maintained and reviewed periodically.	6-4
عقد اجتماعات لمناقشة "الدروس المستفادة" مع كافة الأطراف المعنية بعد وقوع حادثة كبيرة من أجل دراسة التهديدات الجديدة وتحسين التقنيات المستخدمة والدروس المستفادة كجزء من عملية التعافي. “Lessons learned” meetings shall be held with all relevant parties after the occurrence of a major incident to address	7-4

	new threats, improved technology, and lessons learned as part of the recovery process.
8-4	إطلاع مسؤولي التخطيط لاستمرارية الأعمال على طبيعة الحوادث وتأثيراتها حتى يتمكنوا من تحديد تقييمات الأثر على الأعمال وتقييمات المخاطر وخطط عمليات الاستمرارية بصورة مناسبة. Business continuity planning professionals shall be informed about the nature of the incidents and their impacts so they can fine-tune business impact assessments, risk assessments, and continuity of operations plans.
9-4	إشراك مختصي التخطيط لاستمرارية الأعمال في <اسم الجهة> من المراحل الأولى من عمليات اكتشاف حوادث الأمن السيبراني والاستجابة لها لتقليل انقطاع الأعمال خلال الظروف الشديدة؛ حيث من الممكن الاستفادة منهم في التخطيط للاستجابة لحالات معينة مثل هجمات تعطيل الشبكات (Denial of Service "DoS"). Business continuity planning professionals within <entity name> shall be engaged at the earliest stages of incident detection and response to minimize operational disruption during severe circumstances as they may provide valuable assistance in planning responses to certain situations, such as during Denial of Service (DoS) attacks.
5	الحفاظ على المعلومات الاستباقية بشأن التهديدات (Threat Intelligence Feeds Maintenance)
الهدف	ضمان اطلاع <اسم الجهة> على التهديدات وجوانب الاستغلال وكيفية توفير الحماية ضد هذه التهديدات بصورة ملائمة، وذلك من خلال تزويدها بمعلومات استباقية حول التهديدات، حيث تشمل هذه المعلومات بيانات منظمة وتحليلات للهجمات الأخيرة والحالية والمحتملة والتي يمكن أن تشكل تهديداً سيبرانياً لـ<اسم الجهة>.
المخاطر المحتملة	يمكن أن يؤدي الإخفاق في اطلاع <اسم الجهة> على التهديدات وجوانب الاستغلال بصورة ملائمة إلى مخاطر شديدة قد تتسبب بسرقة المعلومات أو الوصول غير المصرح به لها أو الكشف عنها.
الإجراءات المطلوبة	
1-5	جمع المعلومات عن تهديدات الأمن السيبراني مثل المؤشرات (كعنوان بروتوكول الإنترنت للأوامر المشبوهة، واسم النطاق لنظام أسماء النطاقات، والعنوان "URL" الذي يرتبط بمحتوى خبيث) من مجموعة من المصادر، بما في ذلك مستودعات المصادر

	المفتوحة والمعلومات الاستباقية عن التهديدات التجارية والشركاء الخارجيين، وتنظيمها في قاعدة بيانات معرفية. Cybersecurity threat information, such as indicators (e.g., Internet Protocol "IP" address of a suspected command, a suspicious Domain Name System "DNS" domain name, a Uniform Resource Locator "URL" that references malicious content), shall be collected from a variety of sources, including open source repositories, commercial threat feeds, and external partners, and organized in a knowledge base.
2-5	تنظيم وتخزين المؤشرات في قاعدة بيانات معرفية بصيغة حرة مثل قواعد بيانات "Wikis"، وقواعد البيانات المنظمة بهدف تخزين مجموعات المؤشرات وتنظيمها وتتبعها والاستفسار عنها. وتشمل المعلومات المتوفرة في القاعدة المعرفية عموماً ما يلي: • مصدر المؤشر وتاريخ أو وقت الحصول عليه. • القواعد التي تحكم استخدام المؤشر أو مشاركته. • فترة صلاحية المؤشر. • معلومات حول ما إذا كانت الهجمات المصاحبة للمؤشر قد استهدفت جهات أو قطاعات معينة. • أي سجلات مصاحبة للمؤشر لتعداد الثغرات الشائعة (CVE)، وتعداد المنصات الشائعة (CPE)، وتعداد نقاط الضعف الشائعة (CWE)، وتعداد الإعدادات الشائعة (CCE). • المجموعات والجهات المعادية والأسماء الوهمية المصاحبة للمؤشر. • التكتيكات والأساليب والإجراءات التي تستخدمها الجهات المعادية عموماً. • دوافع الجهات المعادية أو نواياها. • الأفراد أو سمات الأفراد المستهدفين بالهجمات المصاحبة. • الأنظمة المستهدفة بالهجمات. Indicators shall be organized and stored in a knowledge base in a free form, such as wikis and structured databases, to store, organize, track, query, and analyze collections of indicators. Information which is commonly recorded in a knowledge base shall include the following:

• Indicator source and indicator collection date or time • Rules governing the use or sharing of an indicator • Indicator validity duration • Information regarding whether or not attacks associated with an indicator have targeted specific organizations or sectors • Any Common Vulnerability Enumeration (CVE), Common Platform Enumeration (CPE), Common Weakness Enumeration (CWE), Common Configuration Enumeration (CCE) records associated with an indicator • Groups, actors or aliases associated with an indicator • TTPs commonly used by an actor • Motives or intent of an associated actor • Individuals or types of individuals targeted in associated attacks • Systems targeted in attacks	
مشاركة المعلومات المتعلقة بالتهديدات ومؤشرات الانتهاك مع الهيئة الوطنية للأمن السيبراني. Threat intelligence and breach indicators shall be shared with NCA.	3-5

الجدول أ - فئات الآثار على الخدمات

Table A – Functional Impact Categories

الفئة	التعريف
لا يوجد None	لا يوجد تأثير على قدرة <اسم الجهة> على تقديم الخدمات لكافة المستخدمين. No effect on <entity name>'s ability to provide all services to all users.
منخفض Low	ما زالت <اسم الجهة> قادرة على تقديم كافة الخدمات الأساسية لكافة المستخدمين ولكنها تفتقد إلى الفعالية. Minimal effect; <entity name> can still provide all critical services to all users but has lost efficiency.
متوسط Medium	لم تعد <اسم الجهة> قادرة على تقديم الخدمات الأساسية لمجموعة فرعية من المستخدمين. <Entity name> has lost the ability to provide critical services to a subset of system users.
مرتفع High	لا تستطيع <اسم الجهة> تقديم بعض الخدمات الأساسية لأي من المستخدمين. <Entity name> is no longer able to provide some critical services to any users.

الجدول ب - فئات الآثار على المعلومات

Table B– Informational Impact Categories

الفئة	التعريف
لا يوجد None	لم يتم تسريب المعلومات أو تغييرها أو حذفها، ولم تتعرض لأي انتهاك أمني. No information was exfiltrated, changed, deleted, or otherwise compromised
انتهاك الخصوصية Privacy Breach	الوصول إلى المعلومات القابلة لتحديد الشخصية (PII) للعاملين والمستفيدين وغيرهم أو تسريبها. Sensitive Personally Identifiable Information (PII) of employees, beneficiaries, etc. was accessed or exfiltrated.
انتهاك المعلومات المملوكة Proprietary Breach	الوصول إلى المعلومات المملوكة، مثل معلومات البنية التحتية الحساسة المحمية (PCII)، أو تسريبها. Unclassified proprietary information, such as Protected Critical Infrastructure Information (PCII), was accessed or exfiltrated.
انتهاك سلامة المعلومات Integrity Loss	تغيير المعلومات المحمية أو المملوكة أو حذفها. Sensitive or proprietary information was changed or deleted.

الجدول ج - فئات التعافي من آثار الحوادث

Table C– Recoverability Effort Categories

الفئة	التعريف
اعتيادي Regular	يمكن التنبؤ بالوقت اللازم للتعافي بالاستعانة بالموارد الحالية. Recovery time is predictable with existing resources.
تكميلي Supplemented	يمكن التنبؤ بالوقت اللازم للتعافي بالاستعانة بموارد إضافية. Recovery time is predictable with additional resources.
ممتد Extended	لا يمكن التنبؤ بالوقت اللازم للتعافي وهناك حاجة إلى موارد إضافية ومساعدة خارجية. Recovery time is unpredictable; additional resources and outside help are needed.
غير قابل للتعافي Not Recoverable	من غير الممكن التعافي من الحادثة (مثل حوادث تسرب بيانات حساسة أو نشرها)، ويجب البدء بالتحقيق فيها. Recovery from the incident is not possible (e.g., sensitive data exfiltrated and posted publicly), and an investigation on the incident shall be conducted.

الجدول د - تصنيف الحوادث وفقاً لمستوى الحدة

Table D – Classification of Incidents Based on Severity Level

مستوى الحدة	الوصف	وقت الاستجابة المستهدف	وقت الحل المستهدف
مرتفع جداً Very High	• تهديد أو أثر مباشر على صورة <اسم الجهة> أو سمعتها أو مصداقيتها. • تأثر العديد من وحدات الأعمال الوظيفية بصورة كبيرة. • تأثر موقع الأعمال بصورة كبيرة. • الحاجة إلى تفعيل إجراءات استمرارية الأعمال. • Direct threat or damage to <entity name>'s image, reputation or credibility. • Sever impact on multiple business functional units. • Critical impact on business location. • Continuity measures may need to be invoked.	فوري	ساعتان
مرتفع High	انقطاع كبير يؤثر على وحدات الأعمال الوظيفية أو الخدمات الرئيسية أو موقع الجهة Severe outage affecting single business functional units, key services or location.	ساعة - ساعتان	5-4 ساعات
متوسط Medium	تدهور متوسط في سير عمل وحدات الأعمال الوظيفية أو المواقع أو الأصول التقنية والمعلوماتية، إضافة إلى أثر يتراوح ما بين المتوسط والمرتفع على وحدات الأعمال غير الهامة في <اسم الجهة>. Moderate degradation to business functional units, locations, and IT assets, in addition to moderate to high impact on non-critical business units within <entity name>.	3-2 ساعات	9-8 ساعات
منخفض Low	• المشكلة صغيرة وعلى نطاق بسيط. • تؤثر المشكلة على عدد قليل من الموارد. • يمكن تحمل المشكلة لفترة زمنية محددة.	5 ساعات	24 ساعة

اختر التصنيف

مستوى الحدة	الوصف	وقت الاستجابة المستهدف	وقت الحل المستهدف
	• Small issue with a localized scope. • Few resources are affected by the issue. • Issue can be tolerated for a particular period of time.		

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 باستمرار.

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>.