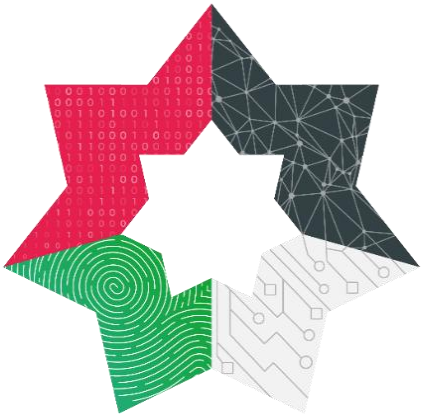
المملكة الأردنية الهاشمية



المركـز الوطنـي للأمـن السيبرانـي
National Cyber Security Center

سياسة الإبلاغ والاستجابة لحوادث الأمن السيبراني

Cyber Security Incident Response and Reporting Policy

(2025)

الصادرة عن المجلس الوطني للأمن السيبراني بموجب قراره رقم (20) المتخذ في

جلسته المنعقدة بتاريخ 21/5/2025

جدول المحتويات

رقم الإصدار	تاريخ الإصدار	ملخص عن التعديلات	أرقام الصفحات المشمولة بالتعديل
1	2025/5/21	إصدار جديد	-
			-
			-
			-

1. المقدمة

تتمثل مهام المركز الوطني للأمن السيبراني في بناء منظومة فعالة للأمن السيبراني في المملكة وتطويرها وتنظيمها لحماية المملكة من تهديدات الفضاء السيبراني ومواجهتها بكفاءة وفاعلية بما يضمن استدامة العمل والحفاظ على الأمن الوطني وسلامة الأشخاص والممتلكات والمعلومات، وفي إطار وجود العديد من المحاولات غير المشروعة من التهديدات والهجمات السيبرانية بمختلف أنواعها مثل اختراق أنظمة المعلومات أو الشبكات أو الأجهزة الإلكترونية، والأهداف المراد منها سرقة البيانات أو تعطيل الخدمات أو التسبب في أضرار لمختلف المؤسسات وشبكات البنى التحتية الحرجة والتي تشكل خطراً على أمن الفضاء السيبراني الوطني، وبموجب ذلك تأتي "**سياسة الإبلاغ والاستجابة لحوادث الأمن السيبراني**" بهدف تحديد قنوات الإبلاغ عن الحادث وتوقيته وزيادة كفاءة إجراءات الاستجابة والوقت المستغرق للاستجابة بما يتوافق مع منهجية الإطار الوطني الأردني للأمن السيبراني.

إن وجود سياسة تحدد آليات تعامل الجهات القطاعية والجهات التابعة لها مع حوادث الأمن السيبراني من شأنها أن تقلل من تأثير هذه الحوادث على سرية وسلامة وتوافر أنظمة المعلومات الوطنية وتطبيقاتها وبياناتها، كما أن اتباع نهج فعّال لإدارة مثل هذه الحوادث يحد من العواقب السلبية على كل من الجهات والأفراد، ويحسن من قدرة الجهة على استعادة العمليات المتضررة بمثل هذه الحوادث على الفور. وبينما لا يمكن منع حوادث الأمن السيبراني دائماً، فإن الإجراءات المناسبة للكشف عن الحوادث وسرعة الإبلاغ عنها والتعامل معها جنباً إلى جنب مع تثقيف وتوعية الأفراد، يمكن أن تقلل من تكرارها وشدتها وعواقبها السلبية المحتملة.

ومن المهم بشكل خاص إبلاغ المركز بالحوادث التي قد تؤدي إلى تعطيل الخدمات الأساسية أو تدمير المعلومات، وكما هو محدد في "تعليمات تصنيف حوادث الأمن السيبراني" الصادرة عن المركز حسب جدول توقيتات الإبلاغ والاستجابة الوارد في هذه السياسة.

2. السند التشريعي وإلزامية التطبيق

أ. استنادا للفقرة (أ) من المادة (4) من قانون الأمن السيبراني التي تنص على (يتولى المجلس المهام والصلاحيات التالية: أ – إقرار الاستراتيجيات والسياسات والمعايير المتعلقة بالأمن السيبراني).

ب. واستنادا لأحكام المادة (8/ب/3) من ذات القانون (تلتزم الوزارات والدوائر الحكومية والمؤسسات الرسمية والعامة والخاصة والأهلية بإبلاغ المركز عن أي حادث يهدد الأمن السيبراني أو يتعلق بأمن الفضاء السيبراني والقيام بكل ما يلزم لتفادي وقوعه).

3. التعاريف:

أ. يكون للكلمات والعبارات والتالية حيثما وردت في هذه السياسة المعاني المخصصة لها أدناه ما لم تدل القرينة على غير ذلك:

القانون: قانون الأمن السيبراني.

المجلس: المجلس الوطني للأمن السيبراني.

المركز: المركز الوطني للأمن السيبراني.

التعليمات: تعليمات تصنيف حوادث الأمن السيبراني.

حادث الأمن السيبراني: الفعل أو الهجوم الذي يشكل خطرا على البيانات أو المعلومات أو نظم المعلومات أو الشبكة المعلوماتية أو البنى التحتية المرتبطة بها و يتطلب استجابة لإيقافه أو للتخفيف من العواقب أو الآثار المترتبة عليه.

الجهة: أي وزارة أو مؤسسة أو دائرة حكومية عامة أو خاصة أو مؤسسة أهلية أو جمعية أو شركة أو مؤسسة فردية مسجلة في المملكة وفق التشريعات النافذة.

الجهة المتضررة: الجهة التي تتعرض أو يشتبه بتعرضها لحادث أمن سيبراني يستهدف أنظمتها المعلوماتية أو التشغيلية.

أصحاب المصلحة: جميع الجهات التي يكون لها دور في الاستجابة لحادث الأمن السيبراني، والذين تتأثر مصالحهم بشكل مباشر أو غير مباشر بالحادث.

إجراءات التشغيل القياسية (Standard Operating Procedures - SOPs): مجموعة من الإجراءات والنشاطات المتفق عليها والتي يتم تنفيذها قبل وخلال وبعد وقوع حادث الأمن السيبراني بهدف تقليل المخاطر والأضرار الناجمة عنه.

الاستجابة: مجموعة من الإجراءات التقنية والأمنية والقانونية المتخذة عند وقوع حادث أمن سيبراني.

خطة الاستجابة للحوادث: مجموعة من الإجراءات التي توجه كيفية استجابة الجهة لحادث أمن سيبراني أو خرق أمني، وتهدف إلى تقليل التأثير واحتواء التهديد واستعادة العمليات الطبيعية والدروس المُستفادة من الحادث.

فريق الاستجابة: مجموعة من الأفراد المختصين في مجال الأمن السيبراني يتولون مهمة الاستجابة لحوادث الأمن السيبراني.

فرق الاستجابة القطاعية (Sectoral CERTs)**:** هي فرق استجابة متخصصة تُشكَّل ضمن القطاعات الحيوية التنظيمية في المملكة لضمان سرعة الاستجابة والاحتواء الفعّال لأي تهديدات أو حوادث أمن سيبراني قد تؤثر على القطاع، وتُناط بها مهام الاستجابة لحوادث الأمن السيبراني ضمن نطاق القطاع الذي تنتمي إليه، وتعمل تحت إشراف وتنسيق المركز الوطني للأمن السيبراني.

ب. تُعتمد التعاريف الواردة في قانون الأمن السيبراني والأنظمة والتعليمات الصادرة بمقتضاه أينما وردت في هذه السياسة.

4. الغاية والأهداف

تهدف هذه السياسة إلى ضمان قيام الجهات والمؤسسات الوطنية بوضع وتطبيق إجراءات تشغيل قياسية (SOPs) وقنوات اتصال واضحة للإبلاغ عن حوادث الأمن السيبراني والاستجابة لها ضمن توقيتات محددة لضمان احتواء الحادث والتقليل من آثاره. على أن تشمل ما يلي:

أ. تحديد الإجراءات والمسؤوليات عند وقوع الحادث.

ب. تحديد قنوات الإبلاغ عند وقوع حادث أمن سيبراني.

ج. احتواء الحادث وإيقاف أي نشاط غير مرغوب فيه بسرعة وكفاءة.

د. الحد من أي انقطاع في الخدمات الأساسية للشبكات وأنظمة المعلومات للجهات.

ه. التوثيق الدقيق للمعلومات وكتابة التقارير المتعلقة بالحادث.

و. منع و/أو الحد من حوادث الأمن السيبراني المستقبلية أو التهديدات والهجمات المحتملة وتوثيق الدروس المستفادة من الحادث.

5. نطاق التطبيق

تطبق هذه السياسة على كافة الوزارات والدوائر الحكومية والمؤسسات الرسمية والعامة والخاصة والأهلية وقطاعات البنى التحتية الحرجة ومقدمي خدمة الاستجابة لحوادث الأمن السيبراني.

6. الأدوار والمسؤوليات

للاستجابة بكفاءة لحادث أمن سيبراني ما، ولتجنب تكرار الجهود وتقليل الفجوات الإجرائية التي قد تحدث وضمان الاستجابة السريعة للحوادث. هنالك مجموعة من الأدوار والمسؤوليات يجب التقيد بها وتنفيذها قبل وقوع الحادث كإجراء وقائي وتحضيري بحيث تكون الجهة جاهزة للتعامل مع أي حادث. على النحو التالي:

أولاً: أدوار ومسؤوليات الجهة:

أ. تلتزم الجهة قبل وقوع أي حادث بما يلي:

1. اتباع السياسات والمعايير والضوابط والقرارات والتوجيهات الأمنية الصادرة عن المركز الوطني للأمن السيبراني والجهات القطاعية.
2. إعداد خطة استجابة تحدث دوريا توضح الأدوار والمسؤوليات الداخلية وقنوات الإبلاغ وإجراءات التشغيل القياسية، بالاستعانة بأفضل الممارسات المتبعة.
3. تسمية ضباط ارتباط خاصين للإبلاغ عن حوادث الأمن السيبراني والتعاون والتنسيق مع الجهات القطاعية والجهات المعنية، وفق قنوات الإبلاغ الواردة في هذه السياسة.
4. تلتزم الجهة بالربط مع مركز العمليات الأمني القطاعي للاستجابة للحوادث التابع للقطاع وفي حال تعذر ذلك، على الجهة الربط مع مركز العمليات الأمنية (SOC) في المركز في حال تحقق الربط على الشبكة الحكومية (SGN)، وبخصوص الجهات غير المتصلة الشبكة الحكومية (SGN) يتوجب عليها الربط مع مركز عمليات أمني (SOC) مرخص من المركز الوطني للأمن السيبراني، للاستفادة من التنبيهات والتحذيرات التي يقدمها عند اكتشاف أي نشاطات مشبوهة على شبكاتهم.

ب. تلتزم الجهة في حال وقوع حادث بما يلي:

عند وقوع حادث أمن سيبراني يجب على الجهة المتضررة اتباع تسلسل إجراءات التصعيد التالي:

1. إبلاغ الجهة القطاعية بما يتلاءم مع توقيتات الإبلاغ والاستجابة الموضحة في هذه السياسة وفقاً للجدول رقم (1) وفي حال عدم الارتباط بجهة قطاعية يتوجب إبلاغ المركز بشكل مباشر.
2. إذا صُنف الحادث بدرجة "شديد الخطورة" أو "خطير"، تتولى الجهة القطاعية عملية إبلاغ المركز الوطني للأمن السيبراني، وعلى الجهة التعاون التام وتسهيل عمل فريق الاستجابة للحادث من المركز أو أي جهة يراها المركز مناسبة، ضمن توقيتات الإبلاغ والاستجابة الموضحة في الجدول رقم (1).
3. إذا صُنف الحادث بدرجة "متوسط" أو "منخفض" تتولى فرق الاستجابة التابعة للجهة أو فرق الاستجابة القطاعية عملية الاستجابة للحوادث أو الاستعانة بمقدمي خدمة الاستجابة لحوادث الأمن السيبراني المرخص لهم، مع الالتزام بإبقاء المركز مطلعاً على سير عملية الاستجابة ولغاية إغلاق ملف الحادثة وتقديم تقرير نهائي للجهة القطاعية.

4. عدم الإفصاح عن أي معلومات متعلقة بالحوادث الأمنية إلى أطراف ثالثة أو خارجية إلا بعد الحصول على موافقة المركز والجهة التنظيمية المعنية وبما يتوافق مع التشريعات الناظمة للجهة.
5. تسهيل عمل موظفي المركز أو فرق الاستجابة القطاعية وتقديم التعاون اللازم.

ج. تلتزم الجهة بعد الانتهاء من الاستجابة للحادث بما يلي:

1. القيام بالأنشطة اللازمة لاستعادة الخدمات والأنظمة المتضررة والتي تشمل على سبيل المثال لا الحصر؛ تثبيت التحديثات والإصلاحات تغيير كلمات المرور وإعادة بناء الأنظمة وإشراك الموردين عند الحاجة.
2. الالتزام بتنفيذ التوصيات والإجراءات والدروس المستفادة بعد الاستجابة لحوادث الأمن السيبراني.
3. في حال الاستعانة بفرق استجابة أخرى أو بمقدم خدمات مُرخص له بالاستجابة لحوادث الأمن السيبراني، تلتزم الجهة المتضررة بتقديم تقرير مفصل بالحادث للجهة القطاعية والتي بدورها تزود المركز بتقرير يوضح مؤشرات الاختراق ومعلومات التهديد وأية معلومات تتعلق بالحادث والإجراءات التي تم تنفيذها خلال وبعد الحادث.

ثانياً: أدوار ومسؤوليات الجهات القطاعية:

أ. إصدار إجراءات تنظيمية خاصة بالقطاع في مجال الاستجابة للحوادث وتلقي البلاغات من الجهات التي تخضع لإشراف ورقابة الجهة القطاعية وبما لا يتعارض مع الإجراءات والسياسات المتعلقة بذات العلاقة.

ب. استحداث فرق استجابة قطاعية، تُعنى بالاستجابة للحوادث.

ج. تقييم المستوى الأمني ومستوى الجاهزية للاستجابة للحوادث السيبرانية في الجهات التابعة للقطاع مع إمكانية الاستعانة بالمركز الوطني للأمن السيبراني لإجراء التقييم عند الحاجة.

د. تصنيف الحادث استناداً لتعليمات تصنيف حوادث الأمن السيبراني لسنة 2023.

ه. التعامل مع الحادث ومحاولة إيقاف أية نشاطات عدائية فعّالة وواضحة واتخاذ الإجراءات التي من شأنها منع اتساع الحادث من عزل للأنظمة أو منع الوصول إلى موارد محددة وذلك للحد من الخسائر المحتملة.

و. استحداث قنوات اتصال وآلية إبلاغ عن الحوادث وربطها مع المركز.

ز. رفع تقرير للمركز بحوادث الأمن السيبراني في الجهات التابعة لها يوضح الإجراءات التي تم تنفيذها خلال وبعد الحادث.

ثالثا: أدوار ومسؤوليات المركز الوطني للأمن السيبراني:

يتولى المركز عند الاستجابة لحوادث الأمن السيبراني ما يلي:

أ. تلقي البلاغات لحوادث الأمن السيبراني من خلال قنوات الإبلاغ الواردة في هذه السياسة وله طلب المعلومات التي يحتاجها والمتعلقة بالحادثة من الجهة القطاعية التي تتبع لها الجهة.

ب. إذا صُنِّف الحادث بدرجة "شديدة الخطورة" أو "خطير"، يتولى المركز أو أي جهة يراها المركز مناسبة في هذه الحالة مسؤولية إدارة وتوجيه الاستجابة وتلتزم الجهات كافة بالتعليمات والتوجيهات التي تصدر عن المركز.

ج. في الحوادث التي قرّر تصنيفها بدرجة "شديد الخطورة" وفي بعض الحالات الخاصة التي يقررها المركز يتم التنسيق مع "المركز الوطني للأمن وإدارة الأزمات" لتفعيل "الخطة الوطنية المُنسقة لمواجهة تداعيات التهديدات والحوادث السيبرانية" الصادرة عنه والتي أقرّها مجلس الوزراء في قراره رقم (15707) تاريخ 2024/3/17.

د. في الحالات التي تتم الاستجابة من خلال الجهة المتضررة نفسها أو من خلال فرق الاستجابة القطاعية أو من قبل مقدمي خدمات الاستجابة المرخص لهم، يقوم المركز ولضمان اكتمال عملية الاستجابة، بالتحقق من صحة نتائج وعمليات الاستجابة والتأكد أنها تلبي المعايير الأساسية، وأنفذ جميع الخطوات المهمة، وأنها قضت تماماً على أي حادث أو ثغرة أمنية.

ه. تزويد الجهة المتضررة والجهة القطاعية التابعة لها التوصيات اللازمة والواجب اتباعها للاستفادة من الدروس ولتلافي تكرار الحادث في المستقبل.

7. آلية الإبلاغ عن حوادث الأمن السيبراني

أ. حددت المادة (8-ب-3) من القانون بأن تلتزم الوزارات والدوائر الحكومية والمؤسسات الرسمية والعامة والخاصة والأهلية "الإبلاغ عن أي حادث يهدد الامن السيبراني أو يتعلق بأمن الفضاء

السيبراني والقيام بكل ما يلزم لتفادي وقوعه". وبناءً عليه يجب على الجهة المتضررة الإبلاغ عن أي حادث تنطبق عليه مواصفات أيٍ من تصنيفات الحوادث الأربعة (شديد الخطورة، خطير، متوسط، منخفض) الواردة في التعليمات النافذة.

ب. يتولى الموظف المعني في الوحدة التنظيمية المختصة أو ضابط الارتباط المكلف لدى الجهة المتضررة بالحادث مسؤولية اطلاع الوزير أو الرئيس أو المدير المعني ووضعه بصورة الموقف فوراً وإبلاغ الجهة القطاعية التي تتبع لها الجهة والتي بدورها تقوم بتصنيف شدة الحادث استناداً لتعليمات تصنيف حوادث الأمن السيبراني لسنة 2023.

ج. تقوم الجهة القطاعية بإبلاغ المركز الوطني للأمن السيبراني في حالات التصنيف "شديد الخطورة " أو "خطير ".

د. **قنوات الإبلاغ:** يتولى المركز مسؤولية تلقي البلاغات من الجهات القطاعية على مدار الساعة وتتبع قنوات الإبلاغ التالية عند وقوع حادث أمن سيبراني:

1. الخط الساخن: 06-5900511- 415/412/411/410.
2. البريد الإلكتروني: Jo-cert@ncsc.jo.
3. الموقع الإلكتروني الخاص لفريق الاستجابة الوطني لحوادث الأمن السيبراني (JOCERT) https://jocert.ncsc.jo.

ه. توقيتات الإبلاغ والاستجابة لحوادث الأمن السيبراني:

عند الإبلاغ عن حوادث الأمن السيبراني يتم التقيد بتوقيتات الإبلاغ التالية وبما يتناسب مع طبيعة الجهة المتضررة بالحادث ووفقاً لتعليمات تصنيف حوادث الأمن السيبراني لسنة 2023، وفقاً لما يلي:

درجة الخطورة	الوصف	زمن الإبلاغ للمركز الوطني للأمن السيبراني والجهة القطاعية	زمن الاستجابة الأولية	زمن الاستجابة الكاملة (الاحتواء والمعالجة)
شديد الخطورة (Critical)	حادث يؤثر بشكل مباشر على العمليات الحيوية أو يسبب توقفاً كاملاً للخدمات الحكومية أو تسريب بيانات حساسة.	خلال 1 ساعة كحد أقصى	خلال 30 دقيقة	خلال 4 إلى 8 ساعات
خطير(High)	حادث يؤثر على أنظمة حساسة ولكن دون توقف تام، أو محاولة اختراق فاشلة تم رصدها.	خلال 2 ساعات	خلال 1 ساعة	خلال 12 ساعة
متوسط (Medium)	نشـــاط مريب تم رصـــده، مثل رسـائل تصـيد أو برامج ضـارة تم اكتشافها قبل تفعيلها.	خلال 4 ساعات	خلال 4 ساعات	خلال 24 ساعة
منخفض (Low)	حوادث غير مؤكدة أو لا تؤثر بشكل مباشر على الأنظمة، مثل محاولات تسجيل دخول فاشلة متعددة.	خلال 24 ساعة	خلال 1 يوم	خلال 3 أيام

جدول 1: توقيتات الإبلاغ والاستجابة

8. الاستجابة لحوادث الأمن السيبراني:

تتولى الجهة والجهة القطاعية الاستجابة لحوادث الأمن السيبراني التي تتعرض لها من خلال فريق الاستجابة للحوادث لديها أو اللجوء إلى فرق الاستجابة القطاعية؛ وذلك عن طريق اكتشاف الحادث الأمني واحتواؤه ومنع انتشاره وتنفيذ الإجراءات التالية:

أ. التحضير(Preparation) : إعداد السياسات، الأدوات، والتدريب اللازم لرفع الجاهزية.

ب. الكشف والتحليل(Detection & Analysis) : رصد الحوادث وتحليلها لتحديد النوع والحجم والأثر.

ج. الاحتواء، الاستئصال والتعافي (Containment, Eradication & Recovery) بعزل الأنظمة المصابة، إزالة التهديدات، واستعادة الوضع الطبيعي.

د. الدروس المستفادة والتقييم والمتابعة (Lesson Learned) : بمراجعة الحادث وتحليل الأداء لتحسين الاستجابة المستقبلية.

9. التنسيق والتعاون

إجراء التنسيق والتعاون ضروري ومهم في الحوادث المصنفة بدرجة "شديد الخطورة" و "خطير"، حيث تتطلب الاستجابة لمثل هذا النوع من الحوادث تنسيق عالي المستوى بين الجهات ذوي العلاقة، ومن الضروري أن تنسق وتتعاون الجهة المتضررة بشكل مستمر مع المركز من خلال فرق الاستجابة القطاعية في كافة مراحل الاستجابة للحادث.

10. الامتثال

أ. تدخل هذه السياسة حيز النفاذ من تاريخ إقرارها من المجلس الوطني للأمن السيبراني.

ب. يجب على جميع الجهات الامتثال لهذه السياسة وتزويد المركز بالمعلومات اللازمة لتمكينه من القيام بعمله وبما لا يتعارض مع القوانين النافذة.

11. الحوكمة

يتولى المركز مراقبة مدى التزام الجهات المعنية كافة بهذه السياسة واتخاذ الإجراء المناسب في حال عدم الالتزام وفقاً لأحكام المادة 16 من قانون الأمن السيبراني وتعليمات تحديد معايير مخالفات أحكام قانون الأمن السيبراني وضوابطها والإجراءات المستحقة عليها لسنة 2025 الصادرة بمقتضاه.