تعليمات تصنيف حوادث الأمن السيبراني لسنة 2023

صادرة بموجب البند (3) من الفقرة (ب) من المادة (6) من قانون الأمن السيبراني رقم 16 لسنة 2019

المادة 1

تسمى هذه التعليمات (تعليمات تصنيف حوادث الأمن السيبراني لسنة 2023) ويعمل بها من تاريخ إقرارها من المجلس الوطني للأمن السيبراني.

المادة 2

أ. يكون للكلمات والعبارات المبينة أدناه المعاني المخصصة لها والمبينة إزاء كل منها ما لم تدل القرينة على خلاف ذلك:

القانون: قانون الأمن السيبراني رقم (16) لسنة 2019.

المملكة: المملكة الأردنية الهاشمية.

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.

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

فريق الاستجابة: مجموعة من الأفراد المختصين في مجال الأمن السيبراني يتولون مهمة الاستجابة لحوادث الأمن السيبراني وفق أحكام هذه التعليمات.

ب. تعتمد التعاريف الواردة بالقانون والأنظمة الصادرة بمقتضاه أينما وردت في هذه التعليمات.

المادة 3

يتولى المركز وبموجب أحكام هذه التعليمات تصنيف حوادث الأمن السيبراني في المملكة بحسب مستوى الخطورة إلى أربع مستويات وفقاً للشكل رقم (1).

المادة 4

أ. يصنف الحادث (شديد الخطورة) إذا أدى إلى تعطل الخدمات الأساسية بشكل كامل أو تسريب أو تدمير أو مسح للبيانات الحساسة ويكون تأثيره واضح على أكثر من بنية تحتية حرجة أو على أكثر من ثلث سكان المملكة.

ب. يتولى المركز عملية الإدارة والاستجابة لحادث الأمن السيبراني المصنف شديد الخطورة.

المادة 5

أ. يصنف الحادث (خطير) في أي من الحالات التالية:

1. الحادث الذي يكون مصدره البرمجيات الخبيثة أو اختراق الشبكات والتي تؤثر على جزء محدود من الخدمات أو محاولات الاختراق غير المؤثرة على البيانات الحساسة والخدمات وكان الحادث على أكثر من بنية تحتية حرجة أو على أكثر من ثلث سكان المملكة.

2. الحادث الذي يؤدي إلى تعطل الخدمات الأساسية بشكل كامل أو محدود أو تسريب أو تدمير أو مسح للبيانات الحساسة أو البرمجيات الخبيثة أو اختراق الشبكات وكان الحادث يقع على أي من الجهات التالية:

- **بنية تحتية حرجة.**
- **الأجهزة الأمنية أو العسكرية.**
- **الوزارات والمؤسسات الحكومية.**
- **الشركات المملوكة للحكومة أو التي تساهم فيها.**
- **سلاسل التزويد التي تزود تلك الجهات.**

3. الحادث الذي يؤدي إلى تعطل كامل للخدمات الأساسية وكان تأثيره على مؤسسات التعليم العالي.

ب. يتولى المركز عملية الإدارة والاستجابة لحادث الأمن السيبراني المصنف خطير.

المادة 6

أ. يصنف الحادث (متوسط) في أي من الحالات التالية:

1. الحادث الذي يكون مصدره عمليات المسح والاستطلاع المؤثرة على البيانات والخدمات ويكون على أكثر من بنية تحتية حرجة.

2. الحادث الذي يكون مصدره محاولات الاختراق غير المؤثرة على البيانات الحساسة والخدمات أو عمليات المسح والاستطلاع المؤثرة على البيانات والخدمات وكان الحادث يقع على أي من الجهات التالية:

- **بنية تحتية حرجة.**
- **الأجهزة الأمنية أو العسكرية.**
- **الوزارات والمؤسسات الحكومية.**
- **الشركات المملوكة للحكومة أو التي تساهم فيها.**
- **سلاسل التزويد التي تزود تلك الجهات.**

3. الحادث الذي يكون مصدره تسريب أو تدمير أو مسح للبيانات الحساسة أو البرمجيات الخبيثة أو اختراق الشبكات والتي تؤثر على جزء محدود من الخدمات الأساسية ويكون تأثيره على مؤسسات التعليم العالي.

4. الحادث الذي يؤدي إلى تعطل كامل للخدمات الأساسية ويكون تأثيره على الشركات الخاصة أو المؤسسات الفردية.

ب. 1. تلتزم الجهات بتوجيهات وتعليمات المركز فيما يتعلق بالاستجابة للحادث المصنف متوسط سواء الاستعانة بفرق الاستجابة أو الاستعانة بالجهات المرخص لها بتقديم خدمة الاستجابة لحوادث الأمن السيبراني.

2. وفي حال الاستعانة بالجهات المرخص لها وفق البند (1) من هذه الفقرة تلتزم الجهة برفع تقرير مفصل للمركز عن الحادث.

المادة 7

أ. يصنف الحادث (منخفض) في أي من الحالات التالية:

1. الحادث الذي يكون مصدره محاولات الاختراق غير المؤثرة على البيانات الحساسة والخدمات أو عمليات المسح والاستطلاع المؤثرة على البيانات والخدمات ويكون تأثيره على مؤسسات التعليم العالي.

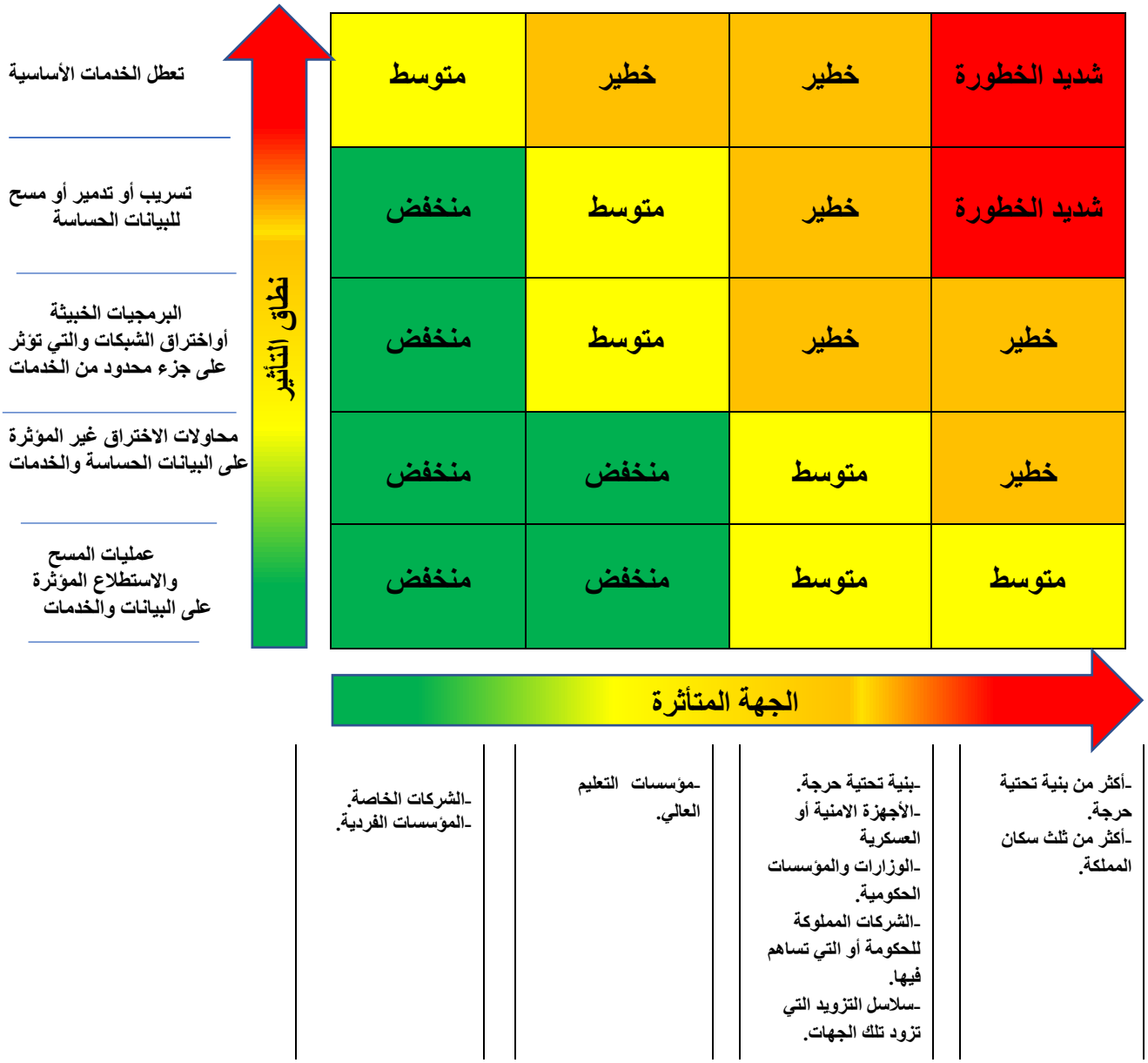
2. إذا لم يكون هناك تعطل كامل للخدمات الأساسية وكان تأثيره على الشركات الخاصة أو المؤسسات الفردية.

ب. تتم عملية الاستجابة للحادث المصنف منخفض سواء من قبل الجهة المتأثرة أو الاستعانة بفرق الاستجابة أو الاستعانة بالجهات المرخص لها بتقديم خدمة الاستجابة لحوادث الأمن السيبراني.

المادة 8

مع مراعاة ما ورد في هذه التعليمات إذا كان حادث الأمن السيبراني يشكل خطراً على أمن المملكة وسلامتها وفق أحكام المادة (9) من القانون فيكون المركز مسؤولاً عن إدارة وتوجيه الاستجابة له وعلى جميع الجهات المعنية الالتزام بتوجيهات المركز وتعليماته المتعلقة بهذا الخصوص.

الشكل رقم (1)


تعطل الخدمات الأساسية
تسريب أو تدمير أو مسح للبيانات الحساسة
البرمجيات الخبيثة أواختراق الشبكات والتي تؤثر على جزء محدود من الخدمات
محاولات الاختراق غير المؤثرة على البيانات الحساسة والخدمات
عمليات المسح والاستطلاع المؤثرة على البيانات والخدمات
نطاق التأثير
متوسط
خطير
خطير
شديد الخطورة
منخفض
متوسط
خطير
شديد الخطورة
منخفض
متوسط
خطير
خطير
منخفض
منخفض
متوسط
خطير
منخفض
منخفض
متوسط
متوسط
الجهة المتأثرة
-الشركات الخاصة.
-المؤسسات الفردية.
-مؤسسات التعليم العالي.
-بنية تحتية حرجة.
-الأجهزة الامنية أو العسكرية
-الوزارات والمؤسسات الحكومية.
-الشركات المملوكة للحكومة أو التي تساهم فيها.
-سلاسل التزويد التي تزود تلك الجهات.
-أكثر من بنية تحتية حرجة.
-أكثر من ثلث سكان المملكة.