الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

# الإطار الوطني لإدارة مخاطر الأمن السيبراني

National Framework for Cybersecurity Risk Management

(NFCRM–1: 2025)

| |
|---|
| إشارة المشاركة: شفاف |
| تصنيف الوثيقة: عام |

**تنويه:** لمواكبة المتغيرات بشأن تحديثات الوثائق الصادرة عن الهيئة الوطنية للأمن السيبراني، تود الهيئة الوطنية للأمن السيبراني التنويه على أهمية الاعتماد الدائم على نسخ الوثائق المنشورة في الموقع الإلكتروني للهيئة https://nca.gov.sa

بسم الله الرحمن الرحيم

# بروتوكول الإشارة الضوئية (TLP):

يستخدم هذا البروتوكول على نطاق واسع في العالم وهناك أربعة ألوان (إشارات ضوئية):

### أحمر (شخصي وسري للمستلم فقط)

المستلم لا يحق له مشاركة المصنف بالإشارة الحمراء مع أي فرد، سواء أكان ذلك من داخل الجهة أم خارجها؛ خارج النطاق المحدد للاستلام.

### برتقالي + مشدد (مشاركة في نفس الجهة)

المستلم يمكنه مشاركة المعلومات في الجهة نفسها مع الأشخاص المعنيين فحسب.

### برتقالي (مشاركة محدودة)

المستلم يمكنه مشاركة المعلومات في الجهة نفسها مع الأشخاص المعنيين فحسب. ومن يتطلب الأمر منه اتخاذ إجراء يخص المعلومة.

### أخضر (مشاركة في نفس المجتمع)

المستلم يمكنه مشاركة المعلومات مع آخرين في الجهة نفسها، أو جهة أخرى على علاقة معهم أو في القطاع نفسه؛ ولا يسمح بتبادلها أو نشرها من خلال القنوات العامة.

### شفاف (غير محدود)

# قائمة المحتويات

المقدمة ..... ٤
التعريفات ..... ٥
أهداف الإطار ..... ٧
نطاق تطبيق الإطار ..... ٧
المسؤوليات في إدارة مخاطر الأمن السيبراني على المستوى الوطني ..... ٨
المسؤوليات في إدارة مخاطر الأمن السيبراني على مستوى الجهة ..... ٨
الالتزامات والأحكام ..... ١٥

# قائمة الأشكال والرسوم التوضيحية

شكل ١: المراحل الرئيسيّة لمنهجية إدارة مخاطر الأمن السيبراني ..... ٩
شكل ٢: مصفوفة تقييم مخاطر الأمن السيبراني ..... ١٢
شكل ٣: مستويات مخاطر الأمن السيبراني ..... ١٢
شكل ٤: وصف مستويات الأثر ..... ١٣
شكل ٥: وصف مستويات الاحتمالية ..... ١٤

# قائمة الجداول

جدول ١: قائمة التعريفات ..... ٥

# ١. المقدمة

تُعد الهيئة الوطنية للأمن السيبراني؛ بموجب تنظيمها الصادر بالأمر الملكي الكريم ذي الرقم (٦٨٠١) في ١٤٣٩/٢/١١هـ الجهة المختصّة في المملكة بالأمن السيبراني؛ والمرجع الوطني في شؤونه. وتهدف إلى تعزيزه؛ حمايةً للمصالح الحيوية للدولة، وأمنها الوطني، والبنى التحتية الحساسة، والقطاعات ذات الأولوية، والخدمات، والأنشطة الحكومية. وتشمل اختصاصات الهيئة ومهماتها، دون حصر؛ وضع السياسات، وآليات الحوكمة، والأطر، والمعايير، والضوابط، والإرشادات المتعلقة بالأمن السيبراني، وتعميمها على الجهات ذات العلاقة، ومتابعة الالتزام بها، وتحديثها. بالإضافة إلى وضع أطر إدارة المخاطر المتعلقة بالأمن السيبراني، ومتابعة الالتزام بها، وتحديثها.

وعلى هذا، قامت الهيئة بإعداد هذا الإطار، الذي يعد مرجعًا ومنهجية، لإدارة مخاطر الأمن السيبراني في المملكة بإشراف الهيئة، إذ يوفر هذا الإطار رؤية واضحة لإدارة مخاطر الأمن السيبراني على مستوى الجهات، وعلى المستوى الوطني. كما يبين الإطار بشكل أساسي منهجية إدارة مخاطر الأمن السيبراني، بالإضافة إلى الأدوار والمسؤوليات، والإجراءات ذات العلاقة، التي تعزز قدرات إدارة مخاطر الأمن السيبراني في المملكة.

# ٢. التعريفات

يكون للمصطلحات المستخدمة في هذا الإطار المعاني المبينة أمام كل منها؛ ما لم يقتض السياق خلاف ذلك:

| المصطلح | التعريف |
|---|---|
| **الهيئة** | الهيئة الوطنية للأمن السيبراني. |
| **الإطار** | الإطار الوطني لإدارة مخاطر الأمن السيبراني، الصادر عن الهيئة. |
| **البنية التحتية الوطنية الحساسة** | تلك العناصر الأساسية للبنية التحتية (أي الأصول، والمرافق، والنظم، والشبكات، والعمليات، والعاملون الأساسيون الذين يقومون بتشغيلها ومعالجتها) والتي قد يؤدي فقدانها، أو تعرضها لانتهاكات أمنية إلى:<br>● أثر سلبي كبير على توافر الخدمات الأساسية أو تكاملها أو تسليمها -بما في ذلك الخدمات التي يمكن أن تؤدي في حال تعرضت سلامتها للخطر إلى خسائر كبيرة في الممتلكات و/أو الأرواح و/أو الإصابات- مع مراعاة الآثار الاقتصادية و/ أو الاجتماعية على المستوى الوطني.<br>● تأثير كبير على الأمن الوطني و/أو الدفاع الوطني و/أو اقتصاد الدولة أو مقدراتها الوطنية. |
| **الأمن السيبراني** | حماية الشبكات، وأنظمة تقنية المعلومات، وأنظمة التقنيات التشغيلية، ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات، وما تحويه من بيانات، من أي اختراق، أو تعطيل، أو تعديل، أو دخول، أو استخدام، أو استغلال غير مشروع. ويشمل مفهوم الأمن السيبراني أمن المعلومات، والأمن الإلكتروني، والأمن الرقمي، ونحو ذلك. |
| **مخاطر الأمن السيبراني** | المخاطر التي تمس أعمال الجهة (بما في ذلك رؤية الجهة أو رسالتها أو إداراتها أو صورتها أو سمعتها أو عملياتها) أو أصول الجهة، أو الأفراد، أو الجهات الأخرى، أو الدولة؛ بسبب إمكانية الاختراق، أو التعطيل، أو التعديل، أو الدخول، أو الاستخدام، أو الاستغلال، أو الإفصاح، أو التدمير غير المشروع للشبكات، وأنظمة تقنية المعلومات، وأنظمة التقنيات التشغيلية، ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات، وما تحويه من بيانات. |
| **ثغرات الأمن السيبراني** | نقاط الضعف، التي قد تكون في الأصول، أو الضوابط، أو الإجراءات التي تجعل الجهة، عرضة لمخاطر الأمن السيبراني. |
| **تهديدات الأمن السيبراني** | أي ظرف أو حدث يمكن أن يؤثر سلبًا على أعمال الجهة (بما في ذلك رؤية الجهة أو رسالتها أو إداراتها أو صورتها أو سمعتها أو عملياتها) أو أصول الجهة، أو الأفراد، أو الجهات الأخرى، أو الدولة؛ من خلال استغلال ثغرات الأمن السيبراني. |

| المصطلح | التعريف |
|---|---|
| **سيناريوهات مخاطر الأمن السيبراني** | سيناريوهات تفصيلية تمثل الأحداث، أو سلسلة الأحداث، التي قد تؤدي إلى تعرض أصول الجهة لتهديدات الأمن السيبراني، أو تتأثر بمثل هذه التهديدات. |
| **الضوابط** | إجراءات الحماية من تهديدات الأمن السيبراني، بما يتسق مع ضوابط الأمن السيبراني، الصادرة عن الهيئة. |
| **مخاطر الأمن السيبراني الكامنة** | مخاطر الأمن السيبراني، وفقًا لسيناريو مخاطر الأمن السيبراني، الذي جرى تحديده، قبل تنفيذ خطط التعامل مع المخاطر، وأي ضوابط مدرجة فيها. |
| **مخاطر الأمن السيبراني المتبقية** | مخاطر الأمن السيبراني بعد الأخذ في الحسبان خطط التعامل مع تلك المخاطر، وأي ضوابط مدرجة فيها. |
| **الأصول** | الموارد الملموسة أو غير الملموسة. وتشمل الأصول أنواعًا مختلفة؛ مثل البيانات والمعلومات، والبنية التحتية التقنية، والبرمجيات، والتطبيقات، والأنظمة، والأجهزة التقنية، والشبكات، وقواعد البيانات، والخدمات، وحسابات التواصل الاجتماعي وغيرها. |
| **الأصول المواجهة للإنترنت** | الأصول التي لديها عناوين بروتوكولات الإنترنت (IP) مخصصة، قابلة للوصول، والتوجيه بشكل عام عبر شبكة الإنترنت. |
| **الاحتمالية** | احتمالية وقوع تهديد الأمن السيبراني، خلال فترة زمنية محددة. ويمكن التعبير عنها بطريقة كمية، أو نوعية. |
| **الأثر** | العواقب والتبعات، الناتجة عن وقوع تهديد الأمن السيبراني. ويمكن التعبير عنه بطريقة كمية، أو نوعية. |
| **المستوى المقبول من المخاطر** | المستوى الذي يمكن تحمل أثره، من قبل صاحب الصلاحية. |
| **حصين** | منظومة وطنية سيبرانية شاملة، تقدم الهيئة من خلالها؛ خدمات ومنتجات سيبرانية مركزية ولامركزية، على المستوى الوطني للجهات المستفيدة (وهي الجهات الحكومية، وجهات البنية التحتية الوطنية الحساسة، والجهات الخاصة) بما يتوافق مع مهام الهيئة واختصاصاتها، ومتطلباتها التنظيمية السيبرانية الوطنية. |

**جدول ١: قائمة التعريفات**

## ٣. أهداف الإطار

يهدف هذا الإطار إلى العمل على إدارة مخاطر الأمن السيبراني بفاعلية، ويشكل بهذا حجر الأساس لمنظومة موحدة، متكاملة، شاملة ومتوائمة؛ قادرة على تحديد مخاطر الأمن السيبراني، وتحليلها، والتعامل معها، ومتابعتها. وتسهم العوامل الآتية في تحقيق هذا الهدف:

- تحديد مخاطر الأمن السيبراني، ذات الأولوية للتعامل معها.
- تعزيز صمود الأمن السيبراني الوطني؛ من خلال تطبيق الضوابط اللازمة، لتقليل مخاطر الأمن السيبراني.
- تحديد أدوار ومسؤوليات إدارة مخاطر الأمن السيبراني.
- تعزيز ثقافة إدارة مخاطر الأمن السيبراني؛ لدى الجهات.
- إدارة مخاطر الأمن السيبراني بشكل فعال؛ يمكّن الجهات من أداء أعمالها، وتحقيق أدوارها ومسؤولياتها في مختلف المجالات والقطاعات.

## ٤. نطاق تطبيق الإطار

ينطبق هذا الإطار على الجهات الحكومية في المملكة العربية السعودية (وتشمل الوزارات، والهيئات، والمؤسسات، وغيرها) والجهات والشركات التابعة لها (داخل المملكة وخارجها) وجهات القطاع الخاص التي تمتلك بنى تحتية وطنية حساسة (Critical National Infrastructure "CNI") أو تقوم بتشغيلها أو استضافتها، (ويشار لها جميعًا في هذه الوثيقة بـ"الجهة"). كما تُشجع الهيئة الجهات الأخرى في المملكة وبشدة على الاستفادة من هذا الإطار؛ لتطبيق أفضل الممارسات، فيما يتعلق بإدارة مخاطر الأمن السيبراني، وتعزيز الأمن السيبراني ورفعه على المستوى الوطني.

# ٥. المسؤوليات في إدارة مخاطر الأمن السيبراني على المستوى الوطني

يجب على كل جهة ضمن نطاق تطبيق هذا الإطار الالتزام بما يلي:

٥,١ تسمية ضابط اتصال مع الهيئة، معني بإدارة مخاطر الأمن السيبراني؛ للعمل على تفعيل هذا الإطار، ومتطلباته، والتزاماته الحالية، والمستقبلية.

٥,٢ حصر الأصول لدى الجهة مثل (الأنظمة الحساسة، والمرافق والأنظمة التشغيلية، وحسابات التواصل الاجتماعي، وغيرها) وتصنيفها، وفق ما يصدر عن الهيئة، ومن ثم مراجعة التصنيف بشكل دوري.

٥,٣ حصر أصول الجهة المواجهة للإنترنت.

٥,٤ الرفع للهيئة بالأصول التي جرى تحديدها في الفقرة ٥,٢ و٥,٣ بشكل دوري وفق الفترة المحددة لذلك، وتحديثها عند وجود أي تغيير، من خلال حصين أو أي قناة أخرى تحددها الهيئة.

٥,٥ الرفع للهيئة بمخاطر الأمن السيبراني، ذات المستوى الكارثي (٥) والمرتفع (٤) لدى الجهة، مباشرةً عند التعرف عليها؛ وفقًا لمصفوفة تقييم مخاطر الأمن السيبراني في الشكل (٢)، ومشاركة خطط التعامل مع مخاطر الأمن السيبراني بشكل دوري، وعند تحديثها، أو عند حدوث أي تغيير عليها، من خلال حصين، أو أي قناة أخرى تحددها الهيئة.

٥,٦ معالجة ما يرد من الهيئة من مخاطر وثغرات وملحوظات في الأمن السيبراني، والإفادة بما جرى حيالها، والإبلاغ عما جرى معالجته، بشكل دوري وفق الفترة المحددة لذلك، وتحديثها عند وجود أي تغيير، من خلال حصين، أو أي قناة أخرى، وفق ما يصدر عن الهيئة.

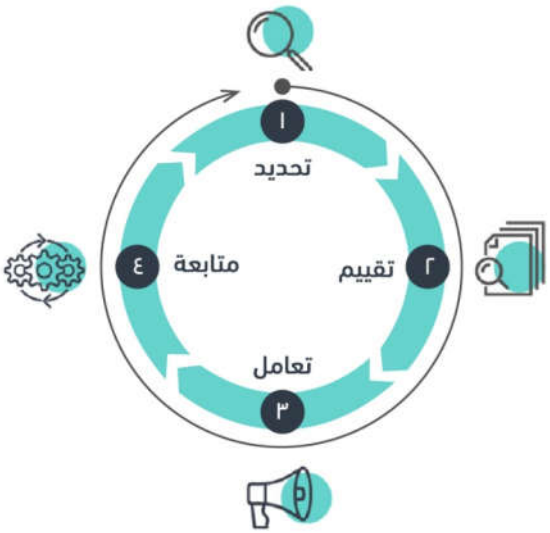
# ٦. المسؤوليات في إدارة مخاطر الأمن السيبراني على مستوى الجهة

يجب على كل جهة ضمن نطاق تطبيق هذا الإطار؛ الالتزام بمنهجية إدارة مخاطر الأمن السيبراني، ومصفوفة تقييم مخاطر الأمن السيبراني، على النحو المنصوص عليه في هذا القسم من الإطار.

## منهجية إدارة مخاطر الأمن السيبراني

تعمل منهجية إدارة مخاطر الأمن السيبراني على تحديد مخاطر الأمن السيبراني الكامنة، وتقييم الأثر، والاحتمالية، وتحديد خطط التعامل مع هذه المخاطر، بحيث يجري اتخاذ قرار التعامل وفقًا لذلك. ويجري استخدام الأصول، وثغرات الأمن السيبراني، وتهديدات الأمن السيبراني، والضوابط كمدخلات محتملة لفهم مخاطر الأمن السيبراني ضمن هذه المنهجية.

تشكل المراحل الموضحة في الشكل (١) الآتي، المراحل الرئيسية في منهجية إدارة مخاطر الأمن السيبراني. كما تشتمل كل مرحلة على عدة مهمات لتعزيز الرؤية والفهم والعمل، ضمن منهجية إدارة مخاطر الأمن السيبراني.




**شكل ١: المراحل الرئيسيّة لمنهجية إدارة مخاطر الأمن السيبراني**

ولكي يجري تطبيق هذه المنهجية بشكل مستدام؛ لا بد من القيام بما يلي:

٦,١ تطوير برنامج مستمر لتفعيل منهجية إدارة مخاطر الأمن السيبراني وتشغيله؛ مع تخصيص الموارد اللازمة.

٦,٢ إشراك أصحاب المصلحة، في المراحل المختلفة؛ مثل اللجنة الإشرافية للأمن السيبراني، وإدارة تقنية المعلومات.

## مرحلة التحديد

في هذه المرحلة، يجري حصر أصول الجهة، وتصنيفها، كما يجري تطوير سيناريوهات مخاطر الأمن السيبراني المتوقعة، وفقًا لتهديدات الأمن السيبراني المحتملة، وثغرات الأمن السيبراني؛ وذلك بهدف تحديد مخاطر الأمن السيبراني الكامنة. وتتكون هذه المرحلة من الخطوات الآتية:

٦,٣ حصر أصول الجهة وتصنيفها.

٦,٤ حصر ثغرات الأمن السيبراني.

٦,٥ حصر تهديدات الأمن السيبراني المحتملة.

٦,٦ تطوير سيناريوهات مخاطر الأمن السيبراني المتوقعة؛ وفقًا لتهديدات الأمن السيبراني المحتملة، وثغرات الأمن السيبراني.

٦,٧ تحديد الضوابط المطبقة حاليًا؛ لمعالجة سيناريوهات مخاطر الأمن السيبراني المتوقعة.

٦,٨ تحديد المستوى المقبول، من مخاطر الأمن السيبراني لدى الجهة.

## مرحلة التقييم

يجري في هذه المرحلة تقييم مخاطر الأمن السيبراني، حسب سيناريوهات مخاطر الأمن السيبراني المتوقعة؛ من خلال دراسة الاحتمالية والأثر. وتتكون هذه المرحلة من الخطوات الآتية:

٦,٩ إجراء تحليل للمخاطر الكامنة في الأمن السيبراني، لجميع سيناريوهات مخاطر الأمن السيبراني المتوقعة، والضوابط المطبقة حاليًا، وتقييم الاحتمالية والأثر؛ وفقًا لمصفوفة تقييم مخاطر الأمن السيبراني بالشكل (٢).

٦,١٠ توثيق نتائج التحليل، والتقييم في سجل مخاطر الأمن السيبراني.

## مرحلة التعامل

يجري في هذه المرحلة اتخاذ قرار التعامل مع مخاطر الأمن السيبراني، سواء أكان ذلك بقبول تلك المخاطر (Accepting) أم مشاركتها (Sharing) أم معالجتها (Mitigating) أم تجنب وقوعها (Avoiding)، ومن ثم تحديد خطط التعامل وتنفيذها. وتتكون هذه المرحلة من الخطوات الآتية:

٦,١١ تحديد خطط التعامل مع مخاطر الأمن السيبراني وتطويرها.

٦,١٢ تقييم مخاطر الأمن السيبراني المتبقية المتوقعة، بعد تنفيذ خطط التعامل مع المخاطر؛ للتأكد من الوصول للمستوى المقبول من المخاطر.

٦,١٣ اتخاذ قرار التعامل مع مخاطر الأمن السيبراني، وتحديد خطط التعامل المتعلقة بالقرار.

٦,١٤ وضع خطط التعامل حسب الأولوية.

٦,١٥ تنفيذ خطط التعامل.

٦,١٦ تحديث سجل مخاطر الأمن السيبراني؛ ليشمل خطط التعامل، ومخاطر الأمن السيبراني المتبقية.

## مرحلة المتابعة

يجري في هذه المرحلة متابعة أنشطة إدارة مخاطر الأمن السيبراني التي تقوم بها الجهة ومراقبتها، وتقييمها من خلال منهجية إدارة مخاطر الأمن السيبراني؛ لتحديث سجل مخاطر الأمن السيبراني دوريًا، أو بناءً على تغير الأصول، أو تهديدات الأمن السيبراني، أو الضوابط التي جرى تطبيقها. وتتكون هذه المرحلة من الخطوات الآتية:

٦,١٧ تطوير تقارير إدارة مخاطر الأمن السيبراني.

٦,١٨ وضع معايير لجمع البيانات الإحصائية، حول متابعة مخاطر الأمن السيبراني.

٦,١٩ متابعة تنفيذ خطط التعامل مع مخاطر الأمن السيبراني دوريًا وإصدار التقارير والبيانات، المتعلقة بذلك.

٦,٢٠ تنفيذ مراحل منهجية إدارة مخاطر الأمن السيبراني دوريًا، أو وفق ما يصدر عن الهيئة، أو عند وجود تحديث لحالة أيٍ من:

- خطط التعامل مع مخاطر الأمن السيبراني.
- تهديدات الأمن السيبراني المحتملة.
- سيناريوهات الأمن السيبراني المتوقعة.
- حالة تطبيق الضوابط.
- التغييرات في البنية التحتية الرقمية.

## مصفوفة تقييم مخاطر الأمن السيبراني

توفر مصفوفة تقييم مخاطر الأمن السيبراني منهجية؛ لتحديد مستويات مخاطر الأمن السيبراني. وتأخذ هذه المصفوفة في الحسبان، احتمالية حدوث سيناريوهات مخاطر الأمن السيبراني، وما قد ينتج عنها من أثر. ويبيّن الشكل (٢) مصفوفة تقييم مخاطر الأمن السيبراني.

**مستوى الخطر= الأثر X الاحتمالية**

| الاحتمالية | | | | | | |
|---|---|---|---|---|---|---|
| ٥ | شبه مؤكد | منخفض | متوسط | مرتفع | كارثي | كارثي |
| ٤ | مرجح | منخفض | متوسط | متوسط | مرتفع | كارثي |
| ٣ | غير مرجح | منخفض | منخفض | متوسط | متوسط | مرتفع |
| ٢ | نادر | منخفض جدًا | منخفض | منخفض | متوسط | متوسط |
| ١ | نادر جدًا | منخفض جدًا | منخفض جدًا | منخفض | منخفض | منخفض |
| | | منخفض جدًا | منخفض | متوسط | مرتفع | كارثي |
| | | ١ | ٢ | ٣ | ٤ | ٥ |

الأثـــر

**شكل ٢: مصفوفة تقييم مخاطر الأمن السيبراني**

يبيّن الشكل (٣) الآتي وصفًا لمستويات مخاطر الأمن السيبراني، إذ يجري تصنيف الخطر باستخدام المعادلة الآتية: (الأثر x الاحتمالية) من مصفوفة تقييم مخاطر الأمن السيبراني.

### مستوى الخطر

| منخفض جدًا | منخفض | متوسط | مرتفع | كارثي |
|---|---|---|---|---|
| ٢-١ | ٧-٣ | ١٤-٨ | ١٩-١٥ | ٢٥-٢٠ |

**شكل ٣: مستويات مخاطر الأمن السيبراني**

## وصف مستويات الأثر

يبيّن الشكل (٤) الآتي وصفًا لمستويات الأثر، إذ يجري تصنيف مستوى الأثر في حال الإخلال بواحد أو أكثر، من عناصر الأمن السيبراني (السرية، والسلامة، والتوافر):

| | (١) منخفض جدًا | (٢) منخفض | (٣) متوسط | (٤) مرتفع | (٥) كارثي |
|---|---|---|---|---|---|
| السريّة | إفصاح أو تسريب لبيانات أو لمعلومات غير حساسة، ويكون تأثير ذلك على الجهة معدومًا. | إفصاح أو تسريب لبيانات أو لمعلومات حساسة، ويكون تأثير ذلك على الجهة طفيفًا. | إفصاح أو تسريب لبيانات أو لمعلومات حساسة، ويكون تأثير ذلك على الجهة ملموسًا. | إفصاح أو تسريب لبيانات أو لمعلومات حساسة، ويكون تأثير ذلك على الجهة كبيرًا. | إفصاح أو تسريب لبيانات أو لمعلومات حساسة، ويكون تأثير ذلك على الجهة كبيرًا؛ لا يمكن تحمله، أو يكون له تأثيرًا على المستوى الوطني. |
| السلامة | تغيير غير مؤثر على أصول الجهة. | تغيير على أصول الجهة، ويكون تأثير ذلك على الجهة طفيفًا. | تغيير على أصول الجهة، ويكون تأثير ذلك على الجهة ملموسًا. | تغيير على أصول الجهة، ويكون تأثير ذلك على الجهة كبيرًا. | تغيير على أصول الجهة، ويكون تأثير ذلك على الجهة كبيرًا؛ لا يمكن تحمله، أو يكون له تأثيرًا على المستوى الوطني. |
| التوافر | توقف غير مؤثر لأصول الجهة. | توقف لأصول الجهة، ويكون تأثير ذلك على الجهة طفيفًا. | توقف لأصول الجهة، ويكون تأثير ذلك على الجهة ملموسًا. | توقف لأصول الجهة، ويكون تأثير ذلك على الجهة كبيرًا. | توقف لأصول الجهة، ويكون تأثير ذلك على الجهة كبيرًا؛ لا يمكن تحمله، أو يكون له تأثيرًا على المستوى الوطني. |

شكل ٤: وصف مستويات الأثر

## وصف مستويات الاحتمالية

يبيّن الشكل (٥) الآتي وصفًا لمستويات الاحتمالية، إذ يجري تصنيف مستوى الاحتمالية بناءً على الفترة الزمنية أو قدرة الاستغلال:

| التقييم | القيمة | الاحتمالية | |
|---|---|---|---|
| | | الفترة الزمنية | قدرة الاستغلال |
| شبه مؤكد | ٥ | من المتوقع تكرار حدوثه في معظم الحالات، ربما عدة مرات في الشهر، أو عدة مرات في السنة. | **أو** يمكن استغلال ثغرة الأمن السيبراني من قبل مهاجم، غير متمكن (على سبيل المثال، script-kiddie) باستخدام أكواد استغلال جاهزة. |
| مرجح | ٤ | من الشائع حدوثه في معظم الحالات بمعدل تكرار مرة واحدة كل سنة. | **أو** يمكن استغلال ثغرة الأمن السيبراني من قبل مهاجم متقدم؛ عبر هجوم متطور، باستخدام أدوات / طرق مخصصة. |
| غير مرجح | ٣ | قد يحدث ذلك في وقت ما، أو مرة كل سنتين إلى ٣ سنوات. | **أو** تعد ثغرة الأمن السيبراني قابلةً للاستغلال من قبل مهاجم متقدم؛ ولكن بشروط معينة فحسب. على سبيل المثال، تصميم دقيق لاستغلال الثغرة أو معرفة كبيرة للشبكة الداخلية. |
| نادر | ٢ | قد يحدث هذا في وقت ما تقريبًا كل ٣ إلى ١٠ سنوات. | **أو** لا يمكن استغلال ثغرة الأمن السيبراني بشكل مباشر، ولكن هناك إمكانية لاستغلالها في المستقبل. |
| نادر جدًا | ١ | تحدث فحسب في ظروف استثنائية، تقدر بأقل من مرة كل ١٠ سنوات إلى ٢٠ سنة. | **أو** لا تعد ثغرة الأمن السيبراني قابلة للاستغلال في الوقت الحاضر. |

شكل ٥: وصف مستويات الاحتمالية

# ٧. الالتزامات والأحكام

## الالتزامات العامة

يجب على جميع الجهات، ضمن نطاق تطبيق هذا الإطار؛ الالتزام بالإطار الوطني لإدارة مخاطر الأمن السيبراني، الصادر عن الهيئة. وكذلك الالتزام بجميع المتطلبات التنظيمية، الصادرة عن الهيئة، والسياسات، والأطر، والضوابط، والمبادئ التوجيهية، والمعايير؛ ذات الصلة.

## أحكام عامة

يجوز للهيئة مراجعة هذا الإطار وتحديثه، وفقًا لمتطلبات إدارة مخاطر الأمن السيبراني؛ وعلى هذا يجب التقيد بأي تحديثات، وفقًا لما تقره الهيئة.


الهيئة الوطنية
للأمن السيبراني
National Cybersecurity Authority