مشروع الإطار الوطني لإدارة مخاطر الأمن السيبراني

National Framework for Cybersecurity Risk Management

(NFCRM – 1:2024)

إشارة المشاركة: أبيض
تصنيف الوثيقة: عام

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 – 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.

- **أبيض – غير محدود**

قائمة المحتويات

الصفحة

قائمة الجداول

قائمة الأشكال والرسوم التوضيحية

١. المقدمة

تُعد الهيئة الوطنية للأمن السيبراني؛ بموجب تنظيمها الصادر بالأمر الملكي الكريم رقم (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 الوطنية 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.

وعليه، قامت الهيئة بإعداد هذا الإطار، الذي يعد مرجعًا ومنهجية لإدارة مخاطر الأمن السيبراني في المملكة بإشراف الهيئة، حيث يوفر هذا الإطار رؤية واضحة لإدارة مخاطر الأمن السيبراني على مستوى الجهات، وعلى المستوى الوطني. كما يوضح 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 المقابلة لها؛ ما لم يقتض السياق خلاف ذلك:

المصطلح	التعريف
الهيئة	الهيئة الوطنية للأمن السيبراني.
الإطار	هو الإطار الوطني لإدارة مخاطر الأمن السيبراني، الصادر عن الهيئة.
البنية التحتية الحساسة	هي 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: ١- 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 الكبيرة. ٢- 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 إداراتـها أو صورتها أو سمعتها) أو أصـولها أو الأفراد أو الجهات الأخرى أو الدولة، بسبب إمكانية حدوث أي اختراق أو تعطيل أو تعديل أو دخول أو استخدام أو استغلال غير مشروع لأصول الجهة.
سيناريوهات مخاطر الأمن السيبراني (Risk Scenarios)	تمثيلات مفصلة للأحداث أو السلسلة من الأحداث التي يمكن أن تؤدي إلى تعرض أصول الجهة للتهديدات السيبرانية والأثر المترتب على حدوث هذه التهديدات.
الضوابط	تدابير للحماية من التهديدات السيبرانية، تكون متوافقة مع ضوابط الأمن السيبراني الصادرة عن الهيئة.
مخاطر الامن السيبراني الكامنة (Inherent Risk)	هي مخاطر الأمن السيبراني وفقاً لسيناريوهات مخاطر الأمن السيبراني التي تم تحديدها قبل تنفيذ خطط الاستجابة للمخاطر وأي ضوابط مضمنه بها.
مخاطر الامن السيبراني المتبقية (Residual Risk)	هي ما تبقى من مخاطر الأمن السيبراني بعد الأخذ بالاعتبار خطط الاستجابة للمخاطر وأي ضوابط مضمنه بها.
الأصول	الموارد الملموسة أو غير الملموسة لدى الجهة. وتتضمن هذه الأصول أنواعاً مختلفة مثل البيانات والمعلومات، والتطبيقات، والأنظمة، والأجهزة التقنية، والشبكات، والبنى التحتية، وقواعد البيانات، والخدمات المُقدمة، وحسابات التواصل الاجتماعي وغيرها.
الأصول الحساسة	هي أصول الجهة التي تحقق معايير الحساسية الصادرة عن الهيئة الوطنية للأمن السيبراني، ومنها الأنظمة، والمرافق والأنظمة التشغيلية، وحسابات التواصل الاجتماعي.
التهديدات السيبرانية	أي ظرف أو حدث من المحتمل أن يؤثر سلباً على مهمة الجهة أو أصولها أو أعمالها أو وظائفها أو مصداقيتها أو سمعتها أو الافراد من خلال استغلال الثغرات السيبرانية.

المصطلح	التعريف
الثغرات السيبرانية	نقاط الضعف التي تكون في الأصول أو في الضوابط أو في الإجراءات والتي قد ينتج عن استغلالها وصول غير مصرح به للأصول يؤدي إلى الاطلاع أو الكشف أو الاختراق أو التعطيل أو التدمير أو التعديل أو الاستخدام غير المشروع.
الاحتمالية	احتمالية وقوع التهديد السيبراني خلال فترة زمنية محددة، ويمكن التعبير عنها بطريقة كمية أو نوعية.
الأثر	العواقب والتبعات الناتجة عن وقوع التهديد السيبراني
المستوى المقبول من المخاطر	المستوى الذي يمكن تحمل أثره من قبل صاحب الصلاحية

جدول 1 : تعريف المصطلحات

٣. أهداف الإطار

يشكل الإطار حجر الأساس لمنظومة موحدة، متكاملة، شاملة ومتوائمة، قادرة على إدارة مخاطر الأمن السيبراني بفاعلية، بما يشمل تحديدها، وتقييمها، والاستجابة لها ومتابعتها. وتساهم العوامل التالية في تحقيق هذا الهدف:

- تحديد مخاطر الأمن السيبراني ذات الأولوية للاستجابة لها.
- تطبيق الضوابط اللازمة لتقليل مخاطر الأمن السيبراني للمساهمة في تعزيز صمود الأمن السيبراني الوطني.
- تحديد أدوار ومسؤوليات إدارة مخاطر الأمن السيبراني.
- تعزيز ثقافة الوعي لدى الجهات بإدارة مخاطر الأمن السيبراني.
- إدارة مخاطر الأمن السيبراني بشكل فعال يمكّن الجهات من أداء أعمالها وتحقيق أهدافها في مختلف المجالات والقطاعات.

٤. نطاق تطبيق الإطار

ينطبق هذا الإطار على:

١. الجهات الحكومية في المملكة العربية السعودية (وتشمل الوزارات، والهيئات، والمؤسسات، وغيرها) والجهات والشركات التابعة لها أو المرتبطة بها، سواء كانت تعمل داخل المملكة أم خارجها.
٢. جهات القطاع الخاص، التي تمتلك بنىً تحتية وطنية حساسة، أو تشغلها أو تستضيفها.
٣. مقدمي خدمات الأمن السيبراني في المملكة العربية السعودية.

كما تشجع الهيئة الجهات الأخرى (بما فيها جهات القطاع الخاص من غير ذات البنى التحتية الحساسة، والجهات غير الربحية) في المملكة على الاستفادة من أحكام هذا الإطار؛ لتطبيق أفضل الممارسات فيما يتعلق بإدارة مخاطر الأمن السيبراني وتعزيز ورفع مستوى الأمن السيبراني لديها.

٥. المسؤوليات في إدارة مخاطر الأمن السيبراني على المستوى الوطني

يجب على الجهات التي تدخل ضمن نطاق تطبيق هذا الإطار، الالتزام بما يلي:

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

٥,٢ تحديد وتصنيف الأصول الحساسة لدى الجهة، وفق ما يصدر من الهيئة، والتي تشمل على سبيل المثال: الأنظمة، والمرافق والأنظمة التشغيلية، وحسابات التواصل الاجتماعي.

٥,٣ تحديد أصول الجهة المنكشفة على الانترنت.

٥,٤ الرفع للهيئة بالأصول التي تم تحديدها في الفقرتين ٥,٢ و٥,٣ بشكل دوري وتحديثها عند وجود أي تغيير، من خلال البوابة الوطنية لخدمات الأمن السيبراني (حصين)، أو أي وسيلة أخرى تحددها الهيئة وخلال المدة المقررة لذلك.

٥,٥ الرفع للهيئة بمخاطر الأمن السيبراني ذات المستوى الكارثي (٥) والمرتفع (٤) لدى الجهة حال التعرف عليها وفقًا لمصفوفة تقييم مخاطر الأمن السيبراني الواردة في قسم ٦ من هذا الإطار، ومشاركة خطط الاستجابة لها بشكل دوري وعند تحديثها أو عند وجود أي تغيير، من خلال البوابة الوطنية لخدمات الأمن السيبراني (حصين)، أو أي وسيلة أخرى تحددها الهيئة وخلال المدة المقررة لذلك.

٥,٦ معالجة ما يرد من الهيئة من مخاطر وثغرات وملاحظات تخص الأمن السيبراني والإفادة بما تم حيالها، وفق ما يصدر عن الهيئة.

٦. المسؤوليات في إدارة مخاطر الأمن السيبراني على مستوى الجهة

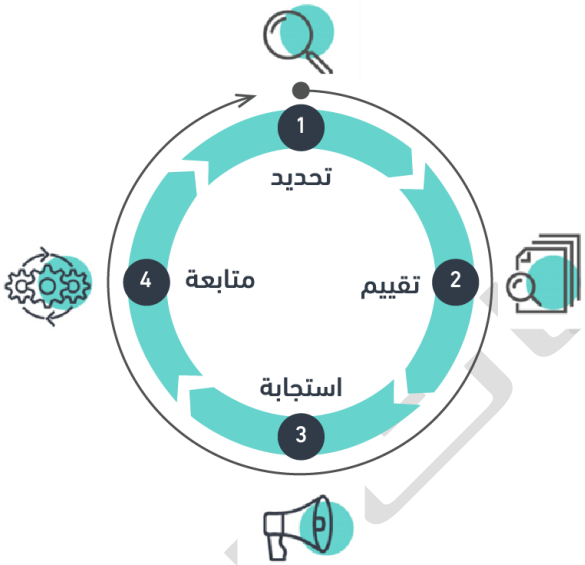
يجب على الجهات ضمن نطاق تطبيق هذا الإطار الالتزام بمنهجية إدارة مخاطر الأمن السيبراني، ومصفوفة تقييم مخاطر الأمن السيبراني، حسب ما ورد في هذا القسم.

منهجية إدارة مخاطر الأمن السيبراني

يتم استخدام العناصر التالية لإدارة مخاطر الأمن السيبراني بشكل فعال: الأصول، الثغرات والتهديدات، والضوابط، كمدخلات محتملة لفهم الرؤية الكاملة لمخاطر الأمن السيبراني. حيث تحدد منهجية إدارة مخاطر الأمن السيبراني،

المخاطر الكامنة قبل تنفيذ أي ضوابط للوقاية والتخفيف، وتقييم أثر تلك المخاطر واحتمالية حدوثها، كما تحدد المنهجية خطط الاستجابة لتلك المخاطر، بحيث يتم اتخاذ قرار الاستجابة.

تشكل المراحل الموضحة في الشكل (١) أدناه المراحل الرئيسية في منهجية إدارة مخاطر الأمن السيبراني. حيث تحتوي كل مرحلة على العديد من المهام لتعزيز الرؤية والفهم والعمل في منهجية إدارة مخاطر الأمن السيبراني.



شكل :1 المراحل الرئيسيّة لمنهجية إدارة مخاطر الأمن السيبراني

لكي يتم تطبيق هذه المنهجية بصورة مستدامة؛ يجب العمل على ما يلي:

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

٦,٢ إشراك أصحاب المصلحة، خلال المراحل المختلفة؛ مثل اللجنة التوجيهية للأمن السيبراني وتقنية المعلومات.

مرحلة التحديد

يتم في هذه المرحلة تحديد وجمع أصول الجهة، وتطوير السيناريوهات المتوقعة للمخاطر السيبرانية، وفقًا للتهديدات والثغرات والهجمات المحتملة؛ وذلك بهدف تحديد مخاطر الأمن السيبراني الكامنة. وتتكون هذه المرحلة من عدد من الخطوات، وهي:

٦,٣ تحديد وحصر أصول الجهة.

٦,٤ تحديد وحصر الثغرات السيبرانية.

٦,٥ تحديد وحصر التهديدات السيبرانية المحتملة.

٦,٦ تطوير السيناريوهات المتوقعة للمخاطر السيبرانية، وفقًا للثغرات والتهديدات المحتملة.

٦,٧ تحديد الضوابط حاليًا لمواجهة السيناريوهات المتوقعة للمخاطر السيبرانية.

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

مرحلة التقييم

يتم في هذه المرحلة تقييم مخاطر الأمن السيبراني حسب السيناريوهات المتوقعة، من خلال دراسة احتمال وقوع هذه السيناريوهات، وتأثيراتها المحتملة. وتتكون هذه المرحلة من عدد من الخطوات، وهي:

٦,٩ إجراء تحليل لمخاطر الأمن السيبراني الكامنة، لجميع السيناريوهات المتوقعة والضوابط المطبقة حالياً، وتقييم احتمالية الحدوث والأثر وفقًا لمصفوفة تقييم مخاطر الأمن السيبراني (حسب ما ورد في البند ٦,٢ من هذا الإطار).

٦,١٠ توثيق نتائج التحليل والتقييم في سجل المخاطر.

مرحلة الاستجابة

يتم في هذه المرحلة اتخاذ قرار الاستجابة للتعامل مع مخاطر الأمن السيبراني سواءً بقبول تلك المخاطر (Accepting) أو مشاركتها (Sharing) أو معالجتها (Mitigating) أو تجنب وقوعها (Avoiding)، وتحديد وتنفيذ خطط الاستجابة. وتتكون هذه المرحلة من عدد من الخطوات، وهي:

٦,١١ تحديد وتطوير خطط الاستجابة.

٦,١٢ تقييم مخاطر الأمن السيبراني المتبقية المتوقعة بعد تنفيذ خطط الاستجابة للمخاطر للتأكد من الوصول للمستوى المقبول من المخاطر.

٦,١٣ اتخاذ قرار الاستجابة، وتحديد خطط الاستجابة المتعلقة بالقرار.

٦,١٤ ترتيب خطط الاستجابة حسب الأولوية.

٦,١٥ تنفيذ خطط الاستجابة.

٦,١٦ تحديث سجل المخاطر ليشمل خطط الاستجابة ومخاطر الأمن السيبراني المتبقية.

مرحلة المتابعة

يتم في هذه المرحلة متابعة ومراقبة أنشطة إدارة مخاطر الأمن السيبراني التي تقوم بها الجهة من خلال منهجية إدارة مخاطر الأمن السيبراني، وتقييمها، لتحديث سجل المخاطر دورياً أو بناء على تغير الأصول أو التهديدات، أو الضوابط التي تم تطبيقها. وتتكون هذه المرحلة من عدد من الخطوات، وهي:

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 الاستجابة لمخاطر الأمن السيبراني دورياً وإصدار التقارير والبيانات المتعلقة بذلك.

٦,٢٠ تنفيذ مراحل منهجية إدارة مخاطر الأمن السيبراني دورياً أو عند وجود تحديث على حالة خطط الاستجابة أو التهديدات المحتملة أو السيناريوهات المتوقعة أو الضوابط المطبقة.

مصفوفة تقييم مخاطر الأمن السيبراني

توفر مصفوفة تقييم مخاطر الأمن السيبراني منهجية لتحديد مستويات مخاطر الأمن السيبراني، وتأخذ هذه المصفوفة بالاعتبار احتمالية حدوث سيناريوهات مخاطر الأمن السيبراني، والأثر الناتج عنه. ويبيّن الشكل (٢) مصفوفة تقييم مخاطر الأمن السيبراني.

مستوى الخطر= الأثر X احتمالية الحدوث

احتمالية الحدوث						
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 جداً	منخفض	منخفض	متوسط	متوسط
١	نادر جداً	منخفض جداً	منخفض جداً	منخفض	منخفض	منخفض
		منخفض جداً	منخفض	متوسط	مرتفع	كارثي
		١	٢	٣	٤	٥
		الأثـر				

شكل ٢: مصفوفة تقييم مخاطر الأمن السيبراني

يبيّن الشكل (٣) أدناه وصف لمستويات مخاطر الأمن السيبراني، حيث يحتسب التصنيف العام للخطر (الأثر x احتمالية الحدوث) من مصفوفة تقييم مخاطر الأمن السيبراني.

مستويات المخاطر

منخفض جداً	منخفض	متوسط	مرتفع	كارثي
١-٣	٤-٨	٩-١٤	١٥-١٩	٢٠-٢٥

شكل3 : مستويات مخاطر الأمن السيبراني

وصف مستويات الأثر

يتم قياس تأثير الخطر، في حال تحقق الوصف لعنصر أو أكثر من عناصر الأمن السيبراني (السرية، والسلامة، والتوافر) وفقا لمستوى الأثر المبين في الجدول التالي:

	(١) منخفض جداً	(٢) منخفض	(٣) متوسط	(٤) مرتفع	(٥) كارثي
السرية	إفصاح أو تسريب لبيانات أو لمعلومات غير حساسة، ويكون تأثير ذلك على الجهة معدوماً	إفصاح أو تسريب لبيانات أو لمعلومات حساسة، ويكون تأثير ذلك على الجهة طفيفاً	إفصاح أو تسريب لبيانات أو لمعلومات حساسة، ويكون تأثير ذلك على الجهة ملموساً	إفصاح أو تسريب لبيانات أو لمعلومات حساسة، ويكون تأثير ذلك على الجهة كبيراً	إفصاح أو تسريب لبيانات أو لمعلومات حساسة، ويكون تأثير ذلك على الجهة كبيراً لا يمكن تحمله أو يكون له تأثير على المستوى الوطني
السلامة	تغيير غير مؤثر على أصول الجهة	تغيير محدود على أصول الجهة، ويكون تأثير ذلك على الجهة طفيفاً	تغيير على أصول الجهة، ويكون تأثير ذلك على الجهة ملموساً	تغيير على أصول الجهة، ويكون تأثير ذلك على الجهة كبيراً	تغيير على أصول الجهة، ويكون تأثير ذلك على الجهة كبيراً لا يمكن تحمله أو يكون له تأثير على المستوى الوطني
التوافر	توقف غير مؤثر لأصول الجهة	توقف محدود لأصول الجهة، ويكون تأثير ذلك على الجهة طفيفاً	توقف لأصول الجهة، ويكون تأثير ذلك على الجهة ملموساً	توقف لأصول الجهة، ويكون تأثير ذلك على الجهة كبيراً	توقف لأصول الجهة، ويكون تأثير ذلك على الجهة كبيراً لا يمكن تحمله أو يكون له تأثير على المستوى الوطني

جدول2 : وصف مستويات الأثر

وصف مستويات احتمالية الحدوث

يتم قياس الاحتمالية على النحو التالي:

التقييم	القيمة	احتمالية الحدوث	
		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 الثغرة الأمنية 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 في كل سنة	أو يمكن استغلال الثغرة الأمنية من قبل مهاجم متقدم عبر هجوم متطور باستخدام أدوات / طرق مخصصة. علاوة على ذلك، يجب تحديد المهاجم بشكل كبير.
غير مرجح	٣	قد يحدث في وقت ما أو مرة واحدة كل ٢-٣ سنوات	أو تعتبر الثغرة قابله للاستغلال من قبل مهاجم متقدم، ولكن بشروط معينة فقط. مثال: تصميم دقيق لاستغلال الثغرة أو معرفة كبيرة للشبكة الداخلية.

نادر	٢	يمكن أن يحدث في وقت ما تقديراً مرة واحدة كل ٣-١٠ سنوات	أو لا يمكن استغلال الضعف بشكل مباشر، ولكن هناك إمكانية لاستغلاله في المستقبل.
نادر جدا	١	تحدث فقط في ظروف استثنائية تقدر بأقل من مرة كل ١٠-٢٠ سنة	أو لا تعتبر الثغرة قابلة للاستغلال في الوقت الحاضر

جدول ٣: وصف مستويات احتمالية الحدوث

٧. الالتزامات والأحكام

٧,١ الالتزامات العامة

يجب على جميع الجهات التي تدخل ضمن نطاق تطبيق هذا الإطار، الالتزام بأحكام هذا الإطار، وجميع المتطلبات التنظيمية وكافة ما تضعه أو تقره الهيئة من سياسات أو أطر أو ضوابط أو إرشادات أو معايير وذات الصلة. وفق اختصاصها النظامي، وبوصفها المرجع الوطني في كل ما يتعلق بالأمن السيبراني في المملكة

٧,٢ أحكام عامة

يجوز للهيئة مراجعة هذا الإطار وتحديثه وفقًا لمتطلبات تنظيم قطاع الأمن السيبراني، ويجب التقيد بأي تحديثات وفقًا لما تحدده الهيئة.


الهيئة الوطنية
للأمن السيبراني
National Cybersecurity Authority