الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

مشروع الإطار الوطني لمشاركة المعلومات والاستجابة للحوادث المتعلقة بالأمن السيبراني

National Framework for Cybersecurity Information Sharing and Incidents Response

(NFCISIR – 1:2026)

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

قائمة الأشكال والرسوم التوضيحية

قائمة الجداول

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 الاستجابة للحوادث المتعلقة بالأمن السيبراني، ومتابعة الالتزام بها، وتحديثها؛ وكذلك إشعار الجهات المعنية بالمخاطر والتهديدات ذات العلاقة بالأمن السيبراني. وقد ألزم التنظيم جميع الجهات ذات العلاقة بإبلاغ الهيئة - بشكل فوري - بأي خطر، أو تهديد، أو اختراق لأمنها السيبراني واقع أو محتمل.

وانطلاقًا من هذه المهمات؛ أصدرت الهيئة هذا الإطار الوطني لمشاركة المعلومات، والاستجابة للحوادث المتعلقة بالأمن السيبراني.

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.
الجهة/ الجهات	تشير إلى أي جهة عامة (وتشمل الوزارات والهيئات والمؤسسات، وما يتبع لها من جهات خارج المملكة)، وكذلك الجهات والشركات التابعة لها، وجهات القطاع الخاص، التي تمتلك بنى تحتية وطنية حساسة، أو تقوم بتشغيلها، أو استضافتها، وغيرها من الجهات في القطاع الخاص، والجهات غير الربحية، والجهات العاملة في المملكة.
الإطار	الإطار الوطني لمشاركة المعلومات والاستجابة للحوادث المتعلقة بالأمن 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) التي قد يؤدي فقدانها، أو تعرضها لانتهاكات أمنية إلى: ● أثر سلبي كبير على توافر الخدمات الأساسية، أو تكاملها، أو تسليمها- بما في ذلك التأثير على الخدمات، التي يمكن أن تؤدي عند تعرض سلامتها للخطر إلى خسائر كبيرة في الممتلكات و/ أو الأرواح و/ أو الإصابات- مع مراعاة الآثار الاقتصادية و/ أو الاجتماعية على المستوى الوطني. ● 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.
حدث	حدث ذو علاقة بحالة الأمن السيبراني الخاصة بشبكة، أو نظام، أو خدمة، أو بيانات، أو أي جهاز تقني آخر.
ثغرات الأمن السيبراني	ضعف في الشبكات أو أنظمة تقنية المعلومات، أو أنظمة التقنيات التشغيلية ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات، قد يؤدي إلى اختراق، أو تعطيل، أو تعديل، أو دخول، أو استخدام، أو استغلال غير مشروع.
تهديدات الأمن السيبراني	أي ظرف، أو حدث يمكن أن يؤثر سلبًا على الشبكات أو أنظمة تقنية المعلومات، أو أنظمة التقنيات التشغيلية ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات، وما تحويه من بيانات؛ سواء أكان ذلك التأثير باختراق، أو تعطيل، أو تعديل، أو دخول، أو استخدام، أو استغلال غير مشروع.
حادثة أمن سيبراني	الحدث الذي وقع على الشبكات أو أنظمة تقنية المعلومات، أو أنظمة التقنيات التشغيلية ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات، وما تحويه من بيانات، سواءً أكان ذلك الحدث اختراقًا أم تعطيلًا، أو تعديلًا، أو دخولًا، أو استخدامًا، أو استغلالًا غير مشروع.

المصطلح	التعريف
عمليات الأمن السيبراني	الأعمال والأنشطة ذات الصلة بالثغرات، والتهديدات والحوادث المتعلقة بالأمن السيبراني؛ وتشمل أعمال الرصد، والتحليل، والجمع، ومشاركة المعلومات، والاستجابة، والمعالجة وما يرتبط بتلك الأعمال من أنشطة، وإجراءات، وتدابير وغيرها.
مشاركة المعلومات المتعلقة بالأمن السيبراني	تبادل المعلومات والبيانات، المتعلقة بالأمن السيبراني، بين الهيئة والجهة، بما في ذلك مشاركة المعلومات المتعلقة بعمليات الأمن السيبراني، وذلك بما يسهم في تعزيز الأمن السيبراني بالجهات. ويشمل ذلك المعلومات التي ترسلها الهيئة للجهات، وكذلك ما تقوم الجهات بإبلاغ الهيئة به. ويجري مشاركة المعلومات باستخدام عدد من النماذج، وفق ما يرد في هذا الإطار؛ ومن ذلك التنبيه الأمني من الهيئة إلى الجهة.
تنبيه أمني	أحد النماذج التي يجري من خلالها مشاركة المعلومات من الهيئة إلى الجهات الوطنية، وذلك للمعلومات المتعلقة بعمليات الأمن السيبراني. ويمكن أن يجري إرسال التنبيه بشكل إلكتروني من خلال (حصين)، أو البريد الإلكتروني، وغير ذلك؛ أو بشكل غير إلكتروني، وذلك حسب ما تقتضيه الحاجة.
مركز عمليات الأمن السيبراني	مركز يقدم خدمات العمليات، المتعلقة بمراقبة أحداث الأمن السيبراني في المنظومة التقنية للجهة؛ وتؤدي إلى اكتشاف التهديدات السيبرانية، ومعرفة كيفية حدوثها، وتقديم الإجراءات والتدابير في كيفية معالجتها، واتخاذ الإجراءات اللازمة لاحتوائها.
خدمات مركز عمليات الأمن السيبراني المُدَار	الخدمات التي تحصل عليها الجهة المستفيدة، من مقدم خدمات مركز عمليات الأمن السيبراني المُدَار؛ بهدف مراقبة أحداث الأمن السيبراني، في المنظومة التقنية لديها؛ لاكتشاف التهديدات السيبرانية، ومعرفة كيفية حدوثها، وتقديم الإجراءات والتدابير في كيفية معالجتها، ليتم تطبيقها من قبل الجهة المستفيدة. وتشمل هذه الخدمات؛ العمليات، وفرق العمل، والأنظمة ذات الصلة، وغيرها.
مقدم خدمات مركز عمليات الأمن السيبراني المدار	الجهة المرخصة من الهيئة، لتقديم خدمات مركز عمليات الأمن السيبراني المُدار في المملكة؛ وفقًا للإطار التنظيمي لترخيص تقديم خدمات مركز عمليات الأمن السيبراني المُدَار.
مقدم خدمات الاستجابة لحوادث الأمن السيبراني	الجهة المرخصة من الهيئة لتقديم خدمات الاستجابة لحادثة الأمن السيبراني والتعامل معها لدى الجهات، وتقديم الإجراءات والتدابير المتعلقة باحتواء الحادثة والتعافي منها.
مقدم خدمات الحوسبة السحابية	أي شخص طبيعي، أو معنوي (مثل الشركات) مرخص من الجهة المختصة في المملكة بتقديم خدمات الحوسبة السحابية، سواء أكان ذلك بشكل مباشر، أو غير مباشر؛ من خلال مراكز بيانات (سواء أكانت داخل المملكة أو خارجها) ويديرها بنفسه بشكل كلي أو جزئي.
حصين (البوابة الوطنية لخدمات الأمن السيبراني)	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 مهمات الهيئة واختصاصاتها، ومتطلباتها التنظيمية السيبرانية الوطنية.

جدول ١: قائمة التعريفات

٣. أهداف الإطار

يهدف الإطار الوطني لمشاركة المعلومات، والاستجابة للحوادث المتعلقة بالأمن السيبراني؛ إلى تحديد المتطلبات التنظيمية الوطنية، التي تنظم آليات مشاركة المعلومات، وكذلك بيان آلية التعامل مع الحوادث السيبرانية. وسوف يعنى هذا الإطار في المرحلة الحالية على جوانب تنظيم وحوكمة مشاركة معلومات عمليات الأمن السيبراني، كما سيتناول آلية التعامل مع الحوادث السيبرانية في جميع مراحلها، وذلك بما يسهم في تحقيق الأهداف الآتية:

- تعزيز الأمن السيبراني للجهات؛ وذلك من خلال رفع مستوى المعرفة الشاملة، بالتهديدات التي تواجه الجهات، والقطاعات الوطنية المختلفة، وتعزيز الدراية الأمنية السيبرانية بشأنها.
- تحديد المهمات والمسؤوليات المتعلقة بحوادث الأمن السيبراني، ومشاركة معلومات عمليات الأمن السيبراني، على المستوى الوطني.
- تحديد الالتزامات المترتبة على الجهات، عند وقوع حوادث الأمن السيبراني، أو عند مشاركة معلومات عمليات الأمن السيبراني، وما يتعلق بذلك من إجراءات، وتدابير، ومدد زمنية، وكذلك قنوات الإبلاغ والتصعيد.
- زيادة حصيلة المعلومات الاستباقية للتهديدات، وحوادث الأمن السيبراني، لدى الجهات في المملكة، ورفع مستوى موثوقيتها.
- رفع مستوى الجاهزية السيبرانية للجهات؛ استعدادًا للتعامل مع هجمات الأمن السيبراني، بشكل استباقي.

٤. نطاق تطبيق الإطار

ينطبق هذا الإطار على جميع الجهات في المملكة؛ ويشمل ذلك الجهات العامة والخاصة، ومقدمي خدمات مركز عمليات الأمن السيبراني المدار، ومقدمي خدمات الاستجابة لحوادث الأمن السيبراني، ومقدمي خدمات الأمن السيبراني ومنتجاته وحلوله، ومقدمو خدمات تقنية المعلومات والتقنيات التشغيلية، وغيرهم من الجهات الخاصة.

٥. التنفيذ والالتزام

وفق ما قررته الفقرة (٣) من (المادة العاشرة) من تنظيم الهيئة الوطنية للأمن السيبراني المشار إليه آنفاً؛ فإنه يجب على جميع الجهات الواقعة ضمن نطاق تطبيق الإطار؛ تنفيذ هذا الإطار، وضمان تحقيق الالتزام الكامل، والمستمر بالأحكام الواردة فيه .

وستقوم الهيئة -بحسب الاقتضاء- بمتابعة التزام الجهات، بما ورد في هذا الإطار، وفق الآلية التي تراها الهيئة مناسبة. كما تتولى الهيئة ضبط مخالفات الأمن السيبراني، والتحقيق فيها، والرقابة والتفتيش على الأماكن والأنشطة ذات الصلة بالأمن السيبراني، واتخاذ الإجراءات النظامية اللازمة، وفق الممكنات النظامية للهيئة الوطنية للأمن السيبراني الصادرة بالمرسوم الملكي رقم (م/١١٧) بتاريخ ١٤٤٦/٦/٢١ هـ.

٦. أحكام مشاركة معلومات عمليات الأمن السيبراني

٦,١ الأحكام الرئيسة المتعلقة بمشاركة معلومات عمليات الأمن السيبراني للجهات

٦,١,١ تجري مشاركة معلومات عمليات الأمن السيبراني، بين الهيئة والجهات، من خلال حصين (البوابة الوطنية لخدمات الأمن السيبراني) أو من خلال أي قناة أخرى تقرها الهيئة.

٦,١,٢ يجب على الجهة إبلاغ الهيئة بشكل فوري ومباشر؛ بأي تهديد، أو اختراق للأمن السيبراني للجهة؛ واقع أو محتمل، والاستمرار بالجمع والرصد، لأي حدث ذي ارتباط بعمليات الأمن السيبراني.

٦,١,٣ يجب على الجهة تنفيذ ما يصدر عن الهيئة من قرارات، ذات صلة، بمشاركة معلومات عمليات الأمن السيبراني؛ بما في ذلك تنفيذ الإجراءات، والتدابير الواردة في التنبيهات الأمنية، وذلك خلال المدة الزمنية التي تحددها الهيئة، وفقًا للآلية والقنوات المعتمدة لمشاركة المعلومات.

٦,١,٤ يجب على الجهة تزويد الهيئة بما تطلبه من أدلة رقمية، أو وثائق، أو بيانات، أو معلومات، أو تقارير وغيرها؛ وذلك عند قيامها بمشاركة معلومات متعلقة بعمليات الأمن السيبراني، ويكون ذلك خلال المدة الزمنية التي تقرها الهيئة وفقًا للآلية والقنوات المعتمدة لمشاركة المعلومات. ويبين الملحق (ج) المدد الزمنية التي سوف تعمل بها الهيئة، في هذا الشأن؛ مالم يستدعي الموقف خلاف ذلك.

٦,١,٥ يجب على الجهة، بذل العناية اللازمة؛ لضمان تحقيق أعلى درجات الدقة والجودة، عند تنفيذ الإجراءات، والتدابير الواردة في النماذج التي يجري من خلالها مشاركة المعلومات، وعند مشاركة المعلومات مع الهيئة؛ وذلك بسبب التبعات ذات الصلة بتعزيز الأمن السيبراني، على المستوى الوطني، التي يجري اتخاذها من قبل الهيئة، بناء على إفادة الجهة. وسوف تتحمل الجهة الإجراءات، التي ستتخذها الهيئة، بشأن أي تقصير في هذا الشأن.

٦,١,٦ عندما تتوفر لدى الجهة معلومات استباقية تخص تهديداً، أو ثغرة، أو حادثة أمن السيبراني على جهة وطنية أخرى؛ فإنه يجب على الجهة مشاركة تلك المعلومات، مع الهيئة بشكل فوري.

٦,١,٧ لا يحق للجهة مشاركة، معلومات عمليات الأمن السيبراني، مع أي طرف أو جهة؛ إلا بعد أخذ الموافقات الخطية اللازمة من الهيئة، أو أن تكون تلك المعلومات منصوصًا على مشاركتها، في أي من الأطر، أو التنظيمات الصادرة عن الهيئة؛ أو أن تكون جزءً من نطاق تعاقد، بين الجهة المستفيدة، ومقدمي الخدمات المرخصين من الهيئة.

٦,١,٨ تعد الجهة مسؤولة مسؤولية تامة أمام الهيئة عن جميع المهمات المتعلقة بعمليات الأمن السيبراني، المقدمة من أطراف خارجية؛ بما في ذلك، مقدم خدمات مركز عمليات الأمن السيبراني المدار، ومقدم خدمات الحوسبة السحابية مع التأكد من تنفيذ أي إجراءات وتدابير، ذات الصلة؛ من شأنها تعزيز الأمن السيبراني في الجهة.

٦,١,٩ عند قيام الجهة بالاستعانة بمقدمي خدمات الحوسبة السحابية؛ فإنه يتوجب على الجهة، تولي مسؤولية التنفيذ التام، لأي إجراءات، وتدابير مطلوبة من الهيئة؛ ذات صلة بعمليات الأمن السيبراني. ويشمل ذلك توفير أي وثائق، أو معلومات، أو بيانات، أو تقارير، ذات صلة بعمليات الأمن السيبراني، لدى مقدمي تلك الخدمات.

٦,١,١٠ في حال قامت الجهة بإلغاء الاشتراك أو عدم التجديد مع مقدم خدمات مركز عمليات الأمن السيبراني المدار، أو مع مقدم خدمات الحوسبة السحابية؛ فيتوجب على الجهة التأكد من نقل جميع السجلات المتعلقة بالأمن السيبراني إلى مقدم الخدمة الجديد.

٦,١,١١ يجب على الجهة، القيام بالتحقق من تصنيف معلومات عمليات الأمن السيبراني، التي يجري مشاركتها مع الهيئة؛ وفق المتطلبات التنظيمية الصادرة من الجهات ذات الاختصاص.

٦,١,١٢ يجب على الجهة تحديد إشارة المشاركة؛ وفق بروتوكول الإشارة الضوئية (TLP) لضبط نطاق مشاركة معلومات عمليات الأمن السيبراني؛ والتعامل مع ما يرد من الهيئة بحسب إشارة المشاركة. يوضح الملحق (أ) إشارة المشاركة وبروتوكول الإشارة الضوئية (TLP) المقرر بهذا الشأن.

٦,١,١٣ يجب على الجهة مراجعة أنواع نماذج المشاركة، بينها وبين الهيئة، ودراسة النماذج المعدة، بهذا الشأن وفق ما هو مبين في الملحق (ب)، والتعامل معها حسبما يقتضيه الوضع، عند مشاركة معلومات عمليات الأمن السيبراني.

٦,٢ الأحكام المتعلقة بمشاركة معلومات عمليات الأمن السيبراني لمقدمي خدمات ومنتجات وحلول تقنية المعلومات والتقنيات التشغيلية

٦,٢,١ يجب على مقدمي خدمات تقنية المعلومات، والتقنيات التشغيلية؛ إبلاغ الهيئة بشكل فوري ومباشر، من خلال حصين (البوابة الوطنية لخدمات الأمن السيبراني) أو من خلال أي قناة أخرى تقرها الهيئة، بالثغرات التي يجري رصدها على منتجاتها أو حلولها، أو الأنظمة التابعة لها، والالتزام بمعالجتها.

٦,٢,٢ يجب على مقدمي خدمات تقنية المعلومات، والتقنيات التشغيلية؛ التعاون التام مع الهيئة، وتمكينها عند مباشرة اختصاصاتها، وتنفيذ مهماتها بشكل كامل، وكذلك الأمر عند قيامها بأي أعمال تحر للأمن السيبراني.

٧. أحكام الاستجابة للحوادث المتعلقة بالأمن السيبراني

٧,١ أحكام الاستجابة للحوادث المتعلقة بالأمن السيبراني للجهة

٧,١,١ تتحمل الجهة المسؤولية الكاملة عن جميع المهمات، والمراحل المرتبطة بالاستجابة للحادثة المتعلقة بالأمن السيبراني، التي تعرضت لها الجهة؛ وتكون خاضعة للمساءلة عليها أمام الهيئة. ويوضح الملحق (د) مراحل عملية الاستجابة للحوادث المتعلقة بالأمن السيبراني المطلوبة خلال أعمال الاستجابة.

٧,١,٢ تتم عملية مشاركة بيانات الاستجابة للحوادث، المتعلقة بالأمن السيبراني من خلال حصين (البوابة الوطنية لخدمات الأمن السيبراني)، أو من خلال أي قناة أخرى تقرها الهيئة.

٧,١,٣ في حال اشتباه أي جهة باحتمالية وقوع حادثة سيبرانية، أو رصدها لحادثة سيبرانية؛ فيجب أن تقوم الجهة بإبلاغ الهيئة بشكل فوري ومباشر، عبر حصين (البوابة الوطنية لخدمات الأمن السيبراني)، حيث ستقوم الهيئة بتصنيف الحادثة السيبرانية (Triage Process) أخذًا في الحسبان المعايير الموضحة في الملحق (هـ) وتحديد أولوية التعامل معها من خلال حصين (البوابة الوطنية لخدمات الأمن السيبراني) ومن ثم التوجيه بإكمال الإجراءات اللازمة.

٧,١,٤ تعد الجهة مسؤولة مسؤولية كاملة، أمام الهيئة، عما يجري رصده من حوادث أمن سيبراني، تعرضت لها؛ واتخاذ ما يلزم حيال تنفيذ أي إجراءات وتدابير، من شأنها الإسهام في تعزيز الأمن السيبراني في الجهة، وتحييد المخاطر السيبرانية ذات الصلة.

٧,١,٥ يجب على الجهة، الإشراف على جميع مهمات الاستجابة للحوادث، المتعلقة بالأمن السيبراني، التي يقوم بها مقدمو الخدمات؛ بما في ذلك مقدم خدمات مركز عمليات الأمن السيبراني المدار، ومقدم خدمات الاستجابة لحوادث الأمن السيبراني، وغيرهم. والتأكد من تنفيذ أي إجراءات وتدابير؛ من شأنها تعزيز الأمن السيبراني في الجهة.

٧,١,٦ عند استعانة الجهة بمقدمي خدمات الحوسبة السحابية؛ فإنه يتوجب عليها تولي مسؤولية التنفيذ التام، لأي إجراءات وتدابير مطلوبة من الهيئة ذات صلة بالاستجابة لحوادث الأمن السيبراني، ويشمل ذلك توفير أي وثائق، أو معلومات، أو بيانات، أو تقارير ذات صلة بعمليات الأمن السيبراني لدى مقدمي تلك الخدمات.

٧,١,٧ يجب على الجهة، وضع خطط الاستجابة لحوادث الأمن السيبراني وآليات التصعيد، وتحديثها بشكل دوري. ويلزم أن تتضمن خطوات محددة للجهة؛ يجب اتباعها للاستجابة لتلك الحوادث، بالإضافة إلى تضمنها على سياسة الاستجابة للحوادث المتعلقة بالأمن السيبراني وإجراءاتها، وإجراءات التبليغات الداخلية، وتعيين المهمات والمسؤوليات.

٧,١,٨ يجب على الجهة عند تصنيفها لحادثة أمن سيبراني مكتشفة؛ تضمين أبعاد تأثير الحادثة على الأمن الوطني، وسلامة الأفراد، والبيئة، والسمعة، والخدمات والأنظمة التقنية، والاعتمادية (مدى تأثر الخدمات الأخرى من الحادثة).

٧,١,٩ يجب على الجهة، إعداد تصنيف داخلي لحوادث الأمن السيبراني؛ يسمح بالربط مع التصنيف المشار إليه في الملحق (هـ). إذ يعد تصنيف حوادث الأمن السيبراني المقرر من الهيئة مرجعًا للجهة المتأثرة بحوادث الأمن السيبراني؛ لتصنيف الحوادث، عند التواصل مع الهيئة.

٧,١,١٠ يجب على الجهة إجراء تمارين سيبرانية، تحاكي حوادث الأمن السيبراني، لاختبار خطة الاستجابة للحوادث المتعلقة بالأمن السيبراني، مرة واحدة على الأقل في السنة. ويجب أن يشارك في التمارين السيبرانية كل من الموظفين المعنيين بمجال تقنية المعلومات، والأمن السيبراني، والاستجابة للحوادث، بالإضافة إلى كبار مديري الأعمال؛ بما في ذلك المسؤول الأول عن الأمن السيبراني في الجهة، والعاملون ذوو العلاقة لدى مقدم خدمات مركز عمليات الأمن السيبراني المدار، ومقدم خدمات الاستجابة لحوادث الأمن السيبراني.

٧,١,١١ يجب على الجهة القيام بتحليل حوادث الأمن السيبراني المرصودة، وتفعيل خطط الاستجابة للحوادث المتعلقة بالأمن السيبراني ومنها الاحتواء والإزالة والاستعادة، وتقديم تقارير دورية بوتيرة تحددها الهيئة، وفق تصنيف تلك الحوادث (كما هو موضح في الملحق (و)).

٧,١,١٢ يجب على الجهة التعاون التام مع الهيئة، والجهات الأخرى التي تحددها الهيئة، وتمكينها خلال مراحل عملية الاستجابة للحوادث، المتعلقة بالأمن السيبراني، مثل التحليل والاحتواء والإزالة والاستعادة.

٧,١,١٣ يجب على الجهة المتأثرة من حادثة الأمن السيبراني، رفع التقارير إلى الهيئة، ضمن الإطار الزمني المحدد (كما هو موضح في الملحق (و))؛ من لحظة الكشف عن حادثة الأمن السيبراني.

٧,١,١٤ يجب على الجهة المتأثرة من حادثة الأمن السيبراني الاستجابة الفورية لجميع المتطلبات التي ترد من الهيئة المتعلقة بالحادثة.

٧,١,١٥ يجب على الجهة المتأثرة من حادثة الأمن السيبراني؛ تقديم المعلومات المتوفرة لديها، عند التبليغ عن الحادثة إلى الهيئة؛ وتشمل تلك المعلومات ما هو موضح في الملحق (ز).

٧,١,١٦ يجوز للهيئة طلب المزيد من المعلومات؛ أو الوثائق الإضافية، من الجهة المتأثرة من حادثة الأمن السيبراني؛ بعد التبليغ عن الحادثة، متى ما دعت الحاجة لذلك.

٧,١,١٧ يجب أن تقدم الجهة المتأثرة من حادثة الأمن السيبراني، تقارير دورية إلى الهيئة، وذلك وفقًا لوتيرة رفع التقارير الدورية ومحتواها؛ حسب ما جرى تحديده في الملحق (و) ضمن هذا الإطار.

٧,١,١٨ يجب على الجهة المتأثرة من حادثة الأمن السيبراني؛ تقديم تقرير ما بعد الحادثة إلى الهيئة؛ وذلك بعد استكمال الجهود اللازمة، وإغلاق الحادثة، وذلك وفق الآلية والأطر الزمنية المقررة في هذا الإطار. كما يجب تقديم المعلومات، كما هو موضح في الملحق (ز) في تقرير ما بعد الحادثة (التقرير النهائي) المتوفرة ضمن الإطار الزمني المطلوب.

٧,١,١٩ يجوز للهيئة طلب أي معلومات، أو وثائق إضافية، من الجهة المتأثرة من حادثة الأمن السيبراني؛ وذلك بعد رفع تقرير ما بعد الحادثة، متى ما دعت الحاجة لذلك.

٧,١,٢٠ لا يحق للجهة مشاركة معلومات تتعلق بأعمال الاستجابة للحوادث المتعلقة بالأمن السيبراني، مع أي طرف أو جهة، إلا بعد أخذ الموافقات الخطية اللازمة من الهيئة، أو أن تكون تلك المعلومات، منصوص على مشاركتها في أي من الأطر أو التنظيمات الصادرة عن الهيئة، أو أن تكون تلك المعلومات، في إطار نطاق التعاقد بين الجهة المستفيدة، ومقدمي الخدمات المرخصين من الهيئة.

٧,١,٢١ يجب على الجهة الاحتفاظ بسجلات دقيقة وكاملة لجميع الحوادث السيبرانية التي تجري الاستجابة لها، والتحقيق فيها، وذلك لمدة لا تقل عن (١٥) سنة من تاريخ اكتشاف الحادثة، وبما يضمن إمكانية الرجوع إليها لأغراض التحقيق، أو التتبع والاستقصاء، ويشمل ذلك -دون حصر- تفاصيل الحادثة، والتسلسل الزمني للأحداث، وبيانات المستجيبين لها، وأي طرف ثالث له علاقة في تقديم أي جزء من أعمال الاستجابة، والجوانب الفنية ذات الصلة.

٧,١,٢٢ يجب على الجهة عدم إتلاف، أو حذف، أو تعديل سجلات حوادث الأمن السيبراني، قبل تسليمها إلى الهيئة الوطنية للأمن السيبراني؛ وفق آلية وقنوات محددة.

٨. الالتزامات والأحكام العامة

٨,١ الالتزامات العامة المترتبة على الجهات ومقدمي الخدمات المذكورين في هذا الإطار

يجب على جميع الجهات ومقدمي الخدمات، ضمن نطاق هذا الإطار؛ الالتزام بالإطار الوطني لمشاركة المعلومات والاستجابة للحوادث المتعلقة بالأمن السيبراني (هذا الإطار). وتشمل تلك الالتزامات الآتي:

٨,١,١ الالتزام بجميع الأحكام التنظيمية، والقرارات، والتوجيهات الصادرة عن الهيئة؛ وفق اختصاصها النظامي.

٨,١,٢ التعاون التام مع الهيئة، عند مباشرة اختصاصاتها التنظيمية، والرقابية، وفقًا لتنظيمها؛ بما في ذلك أي أعمال تحر أو تدقيق، أو تقييم للأمن السيبراني، وتزويد الهيئة بالوثائق، والمعلومات، والبيانات، والتقارير اللازمة لقيامها باختصاصاتها ومهماتها، وتمكينها من فحص الأجهزة والشبكات والنظم والبرمجيات.

٨,١,٣ تعد الإجراءات والتدابير الواردة في التنبيهات الأمنية، أو تلك المتعلقة بحوادث الأمن السيبراني، بمثابة توجيهات وقرارات؛ يجب على الجهة تنفيذها، وذلك خلال المدة الزمنية التي تقرها الهيئة.

٨,١,٤ يعد المسؤول الأول لدى الجهة، مسؤولًا عن تنفيذ جميع المتطلبات في هذا الإطار. ويجوز للمسؤول الأول تفويض من يراه للقيام بتلك المسؤوليات، بما في ذلك المسؤول عن الأمن السيبراني في الجهة، ولا يخلي ذلك مسؤولية الجهة تجاه أمنها السيبراني، والمسؤول الأول لدى الجهة في ضمان الالتزام بتنفيذ جميع الأحكام الواردة في هذا الإطار. ويجب ضمان وجود قناة للتواصل مع الهيئة، على مدار الساعة، وطيلة أيام الأسبوع؛ بما في ذلك التعامل مع ما يرد من خلال حصين (البوابة الوطنية لخدمات الأمن السيبراني) وذلك للقيام بمسؤوليات الجهة تجاه أمنها السيبراني.

٨,١,٥ يجب على الجهات عدم نشر أو مشاركة أو اطلاع أي بيانات تتعلق بعمليات الأمن السيبراني، سواء ما كان يتعلق بعمليات الأمن السيبراني للجهة نفسها، أو ما يتعلق بعمليات الأمن السيبراني للمستفيدين (سواء أكانوا عملاء لدى الجهة، أو مشتركين معها، أو غيرهم)، ويلتزم بذلك إلى أن يجري الحصول على موافقة خطية من الهيئة. ويجوز مشاركة المعلومات المتعلقة بعمليات الأمن السيبراني، بحسب ما هو منصوص عليه، في الأطر والتنظيمات ذات الصلة، الصادرة عن الهيئة.

٨,١,٦ في حالات التحري والتحليل الجنائي الرقمي عند اشتباه وقوع حادثة أمن سيبراني؛ فإنه يجب على الجهات جمع سجلات الأحداث الأمنية وحفظها، وكذلك والأنظمة التقنية والتطبيقات لتلك الحالات، والتأكد من بقاء هذه السجلات والأدلة دون تلف، أو تغيير، أو عبث أثناء جمعها وحفظها؛ وذلك لمدة سنتين كاملتين، اعتباراً من تاريخ بدء أعمال التحري والتحليل الجنائي الرقمي، أو حتى انتفاء الحاجة، وفق ما تقرره الهيئة.

٨,١,٧ اتباع أفضل الممارسات الفنية في تحريز الأدلة الرقمية، والعمل على حفظها، وذلك لتمكين فرق الاستجابة والتحري من تحليل تلك الأدلة عند الحاجة. إضافة إلى عدم حذف البرمجيات الضارة بشكل عشوائي؛ دون الرجوع إلى الهيئة.

٨,٢ أحكام عامة

٨,٢,١ يجوز للهيئة مراجعة هذا الإطار وتحديثه؛ وفقًا لمتطلبات تنظيم قطاع الأمن السيبراني؛ ويجب التقيد بأي تحديثات وفقًا لما تحدده الهيئة.

٨,٢,٢ يجوز للهيئة وضع أدلة لتطبيق هذا الإطار، ويجب على الجهات التقيد بما تصدره الهيئة في هذا الشأن.

٨,٢,٣ يجوز للهيئة قيادة أعمال الاستجابة للحوادث المتعلقة بالأمن السيبراني بناءً على مستوى تصنيفها، وفقًا لتقديرها (حسب الملحق (هـ)).

٩. الملاحق

الملحق (أ): إشارة المشاركة وبروتوكول الإشارة الضوئية (TLP)

يجري تحديد إشارة المشاركة، وفق بروتوكول الإشارة الضوئية (TLP) لتحديد نطاق مشاركة معلومات علميات الأمن السيبراني، والتعامل مع ما يرد من الهيئة؛ بحسب تصنيف البيانات، ووفقاً لضوابط الأمن السيبراني للبيانات، الصادرة من الهيئة الوطنية للأمن السيبراني. ويوضح جدول (٢) أدناه آلية تحديد إشارة المشاركة ومتطلبات التعامل مع المعلومات المستلمة.

إشارة المشاركة	آلية تحديد إشارة مشاركة معلومات عمليات الأمن السيبراني	متطلبات التعامل مع المعلومات المستلمة
أحمر	تعد معلومات عمليات الأمن السيبراني المحددة بإشارة المشاركة (أحمر) معلومات عالية الحساسية، ولا يمكن مشاركتها إلا مع المستلم الذي يمكن له تقديم الدعم، والهيئة. ويمكن أن يترتب على إفشاء هذه المعلومات، أثر كارثي، أو مرتفع على سمعة الجهة أو أعمالها.	لا يمكن إعادة مشاركة معلومات عمليات الأمن السيبراني المحددة بإشارة المشاركة (أحمر).
برتقالي + مشدد	تعد معلومات عمليات الأمن السيبراني المحددة بإشارة المشاركة (برتقالي +مشدد)، معلومات حساسة، ولا يمكن مشاركتها إلا داخل الجهة لأشخاص محددين، والهيئة. ويمكن أن يترتب على إفشاء هذه المعلومات، أثر متوسط على سمعة الجهة أو أعمالها.	يمكن إعادة مشاركة معلومات عمليات الأمن السيبراني المحددة بإشارة المشاركة (برتقالي +مشدد)؛ ضمن جهة مستلمي معلومات عمليات الأمن السيبراني، فحسب، ولأشخاص محددين.
برتقالي	تعد معلومات عمليات الأمن السيبراني المحددة بإشارة المشاركة (برتقالي) معلومات حساسة، ولا يمكن مشاركتها إلا داخل الجهة، أو على أساس الحاجة إلى الاطلاع عليها، والهيئة. ويمكن أن يترتب على إفشاء هذه المعلومات، أثر متوسط على سمعة الجهة أو أعمالها.	يمكن إعادة مشاركة معلومات عمليات الأمن السيبراني المحددة بإشارة المشاركة (برتقالي)؛ ضمن جهة مستلمي معلومات عمليات الأمن السيبراني، أو على أساس الحاجة إلى الاطلاع عليها؛ ويكون ذلك حصراً على الجهات التي تباشر أعمالها من المملكة العربية السعودية فحسب (لا يمكن إعادة مشاركة معلومات عمليات الأمن السيبراني مع جهات خارج المملكة أو مع جهات غير مُصرح لها بالاطلاع على معلومات عمليات الأمن السيبراني داخل المملكة).
أخضر	تعد معلومات عمليات الأمن السيبراني المحددة بإشارة المشاركة (أخضر) مفيدة؛ لنشر الوعي في مجتمعات الأمن السيبراني، أو القطاعات ذات العلاقة، ولكن لا يمكن مشاركتها مع عامة الناس.	يمكن إعادة مشاركة معلومات عمليات الأمن السيبراني المحددة بإشارة المشاركة (أخضر)، ضمن جهة مستلمي معلومات عمليات الأمن السيبراني، أو جهة أخرى على علاقة معهم أو في القطاع نفسه؛ ولا يسمح بتبادلها أو نشرها من خلال القنوات العامة.
شفاف	لا توجد قيود على مشاركة معلومات عمليات الأمن السيبراني، المحددة بإشارة المشاركة (شفاف)؛ ويمكن مشاركتها مع عامة الناس.	يمكن إعادة مشاركة معلومات عمليات الأمن السيبراني المحددة بإشارة المشاركة (شفاف) بدون قيود.

جدول ٢: إشارة المشاركة وبروتوكول الإشارة الضوئية

الملحق (ب): أنواع نماذج المشاركة بين الهيئة والجهات/مقدمي الخدمات المذكورين في هذا الإطار

تسعى الهيئة إلى رفع مستوى فاعلية عملية مشاركة معلومات عمليات الأمن السيبراني على المستوى الوطني؛ وتعزيز قدرات الصمود والاستجابة للتهديدات والمخاطر السيبرانية، وقد جرى تحديد وحصر أنواع النماذج المتوقعة بين الهيئة والجهات، وأصحاب العلاقة من مقدمي الخدمات (على سبيل المثال: مقدمي خدمات مركز عمليات الأمن السيبراني المدار، ومقدمي خدمات الاستجابة لحوادث الأمن السيبراني، ومقدمي خدمات الحوسبة السحابية، والأمن السيبراني، ومنتجاته وحلوله)، واعتماد القالب المناسب لكل منها. ويوضح جدول (٣) أدناه؛ وصف لأنواع المشاركة المتوقعة، خلال أعمال مشاركة معلومات عمليات الأمن السيبراني، على المستوى الوطني. إذ يجري مشاركتها من خلال خدمة مشاركة المعلومات في حصين (البوابة الوطنية لخدمات الأمن السيبراني):

المسمى	الوصف	المرسل	المستقبل
تنبيه أمني عام	مشاركة معلومات عمليات الأمن السيبراني لعدد من الجهات في المملكة، قد تشمل معلومات عن تهديد أو ثغرة. ويحتوي التنبيه في الغالب على إجراءات وتدابير مطلوب من الجهات تطبيقها، والإفادة بالنتائج.	الهيئة	الجهة / مقدمو الخدمات
تنبيه أمني خاص	مشاركة معلومات عمليات الأمن السيبراني لجهة بعينها، كمعلومات عن تهديد أو ثغرة. ويحتوي التنبيه على إجراءات وتدابير مطلوب من الجهة تطبيقها والإفادة بالنتائج.	الهيئة	الجهة / مقدمو الخدمات
طلب معلومات	رفع طلب إلى جهة في المملكة؛ لتزويد الهيئة بمعلومات للقيام باختصاصاتها ومهماتها.	الهيئة	الجهة / مقدمو الخدمات
تقرير استباقي	مشاركة تقرير فني يحتوي على ما جرى استخلاصه، من أنماط، وأدوات وأساليب استخدمها المهاجمون، إضافة إلى تحديد إجراءات وتدابير، قد يستلزم تنفيذها من قبل الجهة، والإفادة بالنتائج.	الهيئة	الجهة / مقدمو الخدمات
حصر معرف رقمي	طلب حصر معرف رقمي، مرتبط بالإنترنت، وتابع للجهة.	الهيئة	الجهة / مقدمو الخدمات
مؤشرات الاختراق والسلوك	تشارك الهيئة معلومات مؤشرات الاختراق (IoC) والسلوك (IoB) مع الجهات في المملكة؛ لتمكينها من اكتشاف التهديدات السيبرانية.	الهيئة	الجهة / مقدمو الخدمات
معلومات استباقية	مشاركة معلومات مرتبطة بتهديد، أو ثغرة، أو حادثة (خارج نطاق الجهة)، أو أنشطة سيبرانية، من شأنها تعزيز الدراية السيبرانية الوطنية.	الجهة / مقدمو الخدمات	الهيئة
استفسار سيبراني	رفع طلب للحصول على معلومة سيبرانية من الهيئة.	الجهة / مقدمو الخدمات	الهيئة

جدول ٣: أنواع نماذج المشاركة بين الهيئة والجهات/مقدمي الخدمات

الملحق (ج): المدد الزمنية لأنواع المشاركة بين الهيئة والجهات في المملكة

تشارك الهيئة الوطنية للأمن السيبراني الجهات في المملكة؛ معلومات عمليات الأمن السيبراني، وتطلب منها اتخاذ إجراءات محددة؛ كتوفير معلومات سيبرانية أو أدلة رقمية، أو أي إجراءات مساعدة في عملية تحليل تهديد أو ثغرة سيبرانية، أو أي إجراءات تسهم في تحييد خطر التهديد على المستوى الوطني. ولكل من طلبات الهيئة مدة زمنية، موضحة في جدول (٤) الآتي:

الأوضاع الطبيعية		
نوع الطلب	تصنيف الطلب	وقت الإجراء المطلوب
الطلبات التي جرى إنشاؤها من قبل الهيئة	فوري	بحد أقصى خلال ساعتين، أو خلال المدة التي تحددها الهيئة عندما يتطلب الأمر أقل من ساعتين.
	عاجل جدا	بحد أقصى خلال ١٢ ساعة، أو خلال المدة التي تحددها الهيئة، عندما يتطلب الأمر أقل من ١٢ ساعة.
	عاجل	بحد أقصى خلال ٤٨ ساعة، أو خلال المدة التي تحددها الهيئة عندما يتطلب الأمر أقل من ٤٨ ساعة.
	عادي	بحد أقصى خلال ٧٢ ساعة، أو خلال المدة التي تحددها الهيئة، عندما يتطلب الأمر أقل من ٧٢.

جدول ٤: المدد الزمنية لأنواع المشاركة بين الهيئة والجهات في المملكة

كما أن المدد الزمنية المحددة، تخضع لتقييم الهيئة، استناداً على مخرجات الدراية السيبرانية، والتي تتضمن حالات التأهب والأزمات، والجدول (٥) الآتي يبين المدد الزمنية لحالات التأهب والأزمات.

عند تفعيل حالات التأهب والأزمات		
نوع الطلب	تصنيف الطلب	وقت الإجراء المطلوب
الطلبات التي جرى إنشاؤها من قبل الهيئة	فوري	بحد أقصى خلال ساعة، أو خلال المدة التي تحددها الهيئة عندما يتطلب الأمر أقل من ساعة.
	عاجل جدا	بحد أقصى خلال ٦ ساعات، أو خلال المدة التي تحددها الهيئة عندما يتطلب الأمر أقل من ٦ ساعات.
	عاجل	بحد أقصى خلال ٢٤ ساعة، أو خلال المدة التي تحددها الهيئة عندما يتطلب الأمر أقل من ٢٤ ساعة.
	عادي	بحد أقصى خلال ٤٨ ساعة، أو خلال المدة التي تحددها الهيئة عندما يتطلب الأمر أقل من ٤٨ ساعة.

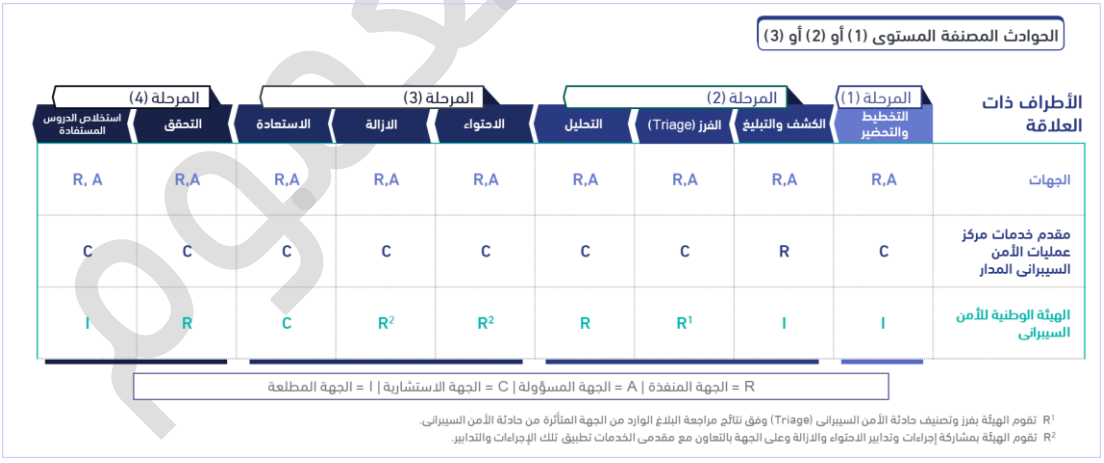
جدول ٥: المدد الزمنية لأنواع المشاركة بين الهيئة والجهات في المملكة عند تفعيل حالات التأهب والأزمات

الملحق (د): مراحل عملية الاستجابة للحوادث المتعلقة بالأمن السيبراني

يتطلب إنشاء نموذج حوكمة وطنية، يعنى بالاستجابة للحوادث المتعلقة بالأمن السيبراني؛ تطوير أربع مراحل للاستجابة لحوادث الأمن السيبراني، وإعدادها على النحو المبين في شكل (١) أدناه:

شكل ١: مراحل عملية الاستجابة للحوادث المتعلقة بالأمن السيبراني

كما يوضح الشكلان (٢) و(٣) أدناه، الأدوار والمسؤوليات المنوطة بالأطراف ذات العلاقة ضمن مراحل الاستجابة لحوادث الأمن السيبراني.



شكل ٢: الأدوار والمسؤوليات للحوادث المصنفة المستوى (١) و (٢) و (٣)

شكل ٣: الأدوار والمسؤوليات للحوادث المصنفة المستوى (٤) أو (٥)

الملحق (هـ): مستويات تصنيف حوادث الأمن السيبراني

تعتمد عملية الاستجابة للحوادث، المتعلقة بالأمن السيبراني، على مدى خطورة الحادثة، التي يجري التعامل معها. ولذلك تُصنف حوادث الأمن السيبراني على المستوى الوطني؛ وفقًا لخمسة مستويات، مدرجة من الأكثر خطورة إلى الأقل، ويعتمد هذا التصنيف على أبعاد التأثير على الخدمات، والأنظمة، والموظفين، والحياة والصحة، والبيانات، والسمعة، ودرجة الأولوية للاستجابة. يعرض الجدول (٦) الآتي تصنيف حوادث الأمن السيبراني، وفقاً لهذا الإطار.

التصنيف	الوصف	الاستجابة
المستوى (١) كارثية	اختراق للبنية التحتية للجهة، أدى إلى إحداث أضرار على الأرواح، أو تعثر احتواء الحادثة الحرجة.	الاستجابة بقيادة الهيئة، حسب ما تراه ضرورياً
المستوى (٢) حرجة	اختراق للبنية التحتية للجهة، أدى إلى إحداث ضرر بالغ على العمليات الأمنية الوطنية، أو الخدمات الحيوية على مستوى المملكة.	الاستجابة بقيادة الهيئة، حسب ما تراه ضرورياً
المستوى (٣) مرتفعة	اختراق للبنية التحتية للجهة، والوصول لبيانات سرية وطنية أو إحداث ضرر لخدمة وطنية.	الاستجابة بقيادة الهيئة، حسب ما تراه ضرورياً، وقد تكون بقيادة الجهة المتأثرة بناءً على طلب الهيئة
المستوى (٤) متوسطة	اختراق نتج عنه، تنقل داخل شبكة الجهة، أو الوصول لبيانات مقيدة وطنية، غير سرية.	الاستجابة بقيادة الجهة المتأثرة من الحادثة، وفقًا لطلب الهيئة، وقد تقوم الهيئة بقيادة الاستجابة، بناءً على تقديرها
المستوى (٥) محدودة	اختراق محدود على محطة عمل، أو خادم، دون الوصول لبيانات وطنية.	الاستجابة بقيادة الجهة المتأثرة من الحادثة، وفقًا لطلب الهيئة، وقد تقوم الهيئة بقيادة الاستجابة، بناءً على تقديرها

جدول ٦: مستويات تصنيف حوادث الأمن السيبراني

الملحق (و): الأطر الزمنية للرفع بتقارير حوادث الأمن السيبراني

يحدد جدول (٧) أدناه الأطر الزمنية المحددة لرفع التقارير الدورية، وتقرير ما بعد الحادثة:

التصنيف	التقارير الدورية	تقرير ما بعد الحادثة (التقرير النهائي)	الجهة المسؤولة عن رفع التبليغات والتقارير
المستوى (١) كارثية	خلال المرحلة الثانية والثالثة؛ إضافة إلى تقرير بعد نهاية كل مرحلة من هذه المراحل، أو وفق ما تحدده الهيئة.	في المرحلة الرابعة، وبحد أقصى، خلال ١٤ يوماً من تاريخ إغلاق الحادثة.	الجهة المتأثرة من حادثة الأمن السيبراني، بدعم من مقدم خدمات مركز عمليات الأمن السيبراني المدار، ومقدم خدمات الاستجابة، لحوادث الأمن السيبراني.
المستوى (٢) حرجة	خلال المرحلة الثانية والثالثة؛ إضافة إلى تقرير بعد نهاية كل مرحلة من هذه المراحل، أو وفق ما تحدده الهيئة.	في المرحلة الرابعة، وبحد أقصى خلال ١٤ يوماً من تاريخ إغلاق الحادثة.	الجهة المتأثرة من حادثة الأمن السيبراني بدعم من مقدم خدمات مركز عمليات الأمن السيبراني المدار، ومقدم خدمات الاستجابة لحوادث الأمن السيبراني.
المستوى (٣) مرتفعة	خلال المرحلة الثانية والثالثة؛ إضافة إلى تقرير بعد نهاية كل مرحلة من هذه المراحل، أو وفق ما تحدده الهيئة.	في المرحلة الرابعة، وبحد أقصى خلال ١٤ يوماً من تاريخ إغلاق الحادثة.	الجهة المتأثرة من حادثة الأمن السيبراني، بدعم من مقدم خدمات مركز عمليات الأمن السيبراني المدار، ومقدم خدمات الاستجابة لحوادث الأمن السيبراني.
المستوى (٤) متوسطة	خلال المرحلة الثانية والثالثة، إضافة إلى تقرير بعد نهاية كل مرحلة من هذه المراحل، أو وفق ما تحدده الهيئة.	في المرحلة الرابعة، وبحد أقصى خلال ١٤ يوماً من تاريخ إغلاق الحادثة.	الجهة المتأثرة من حادثة الأمن السيبراني بدعم محتمل من مقدم خدمات مركز عمليات الأمن السيبراني المدار، ومقدم خدمات الاستجابة لحوادث الأمن السيبراني.
المستوى (٥) محدودة	في نهاية المرحلة الثانية، والمرحلة الثالثة؛ أو وفق ما تحدده الهيئة.	وفقاً لتقدير الهيئة، في المرحلة الرابعة، وبحد أقصى خلال ١٤ يوماً من تاريخ إغلاق الحادثة.	الجهة المتأثرة من حادثة الأمن السيبراني، بدعم محتمل من مقدم خدمات مركز عمليات الأمن السيبراني المدار، ومقدم خدمات الاستجابة لحوادث الأمن السيبراني.

جدول ٧: الأطر الزمنية للرفع بتقارير حوادث الأمن السيبراني

الملحق (ز): معلومات حوادث الأمن السيبراني المطلوبة

يجب على الجهة المتأثرة من حادثة الأمن السيبراني؛ تقديم المعلومات المتوفرة لديها عند التبليغ عن الحادثة؛ وتشمل تلك المعلومات الآتي:

١. اسم الجهة المتأثرة من حادثة الأمن السيبراني، وعنوانها، والقطاع الذي تعمل فيه.
٢. بيانات الاتصال الخاصة بالجهة.
٣. تصنيف الحادثة وفق الملحق (هـ).
٤. اسم مقدم خدمة تشغيل البنية التحتية، في حال استضافة الخوادم خارج الجهة.
٥. مؤشرات الاختراق المتوفرة، عند تقديم البلاغ.
٦. المعرفات الرقمية المتأثرة المتصلة بالإنترنت (Public IPs) والنطاقات ذات الصلة (في حال كانت المعرفات والنطاقات مصنفة من قبل الهيئة؛ فيضمن رقمها المرجعي الوارد في أنظمة الهيئة ذات العلاقة).
٧. بيانات الأصول المتأثرة وفي حال تأثر أحد الأصول المسجلة لدى الهيئة (وفق البندين ٥,٢ و٥,٤ من الإطار الوطني لإدارة مخاطر الأمن السيبراني) بالحادثة، فيتم تضمين اسم الأصل ورقمه المرجعي الوارد في حصين (البوابة الوطنية لخدمات الأمن السيبراني).
٨. وقت الكشف عن الحادثة ومدتها (من وقت الكشف عن الحادثة، إلى وقت إغلاق الحادثة؛ في حال الاغلاق).
٩. الخدمات والأنظمة، وحسابات الدخول، والبيانات المتأثرة، ومستوى تصنيف البيانات، وفق المتطلبات التنظيمية الصادرة، من الجهات المختصة.
١٠. طبيعة الانتهاك الأمني؛ بما في ذلك نوع الهجمة، والثغرات المستغلة، والتقنية المتأثرة.
١١. تقييم الآثار المترتبة على الحادثة.
١٢. المساعدة المطلوبة (حال الحاجة).
١٣. حالة إغلاق الحادثة.
١٤. الخطوات الآتية التي ستعتمدها الجهة المتأثرة من حادثة الأمن السيبراني؛ بما في ذلك تقدير مستوى استعادة الخدمة، إذا لم يتم إغلاق الحادثة.

يجب على الجهة المتأثرة من حادثة الأمن السيبراني؛ تقديم تقرير ما بعد الحادثة إلى الهيئة. كما يجب تقديم المعلومات الآتية في تقرير ما بعد الحادثة (التقرير النهائي) المتوفرة ضمن الإطار الزمني المطلوب:

١. اسم الجهة المتأثرة من حادثة الأمن السيبراني، وعنوانها، والقطاع الذي تعمل فيه.
٢. الرقم التعريفي للاستجابة للحوادث المقدم من قبل الهيئة.
٣. بيانات الاتصال الخاصة بضابط الاتصال.
٤. اسم مقدم خدمة تشغيل البنية التحتية؛ في حال استضافة الخوادم خارج الجهة.
٥. الملخص التنفيذي.
٦. المقدمة والسياق العام، بما في ذلك تفاصيل الحادثة، ومسبباتها، وتصنيفها.

٧. التسلسل الزمني للحادثة.
٨. أثر الحادثة؛ بما في ذلك الخدمات، والبيانات (وفق المتطلبات التنظيمية الصادرة من الجهة المختصة)، والتقنيات وحسابات الدخول المتأثرة.
٩. بيانات الأصول المتأثرة وفي حال تأثر أحد الأصول المسجلة لدى الهيئة (وفق البندين ٥,٢ و٥,٤ من الإطار الوطني لإدارة مخاطر الأمن السيبراني) بالحادثة، فيتم تضمين اسم الأصل ورقمه المرجعي الوارد في حصين (البوابة الوطنية لخدمات الأمن السيبراني).
١٠. مؤشرات الاختراق، وعينات البرمجيات الضارة (من خلال خدمة فحص الملفات والروابط في حصين (البوابة الوطنية لخدمات الأمن السيبراني))، أو المعلومات الاستباقية، التي تخص مجموعات الهجوم.
١١. تحليل وتحديد مسببات الحادثة السيبرانية.
١٢. حجم البيانات التي جرى الاطلاع عليها من قبل المهاجم، أو جرى تسريبها في الحادثة السيبرانية.
١٣. الإجراءات المتخذة، على صعيد الاحتواء، والإزالة، والاستعادة.
١٤. إجراءات الإصلاح المتخذة، والخطوات والضوابط الإضافية، التي سيجري تنفيذها، بما في ذلك خارطة طريق للتنفيذ.
١٥. احتساب التكلفة المتوقعة للحادثة السيبرانية بالريال السعودي (يشمل ذلك خسائر تعطل الخدمات، وإجراءات الاحتواء والإزالة والتعافي).
١٦. الدروس المستفادة من الحادثة.


الهيئة الوطنية
للأمن السيبراني
National Cybersecurity Authority