الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

السياسة الوطنية لمراكز عمليات الأمن السيبراني المُدَارة

National Policy for Managed Security Operations Centers (MSOC)
(NPMSOC-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

١. المقدمة

تعد الهيئة الوطنية للأمن السيبراني؛ 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؛ وذلك وفقاً لتنظيمها الصادر بموجب الأمر الملكي الكريم ذي الرقم (٦٨٠١) في ١٤٣٩/٢/١١هـ. ومن ضمن اختصاصات الهيئة ومهماتها، وضع السياسات وآليات الحوكمة، والأطر، والمعايير، والضوابط، والإرشادات المتعلقة بالأمن السيبراني، وتعميمها على الجهات ذات العلاقة، ومتابعة الالتزام بها، وتحديثها. بالإضافة إلى الترخيص بمزاولة الأفراد والجهات غير الحكومية، للأنشطة والعمليات المتعلقة بالأمن السيبراني؛ التي تحددها الهيئة. كما تشمل اختصاصات الهيئة ومهماتها؛ تحفيز نمو قطاع الأمن السيبراني في المملكة، وتشجيع الابتكار والاستثمار فيه.

ويأتي إعداد هذه السياسة؛ إنفاذاً لما ورد في تنظيم الهيئة المشار إليه، واستناداً على إستراتيجية المرحلة الثانية للهيئة (2.0)، والمبادرات المعتمدة في هذا الشأن؛ ومنها إعداد تنظيمات الأمن السيبراني وتشريعاته على المستوى الوطني، وبناء منظومة القدرات السيبرانية المتقدمة، للمراقبة والرصد ومشاركة المعلومات.

٢. التعريفات

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

المصطلح	التعريف
الهيئة	الهيئة الوطنية للأمن السيبراني.
الجهات	هي الجهات الحكومية، أو الخاصة الربحية، أو غير الربحية، أو أي شكل آخر من أشكال الجهات.
السياسة	السياسة الوطنية لمراكز عمليات الأمن السيبراني المُدَارة، الصادرة عن الهيئة.
الإطار	الإطار التنظيمي لترخيص تقديم خدمات مركز عمليات الأمن السيبراني المُدَار، الصادر من الهيئة.
البنية التحتية الوطنية الحساسة	هي 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: ١- أثر سلبي كبير على توافر الخدمات الأساسية، أو تكاملها أو تسليمها؛ بما في ذلك 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 الكبيرة. ٢- تأثير كبير على الأمن الوطني و/ أو الدفاع الوطني و/ أو اقتصاد الدولة أو مقدراتها الوطنية.
مركز عمليات الأمن السيبراني	هو مركز يقدم خدمات العمليات المتعلقة بمراقبة أحداث الأمن السيبراني في المنظومة التقنية للجهة، التي من شأنها اكتشاف التهديدات السيبرانية، ومعرفة كيفية حدوثها، وتقديم التوصيات في كيفية معالجتها، واتخاذ الإجراءات اللازمة لاحتوائها.
خدمات مركز عمليات الأمن السيبراني المُدَار	الخدمات التي تحصل عليها الجهة المستفيدة من مقدم الخدمة؛ بهدف مراقبة أحداث الأمن السيبراني في المنظومة التقنية للجهة المستفيدة؛ لاكتشاف التهديدات السيبرانية ومعرفة كيفية حدوثها، وتقديم التوصيات في كيفية معالجتها، ليتم تطبيقها من قبل الجهة المستفيدة، وتشمل هذه الخدمات، العمليات، وفرق العمل، والأنظمة، وغيرها.
الجهة المستفيدة	الجهة التي تتعاقد مع مقدم الخدمة؛ بهدف الحصول على خدمات مركز عمليات الأمن السيبراني المُدَار.
مقدم الخدمة	الجهة المرخصة من الهيئة لتقديم خدمات مركز عمليات الأمن السيبراني المُدار في المملكة، وفقًا للإطار التنظيمي لترخيص تقديم خدمات مركز عمليات الأمن السيبراني المُدَار، الصادر من الهيئة.

٣. أهداف السياسة

تهدف السياسة إلى الإسهام في تحقيق الآتي:

١. تعزيز الدراية الأمنية لدى الجهات، وعلى المستوى الوطني.
٢. تمكين الجهات في المملكة من الحصول على خدمات مركز عمليات الأمن السيبراني المُدَار، التي تتّسم بالموثوقية والنضج، والجودة العالية، وعلى النحو الذي يحقق الغرض منها.
٣. تحفيز نمو قطاع الأمن السيبراني في المملكة، وتشجيع الابتكار والاستثمار فيه؛ من خلال إيجاد بيئة عمل منظمة، وتقليص الفجوة بين العرض والطلب في خدمات الأمن السيبراني.
٤. رفع كفاءة الإنفاق في قطاع الأمن السيبراني على المستوى الوطني.

٤. نطاق السياسة

يتم تطبيق هذه السياسة على الجهات الآتية:

أ. الجهات الحكومية، وتشمل الوزارات والهيئات، والمؤسسات والمراكز والمجالس، واللجان والأمانات وغيرها، والشركات والجهات التابعة لها.
ب. جهات القطاع الخاص، التي تمتلك بنى تحتية وطنية حساسة، أو تشغّلها أو تستضيفها.
ج. أي جهات أخرى تلزمها الهيئة بتطبيق هذه السياسة -وفقاً لتقديرها المطلق-، وبما يحقق المستهدفات الوطنية ذات الصلة.

تشجع الهيئة جميع الجهات الأخرى في المملكة غير المشمولة في الفقرات (أ) و (ب) و (ج) آنفة الذكر، بالتعاقد مع مقدم الخدمة؛ وذلك بهدف حصولها على خدمات مركز عمليات الأمن السيبراني المُدَار؛ استناداً إلى احتياجات الأمن السيبراني لديها.

٥. بنود السياسة

يجب على جميع الجهات الملزمة بتطبيق هذه السياسة الالتزام بما يلي:

٥,١ جميع الأحكام التنظيمية والقرارات والتوجيهات الصادرة عن الهيئة؛ وفق اختصاصها النظامي، وبوصفها المرجع الوطني في كل ما يتعلق بالأمن السيبراني في المملكة.
٥,٢ الحصول على موافقة الهيئة المسبقة، لأي مبادرات، أو مشاريع أو خدمات؛ متعلقة بمركز عمليات الأمن السيبراني، سواء أكانت المبادرة على مستوى الجهة، أم على مستوى القطاع، أو غيره.
٥,٣ تنفيذ أعمال مركز عمليات الأمن السيبراني الخاص بالجهة من خلال مقدم خدمة في المستوى الأول، وفقاً للإطار، وذلك لجميع خدمات مركز عمليات الأمن السيبراني المُدَار؛ وعلى النحو المنصوص عليه في الملحق من هذه السياسة.

٦. إجراءات الالتزام ببنود السياسة

يجب على جميع الجهات الملزمة بتطبيق هذه السياسة التقيّد بالإجراءات الآتية:

٦,١ تزويد الهيئة -وفق النموذج الذي تحدده- بتقرير يتضمّن الآتي:

٦,١,١ الوضع الراهن لجميع أعمال مركز عمليات الأمن السيبراني، لدى الجهة؛ شاملاً التقنيات والإجراءات، وفرق العمل، وغيرها.

٦,١,٢ خطة الالتزام ببنود هذه السياسة، التي تشمل، بحسب الأحوال؛ الخطة التصحيحية للانتقال من الالتزامات التعاقدية الحالية، من الجهة التي تقدم خدمات مركز عمليات الأمن السيبراني المُدَار، إلى مقدم خدمة من المستوى الأول وفقاً للإطار، أو خطة تصحيحية للانتقال من مركز عمليات الأمن السيبراني الخاص بالجهة، إلى مقدم خدمة من المستوى الأول وفقاً للإطار.

٦,٢ تزويد الهيئة بالتقرير المشار إليه في الفقرة (٦,١) بحد أقصى خلال (٩٠) يوماً من تاريخ نفاذ هذه السياسة؛ وذلك من خلال قنوات التواصل التي تحددها الهيئة.

٦,٣ إبلاغ الهيئة مباشرة، عند اكتمال انتقال أعمال مركز عمليات الأمن السيبراني في الجهة، إلى مقدم خدمة.

٦,٤ تقوم الهيئة بمراجعة التقارير الواردة لها، بموجب هذا البند، وإبلاغ الجهة المعنية بالموافقة على التقرير، أو طلب إجراء التعديل عليه، أو أي متطلبات إضافية ذات صلة.

٧. أحكام عامة

٧,١ للهيئة؛ وفق تقديرها، وما تقتضيه مصلحة تنظيم القطاع؛ فرض قيود أو متطلبات إضافية، أو إلغاؤها، على الجهات الملزمة بتطبيق هذه السياسة.

٧,٢ تسري أحكام هذه السياسة اعتباراً من تاريخ نشرها على الموقع الإلكتروني للهيئة.

٧,٣ ستقوم الهيئة بمراجعة هذه السياسة وتحديثها كلما دعت الحاجة لذلك، ووفق متطلبات تنظيم قطاع الأمن السيبراني، وتلتزم الجهات الخاضعة لتطبيق هذه السياسة بأي تعديلات تطرأ عليها.

٧,٤ يتوجب على الجهات الخاضعة لهذه السياسة التقيد بجميع النماذج، والمهل التي تقرها الهيئة؛ لإنفاذها.

٨. الملحق

خدمات مراكز عمليات الأمن السيبراني المُدَارة

خدمات تحصل عليها الجهة المستفيدة من مقدم الخدمة؛ بهدف مراقبة أحداث الأمن السيبراني، في المنظومة التقنية للجهة المستفيدة؛ لاكتشاف التهديدات السيبرانية، ومعرفة كيفية حدوثها، وتقديم التوصيات في كيفية معالجتها؛ ليتم تطبيقها من قبل الجهة المستفيدة. وتشمل هذه الخدمات: العمليات، وفرق العمل، والأنظمة، وغيرها.

وفيما يلي توضيح للحد الأدنى من خدمات مركز عمليات الأمن السيبراني المُدار، التي يمكن الحصول عليها من مقدم الخدمة بموجب هذه السياسة:

١. المراقبة المستمرة واكتشاف التهديدات (Threat Monitoring and Detection)

تقديم خدمة المراقبة المستمرة للمنظومة التقنية، في الجهة الوطنية المستفيدة، وتشمل شبكات الجهة وأنظمتها، واكتشاف التهديدات، والهجمات السيبرانية في مراحلها المبكرة، وإصدار التنبيهات (Alerts) من خلال أدوات المراقبة والاكتشاف؛ باستخدام طرق اكتشاف مختلفة مثل، حالات اكتشاف مُعرّفة مسبقاً (detection use-cases) ومؤشرات الاختراق (Indicators of Compromise) وقواعد الاكتشاف (Detection Rules)، وتصنيف التنبيهات حسب خطورتها، وإصدار تنبيهات فورية للجهة المستفيدة عن التهديدات المكتشفة، وتقارير تقنية وتنفيذية دورية عن الحالة السيبرانية. ويجري ذلك عن طريق إدارة أدوات الأمن السيبراني المتخصصة وتشغيلها في المراقبة والاكتشاف.

٢. التحليل والتحقيق للتهديدات المكتشفة (Threat Analysis and Investigation)

قيام مقدم الخدمة بأعمال التحليل والتحقيق في التنبيهات المكتشفة، وربط الأحداث المختلفة وفهمها، ضمن سياق منظومة الجهة، والقدرة على تحديد التنبيهات الصحيحة، ذات العلاقة بحوادث سيبرانية حقيقية. وكذلك تحديد التنبيهات الخاطئة، بناء على أسلوب منهجي للتحليل في جميع التهديدات، وتزويد الجهة الوطنية المستفيدة بتحاليل أولية؛ بالإضافة إلى تقديم تحليلات شاملة، متضمنة مسببات التنبيهات والحوادث. كما تتضمن قيام مقدم الخدمة بعمل مسح لمؤشرات الاختراق (Sweeping) وتصيد التهديدات (Threats Hunting)، وكذلك إجراء التحليل والتحقيق في الحالات التي قامت الجهة الوطنية المستفيدة بتبليغ مقدم الخدمة عنها.

٣. التوصيات لاحتواء التهديدات السيبرانية (Threat Containment Recommendations)

تقديم توصيات متكاملة وفاعلة للجهة الوطنية المستفيدة، في كيفية احتواء التهديدات السيبرانية وتحييدها؛ ليتم تطبيقها من قبل الجهة المستفيدة، للسيطرة على مخاطر الهجمات والتهديدات المكتشفة.


الهيئة الوطنية
للأمن السيبراني
National Cybersecurity Authority