الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

مشروع ضوابط الأمن السيبراني

لجهات القطاع الخاص من غير ذات البنى التحتية الحساسة

Non-CNI Private Sector Organizations Cybersecurity Controls

(NCNICC – 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

قائمة الجداول

قائمة الأشكال والرسوم التوضيحيّة

الملخص التنفيذي

استهدفت رؤية المملكة العربية السعودية ٢٠٣٠ التطوير الشامل للوطن وأمنه، واقتصاده، ورفاهية مواطنيه، وعيشهم الكريم. ومن أحد مستهدفات الرؤية الأساسية، تعزيز القطاع الخاص، وزيادة إسهامه في الناتج المحلي الإجمالي إلى ٦٥٪ بحلول عام ٢٠٣٠ فضلاً عن زيادة إسهام الجهات الصغيرة والمتوسطة، في الناتج المحلي الإجمالي إلى ٣٥٪ وهو الأمر الذي يجعل الجهات الصغيرة، والمتوسطة، والكبيرة، عنصرًا بارزًا في تحقيق هذه الأهداف الاقتصادية. وعلى هذا؛ ينبغي على كل جهة في المملكة العربية السعودية أن تعمل على تحقيق هذا النمو الطموح؛ الالتزام بهذه الضوابط الرامية إلى تحسين صمود الأمن السيبراني، داخل القطاع الخاص. إذ تعنى ضوابط الأمن السيبراني لجهات القطاع الخاص من غير ذات البنى التحتية الحساسة بجميع فئات القطاع الخاص بجميع جهاته (الجهات الصغيرة والمتوسطة والكبيرة)، نظرًا للدعم المحوري الذي تقدمه في تحقيق الأهداف الاقتصادية للمملكة.

يتمثل اختصاص الهيئة الوطنية للأمن السيبراني، بموجب الأمر الملكي الكريم رقم ٦٨٠١ وتاريخ ١٤٣٩/٢/١١ هـ في كونها الجهة التنظيمية المختصة في المملكة بالأمن السيبراني، والمرجع الوطني في شؤونه. لهذا جاءت مهمات هذه الهيئة واختصاصاتها ملبيةً للجوانب الإستراتيجية، ولجوانب تنظيم الأمن السيبراني المتعلقة بوضع السياسات وآليات الحوكمة، والأطر، والمعايير، والضوابط، والإرشادات المتعلقة به. كما جاءت ملبيةً لجوانب المتابعة المستمرة لالتزام الجهات؛ بما يعزز جهود الأمن السيبراني وأهميتها، والحاجة الملحة التي ازدادت مع ازدياد التهديدات، والمخاطر الأمنية في الفضاء السيبراني، أكثر من أي وقت مضى.

وقد نص تنظيم الهيئة أنّ اختصاصها فيما يتعلق بالأمن السيبراني، يشمل جميع الجهات الحكومية والخاصة وغيرها في المملكة. ومن هذا المنطلق؛ قامت الهيئة الوطنية للأمن السيبراني بتطوير ضوابط الأمن السيبراني لجهات القطاع الخاص من غير ذات البنى التحتية الحساسة (NCNICC-1:2024) لتحقيق فضاء سيبراني سعودي آمن وموثوق يمكن النمو والازدهار. وتحدد ضوابط الأمن السيبراني لجهات القطاع الخاص من غير ذات البنى التحتية الحساسة ضوابط الأمن السيبراني الخاصة بالجهات الصغيرة والمتوسطة والكبيرة العاملة في المملكة، وتبين هذه الوثيقة تفاصيل هذه الضوابط، وأهدافها، ونطاق العمل وقابلية التطبيق، وآلية الالتزام ومتابعته.

هذا؛ وقد نُظمت ضوابط الأمن السيبراني لجهات القطاع الخاص من غير ذات البنى التحتية الحساسة، ضمن ثلاث مكونات: حوكمة الأمن السيبراني، وتعزيز الأمن السيبراني، والأمن السيبراني المتعلق بالأطراف الخارجية.

المقدمة

قامت الهيئة الوطنية للأمن السيبراني (ويشار لها في هذه الوثيقة بـ "الهيئة") بتطوير ضوابط الأمن السيبراني لجهات القطاع الخاص من غير ذات البنى التحتية الحساسة (NCNICC-1:2024) بعد دراسة شاملة، لأفضل ممارسات الأمن السيبراني، في الجهات الصغيرة، والمتوسطة، والكبيرة؛ التي أعدتها الجهات الوطنية والدولية. بالإضافة إلى ذلك، جرى تطوير ضوابط الأمن السيبراني لجهات القطاع الخاص من غير ذات البنى التحتية الحساسة ؛ بناء على الضوابط الأساسية للأمن السيبراني (ECC-1:2018) لتقديم نسخة أكثر ملائمة للجهات ضمن نطاق عمل الضوابط.

تنطبق ضوابط الأمن السيبراني لجهات القطاع الخاص من غير ذات البنى التحتية الحساسة على فئتين من الجهات؛ الأولى الجهات الكبيرة، والثانية الجهات الصغيرة، والمتوسطة، وذلك على النحو المحدد في الجدول (١). وتشمل ضوابط الأمن السيبراني لجهات القطاع الخاص من غير ذات

البنى التحتية الحساسة ما يلي:

فئة الجهة	عدد المكونات الأساسية والفرعية والضوابط الأساسية المطلوبة
الفئة ١ (S1): الجهات الكبيرة	• مكونان أساسيان • ١٥ مكونًا فرعيًا • ٢٧ ضابطًا أساسيًا
الفئة ٢ (S2): الجهات الصغيرة والمتوسطة	• مكون أساسي واحد • ٧ مكونات فرعية • ٧ ضوابط أساسية

جدول ١: المكونات والضوابط لضوابط الأمن السيبراني لجهات القطاع الخاص من غير ذات البنى التحتية الحساسة

الأهداف

تهدف هذه الوثيقة في الأساس، إلى وضع الحدّ الأدنى من ضوابط الأمن السيبراني لجهات القطاع الخاص من غير ذات البنى التحتية الحساسة. وتستند الضوابط إلى الممارسات الرائدة في القطاع؛ بما سيمكّن الجهات الخاصة من تقليل مخاطر الأمن السيبراني، التي تنشأ عن التهديدات الداخلية والخارجية. وتتطلب حماية الأصول المعلوماتية والتقنية للجهة التركيز على الأهداف الأساسية للحماية، وهي:

- سرية المعلومة (Confidentiality)
- سلامة المعلومة (Integrity)
- توافر المعلومة (Availability)

وتأخذ هذه الضوابط في الحسبان المحاور الثلاث الأساسية التي يرتكز عليها الأمن السيبراني، وهي:

- الأشخاص (People)
- الإجراء (Process)
- التقنية (Technology)

نطاق العمل وقابلية التطبيق

نطاق عمل ضوابط الأمن السيبراني لجهات القطاع الخاص من غير ذات البنى التحتية الحساسة

تُطبّق هذه الضوابط على الجهات الخاصة، الصغيرة والمتوسطة والكبيرة، في المملكة العربية السعودية (باستثناء جهات القطاع الخاص التي تمتلك بنى تحتية وطنية حساسة (Critical National Infrastructures "CNIs")) أو تقوم بتشغيلها أو استضافتها.

تستهدف ضوابط الأمن السيبراني لجهات القطاع الخاص من غير ذات البنى التحتية الحساسة فئتين: الفئة الأولى (الجهات الكبيرة) والفئة الثانية (الجهات الصغيرة والمتوسطة). وتستند الفئتان، ضمن ضوابط الأمن السيبراني لجهات القطاع الخاص من غير ذات البنى التحتية الحساسة؛ إلى حجم الجهة بالتوافق مع تعريف الهيئة العامة للمنشآت الصغيرة والمتوسطة (منشآت). ويبين الجدول (٢) الآتي فئات الجهات ذات الصلة بضوابط الأمن السيبراني لجهات القطاع الخاص من غير ذات البنى التحتية الحساسة.

فئة الجهة	التعريف	عدد المكونات الأساسية والفرعية والضوابط الأساسية المطلوبة
الفئة (١): الجهات الكبيرة	هي الجهات التي تضم أكثر من ٢٥٠ موظفًا؛ أو تحقق أكثر من ٢٠٠ مليون ريال سعودي من الإيرادات السنوية.	• مكونان اثنان • ١٥ مكونًا فرعيًا • ٢٧ ضابطًا أساسيًا
الفئة (٢): الجهات الصغيرة والمتوسطة	هي الجهات التي تضم ما يتراوح بين ٦ إلى ٢٤٩ موظفًا؛ أو تحقق ما بين ٣ إلى ٢٠٠ مليون ريال سعودي من الإيرادات السنوية.	• مكون واحد • ٧ مكونات فرعية • ٧ ضوابط أساسية

جدول ٢: فئات الجهات ذات الصلة بضوابط الأمن السيبراني لجهات القطاع الخاص من غير ذات البنى التحتية الحساسة

تعد الضوابط الخاصة بالفئة (١) ملزمة للجهات الكبيرة؛ في حين تعد ضوابط الفئة (٢) ملزمة للجهات الصغيرة والمتوسطة. وتشجع الهيئة، الجهات الصغيرة، والمتوسطة، في المملكة بشدة على الاستفادة من ضوابط الفئة (١) لتطبيق أفضل الممارسات؛ فيما يتعلق بتحسين الأمن السيبراني ونضجه داخل الجهة.

كما تشجع الهيئة بشدة جميع الجهات الأخرى في المملكة، خارج نطاق عمل ضوابط الهيئة (مثل: الجهات متناهية الصغر، والجهات غير الربحية) على الاستفادة من هذه الضوابط؛ لتطبيق أفضل الممارسات، فيما يتعلق بتحسين الأمن السيبراني وتطويره داخل الجهة.

قابلية التطبيق داخل الجهة

جرى إعداد هذه الضوابط، بحيث تكون ملائمة لاحتياجات الأمن السيبراني لجميع الجهات الصغيرة، والمتوسطة، والكبيرة، في المملكة العربية السعودية.

وتعتمد قابلية تطبيق ضوابط الأمن السيبراني هذه، على نوع فئة الجهة، كما هو محدد في الجدول (٢) مثال:

- الضوابط ضمن المكون الفرعي رقم (٢-٣) حماية الأنظمة وأجهزة معالجة المعلومات؛ تكون قابلة للتطبيق، وملزمة على الجهات الكبيرة (الفئة ١) بالإضافة إلى الجهات الصغيرة، والمتوسطة (الفئة ٢).
- الضوابط ضمن المكون الفرعي رقم (٢-١) المتعلقة بإدارة الأصول؛ تكون قابلة للتطبيق، وملزمة على الجهات الكبيرة (الفئة ١).

التنفيذ والالتزام

تحقيقًا لما ورد في الفقرة الثالثة من المادة العاشرة في تنظيم الهيئة الوطنية للأمن السيبراني؛ فإنه يجب على جميع الجهات، ضمن نطاق عمل هذه الضوابط؛ تنفيذ ما يحقق الالتزام الدائم والمستمر. وتحتفظ الهيئة بالحقّ في إجراء عمليات التدقيق لقياس التزام الجهات بالضوابط القابلة للتطبيق، وذلك وفقًا لما تراه مناسبًا.

تقوم الهيئة بتقييم التزام الجهات بما ورد في هذه الضوابط، بطرق متعددة، منها؛ التقييمات الخارجية التي يقدمها مقدم خدمات تقييم الالتزام، المرخص من الهيئة الوطنية للأمن السيبراني، وذلك وفق الآلية التي تراها الهيئة مناسبة لذلك.

التحديث والمراجعة

تتولى الهيئة التحديث والمراجعة الدورية، لضوابط الأمن السيبراني لجهات القطاع الخاص من غير ذات البنى التحتية الحساسة؛ حسب متطلبات الأمن السيبراني والمستجدات ذات العلاقة. كما تتولى الهيئة إعلان الإصدار المحدث من الضوابط ونشره، لتطبيقه والالتزام به.

مكونات وهيكلية ضوابط الأمن السيبراني لجهات القطاع الخاص من غير ذات البنى التحتية الحساسة

المكونات الأساسية

يبين الشكل (١) الآتي المكونات الأساسية للضوابط.

شكل ١: المكونات الأساسية للضوابط

المكونات الفرعية

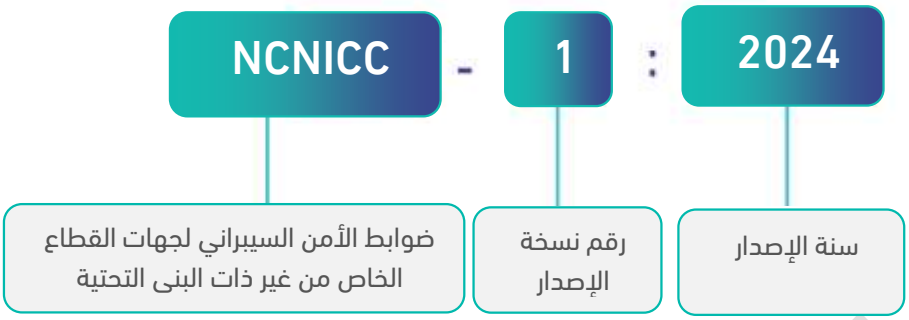
يبين الجدول (٣) الآتي المكونات الفرعية للضوابط.

١. حوكمة الأمن السيبراني	١-١	إدارة الأمن السيبراني	١-٢	سياسات وإجراءات الأمن السيبراني
	١-٣	المراجعة والتدقيق الدوري للأمن السيبراني	١-٤	برنامج التوعية والتدريب بالأمن السيبراني
٢. تعزيز الأمن السيبراني	٢-١	إدارة الأصول	٢-٢	إدارة هويات الدخول والصلاحيات
	٢-٣	حماية الأنظمة وأجهزة معالجة المعلومات	٢-٤	حماية البريد الإلكتروني
	٢-٥	إدارة أمن الشبكات	٢-٦	التشفير
	٢-٧	إدارة النسخ الاحتياطية	٢-٨	إدارة الثغرات
	٢-٩	اختبار الاختراق	٢-١٠	إدارة سجلات الأحداث ومراقبة الأمن السيبراني
	٢-١١	إدارة حوادث وتهديدات الأمن السيبراني	٢-١٢	الأمن المادي
٣. الأمن السيبراني المتعلق بالأطراف الخارجية	٣-١	الأمن السيبراني المتعلق بالأطراف الخارجية		

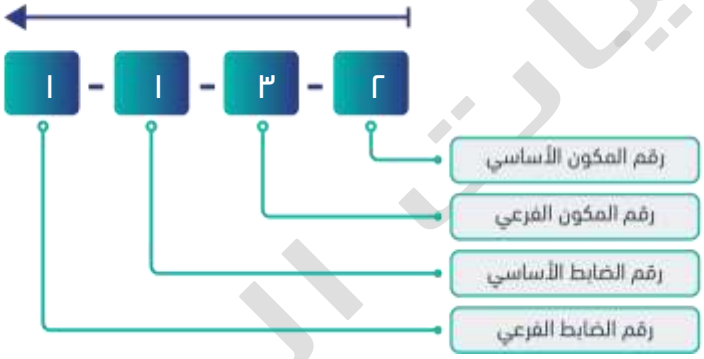
جدول ٣: المكونات الفرعية للضوابط

الهيكلية

يبين الشكلان ٢ و٣ الآتيان معنى رموز الضوابط.



شكل ٢: معنى رموز الضوابط



شكل ٣: هيكلية الضوابط

١		اسم المكون الأساسي
رقم مرجعي للمكون الأساسي		
رقم مرجعي للمكون الفرعي		اسم المكون الفرعي
الهدف		
الضوابط		قابلية تطبيق الضابط
		الفئة (١) / الفئة (٢)
رقم مرجعي للضابط	بنود الضابط	

الجدول ٤: هيكلية الضوابط

تعتمد قابلية تطبيق الضابط على فئة الجهة، وتمّت الإشارة إلى ذلك في كل ضابط، كما هو مبين في الجدول (٥).

قابلية تطبيق الضابط	الوصف
مطلوب	يعد الضابط ملزمًا لفئة الجهة أو يحتوي على ضابط واحد أو أكثر من الضوابط الفرعية ملزمًا للفئة.
موصى به	لا يعد الضابط ملزمًا لفئة الجهة، ولكنها تُشجّع الجهة على تطبيقه

جدول ٥: دليل رموز قابلية تطبيق الضوابط

ضوابط الأمن السيبراني لجهات القطاع الخاص من غير ذات البنى التحتية الحساسة

١ حوكمة الأمن السيبراني (Cybersecurity Governance)

١-١	إدارة الأمن السيبراني		
الهدف	ضمان دعم القيادة في تنفيذ برامج الأمن السيبراني، وإدارتها داخل الجهة.		
الضوابط		قابلية تطبيق الضابط	
		الفئة (١)	الفئة (٢)
١-١-١	يجب إنشاء قسم مختص بالأمن السيبراني في الجهة، ويكون هذا القسم مستقلًا عن قسم تقنية المعلومات.	مطلوب	موصى به
١-٢	سياسات وإجراءات الأمن السيبراني		
الهدف	ضمان توثيق متطلبات الأمن السيبراني ونشرها، والتزام الجهة بها.		
الضوابط		قابلية تطبيق الضابط	
		الفئة (١)	الفئة (٢)
١-٢-١	يجب تحديد سياسات الأمن السيبراني الخاصة بالموظفين، وتوثيقها، واعتمادها. كما يجب نشرها على ذات العلاقة من العاملين في الجهة (مثل: سياسة الأمن السيبراني).	مطلوب	موصى به
١-٢-٢	يجب على الإدارة المعنية بالأمن السيبراني، ضمان تطبيق سياسات الأمن السيبراني في الجهة.	مطلوب	موصى به
١-٣	المراجعة والتدقيق الدوري للأمن السيبراني		
الهدف	ضمان التأكد، من أن ضوابط الأمن السيبراني لدى الجهة؛ مطبقة، وتعمل وفقًا للسياسات والإجراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية الوطنية الصادرة من الهيئة الوطنية للأمن السيبراني ، والمتطلبات الدولية المقرّة تنظيمياً على الجهة.		
الضوابط		قابلية تطبيق الضابط	
		الفئة (١)	الفئة (٢)
١-٣-١	يجب مراجعة ضوابط الأمن السيبراني وتدقيقها، من قبل مقدم خدمات تقييم الالتزام المرخص من الهيئة؛ لتقييم التزام الجهة ضوابط الأمن السيبراني لجهات القطاع الخاص من غير ذات البنى التحتية الحساسة (بحسب المدة الزمنية المطلوبة).	مطلوب (كل ٣ سنوات)	موصى به

٤-١	برنامج التوعية والتدريب بالأمن السيبراني		
الهدف	ضمان التأكد من أن العاملين بالجهة، لديهم التوعية الأمنية اللازمة، وعلى دراية بمسؤولياتهم في مجال الأمن السيبراني.		
الضوابط		قابلية تطبيق الضابط	
		الفئة (١)	الفئة (٢)
١-٤-١	يجب أن تشتمل برامج التوعية بالأمن السيبراني، على الموضوعات الرئيسية، ذات الصلة (مثل: التصيد الإلكتروني، وبرامج الفدية، وكلمات المرور القوية، واتباع أفضل الممارسات على وسائل التواصل الاجتماعي، والإبلاغ عن الحوادث والسلوكيات المشبوهة) ويجب أن تكون مخصصة، حسب مهمات الموظفين واحتياجاتهم.	مطلوب	موصى به
٢-٤-١	يجب تطبيق برنامج التوعية بالأمن السيبراني.	مطلوب	موصى به

٢ تعزيز الأمن السيبراني (Cybersecurity Defense)

١-٢	إدارة الأصول		
الهدف	التأكد من أن الجهة، لديها قائمة جرد دقيقة، وحديثة، للأصول تشمل التفاصيل ذات العلاقة، لجميع الأصول المعلوماتية، والتقنية، المتاحة للجهة، من أجل دعم العمليات التشغيلية للجهة، ومتطلبات الأمن السيبراني؛ لتحقيق سرية الأصول المعلوماتية والتقنية للجهة وسلامتها، ودقتها وتوافرها.		
الضوابط		قابلية تطبيق الضابط	
		الفئة (١)	الفئة (٢)
١-١-٢	يجب تحديد متطلبات الأمن السيبراني لإدارة الأصول المعلوماتية والتقنية للجهة وتوثيقها واعتمادها.	مطلوب	موصى به
٢-١-٢	يجب تطبيق متطلبات الأمن السيبراني لإدارة الأصول المعلوماتية والتقنية للجهة.	موصى به	موصى به
٢-٢	إدارة هويات الدخول والصلاحيات		
الهدف	ضمان حماية الأمن السيبراني للوصول المنطقي (Logical Access) إلى الأصول المعلوماتية والتقنية للجهة؛ من أجل منع الوصول غير المصرح به، وتقييد الوصول إلى ما هو مطلوب لإنجاز الأعمال المتعلقة بالجهة.		
الضوابط		قابلية تطبيق الضابط	
		الفئة (١)	الفئة (٢)

٢-٢-١	يجب تحديد متطلبات الأمن السيبراني لإدارة هويات الدخول والصلاحيات في الجهة وتوثيقها واعتمادها، ويجب أن تغطي بحدّ أدنى ما يلي:	مطلوب	مطلوب
	٢-٢-١-١ التحقق من هوية المستخدم (User Authentication) بناءً على إدارة اسم المستخدم، وكلمة مرور آمنة.	مطلوب	مطلوب
	٢-٢-١-٢ التحقق من الهوية متعدد العناصر (Multi-Factor Authentication) لعمليات الدخول عن بعد والتطبيقات الخارجية.	مطلوب	موصى به
	٢-٢-١-٣ إدارة تصاريح المستخدمين وصلاحياتهم (Authorization) بناءً على مبادئ التحكم بالدخول والصلاحيات: مبدأ الحاجة إلى المعرفة والاستخدام (Need-to-Know and Need-to-Use) ومبدأ الحد الأدنى من الصلاحيات والامتيازات (Least Privilege) ومبدأ فصل المهام (Segregation of Duties).	مطلوب	موصى به
	٢-٢-١-٤ إدارة الصلاحيات الهامة والحساسة (Privileged Access Management).	مطلوب	موصى به
	٢-٢-١-٥ المراجعة الدورية لهويات الدخول والصلاحيات.	مطلوب	موصى به
٢-٢-٢	يجب تطبيق متطلبات الأمن السيبراني، لإدارة هويات الدخول والصلاحيات في الجهة.	مطلوب	موصى به
٢-٣	حماية الأنظمة وأجهزة معالجة المعلومات		
الهدف	ضمان حماية الأنظمة، وأجهزة معالجة المعلومات؛ بما في ذلك أجهزة المستخدمين، والخوادم وأجهزة الشبكة للجهة، من المخاطر السيبرانية.		
الضوابط		قابلية تطبيق الضابط	
		الفئة (١)	الفئة (٢)
٢-٣-١	يجب تحديد متطلبات الأمن السيبراني وتوثيقها واعتمادها لحماية الأنظمة، وأجهزة معالجة المعلومات للجهة، ويجب أن تغطي بحد أدنى ما يلي:	مطلوب	مطلوب
	٢-٣-١-١ الحماية من الفيروسات، والبرامج، والأنشطة المشبوهة، والبرمجيات الضارة (Malware) على الخوادم، وأجهزة المستخدمين والأجهزة المحمولة، باستخدام تقنيات الحماية الحديثة وآلياتها (مثل الفحص الآلي، والتحديث الآلي) وإدارتها بشكل آمن.	مطلوب	مطلوب

	٢-٣-١-٢ تغيير الإعدادات الافتراضية/ الضعيفة (مثل إلغاء تنشيط الخدمات غير الضرورية. تغيير كلمات المرور الافتراضية، وتقييد استخدام الوسائط القابلة للإزالة).	مطلوب	مطلوب
٢-٣-٢	يجب تطبيق متطلبات الأمن السيبراني لحماية الأنظمة، وأجهزة معالجة المعلومات للجهة.	مطلوب	مطلوب
٢-٤	حماية البريد الإلكتروني		
الهدف	ضمان حماية البريد الإلكتروني للجهة من المخاطر السيبرانية.		
الضوابط		قابلية تطبيق الضابط	
		الفئة (١)	الفئة (٢)
٢-٤-١	يجب تحديد متطلبات الأمن السيبراني وتوثيقها واعتمادها لحماية البريد الإلكتروني للجهة، كما يجب أن تغطي بحد أدنى ما يلي:	مطلوب	موصى به
	٢-٤-١-١ تحليل (Filtering) رسائل البريد الإلكتروني وتصفيتها (وبالذات رسائل التصيد الإلكتروني (Phishing Emails) والرسائل الاقتحامية (Spam Emails) باستخدام تقنيات وآليات الحماية الحديثة للبريد الإلكتروني.	مطلوب	موصى به
	٢-٤-١-٢ توثيق مجال البريد الإلكتروني للجهة من خلال منصة حصين باستخدام إطار سياسة المرسل (Sender Policy Framework "SPF") والبريد المعرف بمفاتيح النطاق (Domain Keys Identified Mail "DKIM") وسياسة مصادقة الرسائل والإبلاغ عنها (Domain Message Authentication Reporting and Conformance "DMARC").	مطلوب	موصى به
٢-٤-٢	يجب تطبيق متطلبات الأمن السيبراني، الخاصة بحماية البريد الإلكتروني للجهة.	مطلوب	موصى به
٢-٥	إدارة أمن الشبكات		
الهدف	ضمان حماية شبكات الجهة من المخاطر السيبرانية.		
الضوابط		قابلية تطبيق الضابط	
		الفئة (١)	الفئة (٢)
٢-٥-١	يجب تحديد متطلبات الأمن السيبراني وتوثيقها واعتمادها لإدارة أمن شبكات الجهة. ويجب أن تغطي بحد أدنى ما يلي:	مطلوب	مطلوب
	٢-٥-١-١ استخدام جدران الحماية للشبكة، وبوابات الوصول الآمنة.	مطلوب	مطلوب

	٢-٥-١-٢ العزل، والتقسيم المادي، أو المنطقي، لأجزاء الشبكات بشكل آمن.	موصى به	موصى به
	٢-٥-١-3 أمن الشبكات اللاسلكية، وحمايتها، باستخدام وسائل آمنة؛ للتحقق من الهوية والتشفير.	مطلوب	مطلوب
٢-٥-٢	يجب تطبيق، متطلبات الأمن السيبراني، لإدارة أمن شبكات الجهة.	مطلوب	موصى به
٢-٦	التشفير		
الهدف	ضمان الاستخدام السليم والفعال للتشفير؛ لحماية الأصول المعلوماتية الإلكترونية للجهة.		
الضوابط		قابلية تطبيق الضابط	
		الفئة (١)	الفئة (٢)
٢-٦-١	يجب تحديد متطلبات الأمن السيبراني للتشفير وتوثيقها واعتمادها في الجهة، ويجب أن تغطي في حدها الأدنى ما يلي:	مطلوب	موصى به
	٢-٦-١-١ استخدام تشفير البيانات أثناء التخزين والنقل.	موصى به	موصى به
	٢-٦-١-٢ استخدام أساليب وخوارزميات تشفير، آمنة وحديثة، عند إنشاء البيانات وتخزينها ونقلها، وكذلك الأمر مع جميع وسائط اتصالات الشبكة، وحسب متطلبات "المستوى المتوسط" في معايير التشفير الوطنية (NCS-1:2020).	مطلوب	موصى به
٢-٦-٢	يجب تطبيق متطلبات الأمن السيبراني للتشفير في الجهة.	مطلوب	موصى به
٢-٧	إدارة النسخ الاحتياطية		
الهدف	ضمان حماية بيانات الجهة ومعلوماتها والإعدادات التقنية للأنظمة والتطبيقات الخاصة بالجهة من الأضرار غير المتوقعة.		
الضوابط		قابلية تطبيق الضابط	
		الفئة (١)	الفئة (٢)
٢-٧-١	يجب تحديد متطلبات الأمن السيبراني لإدارة النسخ الاحتياطية للجهة وتوثيقها واعتمادها، ويجب أن تغطي بحد أدنى ما يلي:	مطلوب	مطلوب
	٢-٧-١-١ نسخ احتياطية للأنظمة الأعمال الحساسة.	مطلوب	مطلوب
	٢-٧-١-٢ إجراء فحص دوري؛ للتأكد من فعالية استعادة النسخ الاحتياطية.	مطلوب	موصى به
٢-٧-٢	يجب تطبيق متطلبات الأمن السيبراني لإدارة النسخ الاحتياطية للجهة.	مطلوب	موصى به
٢-٨	إدارة الثغرات		

الهدف	ضمان اكتشاف الثغرات التقنية في الوقت المناسب، ومعالجتها بشكل فعال؛ وذلك لمنع احتمالية استغلال هذه الثغرات من قبل الهجمات السيبرانية أو تقليلها، وتقليل الآثار المترتبة على أعمال الجهة.		
الضوابط		قابلية تطبيق الضابط	
		الفئة (١)	الفئة (٢)
١-٨-٢	يجب تحديد متطلبات الأمن السيبراني لإدارة الثغرات التقنية للجهة وتوثيقها واعتمادها، ويجب أن تغطي بحد أدنى ما يلي:	مطلوب	مطلوب
	١-١-٨-٢ تحديث الأنظمة والبرمجيات والأجهزة وإصلاحها بانتظام.	مطلوب	مطلوب
	٢-١-٨-٢ فحص الثغرات واكتشافها دورياً.	مطلوب	موصى به
	٣-١-٨-٢ معالجة الثغرات؛ بما في ذلك اختبار إصلاحات الثغرات وتثبيتها.	مطلوب	موصى به
٢-٨-٢	يجب تطبيق متطلبات الأمن السيبراني لإدارة الثغرات التقنية للجهة.	مطلوب	موصى به
٩-٢	اختبار الاختراق		
الهدف	اختبار مدى فعالية قدرات تعزيز الأمن السيبراني في الجهة وتقييمها؛ وذلك من خلال عمل محاكاة لتقنيات الهجوم السيبراني الفعلية وأساليبها، ولاكتشاف نقاط الضعف الأمنية، غير المعروفة، في البنية التّحتية الفنية، والتي قد تؤدي إلى الاختراق السيبراني للجهة.		
الضوابط		قابلية تطبيق الضابط	
		الفئة (١)	الفئة (٢)
١-٩-٢	يجب تحديد متطلبات الأمن السيبراني لعمليات اختبار الاختراق في الجهة وتوثيقها واعتمادها، ويجب أن تغطي في الحد الأدنى نطاق عمل اختبار الاختراق؛ ليشمل جميع الخدمات المقدمة خارجيا (عن طريق الإنترنت) ومكوناتها التقنية؛ ومنها: البنية التحتية، المواقع الإلكترونية، تطبيقات الويب، تطبيقات الهواتف المحمولة، البريد الإلكتروني والدخول عن بعد.	مطلوب	موصى به
٢-٩-٢	يجب تطبيق متطلبات الأمن السيبراني لعمليات اختبار الاختراق في الجهة.	مطلوب	موصى به
١٠-٢	إدارة سجلات الأحداث ومراقبة الأمن السيبراني		
الهدف	ضمان تجميع سجلات أحداث الأمن السيبراني في الوقت المناسب وتحليلها ومراقبتها؛ من أجل الاكتشاف الاستباقي للهجمات السيبرانية المحتملة أو لتحليلها بعد وقوعها.		
الضوابط		قابلية تطبيق الضابط	
		الفئة (١)	الفئة (٢)

٢-١٠-١	يجب تحديد متطلبات إدارة سجلات الأحداث وتوثيقها واعتمادها، ومراقبة الأمن السيبراني للجهة، ويجب أن تغطي هذه العمليات بحد أدنى ما يلي:	مطلوب	موصى به
	٢-١٠-١-١ تفعيل سجلات الأحداث (Event logs) الخاصة بالأمن السيبراني، على الأصول المعلوماتية الحساسة، لدى الجهة.	مطلوب	موصى به
	٢-١٠-١-٢ الاشتراك لدى مقدم خدمات مركز عمليات الأمن السيبراني المدار، المرخص له من قبل الهيئة.	مطلوب	موصى به
٢-١٠-٢	يجب تطبيق متطلبات إدارة سجلات الأحداث، ومراقبة الأمن السيبراني في الجهة دورياً.	مطلوب	موصى به
٢-١١	إدارة حوادث وتهديدات الأمن السيبراني		
الهدف	ضمان تحديد واكتشاف حوادث الأمن السيبراني في الوقت المناسب وإدارتها والتعامل معها بشكل فعّال.		
الضوابط		قابلية تطبيق الضابط	
		الفئة (١)	الفئة (٢)
٢-١١-١	يجب تحديد متطلبات إدارة حوادث وتهديدات الأمن السيبراني في الجهة وتوثيقها واعتمادها، ويجب أن تغطي هذه العمليات بحد أدنى ما يلي:	مطلوب	مطلوب
	٢-١١-١-١ وضع الخطط التفصيلية للاستجابة لحوادث الأمن السيبراني المرتبطة باختراق البيانات، وفيروس الفدية، وآليات التصعيد ذات الصلة.	موصى به	موصى به
	٢-١١-١-٢ تبليغ الهيئة، عند حدوث حادثة أمن سيبراني.	مطلوب	مطلوب
	٢-١١-١-٣ المساهمة في مشاركة معلومات الأمن السيبراني مع الهيئة.	مطلوب	موصى به
٢-١١-٢	يجب تطبيق متطلبات إدارة حوادث الأمن السيبراني وتهديداتها في الجهة دورياً.	مطلوب	موصى به
٢-١٢	الأمن المادي		
الهدف	ضمان حماية الأصول المعلوماتية والتقنية للجهة؛ من الوصول المادي غير المصرح به، والفقدان، والسرقة، والتخريب.		
الضوابط		قابلية تطبيق الضابط	
		الفئة (١)	الفئة (٢)

٢-١٢-١	يجب تحديد متطلبات الأمن السيبراني وتوثيقها واعتمادها للأمن المادي للأصول المعلوماتية والتقنية للجهة، ويجب أن تغطي هذه العمليات بحد أدنى ما يلي:	موصى به	موصى به
	٢-١٢-١-١ أمن إتلاف الأصول المادية وإعادة استخدامها (وتشمل: الوثائق الورقية، ووسائط الحفظ والتخزين).	موصى به	موصى به
	٢-١٢-١-٢ حماية الوصول المادي إلى غرف تقنية المعلومات/ الأجهزة الإلكترونية الحساسة/ الأجهزة الطرفية المحمولة، أو الوثائق.	موصى به	موصى به
٢-١٢-٢	يجب تطبيق متطلبات الأمن السيبراني للأمن المادي للأصول المعلوماتية والتقنية للجهة.	موصى به	موصى به

٣ الأمن السيبراني المتعلق بالأطراف الخارجية (Third-Party Cybersecurity)

٣-١	الأمن السيبراني المتعلق بالأطراف الخارجية	
الهدف	ضمان حماية أصول الجهة، من مخاطر الأمن السيبراني، المتعلقة بالأطراف الخارجية؛ بما في ذلك خدمات الإسناد لتقنية المعلومات (Outsourcing) والخدمات المدارة (Managed Services).	
الضوابط		قابلية تطبيق الضابط
		الفئة (١) / الفئة (٢)
٣-١-١	يجب تحديد متطلبات الأمن السيبراني وتوثيقها واعتمادها ضمن العقود والاتفاقيات، مع الأطراف الخارجية للجهة. ويجب أن تحتوي في الحد الأدنى على المحافظة على سرية المعلومات.	موصى به / موصى به

ملاحق

ملحق (أ): مصطلحات وتعريفات

يبين الجدول ٦ الآتي؛ بعض المصطلحات، وتعريفاتها، التي ورد ذكرها في هذه الوثيقة.

المصطلح	التعريف
الأصل	أي شيء ملموس، أو غير ملموس؛ له قيمة بالنسبة للجهة. وهناك أنواع كثيرة من الأصول؛ بعضها يتضمن أشياء واضحة؛ مثل: الأشخاص، والآلات، والمرافق، وبراءات الاختراع، والبرمجيات والخدمات. ويمكن أن يشمل المصطلح أيضاً أشياء أقل وضوحاً؛ مثل: المعلومات والخصائص (سمعة الجهة وصورتها العامة، أو المهارة والمعرفة).
هجوم	أي نوع من الأنشطة الخبيثة، التي تحاول الوصول بشكل غير مشروع، أو جمع موارد النظم المعلوماتية، أو المعلومات نفسها، أو تعطيلها، أو منعها، أو تحطيمها، أو تدميرها.
تدقيق	المراجعة المستقلة، ودراسة السجلات والأنشطة؛ لتقييم مدى فعالية ضوابط الأمن السيبراني، ولضمان الالتزام بالسياسات، والإجراءات التشغيلية، والمعايير والمتطلبات التشريعية والتنظيمية ذات العلاقة.
التحقق	التأكد من هوية المستخدم، أو العملية أو الجهاز. وغالباً ما يكون هذا الأمر شرطاً أساسياً، للسماح بالوصول، إلى الموارد في النظام.
صلاحية المستخدم	خاصية التحديد والتأكد من حقوق / صلاحية المستخدم، للوصول إلى الموارد والأصول المعلوماتية والتقنيةللجهة، والسماح له، وفقاًلما حدد مسبقاً في حقوق /صلاحياتالمستخدم .
توافر المعلومة (Availability)	ضمان الوصول إلى المعلومات، والبيانات، والأنظمة، والتطبيقات، واستخدامها في الوقت المناسب.
النسخ الاحتياطية	هو نسخ الملفات، والأجهزة والبيانات والإجراءات المتاحة للاستخدام في حالة الأعطال أو الفقدان، أو إذا حذف الأصل منها أو توقف عن الخدمة.
سرية المعلومة (Confidentiality)	الاحتفاظ بقيود مصرح للوصول إلى المعلومات، والإفصاح عنها، بما في ذلك وسائل حماية معلومات الخصوصية، والملكية الشخصية.

المصطلح	التعريف
التشفير	(ويسمى أيضاً علم التشفير) وهي القواعد التي تشتمل على مبادئ ووسائل وطرق تخزين البيانات أو المعلومات ونقلها، في شكل معين وذلك من أجل إخفاء محتواها الدلالي، ومنع الاستخدام غير المصرح به أو منع التعديل غير المكتشف، بحيث لا يمكن لغير الأشخاص المعنيين قراءتها ومعالجتها.
الهجوم السيبراني	الاستغلال المتعمّد لأنظمة الحاسب الآلي، والشبكات، والجهات التي يعتمد عملها على تقنية المعلومات، والاتصالات الرقمية؛ بهدف إحداث أضرار.
المخاطر السيبرانية	المخاطر التي تؤثر على عمليات أعمال الجهة، (بما في ذلك رؤية الجهة، أو رسالتها، أو إداراتها، أو صورتها، أو سمعتها) أو أصول الجهة، أو الأفراد، أو الجهات الأخرى، أو الدولة، بسبب إمكانية الوصول غير المصرح به، أو الاستخدام، أو الإفصاح، أو التعطيل، أو التعديل، أو تدمير المعلومات و/أو نظم المعلومات.
الأمن السيبراني	حسب ما نص عليه تنظيم الهيئة الصادر بالأمر الملكي رقم(٦٨٠١) وتاريخ (١١/ ٢/١٤٣٩ هـ)، فإن الأمن السيبراني يتمثل في حماية الشبكات وأنظمة تقنية المعلومات، وأنظمة التقنيات التشغيلية، ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات، وما تحتويه 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.
فعالية	تشير الفعالية إلى الدرجة التي يتم بها تحقيق تأثير مخطط له. وتعد الأنشطة المخططة فعالة؛ إذا جرى تنفيذ هذه الأنشطة بالفعل، وتعد النتائج المخطط لها فعالة؛ إذا تم تحقيق هذه النتائج بالفعل. يمكن استخدام مؤشرات قياس الأداء (Key Performance Indicators KPIs) لقياس وتقييم مستوى الفعالية.
حدث	أمر يحدث في مكان محدد (مثل الشبكة والأنظمة والتطبيقات وغيرها) وفي وقت محدد.
حصين	البوابة الوطنية لخدمات الأمن السيبراني.
هوية	وسيلة التحقق من هوية المستخدم، أو العملية، أو الجهاز. وهي عادة شرط أساسي لمنح حق الوصول إلى الموارد في النظام.
حادثة	انتهاك أمني بمخالفة سياسات الأمن السيبراني، أو سياسات الاستخدام المقبول، أو متطلبات الأمن السيبراني أو ممارساته أو ضوابطه.

المصطلح	التعريف
سلامة المعلومة (Integrity)	الحماية ضد تعديل المعلومات أو تخريبها بشكل غير مصرح به. وتتضمن ضمان عدم الإنكار للمعلومات (Non-Repudiation) والموثوقية.
الحد الأدنى من الصلاحيات	مبدأ أساسي في الأمن السيبراني، يهدف إلى منح المستخدمين صلاحيات الوصول، التي يحتاجونها لتنفيذ مسؤولياتهم الرسمية فحسب.
البرمجيات الضارة	برنامج يصيب الأنظمة بطريقة خفية (في الغالب) لانتهاك سرية البيانات أو التطبيقات أو نظم التشغيل أو سلامتها ودقتها أو توافرها.
التحقق من الهوية متعدد العناصر (MFA)	نظام أمني يتحقق من هوية المستخدم؛ يتطلب استخدام عدة عناصر مستقلة من آليات التحقق من الهوية. تتضمن آليات التحقق عدة عناصر: • المعرفة (أمر يعرفه المستخدم فحسب (مثل كلمة المرور)). • الحيازة (أمر يملكه المستخدم فحسب "مثل برنامج أو جهاز توليد أرقام عشوائية أو الرسائل القصيرة المؤقتة، لتسجيل الدخول، ويطلق عليها: (One-Time-Password). • الملازمة (صفة أو سمة حيوية متعلقة بالمستخدم نفسه فحسب (مثل بصمة الإصبع)).
الحاجة إلى المعرفة والحاجة إلى الاستخدام	القيود المفروضة على البيانات، وهي تعد حساسة، ما لم يكن لدى الشخص حاجة محددة للاطلاع على البيانات لغرض ما متعلق بأعمال ومهمات رسمية.
الجهة	جهات القطاع الخاص؛ بما في ذلك الشركات الصغيرة والمتوسطة والكبيرة، باستثناء الجهات متناهية الصغر، والجهات غير الحكومية، والقطاع الحكومي، والبنى التحتية الوطنية الحساسة.
الاسناد الخارجي	الحصول على (السلع أو الخدمات) عن طريق التعاقد، مع مورد، أو مزود خدمة.
حزم التحديثات والإصلاحات	حزم بيانات داعمة لتحديث نظام التشغيل للحاسب الآلي أو إصلاحه أو تحسينه أو دعم لتطبيقاته أو برامجه. وهذا يشمل إصلاح الثغرات الأمنية وغيرها من الأخطاء، إذ تسمى هذه الحزم عادةً (إصلاحات) أو (إصلاح الأخطاء، وتحسين إمكانية الاستخدام أو الأداء).

المصطلح	التعريف
رسائل التصيّد الإلكتروني	محاولة الحصول على معلومات حساسة؛ مثل أسماء المستخدمين، وكلمات المرور، أو تفاصيل بطاقة الائتمان، ويكون ذلك غالباً لأسباب ونوايا ضارة وخبيثة، يتحقق بالتنكر على هيئة جهة جديرة بالثقة في رسائل بريد إلكترونية.
الأمن المادي	يصف الأمن المادي، التدابير الأمنية، التي جرى تصميمها؛ لمنع الوصول غير المصرح به إلى المرافق والمعدات والموارد التابعة للجهة، وحماية الأفراد والممتلكات من التلف أو الضرر (مثل التجسس أو السرقة، أو الهجمات الإرهابية). وينطوي الأمن المادي على استخدام طبقات متعددة من نظم مترابطة، تشمل الدوائر التلفزيونية المغلقة (CCTV) وحراس الأمن، والحدود الأمنية، والأقفال، وأنظمة التحكم في الوصول، والعديد من التقنيات الأخرى.
سياسة	وثيقة تحدد بنودها التز اماً عاماً أو توجيهاً أو نية؛ ما كما جرى التعبير عن ذلك رسمياً، من قبل صاحب الصلاحية للجهة. وسياسة الأمن السيبراني هي وثيقة تعبر بنودها عن الالتزام الرسمي للإدارة العليا للجهة، بتنفيذ وتحسين برنامج الأمن السيبراني في الجهة، وتشتمل السياسة على أهداف الجهة فيما يتعلق ببرنامج الأمن السيبراني وضوابطه، ومتطلباته، وآلية تحسينه وتطويره.
إدارة الصلاحيات الهامة والحساسة	عملية إدارة الصلاحيات ذات الخطورة العالية على أنظمة الجهة، والتي تحتاج في الغالب إلى تعامل خاص؛ لتقليل المخاطر، التي قد تنشأ من سوء استخدامها.
إجراء	وثيقة تحتوي على وصف تفصيلي، للخطوات الضرورية، لأداء عمليات أو أنشطة محددة، في الالتزام بالمعايير، والسياسات ذات العلاقة. وتعرّف الإجراءات على أنها جزء من العمليات.
عملية	مجموعة من الأنشطة المترابطة أو التفاعلية، تحول المدخلات إلى مخرجات. وهذه الأنشطة، متأثرة بسياسات الجهة.
الاستعادة	إجراء أو عملية لاستعادة منقطع أو تالف أو مسروق أو ضائع أو التحكم فيه.

المصطلح	التعريف
فصل المهمات	مبدأ أساسي في الأمن السيبراني؛ يهدف إلى تقليل الأخطاء، والاحتيال، خلال مراحل تنفيذ عملية محددة؛ عن طريق التأكد، من ضرورة وجود أكثر من شخص؛ لإكمال هذه المراحل، وبصلاحيات مختلفة.
طرف خارجي	أي جهة تعمل على أنها طرف في علاقة تعاقدية لتقديم السلع، أو الخدمات (وهذا يشمل موردي الخدمات ومزوديها).
تهديد	أي ظرف أو حدث، من المحتمل أن يؤثر سلباً، على أعمال الجهة (بما في ذلك مهمتها، أو وظائفها، أو مصداقيتها، أو سمعتها) أو أصولها، أو منسوبيها، مستغلًا أحد أنظمة المعلومات؛ عن طريق الوصول غير المصرح به إلى المعلومات أو تدميرها أو كشفها أو تغييرها أو حجب الخدمة. وأيضاً قدرة مصدر التهديد على النجاح في استغلال إحدى نقاط الضعف الخاصة بنظام معلومات معين. وهذا التعريف يشمل التهديدات السيبرانية.
الثغرة	أي نوع من نقاط الضعف في نظام الحاسب الآلي؛ أو برامجه، أو تطبيقاته، أو في مجموعة من الإجراءات؛ أو في أي شيء يجعل الأمن السيبراني عرضة للتهديد.

الجدول (٦): مصطلحات وتعريفات

ملحق (ب): قائمة الاختصارات

يوضح الجدول (٧) الآتي معنى الاختصارات التي ورد ذكرها في هذه الوثيقة.

الاختصار	معناه
CNI	Critical National Infrastructure البنية التحتية الحساسة
DKIM	Domain Keys Identified Mail البريد المحدد بمفاتيح المجال
DMARC	Domain Message Authentication, Reporting and Conformance إعداد التقارير والتوافق المستندة إلى المجال
ECC	Essential Cybersecurity Controls الضوابط الأساسية للأمن السيبراني
IT	Information Technology تقنية المعلومات
MFA	Multi-Factor Authentication التحقق من الهوية متعدد العناصر
Monsha'at	Small and Medium Enterprises General Authority الهيئة العامة للمنشآت الصغيرة والمتوسطة
NCA	National Cybersecurity Authority الهيئة الوطنية للأمن السيبراني
NCNICC	Non-Critical National Infrastructure Private Sector Organizations Cybersecurity Controls ضوابط الأمن السيبراني لجهات القطاع الخاص من غير ذات البنى التحتية الحساسة
SPF	Sender Policy Framework إطار سياسة المرسل

الجدول (٧): قائمة الاختصارات


الهيئة الوطنية
للأمن السيبراني
National Cybersecurity Authority