الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

ضوابط الأمن السيبراني

لجهات القطاع الخاص من غير ذات البنى التحتية الحساسة

Non-CNI Private Sector Entities Cybersecurity Controls

(NCNICC – 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 (شخصى 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 الجداول

قائمة الأشكال والرسوم التوضيحيّة

الملخص التنفيذي

استهدفت رؤية المملكة العربية السعودية 2030 التطوير الشامل للوطن وأمنه، واقتصاده، ورفاهية مواطنيه، وعيشهم الكريم. وقد أكدت الرؤية على إيمان المملكة بأهمية القطاع الخاص، واستهدفت الوصول بإسهاماته في الناتج المحلي الإجمالي إلى 65% بحلول عام 2030، ورفع إسهام المنشآت الصغيرة والمتوسطة في الناتج المحلي الإجمالي إلى 35%. ومن الأهمية في هذا الجانب أن تحقيق هذه المنجزات يتطلب تعزيز الأمن السيبراني، لدى جميع جهات القطاع الخاص (الصغيرة، والمتوسطة، والكبيرة).

وتختص الهيئة الوطنية للأمن السيبراني، بموجب الأمر الملكي الكريم رقم (6801) وتاريخ 1439/2/11هـ في كونها الجهة التنظيمية المعنية 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.

ومن هذا المنطلق؛ قامت الهيئة الوطنية للأمن السيبراني بإعداد ضوابط الأمن السيبراني لجهات القطاع الخاص من غير ذات البنى التحتية الحساسة (NCNICC-1:2025) 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 في المملكة، وتمثل تنظيماً للحد الأدنى من متطلبات الأمن السيبراني، ضمن ثلاث مكونات: حوكمة الأمن السيبراني، وتعزيز الأمن السيبراني، والأمن السيبراني المتعلق بالأطراف الخارجية. كما تبين هذه الوثيقة تفاصيل هذه الضوابط، وأهدافها، ونطاق العمل وقابلية التطبيق، وآلية الالتزام ومتابعته.

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-1:2025) (ويشار لها في هذه الوثيقة بـ "هذه الضوابط") بعد دراسة شاملة لأفضل الممارسات الدولية للأمن السيبراني، في الجهات الصغيرة، والمتوسطة، والكبيرة. وقد جرى تطوير هذه الضوابط بناء على الضوابط الأساسية للأمن السيبراني لتقديم نسخة أكثر ملاءمة للجهات، ضمن نطاق عمل الضوابط.

وتنطبق ضوابط الأمن السيبراني لجهات القطاع الخاص من غير ذات البنى التحتية الحساسة، على فئتين من الجهات؛ وفق تعريف الهيئة العامة للمنشآت الصغيرة والمتوسطة (منشآت)؛ الأولى الجهات الكبيرة، والثانية الجهات الصغيرة والمتوسطة، وذلك على النحو المحدد في الجدول (1). وتشمل ضوابط الأمن السيبراني لجهات القطاع الخاص من غير ذات البنى التحتية الحساسة ما يلي:

جدول (1): فئات وعدد مكونات ضوابط الأمن السيبراني لجهات القطاع الخاص من غير ذات البنى التحتية الحساسة الملزمة

فئة الجهة	عدد المكونات الأساسية والفرعية والضوابط الأساسية الملزمة
الفئة (أ): الجهات الكبيرة*	• 3 مكونات أساسية • 22 مكونًا فرعياً • 65 ضابطًا أساسياً
الفئة (ب): الجهات الصغيرة والمتوسطة*	• مكون أساسي واحد • 13 مكونًا فرعياً • 26 ضابطًا أساسياً

* وفق تعريف الهيئة العامة للمنشآت الصغيرة والمتوسطة (منشآت)

الأهداف

تهدف هذه الوثيقة، إلى وضع الحدّ الأدنى من ضوابط الأمن السيبراني لجهات القطاع الخاص من غير ذات البنى التحتية الحساسة. وتستند الضوابط إلى الممارسات الدولية الرائدة في الأمن السيبراني؛ بما سيمكّن جهات القطاع الخاص من غير ذات البنى التحتية الحساسة، 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

تُطبَّق هذه الضوابط على الجهات الخاصة من غير ذات البنى التحتية الحساسة، الصغيرة والمتوسطة والكبيرة في المملكة العربية السعودية؛ التي يتم التعميم عليها من قبل الهيئة. وتقع على عاتق جميع الجهات خارج نطاق عمل هذه الضوابط في المملكة، مسؤولية الاستفادة من هذه الضوابط، حسب الاقتضاء؛ لتنفيذ أفضل الممارسات وتعزيز أمنها السيبراني.

وتستهدف الضوابط فئتين: الفئة الأولى (الجهات الكبيرة) والفئة الثانية (الجهات الصغيرة والمتوسطة). وتستند الفئتان، ضمن الضوابط إلى حجم الجهة، بالتوافق مع تعريف الهيئة العامة للمنشآت الصغيرة والمتوسطة (منشآت)، ويوضح الجدول (2) الآتي فئات الجهات ذات الصلة بضوابط الأمن السيبراني لجهات القطاع الخاص من غير ذات البنى التحتية الحساسة.

جدول (2): 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 الملزمة
الفئة (أ): الجهات الكبيرة*	هي الجهات التي تضم أكثر من 250 موظفًا بدوام كامل؛ أو تحقق أكثر من 200 مليون ريال سعودي من الإيرادات السنوية.	• 3 مكونات أساسية • 22 مكونًا فرعياً • 65 ضابطًا أساسياً
الفئة (ب): الجهات الصغيرة والمتوسطة*	هي الجهات التي تضم ما يتراوح بين 6 إلى 249 موظفًا بدوام كامل؛ أو تحقق ما بين 3 إلى 200 مليون ريال سعودي من الإيرادات السنوية.	• مكون أساسي واحد • 13 مكونًا فرعياً • 26 ضابطًا أساسياً

تعد الضوابط الخاصة بالفئة (أ) ملزمة للجهات الكبيرة التي يتم التعميم عليها من قبل الهيئة؛ في حين تعد ضوابط الفئة (ب) ملزمة للجهات الصغيرة والمتوسطة التي يتم التعميم عليها من قبل الهيئة. وللهيئة -وفق ما تقرره- إلزام الجهة بضوابط إضافية متى ما دعت الحاجة لذلك.

* وفق تعريف الهيئة العامة للمنشآت الصغيرة والمتوسطة (منشآت)

قابلية التطبيق داخل الجهة

أعدت هذه الضوابط لتكون ملائمة لاحتياجات الأمن السيبراني لجهات القطاع الخاص من غير ذات البنى التحتية الحساسة (الصغيرة والمتوسطة والكبيرة) في المملكة العربية السعودية، حيث تضع الحدّ الأدنى من ضوابط الأمن السيبراني لتلك الجهات. وتعتمد قابلية تطبيق الضوابط على فئة الجهة، ضمن النطاق المحدد في الجدول (2). ويوضح عنصر قابلية التطبيق للضوابط؛ المثال الآتي:

- الضوابط الفرعية ضمن الضابط الأساسي رقم (2-3-1) حماية الأنظمة وأجهزة معالجة المعلومات تكون قابلة التطبيق، وملزمة على كل من الجهات الكبيرة (الفئة (أ)) والجهات الصغيرة والمتوسطة (الفئة (ب)).
- الضوابط ضمن المكون الفرعي رقم (1-1) إدارة الأمن السيبراني، تكون قابلة التطبيق، وملزمة على الجهات الكبيرة (الفئة (أ)) فحسب.

التنفيذ والالتزام

تحقيقًا لما ورد في الفقرة الثالثة، من المادة العاشرة، في تنظيم الهيئة الوطنية للأمن السيبراني؛ يجب على جميع الجهات، ضمن نطاق عمل هذه الضوابط؛ تنفيذ ما يحقق الالتزام الدائم والمستمر بها.

تقوم الهيئة -وفق الآلية التي تراها مناسبة- بتقييم التزام الجهات، بما ورد في هذه الضوابط.

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 هذه الضوابط ونشره، لتطبيقه والالتزام به.

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

المكونات الأساسية

يوضح الشكل (1) الآتي المكونات الأساسية للضوابط.

شكل (1): المكونات الأساسية للضوابط

المكونات الفرعية

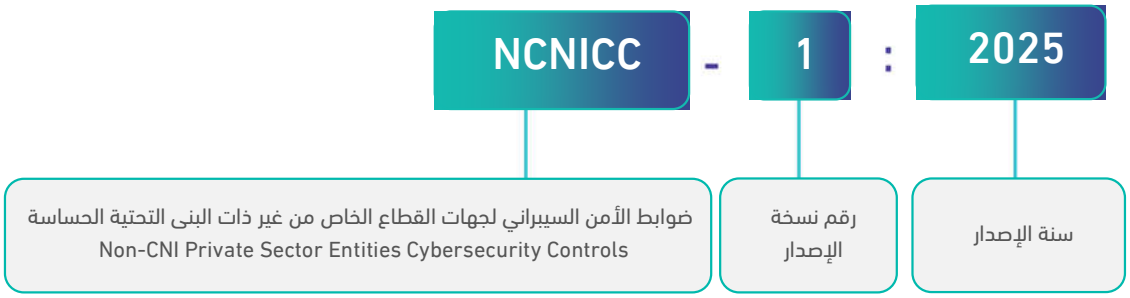
يوضح الجدول (3) الآتي المكونات الفرعية للضوابط.

جدول (3): المكونات الفرعية للضوابط

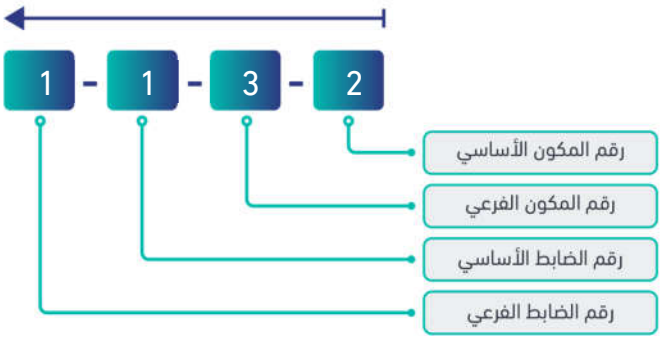
1. حوكمة الأمن السيبراني Cybersecurity Governance	1-1	إدارة الأمن السيبراني	2-1	سياسات وإجراءات الأمن السيبراني
	3-1	إدارة مخاطر الأمن السيبراني	4-1	المراجعة والتدقيق الدوري للأمن السيبراني
	5-1	برنامج التوعية والتدريب بالأمن السيبراني		
2. تعزيز الأمن السيبراني Cybersecurity Defense	1-2	إدارة الأصول	2-2	إدارة هويات الدخول والصلاحيات
	3-2	حماية الأنظمة وأجهزة معالجة المعلومات	4-2	حماية البريد الإلكتروني
	5-2	إدارة أمن الشبكات	6-2	أمن الأجهزة المحمولة
	7-2	حماية البيانات والمعلومات	8-2	التشفير
	9-2	إدارة النسخ الاحتياطية	10-2	إدارة الثغرات
	11-2	اختبار الاختراق	12-2	إدارة سجلات الأحداث ومراقبة الأمن السيبراني
	13-2	إدارة حوادث وتهديدات الأمن السيبراني	14-2	الأمن المادي
	15-2	حماية تطبيقات الويب		
3. الأمن السيبراني المتعلق بالأطراف الخارجية والحوسبة السحابية Third-Party and Cloud Computing Cybersecurity	1-3	الأمن السيبراني المتعلق بالأطراف الخارجية	2-3	الأمن السيبراني المتعلق بالحوسبة السحابية والاستضافة

الهيكلية

يوضح الشكلان (2) و(3) الآتيان معنى رموز الضوابط.



شكل (2): معنى رموز الضوابط



شكل (3): هيكلية الضوابط

يوضح الجدول (4) الآتي هيكلية الضوابط.

جدول (4): هيكلية الضوابط

1			اسم المكون الأساسي
رقم مرجعي للمكون الأساسي			
رقم مرجعي للمكون الفرعي			اسم المكون الفرعي
الهدف			
الضوابط		قابلية تطبيق الضابط	
		الفئة (أ)	الفئة (ب)
رقم مرجعي للضابط	بنود الضابط		

تعتمد قابلية تطبيق الضابط على فئة الجهة. وقد جرت الإشارة إلى ذلك في كل ضابط، كما هو مبين في الجدول (5).

جدول (5): دليل رموز قابلية تطبيق الضوابط

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

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

1 حوكمة الأمن السيبراني (Cybersecurity Governance)

1-1	إدارة الأمن السيبراني		
الهدف	ضمان دعم الإدارة العليا في إدارة برامج الأمن السيبراني وتطبيقها، داخل الجهة.		
الضوابط		قابلية تطبيق الضابط	
		الفئة (أ)	الفئة (ب)
1-1-1	يجب إنشاء وحدة إدارية، معنية بالأمن السيبراني في الجهة، وترتبط برئيس الجهة، أو من يفوضه بذلك. وتكون مستقلة عن وحدة تقنية المعلومات.	ملزم	موصى به
2-1-1	يجب أن يشغل رئاسة الإدارة المعنية بالأمن السيبراني والوظائف الإشرافية والحساسة بها مواطنون متفرغون وذو كفاءة عالية في مجال الأمن السيبراني.	ملزم	موصى به
3-1-1	يجب على صاحب الصلاحية تحديد وتوثيق واعتماد الهيكل التنظيمي للحوكمة والأدوار والمسؤوليات الخاصة بالأمن السيبراني للجهة، وتكليف الأشخاص المعنيين بها، كما يجب تقديم الدعم اللازم لإنفاذ ذلك، مع الأخذ بالاعتبار عدم تعارض المصالح.	ملزم	موصى به
2-1	سياسات وإجراءات الأمن السيبراني		
الهدف	ضمان توثيق متطلبات الأمن السيبراني ونشرها، والتزام الجهة بها.		
الضوابط		قابلية تطبيق الضابط	
		الفئة (أ)	الفئة (ب)
1-2-1	يجب تحديد سياسات الأمن السيبراني، وتوثيقها، واعتمادها ونشرها على العاملين المعنيين بها في الجهة.	ملزم	موصى به
2-2-1	يجب على الوحدة الإدارية المعنية بالأمن السيبراني في الجهة؛ ضمان تطبيق سياسات الأمن السيبراني في الجهة.	ملزم	موصى به
3-2-1	يجب على الوحدة الإدارية المعنية بالأمن السيبراني في الجهة؛ مراجعة سياسات الأمن السيبراني في الجهة دوريًا.	ملزم	موصى به
3-1	إدارة مخاطر الأمن السيبراني		
الهدف	ضمان إدارة مخاطر الأمن السيبراني، على نحو ممنهج؛ يهدف إلى حماية الأصول المعلوماتية والتقنية للجهة.		
الضوابط		قابلية تطبيق الضابط	
		الفئة (أ)	الفئة (ب)
1-3-1	يجب تحديد منهجية إدارة مخاطر الأمن السيبراني وإجراءاتها في الجهة، وتوثيقها واعتمادها.	ملزم	موصى به
2-3-1	يجب تطبيق منهجية إدارة مخاطر الأمن السيبراني وإجراءاتها في الجهة.	ملزم	موصى به

3-3-1	يجب مراجعة منهجية إدارة مخاطر الأمن السيبراني وإجراءاتها في الجهة دوريًا.	ملزم	موصى به
4-1	المراجعة والتدقيق الدوري للأمن السيبراني		
الهدف	ضمان التأكد، من أن ضوابط الأمن السيبراني؛ مطبقة لدى الجهة، وتعمل وفقًا للسياسات والإجراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية الوطنية، الصادرة من الهيئة الوطنية للأمن السيبراني، والمتطلبات الدولية المقرّة تنظيميًا على الجهة.		
الضوابط		قابلية تطبيق الضابط	
		الفئة (أ)	الفئة (ب)
1-4-1	يجب مراجعة ضوابط الأمن السيبراني وتدقيقها، من قبل طرف مستقل عن الوحدة الإدارية المعنية بالأمن السيبراني في الجهة، ووفق ما تقره الهيئة؛ لتقييم التزام الجهة بضوابط الأمن السيبراني لجهات القطاع الخاص من غير ذات البنى التحتية الحساسة.	ملزم	موصى به
2-4-1	يجب على الوحدة الإدارية المعنية بالأمن السيبراني في الجهة؛ مراجعة تطبيق ضوابط الأمن السيبراني دوريًا.	ملزم	موصى به
5-1	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 (أ)	الفئة (ب)
1-5-1	يجب أن تشتمل برامج التوعية بالأمن السيبراني، على الموضوعات الرئيسية ذات الصلة بالأمن السيبراني، والمهمة في حماية الجهة من التهديدات السيبرانية (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.	ملزم	موصى به
2-5-1	يجب تطبيق برامج التوعية بالأمن السيبراني المعتمدة من الجهة.	ملزم	موصى به
3-5-1	يجب مراجعة برامج التوعية بالأمن السيبراني المعتمدة من الجهة دوريًا.	ملزم	موصى به

٢ تعزيز الأمن السيبراني (Cybersecurity Defense)

1-2	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 (أ)	الفئة (ب)
1-1-2	يجب تحديد متطلبات الأمن السيبراني لإدارة الأصول المعلوماتية والتقنية للجهة، وتوثيقها واعتمادها.	ملزم	ملزم
2-1-2	يجب تطبيق متطلبات الأمن السيبراني لإدارة الأصول المعلوماتية والتقنية للجهة.	ملزم	ملزم
3-1-2	يجب مراجعة متطلبات الأمن السيبراني لإدارة الأصول المعلوماتية والتقنية للجهة دوريًا.	ملزم	موصى به
2-2	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 (أ)	الفئة (ب)
1-2-2	يجب تحديد متطلبات الأمن السيبراني لإدارة هويات الدخول والصلاحيات في الجهة، وتوثيقها واعتمادها. ويجب أن تغطي بحدّ أدنى ما يلي:	ملزم	ملزم
	1-1-2-2 التحقق من هوية المستخدم (User Authentication) بناءً على الإدارة الآمنة لاسم المستخدم، وكلمة المرور.	ملزم	ملزم
	2-1-2-2 التحقق من الهوية متعدد العناصر (Multi-Factor Authentication "MFA") لعمليات الدخول عن بعد بما يشمل البريد الإلكتروني، والتطبيقات الخارجية.	ملزم	ملزم
	3-1-2-2 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 المهمات (Segregation of Duties).	ملزم	ملزم
	4-1-2-2 إدارة الصلاحيات الهامة والحساسة (Privileged Access Management).	ملزم	موصى به
	5-1-2-2 المراجعة الدورية لهويات الدخول والصلاحيات.	ملزم	ملزم

2-2-2	يجب تطبيق متطلبات الأمن السيبراني لإدارة هويات الدخول والصلاحيات في الجهة.	ملزم	ملزم
3-2-2	يجب مراجعة متطلبات الأمن السيبراني لإدارة هويات الدخول والصلاحيات في الجهة دوريًا.	ملزم	موصى به
3-2	حماية الأنظمة وأجهزة معالجة المعلومات		
الهدف	ضمان حماية الأنظمة وأجهزة معالجة المعلومات؛ بما في ذلك أجهزة المستخدمين، والخوادم وأجهزة الشبكة للجهة، من مخاطر الأمن السيبراني.		
الضوابط		قابلية تطبيق الضابط	
		الفئة (أ)	الفئة (ب)
1-3-2	يجب تحديد متطلبات الأمن السيبراني لحماية الأنظمة وأجهزة معالجة المعلومات للجهة، وتوثيقها، واعتمادها. ويجب أن تغطي بحدّ أدنى ما يلي:	ملزم	ملزم
	1-1-3-2 الحماية من الفيروسات، والبرامج والأنشطة المشبوهة، والبرمجيات الضارة (Malware) على الخوادم، وأجهزة المستخدمين والأجهزة المحمولة، باستخدام تقنيات الحماية الحديثة، وآلياتها وإدارتها بشكل آمن.	ملزم	ملزم
	2-1-3-2 تغيير الإعدادات الافتراضية (مثل إلغاء تنشيط الخدمات غير الضرورية، تغيير كلمات المرور الافتراضية، وتقييد استخدام الوسائط القابلة للإزالة).	ملزم	ملزم
	3-1-3-2 مزامنة التوقيت (Clock Synchronization) مركزياً ومن مصدر دقيق وموثوق، ومن هذه المصادر ما توفره الهيئة السعودية للمواصفات والمقاييس والجودة.	ملزم	ملزم
2-3-2	يجب تطبيق متطلبات الأمن السيبراني لحماية الأنظمة وأجهزة معالجة المعلومات للجهة.	ملزم	ملزم
3-3-2	يجب مراجعة متطلبات الأمن السيبراني لحماية الأنظمة وأجهزة معالجة المعلومات للجهة دوريًا.	ملزم	موصى به
4-2	حماية البريد الإلكتروني		
الهدف	ضمان حماية البريد الإلكتروني للجهة، من مخاطر الأمن السيبراني.		
الضوابط		قابلية تطبيق الضابط	
		الفئة (أ)	الفئة (ب)
1-4-2	يجب تحديد متطلبات الأمن السيبراني لحماية البريد الإلكتروني للجهة، وتوثيقها، واعتمادها. ويجب أن تغطي بحدّ أدنى ما يلي:	ملزم	ملزم
	1-1-4-2 تحليل رسائل البريد الإلكتروني، وتصفيتها (Filtering) وبخاصة رسائل التصيّد الإلكتروني (Phishing Emails) والرسائل الاقتحامية (Spam Emails) باستخدام تقنيات الحماية الحديثة وآلياتها للبريد الإلكتروني.	ملزم	ملزم

	2-1-4-2 توثيق مجال البريد الإلكتروني للجهة؛ من خلال منصة حصين، باستخدام إطار سياسة المرسل (Sender Policy Framework "SPF") والبريد المعرّف بمفاتيح النطاق (Domain Keys Identified Mail "DKIM") وسياسة مصادقة الرسائل والإبلاغ عنها (Domain Message Authentication Reporting and Conformance "DMARC").	ملزم	ملزم
	3-1-4-2 الحماية من التهديدات المتقدمة المستمرة (APT Protection)، التي تستخدم عادة الفيروسات والبرمجيات الضارة غير المعروفة مسبقاً (Zero-Day Malware)، وإدارتها بشكل آمن.	ملزم	موصى به
2-4-2	يجب تطبيق متطلبات الأمن السيبراني لحماية البريد الإلكتروني للجهة.	ملزم	ملزم
3-4-2	يجب مراجعة متطلبات الأمن السيبراني لحماية البريد الإلكتروني للجهة دوريًا.	ملزم	موصى به
5-2	إدارة أمن الشبكات		
الهدف	ضمان حماية شبكات الجهة من مخاطر الأمن السيبراني.		
الضوابط		قابلية تطبيق الضابط	
		الفئة (أ)	الفئة (ب)
1-5-2	يجب تحديد متطلبات الأمن السيبراني لإدارة أمن شبكات الجهة، وتوثيقها، واعتمادها. ويجب أن تغطي بحدّ أدنى ما يلي:	ملزم	ملزم
	1-1-5-2 استخدام جدران الحماية للشبكة، وبوابات الوصول الآمنة.	ملزم	ملزم
	2-1-5-2 العزل، والتقسيم المادي، أو المنطقي، لأجزاء الشبكات بشكل آمن.	ملزم	موصى به
	3-1-5-2 أمن الشبكات اللاسلكية، وحمايتها، باستخدام وسائل آمنة؛ للتحقق من الهوية والتشفير.	ملزم	ملزم
	4-1-5-2 أمن التصفح والاتصال بالإنترنت، ويشمل ذلك التقييد الحازم للمواقع الإلكترونية المشبوهة، ومواقع مشاركة وتخزين الملفات، ومواقع الدخول عن بعد.	ملزم	موصى به
	5-1-5-2 قيود وإدارة منافذ وبروتوكولات وخدمات الشبكة.	ملزم	موصى به
	6-1-5-2 أنظمة الحماية المتقدمة لاكتشاف ومنع الاختراقات (Intrusion Prevention Systems).	ملزم	موصى به
	7-1-5-2 الحماية من هجمات تعطيل الشبكات (Distributed Denial of Service Attack "DDoS") للحد من المخاطر السيبرانية الناتجة عن هجمات تعطيل الشبكات.	ملزم	موصى به
2-5-2	يجب تطبيق متطلبات الأمن السيبراني لإدارة أمن شبكات الجهة.	ملزم	ملزم
3-5-2	يجب مراجعة متطلبات الأمن السيبراني لإدارة أمن شبكات الجهة دوريًا.	ملزم	موصى به

6-2	أمن الأجهزة المحمولة		
الهدف	ضمان حماية أجهزة الجهة المحمولة (بما في ذلك أجهزة الحاسب المحمول والهواتف الذكية والأجهزة الذكية اللوحية) من مخاطر الأمن السيبراني. وضمان التعامل بشكل آمن مع المعلومات الحساسة والمعلومات الخاصة بأعمال الجهة وحمايتها أثناء النقل والتخزين في حال السماح باستخدام الأجهزة الشخصية للعاملين في الجهة (مبدأ "BYOD").		
الضوابط		قابلية تطبيق الضابط	
		الفئة (أ)	الفئة (ب)
1-6-2	يجب تحديد متطلبات الأمن السيبراني الخاصة بأمن الأجهزة المحمولة والأجهزة الشخصية للعاملين (BYOD) في حال السماح بارتباطها بشبكة الجهة، وتوثيقها، واعتمادها.	ملزم	ملزم
2-6-2	يجب تطبيق متطلبات الأمن السيبراني الخاصة بأمن الأجهزة المحمولة والأجهزة الشخصية للعاملين (BYOD).	ملزم	ملزم
3-6-2	يجب مراجعة متطلبات الأمن السيبراني الخاصة بأمن الأجهزة المحمولة والأجهزة الشخصية للعاملين (BYOD) دوريًا.	ملزم	موصى به
7-2	حماية البيانات والمعلومات		
الهدف	ضمان حماية سرية وسلامة بيانات ومعلومات الجهة ودقتها وتوافرها، وذلك وفقاً للسياسات والإجراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية ذات العلاقة.		
الضوابط		قابلية تطبيق الضابط	
		الفئة (أ)	الفئة (ب)
1-7-2	يجب تحديد متطلبات الأمن السيبراني لحماية بيانات ومعلومات الجهة والتعامل معها وفقًا للمتطلبات التشريعية والتنظيمية ذات العلاقة، وتوثيقها، واعتمادها. ويجب أن تغطي بحدّ أدنى ما يلي:	ملزم	ملزم
1-1-7-2	استخدام تقنيات منع تسريب البيانات (Data Leakage Prevention) وتقنيات إدارة الصلاحيات (Rights Management).	ملزم	موصى به
2-1-7-2	استخدام خدمة حماية العلامة التجارية لحماية هوية الجهة من الانتحال (Brand Protection).	ملزم	موصى به
3-1-7-2	أمن استخدام الطابعات والماسحات الضوئية وآلات التصوير.	ملزم	ملزم
4-1-7-2	أمن إتلاف الأصول، وإعادة استخدامها (وتشمل: الوثائق الورقية، ووسائط الحفظ والتخزين).	ملزم	ملزم
2-7-2	يجب تطبيق متطلبات الأمن السيبراني لحماية بيانات ومعلومات الجهة، حسب مستوى تصنيفها.	ملزم	ملزم
3-7-2	يجب مراجعة متطلبات الأمن السيبراني لحماية بيانات ومعلومات الجهة دوريًا.	ملزم	موصى به
8-2	التشفير		
الهدف	ضمان الاستخدام السليم والفعال للتشفير؛ لحماية الأصول التقنية للجهة.		
الضوابط		قابلية تطبيق الضابط	

		الفئة (أ)	الفئة (ب)
1-8-2	يجب تحديد متطلبات الأمن السيبراني للتشفير في الجهة، وتوثيقها، واعتمادها. ويجب أن تغطي بحدّ أدنى ما يلي:	ملزم	ملزم
	1-1-8-2 استخدام تشفير البيانات، أثناء التخزين والنقل.	ملزم	ملزم
	2-1-8-2 استخدام أساليب وخوارزميات تشفير، آمنة وحديثة، عند إنشاء البيانات وتخزينها ونقلها، وكذلك الأمر مع جميع وسائط اتصالات الشبكة، وحسب متطلبات (المستوى الأساسي) من المعايير الوطنية للتشفير الصادرة عن الهيئة.	ملزم	موصى به
2-8-2	يجب تطبيق متطلبات الأمن السيبراني للتشفير في الجهة.	ملزم	ملزم
3-8-2	يجب مراجعة متطلبات الأمن السيبراني للتشفير في الجهة دوريًا.	ملزم	موصى به
9-2	إدارة النسخ الاحتياطية		
الهدف	ضمان حماية بيانات الجهة ومعلوماتها والإعدادات التقنية للأنظمة والتطبيقات الخاصة بالجهة من الأضرار غير المتوقعة الناجمة عن مخاطر الأمن السيبراني.		
الضوابط		قابلية تطبيق الضابط	
		الفئة (أ)	الفئة (ب)
1-9-2	يجب تحديد متطلبات الأمن السيبراني لإدارة النسخ الاحتياطية للجهة، وتوثيقها واعتمادها. ويجب أن تغطي بحدّ أدنى ما يلي:	ملزم	ملزم
	1-1-9-2 إجراء النسخ الاحتياطي لأنظمة الأعمال الحساسة بشكل دوري.	ملزم	ملزم
	2-1-9-2 إجراء فحص دوري؛ للتأكد من فعالية استعادة النسخ الاحتياطية.	ملزم	ملزم
2-9-2	يجب تطبيق متطلبات الأمن السيبراني لإدارة النسخ الاحتياطية للجهة.	ملزم	ملزم
3-9-2	يجب مراجعة متطلبات الأمن السيبراني لإدارة النسخ الاحتياطية للجهة دوريًا.	ملزم	موصى به
10-2	إدارة الثغرات		
الهدف	ضمان اكتشاف الثغرات التقنية في الوقت المناسب، ومعالجتها بشكل فعال؛ وذلك لمنع احتمالية استغلال هذه الثغرات في الهجمات السيبرانية، أو تقليلها، وتقليل الآثار المترتبة على أعمال الجهة.		
الضوابط		قابلية تطبيق الضابط	
		الفئة (أ)	الفئة (ب)
1-10-2	يجب تحديد متطلبات الأمن السيبراني لإدارة الثغرات التقنية للجهة، وتوثيقها واعتمادها. ويجب أن تغطي بحدّ أدنى ما يلي:	ملزم	ملزم
	1-1-10-2 تحديث الأنظمة، والبرمجيات والأجهزة، وإصلاحها بانتظام (Patch Management).	ملزم	ملزم
	2-1-10-2 فحص الثغرات، واكتشافها دورياً لجميع أصول الجهة.	ملزم	موصى به

	2-10-1-3 فحص الثغرات، واكتشافها دورياً للتطبيقات الخارجية.	ملزم	ملزم
	2-10-1-4 إدارة الثغرات ومعالجتها بناء على تصنيفها؛ بما في ذلك اختبار إصلاحات الثغرات قبل تثبيتها.	ملزم	ملزم
2-10-2	يجب تطبيق متطلبات الأمن السيبراني لإدارة الثغرات التقنية للجهة.	ملزم	ملزم
3-10-2	يجب مراجعة متطلبات الأمن السيبراني لإدارة الثغرات التقنية للجهة دوريًا.	ملزم	موصى به
11-2	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 التّحتيّة الفنية، التي قد تؤدي إلى الاختراق السيبراني للجهة.		
الضوابط		قابلية تطبيق الضابط	
		الفئة (أ)	الفئة (ب)
1-11-2	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 خارجياً (عن طريق الإنترنت) ومكوناتها التقنية، ومنها: البنية التحتية، والمواقع الإلكترونية، وتطبيقات الويب، وتطبيقات الهواتف المحمولة، والبريد الإلكتروني، والدخول عن بعد.	ملزم	موصى به
2-11-2	يجب تطبيق متطلبات الأمن السيبراني لعمليات اختبار الاختراق في الجهة.	ملزم	موصى به
3-11-2	يجب مراجعة متطلبات الأمن السيبراني لعمليات اختبار الاختراق في الجهة دوريًا.	ملزم	موصى به
12-2	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 (أ)	الفئة (ب)
1-12-2	يجب تحديد متطلبات إدارة سجلات الأحداث ومراقبة الأمن السيبراني للجهة، وتوثيقها واعتمادها. ويجب أن تغطي بحدّ أدنى ما يلي:	ملزم	ملزم
	2-12-1-1 تفعيل سجلات الأحداث (Event logs) الخاصة بالأمن السيبراني، على الأصول المعلوماتية الحساسة، لدى الجهة.	ملزم	ملزم
	2-12-1-2 الاشتراك لدى مقدم خدمات مركز عمليات الأمن السيبراني المدار؛ المرخص له من قبل الهيئة.	ملزم	موصى به
2-12-2	يجب تطبيق متطلبات إدارة سجلات الأحداث ومراقبة الأمن السيبراني للجهة.	ملزم	ملزم

3-12-2	يجب مراجعة متطلبات إدارة سجلات الأحداث ومراقبة الأمن السيبراني للجهة دوريًا.	ملزم	موصى به
13-2	إدارة حوادث وتهديدات الأمن السيبراني		
الهدف	ضمان اكتشاف حوادث الأمن السيبراني وتحديدها في الوقت المناسب، وإدارتها، والتعامل معها بشكل فعّال.		
الضوابط		قابلية تطبيق الضابط	
		الفئة (أ)	الفئة (ب)
1-13-2	يجب تحديد متطلبات إدارة حوادث وتهديدات الأمن السيبراني في الجهة، وتوثيقها واعتمادها. ويجب أن تغطي بحدّ أدنى ما يلي:	ملزم	ملزم
	1-1-13-2 وضع الخطط التفصيلية، للاستجابة لحوادث الأمن السيبراني (مثل اختراق البيانات، وفيروس الفدية)، وآليات التصعيد ذات الصلة.	ملزم	موصى به
	2-1-13-2 تبليغ الهيئة؛ عند حدوث حادثة أمن سيبراني.	ملزم	ملزم
	3-1-13-2 مشاركة معلومات الأمن السيبراني، مع الهيئة.	ملزم	ملزم
2-13-2	يجب تطبيق متطلبات إدارة حوادث وتهديدات الأمن السيبراني في الجهة.	ملزم	ملزم
3-13-2	يجب مراجعة متطلبات إدارة حوادث وتهديدات الأمن السيبراني في الجهة دوريًا.	ملزم	موصى به
14-2	الأمن المادي		
الهدف	ضمان حماية الأصول المعلوماتية والتقنية للجهة؛ من الوصول المادي، غير المصرح به، وكذلك من الفقدان، والسرقة، والتخريب.		
الضوابط		قابلية تطبيق الضابط	
		الفئة (أ)	الفئة (ب)
1-14-2	يجب تحديد متطلبات الأمن السيبراني للأمن المادي للأصول المعلوماتية والتقنية للجهة، وتوثيقها واعتمادها. ويجب أن تغطي بحدّ أدنى ما يلي:	ملزم	ملزم
	1-1-14-2 حماية الوصول المادي إلى غرف تقنية المعلومات والأجهزة الإلكترونية الحساسة.	ملزم	ملزم
	2-1-14-2 حماية الوصول المادي للأصول المعلوماتية والتقنية للجهة (مثل أجهزة الحاسب الآلي، ووسائط التخزين والطابعات) والوثائق.	ملزم	موصى به
	3-1-14-2 حماية سجلات أنظمة المراقبة (CCTV).	ملزم	ملزم
2-14-2	يجب تطبيق متطلبات الأمن السيبراني للأمن المادي للأصول المعلوماتية والتقنية للجهة.	ملزم	ملزم
3-14-2	يجب مراجعة متطلبات الأمن السيبراني للأمن المادي للأصول المعلوماتية والتقنية للجهة دوريًا.	ملزم	موصى به
15-2	حماية تطبيقات الويب		
الهدف	ضمان حماية تطبيقات الويب الخارجية للجهة من المخاطر السيبرانية.		

الضوابط		قابلية تطبيق الضابط	
		الفئة (أ)	الفئة (ب)
1-15-2	يجب تحديد متطلبات الأمن السيبراني لحماية تطبيقات الويب الخارجية للجهة من المخاطر السيبرانية وتوثيقها واعتمادها. ويجب أن تغطي بحدّ أدنى ما يلي:	ملزم	موصى به
	1-1-15-2استخدام جدار الحماية لتطبيقات الويب (Web Application Firewall).	ملزم	موصى به
	2-1-15-2 استخدام مبدأ المعمارية متعددة المستويات (Multi-tier Architecture).	ملزم	موصى به
	3 -1-15-2 استخدام بروتوكولات آمنة (مثل بروتوكول HTTPS).	ملزم	موصى به
	4-1-15-2 توضيح سياسة الاستخدام الآمن للمستخدمين.	ملزم	موصى به
	5-1-15-2 التحقق من الهوية على أن يتم تحديد عناصر التحقق المناسبة وعددها وكذلك تقنيات التحقق المناسبة بناء على نتائج تقييم الأثر المحتمل لفشل عملية التحقق وتخطيها، وذلك لعمليات دخول المستخدمين.	ملزم	موصى به
2-15-2	يجب تطبيق متطلبات الأمن السيبراني لحماية تطبيقات الويب الخارجية للجهة.	ملزم	موصى به
3-15-2	يجب مراجعة متطلبات الأمن السيبراني لحماية تطبيقات الويب الخارجية للجهة دوريًا.	ملزم	موصى به

3 الأمن السيبراني المتعلق بالأطراف الخارجية والحوسبة السحابية
(Third-Party and Cloud Computing Cybersecurity)

1-3	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 (أ)	الفئة (ب)
1-1-3	يجب تحديد متطلبات الأمن السيبراني ضمن العقود والاتفاقيات مع الأطراف الخارجية للجهة (مثل اتفاقية مستوى الخدمة SLA)، وتوثيقها واعتمادها. ويجب أن تحتوي بحد أدنى ما يلي:	ملزم	موصى به
	1-1-1-3 متطلب المحافظة على سرية المعلومات.	ملزم	موصى به
	2-1-1-3 إجراءات التواصل في حال حدوث حادثة أمن سيبراني مع الأطراف الخارجية التي قد تتأثر بإصابتها بيانات الجهة أو الخدمات المقدمة لها.	ملزم	موصى به
2-1-3	يجب تطبيق متطلبات الأمن السيبراني ضمن العقود والاتفاقيات مع الأطراف الخارجية للجهة.	ملزم	موصى به
3-1-3	يجب مراجعة متطلبات الأمن السيبراني ضمن العقود والاتفاقيات مع الأطراف الخارجية للجهة دوريًا.	ملزم	موصى به
2-3	الأمن السيبراني المتعلق بالحوسبة السحابية والاستضافة		
الهدف	ضمان معالجة المخاطر السيبرانية وتنفيذ متطلبات الأمن السيبراني للحوسبة السحابية والاستضافة بشكل ملائم وفعّال. وضمان حماية الأصول المعلوماتية والتقنية للجهة على خدمات الحوسبة السحابية التي تتم استضافتها أو معالجتها أو إدارتها بواسطة أطراف خارجية.		
الضوابط		قابلية تطبيق الضابط	
		الفئة (أ)	الفئة (ب)
1-2-3	يجب تحديد متطلبات الأمن السيبراني الخاصة باستخدام خدمات الحوسبة السحابية والاستضافة وتوثيقها واعتمادها. وضمان التوافق مع المتطلبات التشريعية والتنظيمية ذات العلاقة، وبالإضافة إلى ما ينطبق من الضوابط ضمن المكونات الرئيسية رقم (1) و (2) والمكون الفرعي رقم (1-3) الضرورية لحماية بيانات الجهة أو الخدمات المقدمة لها، يجب أن تغطي متطلبات الأمن السيبراني الخاصة باستخدام خدمات الحوسبة السحابية والاستضافة بحد أدنى ما يلي:	ملزم	موصى به
	1-1-2-3 تصنيف البيانات قبل استضافتها لدى مقدمي خدمات الحوسبة السحابية والاستضافة، وإعادتها للجهة (بصيغة قابلة للاستخدام) عند انتهاء الخدمة.	ملزم	موصى به
	2-1-2-3 فصل البيئة الخاصة بالجهة (وخصوصاً الخوادم الافتراضية) عن غيرها من البيئات التابعة لجهات أخرى في خدمات الحوسبة السحابية.	ملزم	موصى به

2-2-3	يجب تطبيق متطلبات الأمن السيبراني الخاصة بخدمات الحوسبة السحابية والاستضافة للجهة.	ملزم	موصى به
3-2-3	يجب مراجعة متطلبات الأمن السيبراني الخاصة بخدمات الحوسبة السحابية والاستضافة دورياً.	ملزم	موصى به

ملاحق

ملحق (أ): مصطلحات وتعريفات

يوضح الجدول (6) الآتي؛ بعض المصطلحات التي ورد ذكرها في هذه الوثيقة وتعريفاتها.

الجدول (6): مصطلحات وتعريفات

المصطلح	التعريف
الأصل **Asset**	أي شيء ملموس، أو غير ملموس؛ له قيمة بالنسبة للجهة. هناك أنواع كثيرة من الأصول؛ بعض هذه الأصول تتضمن أشياء واضحة، مثل: الأشخاص، والآلات، والمرافق، وبراءات الاختراع، والبرمجيات والخدمات. ويمكن أن يشمل المصطلح أيضًا أشياء أقل وضوحًا؛ مثل: المعلومات والخصائص (سمعة الجهة وصورتها العامة، أو المهارة والمعرفة).
هجوم **Attack**	أي نوع من الأنشطة الخبيثة، التي تحاول الوصول بشكل غير مشروع، أو تعمل على جمع موارد النظم المعلوماتية، أو المعلومات نفسها، أو تعطيلها، أو منعها، أو تحطيمها، أو تدميرها.
تدقيق **Audit**	المراجعة المستقلة، ودراسة السجلات والأنشطة؛ لتقييم مدى فعالية ضوابط الأمن السيبراني، ولضمان الالتزام بالسياسات، والإجراءات التشغيلية، والمعايير والمتطلبات التشريعية والتنظيمية ذات العلاقة.
التحقق **Authentication**	التأكد من هوية المستخدم، أو العملية أو الجهاز. وغالباً ما يكون هذا الأمر شرطًا أساسيًا، للسماح بالوصول، إلى الموارد في النظام.
صلاحية المستخدم **Authorization**	خاصية التحديد والتأكد من حقوق المستخدم أو صلاحيته، للوصول إلى الموارد، والأصول المعلوماتية والتقنية للجهة، والسماح له، وفقًا لما حدد مسبقًا في حقوق / صلاحية المستخدم.
التوافر **Availability**	ضمان الوصول إلى المعلومات، والبيانات، والأنظمة، والتطبيقات، واستخدامها في الوقت المناسب.
النسخ الاحتياطية **Backup**	هو نسخ الملفات، والأجهزة والبيانات والإجراءات، المتاحة للاستخدام في حال الأعطال أو الفقدان، أو إذا جرى حذف الأصل منها، أو توقف عن الخدمة.
السرية **Confidentiality**	الاحتفاظ بقيود مصرح بها للوصول إلى المعلومات، والإفصاح عنها، بما في ذلك وسائل حماية المعلومات.
التشفير **Cryptography**	ويسمى أيضًا علم التشفير وهي القواعد، التي تشتمل على مبادئ تخزين البيانات أو المعلومات ووسائل ذلك وطرقه، وكذلك نقلها، 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.
البنية التحتية الوطنية الحساسة **Critical National Infrastructure**	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: • 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. • تأثير كبير على الأمن الوطني و/ أو الدفاع الوطني و/ أو اقتصاد الدولة أو مقدراتها الوطنية.

الهجوم السيبراني **Cyber-Attack**	الاستغلال المتعمّد لأنظمة الحاسب الآلي، والشبكات، والجهات التي يعتمد عملها على تقنية المعلومات، والاتصالات الرقمية؛ بهدف إحداث أضرار.
مخاطر الأمن السيبراني **Cybersecurity Risks**	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.
الأمن السيبراني **Cybersecurity**	حسب ما نص عليه تنظيم الهيئة الصادر بالأمر الملكي ذي رقم (6801) والتاريخ 1439/2/11 هـ، فإن الأمن السيبراني هو 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.
فعالية **Effectiveness**	تشير إلى الدرجة التي يجري 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 مستوى الفعالية وتقييمه.
الجهة **Entity**	جهات القطاع الخاص الصغيرة، والمتوسطة، والكبيرة؛ من غير ذات البنى التحتية الحساسة، باستثناء الجهات متناهية الصغر، والجهات غير الحكومية، والقطاع الحكومي، والبنى التحتية الوطنية الحساسة.
حدث **Event**	أمر يحدث في مكان محدد (مثل الشبكة والأنظمة والتطبيقات وغيرها) وفي وقت محدد.
حصين **Haseen**	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.
هوية **Identification**	وسيلة التحقق من هوية المستخدم، أو العملية، أو الجهاز. وهي عادة شرط أساسي لمنح حق الوصول إلى الموارد في النظام.
حادثة **Incident**	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.
سلامة المعلومة **Integrity**	الحماية ضد تعديل المعلومات أو تخريبها بشكل غير مصرح به. وتتضمن الموثوقية وضمان عدم الإنكار للمعلومات (Non-Repudiation).
الحد الأدنى من الصلاحيات **Least Privilege**	مبدأ أساسي في الأمن السيبراني؛ يهدف إلى منح المستخدمين صلاحيات الوصول، التي يحتاجونها لتنفيذ مسؤولياتهم الرسمية فحسب.
البرمجيات الضارة **Malware**	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 **Multi-Factor Authentication (MFA)**	نظام أمني يتحقق من هوية المستخدم؛ يتطلب استخدام عدة عناصر مستقلة من آليات التحقق من الهوية. وتتضمن 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 **Need-to-know and Need-to-use**	القيود المفروضة على البيانات، والتي تعد حساسة، ما لم يكن لدى الشخص حاجة محددة، للاطلاع على البيانات؛ لغرض ما متعلق بأعمال ومهمات رسمية.
الإسناد الخارجي **Outsourcing**	الحصول على (السلع أو الخدمات) عن طريق التعاقد، مع مورد، أو مزود خدمة.
حزم التحديثات والإصلاحات **Patch**	حزم بيانات داعمة لتحديث أو إصلاح أو تحسين نظام التشغيل للحاسب الآلي أو لتطبيقاته أو برامجه. وهذا يشمل إصلاح الثغرات الأمنية وغيرها من الأخطاء، حيث تسمى هذه الحزم عادةً إصلاحات أو إصلاح الأخطاء وتحسين إمكانية الاستخدام أو الأداء.
رسائل التصيّد الإلكتروني **Phishing Emails**	محاولة الحصول على معلومات حساسة؛ مثل أسماء المستخدمين، وكلمات المرور، أو تفاصيل بطاقة الائتمان، لأسباب ونوايا ضارة وخبيثة في الغالب، وذلك بالتنكر على هيئة جهة جديرة بالثقة، في رسائل بريد إلكترونية.
الأمن المادي **Physical Security**	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 **Policy**	وثيقة تحدد بنودها التزامًا عامًا، أو توجيهًا، أو نية ما، كما جرى التعبير عن ذلك رسمياً من قبل صاحب الصلاحية للجهة. وسياسة الأمن السيبراني، هي وثيقة تنص بنودها على الالتزام الرسمي للإدارة العليا للجهة، بتنفيذ برنامج الأمن السيبراني وتحسينه في الجهة، وتشتمل السياسة على أهداف الجهة فيما يتعلق ببرنامج الأمن السيبراني، وضوابطه، ومتطلباته، وآلية تحسينه وتطويره.
إدارة الصلاحيات الهامة والحساسة **Privileged Access Management**	عملية إدارة الصلاحيات، ذات الخطورة العالية، على أنظمة الجهة، تحتاج في الغالب إلى تعامل خاص؛ لتقليل المخاطر، التي قد تنشأ من سوء استخدامها.
إجراء **Procedure**	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 **Process**	مجموعة من الأنشطة المترابطة، أو التفاعلية؛ تحول المدخلات إلى مخرجات. وهذه الأنشطة، متأثرة بسياسات الجهة.
الاستعادة **Recovery**	إجراء، أو عملية لاستعادة شيء منقطع، أو تالف، أو مسروق، أو ضائع، أو التحكم فيه.

فصل المهام **Segregation of Duties**	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 **Third-Party**	أي جهة تعمل على أنها طرف في علاقة تعاقدية، لتقديم السلع، أو الخدمات (وهذا يشمل موردي الخدمات ومزوديها).
تهديد **Threat**	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 أم تعطيل أو تعديل أو دخول أو استخدام أو استغلال غير مشروع.
الثغرة **Vulnerability**	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.

ملحق (ب): قائمة الاختصارات

يوضح الجدول (7) الآتي معنى الاختصارات التي ورد ذكرها في هذه الوثيقة.

الجدول (7): قائمة الاختصارات

الاختصار	معناه
BYOD	Bring Your Own Device أحضر الجهاز الخاص بك
CCTV	Closed-Circuit Television الدائرة التلفزيونية المغلقة
CNI	Critical National Infrastructure البنية التحتية الحساسة
DKIM	Domain Keys Identified Mail البريد المعرّف بمفاتيح النطاق
DMARC	Domain Message Authentication, Reporting and Conformance سياسة مصادقة الرسائل والإبلاغ عنها
ECC	Essential Cybersecurity Controls الضوابط الأساسية للأمن السيبراني
KPI	Key Performance Indicator مؤشر قياس الأداء
MFA	Multi-Factor Authentication التحقق من الهوية متعدد العناصر
NCNICC	Non-CNI Private Sector Entities Cybersecurity Controls ضوابط الأمن السيبراني لجهات القطاع الخاص من غير ذات البنى التحتية الحساسة
NCS	National Cryptographic Standards المعايير الوطنية للتشفير
SPF	Sender Policy Framework إطار سياسة المرسل


الهيئة الوطنية
للأمن السيبراني
National Cybersecurity Authority