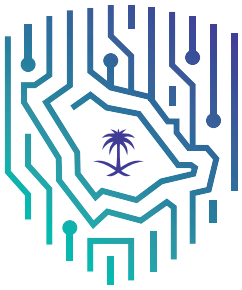


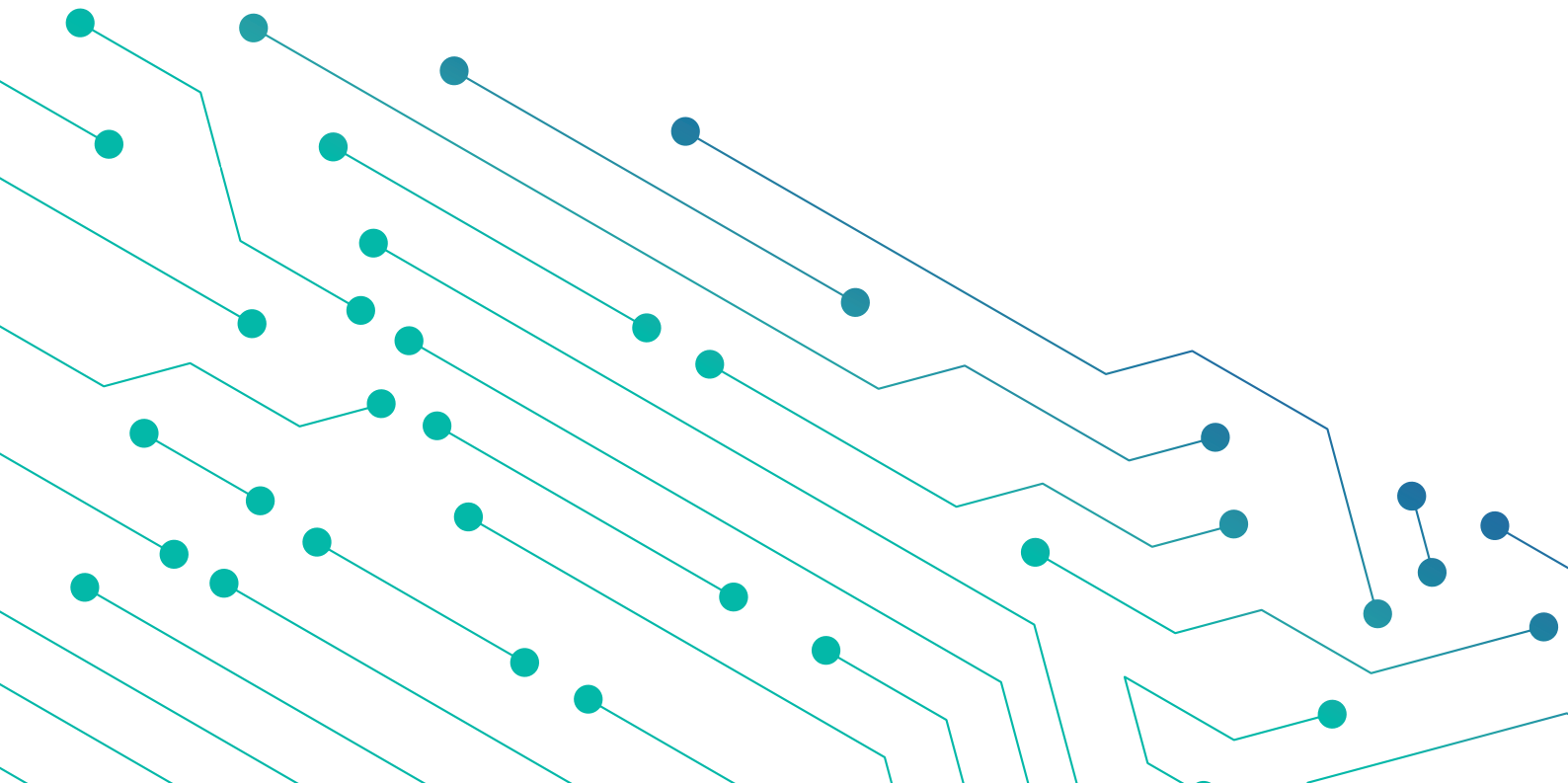
الهيئة الوطنية للأمن السيبـراني
National Cybersecurity Authority

الضوابط الأساسية
للأمــن السيبرانــي

Essential Cybersecurity Controls

(ECC – 1 : 2018)

إشــارة المـشـاركـة: أبيض
تصنيف الوثيقة: غير مصنف



بسم الله الرحمن الرحيم

بروتوكول الإشارة الضوئية (TLP):

تم إنشاء نظام بروتوكول الإشارة الضوئية لمشاركة أكبر قدر من المعلومات الحساسة ويستخدم 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 من داخل او خارج المنشأة خارج النطاق المحدد للاستلام.

برتقالي – مشاركة محدودة

المستلم بالإشارة البرتقالية يمكنه مشاركة المعلومات في نفس المنشأة مع الأشخاص المعنيين فقط، ومن يتطلب الأمر منه اتخاذ إجراء يخص المعلومة.

أخضر – مشاركة في نفس المجتمع

حيث يمكنك مشاركتها مع آخرين من منشأتك أو منشأة أخرى على علاقة معكم أو بنفس القطاع، ولا يسمح بتبادلها أو نشرها من خلال القنوات العامة.

أبيض – غير محدود

قائمة المحتويات

الملخص التنفيذي

استهدفت رؤية المملكة العربية السعودية ٢٠٣٠ التطوير الشامل للوطن وأمنه واقتصاده ورفاهية مواطنيه وعيشهم الكريم، ولقد كان من الطبيعي أن يكون أحد مستهدفاتها التحول نحو العالم الرقمي وتنمية البنية التحتية الرقمية؛ بما يعبر عن مواكبة التقدم العالمي المتسارع في الخدمات الرقمية وفي الشبكات العالمية المتجددة، وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية، ويتماشى مع تنامي قدرات المعالجة الحاسوبية وقدرات التخزين الهائلة للبيانات وتراسلها، وبما يهيئ للتعامل مع معطيات الذكاء الاصطناعي وتحولات الثورة الصناعية الرابعة.

إن هذا التحول يتطلب انسيابية المعلومات وأمانها وتكامل أنظمتها، ويستوجب المحافظة على الأمن السيبراني للمملكة العربية السعودية، وتعزيزه، حمايةً للمصالح الحيوية للدولة وأمنها الوطني والبنى التحتية الحساسة والقطاعات ذات الأولوية والخدمات والأنشطة الحكومية؛ لذلك أتى تأسيس الهيئة الوطنية للأمن السيبراني والموافقة على تنظيمها بموجب الأمر الملكي الكريم رقم ٦٨٠١ وتاريخ ١٤٣٩/٢/١١هـ، وجعلها الجهة المختصة في المملكة بالأمن السيبراني، والمرجع الوطني في شؤونه.

لقد جاءت مهمات هذه الهيئة واختصاصاتها ملبيةً للجوانب الاستراتيجية، ولجوانب وضع السياسات وآليات الحوكمة والأطر والمعايير والضوابط والإرشادات المتعلقة بالأمن السيبراني وتعميمها على الجهات.

كما جاءت ملبية لجوانب التحديث ومتابعة الالتزام من قبل الجهات الحكومية وغير الحكومية بما يعزز دور الأمن السيبراني وأهميته والحاجة الملحة التي ازدادت مع ازدياد التهديدات والمخاطر الأمنية في الفضاء السيبراني أكثر من أي وقت مضى.

وقد نص التنظيم المشار إليه أن مسؤولية هذه الهيئة لا يُخلي أي جهة عامة أو خاصة أو غيرها من مسؤوليتها تجاه أمنها السيبراني، وهو ما أكده الأمر السامي الكريم رقم ٥٧٢٣١ وتاريخ ١٤٣٩/١١/١٠هـ بأن «على جميع الجهات الحكومية رفع مستوى أمنها السيبراني لحماية شبكاتها وأنظمتها وبياناتها الإلكترونية، والالتزام بما تصدره الهيئة الوطنية للأمن السيبراني من سياسات وأطر ومعايير وضوابط وإرشادات بهذا الشأن».

ومن هذا المنطلق، قامت الهيئة الوطنية للأمن السيبراني بتطوير الضوابط الأساسية للأمن السيبراني (ECC – 1 : 2018) لوضع الحد الأدنى من متطلبات الأمن السيبراني في الجهات الوطنية التي تندرج تحت نطاق عمل هذه الضوابط. وتوضح هذه الوثيقة تفاصيل هذه الضوابط، وأهدافها، ونطاق العمل وقابلية التطبيق، وآلية الالتزام ومتابعته.

وعلى مختلف الجهات الوطنية تنفيذ ما يحقق الالتزام الدائم والمستمر بهذه الضوابط، تحقيقاً لما ورد في الفقرة الثالثة من المادة العاشرة في تنظيم الهيئة الوطنية للأمن السيبراني وكذلك ما ورد في الأمر السامي الكريم رقم ٥٧٢٣١ وتاريخ ١٤٣٩/١١/١٠ هـ.

المقدمة

قامت الهيئة الوطنية للأمن السيبراني (ويشار لها في هذه الوثيقة بـ "الهيئة") بتطوير الضوابط الأساسية للأمن السيبراني (ECC – 1 : 2018) بعد دراسة عدة معايير وأطر وضوابط للأمن السيبراني قامت بإعدادها سابقاً عدة جهات ومنظمات (محلية ودولية)، ودراسة متطلبات التشريعات والتنظيمات والقرارات الوطنية ذات العلاقة، وبعد الاطلاع على أفضل الممارسات والتجارب في مجال الأمن السيبراني والاستفادة منها، وتحليل ما تم رصده من حوادث وهجمات سيبرانية على مستوى الجهات الحكومية وغيرها من الجهات الحساسة، وبعد استطلاع آراء العديد من الجهات الوطنية وأخذ مرئياتها.

تتكون هذه الضوابط من:

- ٥ مكونات أساسية (Main Domains) لضوابط الأمن السيبراني
- ٢٩ مكوناً فرعياً (Subdomains) لضوابط الأمن السيبراني
- ١١٤ ضابطاً أساسياً (Controls) للأمن السيبراني

كما أن هذه الضوابط مرتبطة مع المتطلبات التشريعية والتنظيمية الوطنية والدولية ذات العلاقة.

الأهداف

تهدف هذه الضوابط إلى توفير الحد الأدنى من المتطلبات الأساسية للأمن السيبراني المبنية على أفضل الممارسات والمعايير لتقليل المخاطر السيبرانية على الأصول المعلوماتية والتقنية للجهات من التهديدات (Threats) 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 بالاعتبار المحاور الأربعة الأساسية التي يرتكز عليها الأمن السيبراني، وهي:

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

نطاق العمل وقابلية التطبيق

نطاق عمل الضوابط

تُطبَّق هذه الضوابط على الجهات الحكومية في المملكة العربية السعودية (وتشمل الـوزارات والهيئات والمؤسسات وغيرها) والجهات والشركات التابعة لها، وجهات القطاع الخاص التي تمتلك بنى تحتية وطنية حساسة ("CNIs" Critical National Infrastructures) أو تقوم بتشغيلها أو استضافتها، (ويشار لها جميعاً في هذا الوثيقة بـ "الجهة"). كما تُشجع الهيئة الجهات الأخرى في المملكة وبشدة على الاستفادة من هذه الضوابط لتطبيق أفضل الممارسات فيما يتعلق بتحسين الأمن السيبراني وتطويره داخل الجهة.

قابلية التطبيق داخل الجهة (ECC Statement of Applicability)

تم إعداد هذه الضوابط بحيث تكون ملائمة لاحتياجات الأمن السيبراني لجميع الجهات والقطاعات في المملكة العربية السعودية بتنوع طبيعة أعمالها، ويجب على كل جهة الالتزام بجميع الضوابط القابلة للتطبيق عليها.

من الأمثلة على الضوابط التي تتفاوت فيها قابلية التطبيق من جهة إلى أخرى حسب طبيعة أعمال الجهة واستخدامها للتقنيات المذكورة:

- الضوابط ضمن المكون الفرعي رقم (٤-٢) المتعلقة بالأمن السيبراني للحوسبة السحابية والاستضافة (Cloud Computing and Hosting Cybersecurity) تكون قابلة التطبيق وملزمة على الجهة التي تستخدم حالياً خدمات الحوسبة السحابية والاستضافة أو تخطط لاستخدامها.
- الضوابط ضمن المكون الرئيسي رقم (0) المتعلقة بالأمن السيبراني لأنظمة التحكم الصناعي (Industrial Control Systems Cybersecurity) تكون قابلة التطبيق وملزمة على الجهة التي تستخدم حالياً أنظمة التحكم الصناعي أو تخطط لاستخدامها.

التنفيذ والالتزام

تحقيقاً لما ورد في الفقرة الثالثة من المادة العاشرة في تنظيم الهيئة الوطنية للأمن السيبراني وكذلك ما ورد في الأمر السامي الكريم رقم ٥٧٢٣١ وتاريخ ١٤٣٩/١١/١٠ هـ، يجب على جميع الجهات ضمن نطاق عمل هذه الضوابط تنفيذ ما يحقق الالتزام الدائم والمستمر بهذه الضوابط.

تقوم الهيئة بتقييم التزام الجهات بما ورد في هذه الضوابط بطرق متعددة، منها: التقييم الذاتي للجهات، التقارير الدورية لأداة الالتزام و/أو الزيارات الميدانية للتدقيق، وفق الآلية التي تراها الهيئة مناسبة لذلك.

أداة التقييم وقياس الالتزام

سوف تقوم الهيئة بإصدار أداة (ECC – 1 : 2018 Assessment and Compliance Tool) لتنظيم عملية تقييم وقياس مدى التزام الجهات بتطبيق الضوابط الأساسية للأمن السيبراني.

التحديث والمراجعة

تتولى الهيئة التحديث والمراجعة الدورية للضوابط الأساسية للأمن السيبراني حسب متطلبات الأمن السيبراني والمستجدات ذات العلاقة. كما تتولى الهيئة إعلان الإصدار المحدث من الضوابط لتطبيقه والالتزام به.

مكونات وهيكلية الضوابط الأساسية للأمن السيبراني

المكونات الأساسية

يوضح الشكل ١ أدناه المكونات الأساسية للضوابط.

شكل ١: المكونات الأساسية للضوابط

المكونات الفرعية

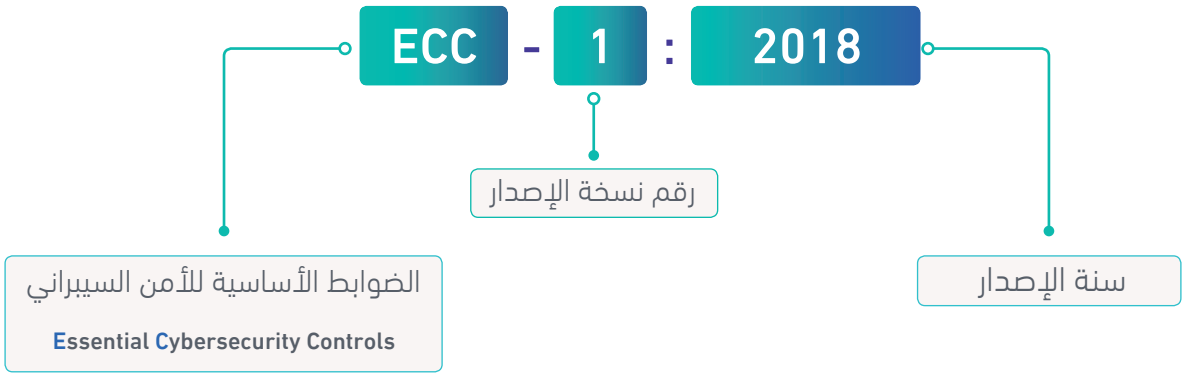
يوضح الشكل ٢ أدناه المكونات الفرعية للضوابط.

١ - حوكمة الأمن السيبراني Cybersecurity Governance	١-١	إستراتيجية الأمن السيبراني Cybersecurity Strategy	١-٢	إدارة الأمن السيبراني Cybersecurity Management
	١-٣	سياسات وإجراءات الأمن السيبراني Cybersecurity Policies and Procedures	١-٤	أدوار ومسؤوليات الأمن السيبراني Cybersecurity Roles and Responsibilities
	١-٥	إدارة مخاطر الأمن السيبراني Cybersecurity Risk Management	١-٦	الأمن السيبراني ضمن إدارة المشاريع المعلوماتية والتقنية Cybersecurity in Information Technology Projects
	١-٧	الالتزام بتشريعات وتنظيمات ومعايير الأمن السيبراني Cybersecurity Regulatory Compliance	١-٨	المراجعة والتدقيق الدوري للأمن السيبراني Cybersecurity Periodical Assessment and Audit
	١-٩	الأمن السيبراني المتعلق بالموارد البشرية Cybersecurity in Human Resources	١-١٠	برنامج التوعية والتدريب بالأمن السيبراني Cybersecurity Awareness and Training Program
٢ - تعزيز الأمن السيبراني Cybersecurity Defense	٢ - ١	إدارة الأصول Asset Management	٢ - ٢	إدارة هويات الدخول والصلاحيات Identity and Access Management
	٢ - ٣	حماية الأنظمة وأجهزة معالجة المعلومات Information System and Processing Facilities Protection	٢ - ٤	حماية البريد الإلكتروني Email Protection
	٢ - ٥	إدارة أمن الشبكات Networks Security Management	٢ - ٦	أمن الأجهزة المحمولة Mobile Devices Security
	٢ - ٧	حماية البيانات والمعلومات Data and Information Protection	٢ - ٨	التشفير Cryptography
	٢ - ٩	إدارة النسخ الاحتياطية Backup and Recovery Management	٢ - ١٠	إدارة الثغرات Vulnerabilities Management
	٢ - ١١	اختبار الاختراق Penetration Testing	٢ - ١٢	إدارة سجلات الأحداث ومراقبة الأمن السيبراني Cybersecurity Event Logs and Monitoring Management
	٢ - ١٣	إدارة حوادث وتهديدات الأمن السيبراني Cybersecurity Incident and Threat Management	٢ - ١٤	الأمن المادي Physical Security
	٢ - ١٥	حماية تطبيقات الويب Web Application Security		
٣ - صمود الأمن السيبراني Cybersecurity Resilience	٣ - ١	جوانب صمود الأمن السيبراني في إدارة استمرارية الأعمال Cybersecurity Resilience aspects of Business Continuity Management (BCM)		
٤ - الأمن السيبراني المتعلق بالأطراف الخارجية والحوسبة السحابية Third-Party and Cloud Computing Cybersecurity	٤ - ١	الأمن السيبراني المتعلق بالأطراف الخارجية Third-Party Cybersecurity	٤ - ٢	الأمن السيبراني المتعلق بالحوسبة السحابية والاستضافة Cloud Computing and Hosting Cybersecurity
٥ - الأمن السيبراني لأنظمة التحكم الصناعي ICS Cybersecurity	٥ - ١	حماية أجهزة وأنظمة التحكم الصناعي Industrial Control Systems (ICS) Protection		

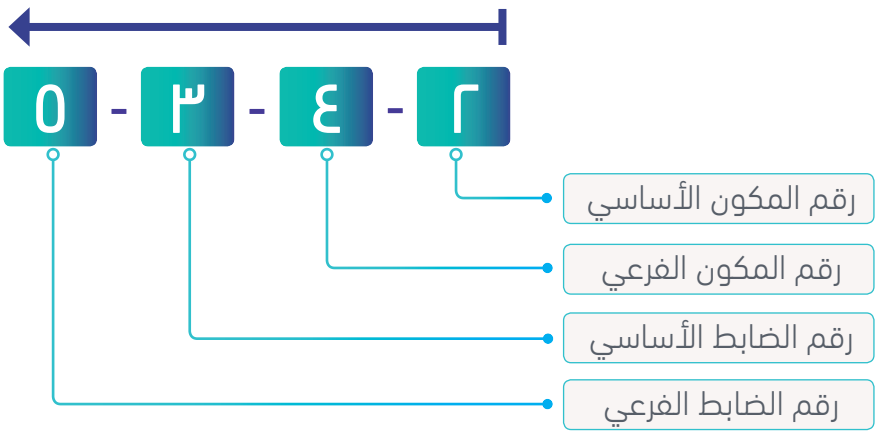
شكل ٢: المكونات الفرعية للضوابط

الهيكلية

يوضح الشكلان ٣ و٤ أدناه معنى رموز الضوابط.



شكل ٣: معنى رموز الضوابط



شكل ٤: هيكلية الضوابط

يوضح الجدول (١) أدناه طريقة هيكلية الضوابط

جدول ١: هيكلية الضوابط

١	اسم المكون الأساسي
رقم مرجعي للمكون الأساسي	
رقم مرجعي للمكون الفرعي	اسم المكون الفرعي
الهدف	
الضوابط	
رقم مرجعي للضابط	بنود الضابط

الضوابط الأساسية للأمن السيبراني

تفاصيل الضوابط الأساسية للأمن السيبراني

١ حوكمة الأمن السيبراني (Cybersecurity Governance)

١-١	إستراتيجية الأمن السيبراني
الهدف	ضمان إسهام خطط العمل للأمن السيبراني والأهداف والمبادرات والمشاريع داخل الجهة في تحقيق المتطلبات التشريعية والتنظيمية ذات العلاقة.
الضوابط	
١-١-١	يجب تحديد وتوثيق واعتماد إستراتيجية الأمن السيبراني للجهة ودعمها من قبل رئيس الجهة أو من ينيبه (ويشار له في هذه الضوابط باسم «صاحب الصلاحية»)، وأن تتماشى الأهداف الإستراتيجية للأمن السيبراني للجهة مع المتطلبات التشريعية والتنظيمية ذات العلاقة.
١-١-٢	يجب العمل على تنفيذ خطة عمل لتطبيق إستراتيجية الأمن السيبراني من قبل الجهة.
١-١-٣	يجب مراجعة إستراتيجية الأمن السيبراني على فترات زمنية مخطط لها (أو في حالة حدوث تغييرات في المتطلبات التشريعية والتنظيمية ذات العلاقة).
١-٢	إدارة الأمن السيبراني
الهدف	ضمان التزام ودعم صاحب الصلاحية للجهة فيما يتعلق بإدارة وتطبيق برامج الأمن السيبراني في تلك الجهة وفقاً للمتطلبات التشريعية والتنظيمية ذات العلاقة.
الضوابط	
١-٢-١	يجب إنشاء إدارة معنية بالأمن السيبراني في الجهة مستقلة عن إدارة تقنية المعلومات والاتصالات (ICT/ IT) (وفقاً للأمر السامي الكريم رقم ٣٧١٤٠ وتاريخ ١٤ / ٨ / ١٤٣٨ هـ). ويفضل ارتباطها مباشرة برئيس الجهة أو من ينيبه، مع الأخذ بالاعتبار عدم تعارض المصالح.
١-٢-٢	يجب أن يشغل رئاسة الإدارة المعنية بالأمن السيبراني والوظائف الإشرافية والحساسة بها مواطنون متفرغون وذو كفاءة عالية في مجال الأمن السيبراني.
١-٢-٣	يجب إنشاء لجنة إشرافية للأمن السيبراني بتوجيه من صاحب الصلاحية للجهة لضمان التزام ودعم ومتابعة تطبيق برامج وتشريعات الأمن السيبراني، ويتم تحديد وتوثيق واعتماد أعضاء اللجنة ومسؤولياتها وإطار حوكمة أعمالها على أن يكون رئيس الإدارة المعنية بالأمن السيبراني أحد أعضائها. ويفضل ارتباطها مباشرة برئيس الجهة أو من ينيبه، مع الأخذ بالاعتبار عدم تعارض المصالح.
١-٣	سياسات وإجراءات الأمن السيبراني
الهدف	ضمان توثيق ونشر متطلبات الأمن السيبراني والتزام الجهة بها، وذلك وفقاً لمتطلبات الأعمال التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

الضوابط	
١-٣-١	يجب على الإدارة المعنية بالأمن السيبراني في الجهة تحديد سياسات وإجراءات الأمن السيبراني وما تشمله من ضوابط ومتطلبات الأمن السيبراني، وتوثيقها واعتمادها من قبل صاحب الصلاحية في الجهة، كما يجب نشرها إلى ذوي العلاقة من العاملين في الجهة والأطراف المعنية بها.
١-٣-٢	يجب على الإدارة المعنية بالأمن السيبراني ضمان تطبيق سياسات وإجراءات الأمن السيبراني في الجهة وما تشمله من ضوابط ومتطلبات.
١-٣-٣	يجب أن تكون سياسات وإجراءات الأمن السيبراني مدعومة بمعايير تقنية أمنية (على سبيل المثال: المعايير التقنية الأمنية لجدار الحماية وقواعد البيانات، وأنظمة التشغيل، إلخ).
١-٣-٤	يجب مراجعة سياسات وإجراءات ومعايير الأمن السيبراني وتحديثها على فترات زمنية مخطط لها (أو في حالة حدوث تغييرات في المتطلبات التشريعية والتنظيمية والمعايير ذات العلاقة)، كما يجب توثيق التغييرات واعتمادها.
١-٤	**أدوار ومسؤوليات الأمن السيبراني**
الهدف	ضمان تحديد أدوار ومسؤوليات واضحة لجميع الأطراف المشاركة في تطبيق ضوابط الأمن السيبراني في الجهة.
الضوابط	
١-٤-١	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.
١-٤-٢	يجب مراجعة أدوار ومسؤوليات الأمن السيبراني في الجهة وتحديثها على فترات زمنية مخطط لها (أو في حالة حدوث تغييرات في المتطلبات التشريعية والتنظيمية ذات العلاقة).
١-٥	**إدارة مخاطر الأمن السيبراني**
الهدف	ضمان إدارة مخاطر الأمن السيبراني على نحو ممنهج يهدف إلى حماية الأصول المعلوماتية والتقنية للجهة، وذلك وفقاً للسياسات والإجراءات التنظيمية للجهة والمتطلبات التشريعية والتنظيمية ذات العلاقة.
الضوابط	
١-٥-١	يجب على الإدارة المعنية بالأمن السيبراني في الجهة تحديد وتوثيق واعتماد منهجية وإجراءات إدارة مخاطر الأمن السيبراني في الجهة. وذلك وفقاً لاعتبارات السرية وتوافر وسلامة الأصول المعلوماتية والتقنية.
١-٥-٢	يجب على الإدارة المعنية بالأمن السيبراني تطبيق منهجية وإجراءات إدارة مخاطر الأمن السيبراني في الجهة.
١-٥-٣	يجب تنفيذ إجراءات تقييم مخاطر الأمن السيبراني بحد أدنى في الحالات التالية: ١-٥-٣-١ في مرحلة مبكرة من المشاريع التقنية. ١-٥-٣-٢ قبل إجراء تغيير جوهري في البنية التقنية. ١-٥-٣-٣ عند التخطيط للحصول على خدمات طرف خارجي. ١-٥-٣-٤ عند التخطيط وقبل إطلاق منتجات وخدمات تقنية جديدة.

١-٥-٤	يجب مراجعة منهجية وإجراءات إدارة مخاطر الأمن السيبراني وتحديثها على فترات زمنية مخطط لها (أو في حالة حدوث تغييرات في المتطلبات التشريعية والتنظيمية والمعايير ذات العلاقة)، كما يجب توثيق التغييرات واعتمادها.
١-٦	**الأمن السيبراني ضمن إدارة المشاريع المعلوماتية والتقنية**
الهدف	التأكد من أن متطلبات الأمن السيبراني مضمنة في منهجية وإجراءات إدارة مشاريع الجهة لحماية السرية وسلامة الأصول المعلوماتية والتقنية للجهة ودقتها وتوافرها، وذلك وفقاً للسياسات والإجراءات التنظيمية للجهة والمتطلبات التشريعية والتنظيمية ذات العلاقة.
الضوابط	
١-٦-١	يجب تضمين متطلبات الأمن السيبراني في منهجية وإجراءات إدارة المشاريع وفي إدارة التغيير على الأصول المعلوماتية والتقنية في الجهة لضمان تحديد مخاطر الأمن السيبراني ومعالجتها كجزء من دورة حياة المشروع التقني، وأن تكون متطلبات الأمن السيبراني جزء أساسي من متطلبات المشاريع التقنية.
١-٦-٢	يجب أن تغطي متطلبات الأمن السيبراني لإدارة المشاريع والتغييرات على الأصول المعلوماتية والتقنية للجهة بحد أدنى ما يلي: ١-٦-٢-١ تقييم الثغرات ومعالجتها. ١-٦-٢-٢ اجراء مراجعة للإعدادات والتحصين (Secure Configuration and Hardening) وحزم التحديثات قبل إطلاق وتدشين المشاريع والتغييرات.
١-٦-٣	يجب أن تغطي متطلبات الأمن السيبراني لمشاريع تطوير التطبيقات والبرمجيات الخاصة للجهة بحد أدنى ما يلي: ١-٦-٣-١ استخدام معايير التطوير الآمن للتطبيقات (Secure Coding Standards). ١-٦-٣-٢ استخدام مصادر مرخصة وموثوقة لأدوات تطوير التطبيقات والمكتبات الخاصة بها (Libraries). ١-٦-٣-٣ اجراء اختبار للتحقق من مدى استيفاء التطبيقات للمتطلبات الأمنية السيبرانية للجهة. ١-٦-٣-٤ أمن التكامل (Integration) بين التطبيقات. ١-٦-٣-٥ اجراء مراجعة للإعدادات والتحصين (Secure Configuration and Hardening) وحزم التحديثات قبل إطلاق وتدشين التطبيقات.
١-٦-٤	يجب مراجعة متطلبات الأمن السيبراني في إدارة المشاريع في الجهة دورياً.
١-٧	**الالتزام بتشريعات وتنظيمات ومعايير الأمن السيبراني**
الهدف	ضمان التأكد من أن برنامج الأمن السيبراني لدى الجهة يتوافق مع المتطلبات التشريعية والتنظيمية ذات العلاقة.
الضوابط	
١-٧-١	يجب على الجهة الالتزام بالمتطلبات التشريعية والتنظيمية الوطنية المتعلقة بالأمن السيبراني.
١-٧-٢	في حال وجود اتفاقيات أو إلتزامات دولية معتمدة محلياً تتضمن متطلبات خاصة بالأمن السيبراني، فيجب على الجهة الالتزام بتلك المتطلبات.

١-٨	المراجعة والتدقيق الدوري للأمن السيبراني
الهدف	ضمان التأكد من أن ضوابط الأمن السيبراني لدى الجهة مطبقة وتعمل وفقاً للسياسات والإجراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية الوطنية ذات العلاقة، والمتطلبات الدولية المقرّة تنظيمياً على الجهة.
الضوابط	
١-٨-١	يجب على الإدارة المعنية بالأمن السيبراني في الجهة مراجعة تطبيق ضوابط الأمن السيبراني دورياً.
١-٨-٢	يجب مراجعة وتدقيق تطبيق ضوابط الأمن السيبراني في الجهة، من قبل أطراف مستقلة عن الإدارة المعنية بالأمن السيبراني (مثل الإدارة المعنية بالمراجعة في الجهة). على أن تتم المراجعة والتدقيق بشكل مستقل يراعى فيه مبدأ عدم تعارض المصالح، وذلك وفقاً للمعايير العامة المقبولة للمراجعة والتدقيق والمتطلبات التشريعية والتنظيمية ذات العلاقة.
١-٨-٣	يجب توثيق نتائج مراجعة وتدقيق الأمن السيبراني، وعرضها على اللجنة الإشرافية للأمن السيبراني وصاحب الصلاحية. كما يجب أن تشتمل النتائج على نطاق المراجعة والتدقيق، والملاحظات المكتشفة، والتوصيات والإجراءات التصحيحية، وخطة معالجة الملاحظات.
١-٩	الأمن السيبراني المتعلق بالموارد البشرية
الهدف	ضمان التأكد من أن مخاطر ومتطلبات الأمن السيبراني المتعلقة بالعاملين (موظفين ومتعاقدين) في الجهة تعالج بفعالية قبل وأثناء وعند انتهاء/إنهاء عملهم، وذلك وفقاً للسياسات والإجراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية ذات العلاقة.
الضوابط	
١-٩-١	يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني المتعلقة بالعاملين قبل توظيفهم وأثناء عملهم وعند انتهاء/إنهاء عملهم في الجهة.
١-٩-٢	يجب تطبيق متطلبات الأمن السيبراني المتعلقة بالعاملين في الجهة.
١-٩-٣	يجب أن تغطي متطلبات الأمن السيبراني قبل بدء علاقة العاملين المهنية بالجهة بحد أدنى ما يلي: ١-٩-٣-١ تضمين مسؤوليات الأمن السيبراني وبنود المحافظة على سرية المعلومات (Non-Disclosure Clauses) في عقود العاملين في الجهة (لتشمل خلال وبعد انتهاء/إنهاء العلاقة الوظيفية مع الجهة). ١-٩-٣-٢ إجراء المسح الأمني (Screening or Vetting) للعاملين في وظائف الأمن السيبراني والوظائف التقنية ذات الصلاحيات الهامة والحساسة.
١-٩-٤	يجب أن تغطي متطلبات الأمن السيبراني خلال علاقة العاملين المهنية بالجهة بحد أدنى ما يلي: ١-٩-٤-١ التوعية بالأمن السيبراني (عند بداية المهنة الوظيفية وخلالها). ١-٩-٤-٢ تطبيق متطلبات الأمن السيبراني والالتزام بها وفقاً لسياسات وإجراءات وعمليات الأمن السيبراني للجهة.
١-٩-٥	يجب مراجعة وإلغاء الصلاحيات للعاملين مباشرة بعد انتهاء/إنهاء الخدمة المهنية لهم بالجهة.
١-٩-٦	يجب مراجعة متطلبات الأمن السيبراني المتعلقة بالعاملين في الجهة دورياً.

١-١٠	برنامج التوعية والتدريب بالأمن السيبراني
الهدف	ضمان التأكد من أن العاملين بالجهة لديهم التوعية الأمنية اللازمة وعلى دراية بمسؤولياتهم في مجال الأمن السيبراني. والتأكد من تزويد العاملين بالجهة بالمهارات والمؤهلات والدورات التدريبية المطلوبة في مجال الأمن السيبراني لحماية الأصول المعلوماتية والتقنية للجهة والقيام بمسؤولياتهم تجاه الأمن السيبراني.
الضوابط	
١-١٠-١	يجب تطوير واعتماد برنامج للتوعية بالأمن السيبراني في الجهة من خلال قنوات متعددة دورياً، وذلك لتعزيز الوعي بالأمن السيبراني وتهديداته ومخاطره، وبناء ثقافة إيجابية للأمن السيبراني.
١-١٠-٢	يجب تطبيق البرنامج المعتمد للتوعية بالأمن السيبراني في الجهة.
١-١٠-٣	يجب أن يغطي برنامج التوعية بالأمن السيبراني كيفية حماية الجهة من أهم المخاطر والتهديدات السيبرانية وما يستجد منها، بما في ذلك: ١-١٠-٣-١ التعامل الآمن مع خدمات البريد الإلكتروني خصوصاً مع رسائل التصيد الإلكتروني. ١-١٠-٣-٢ التعامل الآمن مع الأجهزة المحمولة ووسائط التخزين. ١-١٠-٣-٣ التعامل الآمن مع خدمات تصفح الإنترنت. ١-١٠-٣-٤ التعامل الآمن مع وسائل التواصل الاجتماعي.
١-١٠-٤	يجب توفير المهارات المتخصصة والتدريب اللازم للعاملين في المجالات الوظيفية ذات العلاقة المباشرة بالأمن السيبراني في الجهة، وتصنيفها بما يتماشى مع مسؤولياتهم الوظيفية فيما يتعلق بالأمن السيبراني، بما في ذلك: ١-١٠-٤-١ موظفو الإدارة المعنية بالأمن السيبراني. ١-١٠-٤-٢ الموظفون العاملون في تطوير البرامج والتطبيقات والموظفون المشغلون للأصول المعلوماتية والتقنية للجهة. ١-١٠-٤-٣ الوظائف الإشرافية والتنفيذية.
١-١٠-٥	يجب مراجعة تطبيق برنامج التوعية بالأمن السيبراني في الجهة دورياً.

٢ تعزيز الأمن السيبراني (Cybersecurity Defense)

٢-١	إدارة الأصول (Asset Management)
الهدف	للتأكد 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 وسلامة الأصول المعلوماتية والتقنية للجهة ودقتها وتوافرها.
الضوابط	
٢-١-١	يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني لإدارة الأصول المعلوماتية والتقنية للجهة.
٢-١-٢	يجب تطبيق متطلبات الأمن السيبراني لإدارة الأصول المعلوماتية والتقنية للجهة.
٢-١-٣	يجب تحديد وتوثيق واعتماد ونشر سياسة الاستخدام المقبول للأصول المعلوماتية والتقنية للجهة.
٢-١-٤	يجب تطبيق سياسة الاستخدام المقبول للأصول المعلوماتية والتقنية للجهة.
٢-١-٥	يجب تصنيف الأصول المعلوماتية والتقنية للجهة وترميزها (Labeling) والتعامل معها وفقاً للمتطلبات التشريعية والتنظيمية ذات العلاقة.
٢-١-٦	يجب مراجعة متطلبات الأمن السيبراني لإدارة الأصول المعلوماتية والتقنية للجهة دورياً.
٢-٢	**إدارة هويات الدخول والصلاحيات (Identity and Access Management)**
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	
٢-٢-١	يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني لإدارة هويات الدخول والصلاحيات في الجهة.
٢-٢-٢	يجب تطبيق متطلبات الأمن السيبراني لإدارة هويات الدخول والصلاحيات في الجهة.
٢-٢-٣	يجب أن تغطي متطلبات الأمن السيبراني المتعلقة بإدارة هويات الدخول والصلاحيات في الجهة بحد أدنى ما يلي: ٢-٢-٣-١ التحقق من هوية المستخدم (User Authentication) بناءً على إدارة تسجيل المستخدم، وإدارة كلمة المرور. ٢-٢-٣-٢ التحقق من الهوية متعدد العناصر (Multi-Factor Authentication) لعمليات الدخول عن بعد. ٢-٢-٣-٣ إدارة تصاريح وصلاحيات المستخدمين (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"). ٢-٢-٣-٤ إدارة الصلاحيات الهامة والحساسة (Privileged Access Management). ٢-٢-٣-٥ المراجعة الدورية لهويات الدخول والصلاحيات.
٢-٢-٤	يجب مراجعة تطبيق متطلبات الأمن السيبراني لإدارة هويات الدخول والصلاحيات في الجهة دورياً.

٢-٣	حماية الأنظمة وأجهزة معالجة المعلومات (Information System and Processing Facilities Protection)
الهدف	ضمان حماية الأنظمة وأجهزة معالجة المعلومات بما في ذلك أجهزة المستخدمين والبنى التحتية للجهة من المخاطر السيبرانية.
الضوابط	
٢-٣-١	يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني لحماية الأنظمة وأجهزة معالجة المعلومات للجهة.
٢-٣-٢	يجب تطبيق متطلبات الأمن السيبراني لحماية الأنظمة وأجهزة معالجة المعلومات للجهة.
٢-٣-٣	يجب أن تغطي متطلبات الأمن السيبراني لحماية الأنظمة وأجهزة معالجة المعلومات للجهة بحد أدنى ما يلي: ٢-٣-٣-١ الحماية من الفيروسات والبرامج والأنشطة المشبوهة والبرمجيات الضارة (Malware) على أجهزة المستخدمين والخوادم باستخدام تقنيات وآليات الحماية الحديثة والمتقدمة، وإدارتها بشكل آمن. ٢-٣-٣-٢ التقييد الحازم لاستخدام أجهزة وسائط التخزين الخارجية والأمن المتعلق بها. ٢-٣-٣-٣ إدارة حزم التحديثات والإصلاحات للأنظمة والتطبيقات والأجهزة (Patch Management). ٢-٣-٣-٤ مزامنة التوقيت (Clock Synchronization) مركزياً ومن مصدر دقيق وموثوق، ومن هذه المصادر ما توفره الهيئة السعودية للمواصفات والمقاييس والجودة.
٢-٣-٤	يجب مراجعة متطلبات الأمن السيبراني لحماية الأنظمة وأجهزة معالجة المعلومات للجهة دورياً.
٢-٤	حماية البريد الإلكتروني (Email Protection)
الهدف	ضمان حماية البريد الإلكتروني للجهة من المخاطر السيبرانية.
الضوابط	
٢-٤-١	يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني لحماية البريد الإلكتروني للجهة.
٢-٤-٢	يجب تطبيق متطلبات الأمن السيبراني لحماية البريد الإلكتروني للجهة.
٢-٤-٣	يجب أن تغطي متطلبات الأمن السيبراني لحماية البريد الإلكتروني للجهة بحد أدنى ما يلي: ٢-٤-٣-١ تحليل وتصفية (Filtering) رسائل البريد الإلكتروني (وخصوصاً رسائل التصيّد الإلكتروني «Phishing Emails» والرسائل الاقتحامية «Spam Emails») باستخدام تقنيات وآليات الحماية الحديثة والمتقدمة للبريد الإلكتروني. ٢-٤-٣-٢ التحقق من الهوية متعدد العناصر (Multi-Factor Authentication) للدخول عن بعد والدخول عن طريق صفحة موقع البريد الإلكتروني (Webmail). ٢-٤-٣-٣ النسخ الاحتياطي والأرشفة للبريد الإلكتروني. ٢-٤-٣-٤ الحماية من التهديدات المتقدمة المستمرة (APT Protection)، التي تستخدم عادة الفيروسات والبرمجيات الضارة غير المعروفة مسبقاً (Zero-Day Malware)، وإدارتها بشكل آمن. ٢-٤-٣-٥ توثيق مجال البريد الإلكتروني للجهة بالطرق التقنية، مثل طريقة إطار سياسة المرسل (Sender Policy Framework).
٢-٤-٤	يجب مراجعة تطبيق متطلبات الأمن السيبراني الخاصة بحماية البريد الإلكتروني للجهة دورياً.

٢-٥	إدارة أمن الشبكات (Networks Security Management)
الهدف	ضمان حماية شبكات الجهة من المخاطر السيبرانية.
الضوابط	
٢-٥-١	يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني لإدارة أمن شبكات الجهة.
٢-٥-٢	يجب تطبيق متطلبات الأمن السيبراني لإدارة أمن شبكات الجهة.
٢-٥-٣	يجب أن تغطي متطلبات الأمن السيبراني لإدارة أمن شبكات الجهة بحد أدنى ما يلي: ٢-٥-٣-١ العزل والتقسيم المادي أو المنطقي لأجزاء الشبكات بشكل آمن، واللازم للسيطرة على مخاطر الأمن السيبراني ذات العلاقة، باستخدام جدار الحماية (Firewall) ومبدأ الدفاع الأمني متعدد المراحل (Defense-in-Depth). ٢-٥-٣-٢ عزل شبكة بيئة الإنتاج عن شبكات بيئات التطوير والاختبار. ٢-٥-٣-٣ أمن التصفح والاتصال بالإنترنت، ويشمل ذلك التقييد الحازم للمواقع الالكترونية المشبوهة، ومواقع مشاركة وتخزين الملفات، ومواقع الدخول عن بعد. ٢-٥-٣-٤ أمن الشبكات اللاسلكية وحمايتها باستخدام وسائل آمنة للتحقق من الهوية والتشفير، وعدم ربط الشبكات اللاسلكية بشبكة الجهة الداخلية إلا بناءً على دراسة متكاملة للمخاطر المترتبة على ذلك والتعامل معها بما يضمن حماية الأصول التقنية للجهة. ٢-٥-٣-٥ قيود وإدارة منافذ وبروتوكولات وخدمات الشبكة. ٢-٥-٣-٦ أنظمة الحماية المتقدمة لاكتشاف ومنع الاختراقات (Intrusion Prevention Systems). ٢-٥-٣-٧ أمن نظام أسماء النطاقات (DNS). ٢-٥-٣-٨ حماية قناة تصفح الإنترنت من التهديدات المتقدمة المستمرة (APT Protection)، التي تستخدم عادة الفيروسات والبرمجيات الضارة غير المعروفة مسبقاً (Zero-Day Malware)، وإدارتها بشكل آمن.
٢-٥-٤	يجب مراجعة تطبيق متطلبات الأمن السيبراني لإدارة أمن شبكات الجهة دورياً.
٢-٦	**أمن الأجهزة المحمولة (Mobile Devices Security)**
الهدف	ضمان حماية أجهزة الجهة المحمولة (بما في ذلك أجهزة الحاسب المحمول والهواتف الذكية والأجهزة الذكية اللوحية) من المخاطر السيبرانية. وضمان التعامل بشكل آمن مع المعلومات الحساسة والمعلومات الخاصة بأعمال الجهة وحمايتها أثناء النقل والتخزين عند استخدام الأجهزة الشخصية للعاملين في الجهة (مبدأ «BYOD»).
الضوابط	
٢-٦-١	يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني الخاصة بأمن الأجهزة المحمولة والأجهزة الشخصية للعاملين (BYOD) عند ارتباطها بشبكة الجهة.
٢-٦-٢	يجب تطبيق متطلبات الأمن السيبراني الخاصة بأمن الأجهزة المحمولة وأجهزة (BYOD) للجهة.

٢-٦-٣	يجب أن تغطي متطلبات الأمن السيبراني الخاصة بأمن الأجهزة المحمولة وأجهزة (BYOD) للجهة بحد أدنى ما يلي: ٢-٦-٣-١ فصل وتشفير البيانات والمعلومات (الخاصة بالجهة) المخزنة على الأجهزة المحمولة وأجهزة (BYOD). ٢-٦-٣-٢ الاستخدام المحدد والمقيد بناءً على ما تتطلبه مصلحة أعمال الجهة. ٢-٦-٣-٣ حذف البيانات والمعلومات (الخاصة بالجهة) المخزنة على الأجهزة المحمولة وأجهزة (BYOD) عند فقدان الأجهزة أو بعد انتهاء/إنهاء العلاقة الوظيفية مع الجهة. ٢-٦-٣-٤ التوعية الأمنية للمستخدمين.
٢-٦-٤	يجب مراجعة تطبيق متطلبات الأمن السيبراني الخاصة لأمن الأجهزة المحمولة وأجهزة (BYOD) للجهة دورياً.
٢-٧	**حماية البيانات والمعلومات (Data and Information Protection)**
الهدف	ضمان حماية السرية وسلامة بيانات ومعلومات الجهة ودقتها وتوافرها، وذلك وفقاً للسياسات والإجراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية ذات العلاقة.
الضوابط	
٢-٧-١	يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني لحماية بيانات ومعلومات الجهة، والتعامل معها وفقاً للمتطلبات التشريعية والتنظيمية ذات العلاقة.
٢-٧-٢	يجب تطبيق متطلبات الأمن السيبراني لحماية بيانات ومعلومات الجهة.
٢-٧-٣	يجب أن تغطي متطلبات الأمن السيبراني لحماية البيانات والمعلومات بحد أدنى ما يلي: ٢-٧-٣-١ ملكية البيانات والمعلومات. ٢-٧-٣-٢ تصنيف البيانات والمعلومات وآلية ترميزها (Classification and Labeling Mechanisms). ٢-٧-٣-٣ خصوصية البيانات والمعلومات.
٢-٧-٤	يجب مراجعة تطبيق متطلبات الأمن السيبراني لحماية بيانات ومعلومات الجهة دورياً.
٢-٨	**التشفير (Cryptography)**
الهدف	ضمان الاستخدام السليم والفعال للتشفير لحماية الأصول المعلوماتية الإلكترونية للجهة، وذلك وفقاً للسياسات والإجراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية ذات العلاقة.
الضوابط	
٢-٨-١	يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني للتشفير في الجهة.
٢-٨-٢	يجب تطبيق متطلبات الأمن السيبراني للتشفير في الجهة.
٢-٨-٣	يجب أن تغطي متطلبات الأمن السيبراني للتشفير بحد أدنى ما يلي: ٢-٨-٣-١ معايير حلول التشفير المعتمدة والقيود المطبقة عليها (تقنياً وتنظيمياً). ٢-٨-٣-٢ الإدارة الآمنة لمفاتيح التشفير خلال عمليات دورة حياتها. ٢-٨-٣-٣ تشفير البيانات أثناء النقل والتخزين بناء على تصنيفها وحسب المتطلبات التشريعية والتنظيمية ذات العلاقة.
٢-٨-٤	يجب مراجعة تطبيق متطلبات الأمن السيبراني للتشفير في الجهة دورياً.

٢-٩	إدارة النسخ الاحتياطية (Backup and Recovery Management)
الهدف	ضمان حماية بيانات ومعلومات الجهة والإعـدادات التقنية للأنظمة والتطبيقات الخاصة بالجهة من الأضرار الناجمة عن المخاطر السيبرانية، وذلك وفقاً للسياسات والإجراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية ذات العلاقة.
الضوابط	
٢-٩-١	يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني لإدارة النسخ الاحتياطية للجهة.
٢-٩-٢	يجب تطبيق متطلبات الأمن السيبراني لإدارة النسخ الاحتياطية للجهة.
٢-٩-٣	يجب أن تغطي متطلبات الأمن السيبراني لإدارة النسخ الاحتياطية بحد أدنى ما يلي: ٢-٩-٣-١ نطاق النسخ الاحتياطية وشموليتها للأصول المعلوماتية والتقنية الحساسة. ٢-٩-٣-٢ القدرة السريعة على استعادة البيانات والأنظمة بعد التعرض لحوادث الأمن السيبراني. ٢-٩-٣-٣ إجراء فحص دوري لمدى فعالية استعادة النسخ الاحتياطية.
٢-٩-٤	يجب مراجعة تطبيق متطلبات الأمن السيبراني لإدارة النسخ الإحتياطية للجهة.
٢-١٠	إدارة الثغرات (Vulnerabilities Management)
الهدف	ضمان اكتشاف الثغرات التقنية في الوقت المناسب ومعالجتها بشكل فعال، وذلك لمنع أو تقليل احتمالية استغلال هذه الثغرات من قبل الهجمات السيبرانية وتقليل الآثار المترتبة على أعمال الجهة.
الضوابط	
٢-١٠-١	يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني لإدارة الثغرات التقنية للجهة.
٢-١٠-٢	يجب تطبيق متطلبات الأمن السيبراني لإدارة الثغرات التقنية للجهة.
٢-١٠-٣	يجب أن تغطي متطلبات الأمن السيبراني لإدارة الثغرات بحد أدنى ما يلي: ٢-١٠-٣-١ فحص واكتشاف الثغرات دورياً. ٢-١٠-٣-٢ تصنيف الثغرات حسب خطورتها. ٢-١٠-٣-٣ معالجة الثغرات بناءً على تصنيفها والمخاطر السيبرانية المترتبة عليها. ٢-١٠-٣-٤ إدارة حزم التحديثات والإصلاحات الأمنية لمعالجة الثغرات. ٢-١٠-٣-٥ التواصل والاشتراك مع مصادر موثوقة فيما يتعلق بالتنبيهات المتعلقة بالثغرات الجديدة والمحدثة.
٢-١٠-٤	يجب مراجعة تطبيق متطلبات الأمن السيبراني لإدارة الثغرات التقنية للجهة دورياً.
٢-١١	اختبار الاختراق (Penetration Testing)
الهدف	تقييم واختبار مدى فعالية قدرات تعزيز الأمن السيبراني في الجهة، وذلك من خلال عمل محاكاة لتقنيات وأساليب الهجوم السيبراني الفعلية. ولاكتشاف نقاط الضعف الأمنية غير المعروفة والتي قد تؤدي إلى الاختراق السيبراني للجهة. وذلك وفقاً للمتطلبات التشريعية والتنظيمية ذات العلاقة.
الضوابط	
٢-١١-١	يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني لعمليات اختبار الاختراق في الجهة.
٢-١١-٢	يجب تنفيذ عمليات اختبار الاختراق في الجهة.

٢-١١-٣	يجب أن تغطي متطلبات الأمن السيبراني لاختبار الاختراق بحد أدنى ما يلي: ٢-١١-٣-١ نطاق عمل اختبار الاختراق، ليشمل جميع الخدمات المقدمة خارجياً (عن طريق الإنترنت) ومكوناتها التقنية، ومنها: البنية التحتية، المواقع الإلكترونية، تطبيقات الويب، تطبيقات الهواتف الذكية واللوحية، البريد الإلكتروني والدخول عن بعد. ٢-١١-٣-٢ عمل اختبار الاختراق دورياً.
٢-١١-٤	يجب مراجعة تطبيق متطلبات الأمن السيبراني لعمليات اختبار الاختراق في الجهة دورياً.
٢-١٢	**إدارة سجلات الأحداث ومراقبة الأمن السيبراني (Cybersecurity Event Logs and Monitoring Management)**
الهدف	ضمان تجميع وتحليل ومراقبة سجلات أحداث الأمن السيبراني في الوقت المناسب من أجل الاكتشاف الاستباقي للهجمات السيبرانية وإدارة مخاطرها بفعالية لمنع أو تقليل الآثار المترتبة على أعمال الجهة.
الضوابط	
٢-١٢-١	يجب تحديد وتوثيق واعتماد متطلبات إدارة سجلات الأحداث ومراقبة الأمن السيبراني للجهة.
٢-١٢-٢	يجب تطبيق متطلبات إدارة سجلات الأحداث ومراقبة الأمن السيبراني للجهة.
٢-١٢-٣	يجب أن تغطي متطلبات إدارة سجلات الأحداث ومراقبة الأمن السيبراني بحد أدنى ما يلي: ٢-١٢-٣-١ تفعيل سجلات الأحداث (Event logs) الخاصة بالأمن السيبراني على الأصول المعلوماتية الحساسة لدى الجهة. ٢-١٢-٣-٢ تفعيل سجلات الأحداث الخاصة بالحسابات ذات الصلاحيات الهامة والحساسة على الأصول المعلوماتية وأحداث عمليات الدخول عن بعد لدى الجهة. ٢-١٢-٣-٣ تحديد التقنيات اللازمة (SIEM) لجمع سجلات الأحداث الخاصة بالأمن السيبراني. ٢-١٢-٣-٤ المراقبة المستمرة لسجلات الأحداث الخاصة بالأمن السيبراني. ٢-١٢-٣-٥ مدة الاحتفاظ بسجلات الأحداث الخاصة بالأمن السيبراني (على ألا تقل عن ١٢ شهر).
٢-١٢-٤	يجب مراجعة تطبيق متطلبات إدارة سجلات الأحداث ومراقبة الأمن السيبراني في الجهة دورياً.
٢-١٣	**إدارة حوادث وتهديدات الأمن السيبراني (Cybersecurity Incident and Threat Management)**
الهدف	ضمان تحديد واكتشاف حوادث الأمن السيبراني في الوقت المناسب وإدارتها بشكل فعّال والتعامل مع تهديدات الأمن السيبراني استباقياً من أجل منع أو تقليل الآثار المترتبة على أعمال الجهة. مع مراعاة ما ورد في الأمر السامي الكريم رقم ٣٧١٤٠ وتاريخ ١٤ / ٨ / ١٤٣٨هـ.
الضوابط	
٢-١٣-١	يجب تحديد وتوثيق واعتماد متطلبات إدارة حوادث وتهديدات الأمن السيبراني في الجهة.
٢-١٣-٢	يجب تطبيق متطلبات إدارة حوادث وتهديدات الأمن السيبراني في الجهة.
٢-١٣-٣	يجب أن تغطي متطلبات إدارة حوادث وتهديدات الأمن السيبراني بحد أدنى ما يلي: ٢-١٣-٣-١ وضع خطط الاستجابة للحوادث الأمنية وآليات التصعيد. ٢-١٣-٣-٢ تصنيف حوادث الأمن السيبراني. ٢-١٣-٣-٣ تبليغ الهيئة عند حدوث حادثة أمن سيبراني. ٢-١٣-٣-٤ مشاركة التنبيهات والمعلومات الاستباقية ومؤشرات الاختراق وتقارير حوادث الأمن السيبراني مع الهيئة. ٢-١٣-٣-٥ الحصول على المعلومات الاستباقية (Threat Intelligence) والتعامل معها.
٢-١٣-٤	يجب مراجعة تطبيق متطلبات إدارة حوادث وتهديدات الأمن السيبراني في الجهة دورياً.

٢-١٤	الأمن المادي (Physical Security)
الهدف	ضمان حماية الأصول المعلوماتية والتقنية للجهة من الوصول المادي غير المصرح به والفقدان والسرقة والتخريب.
الضوابط	
٢-١٤-١	يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني لحماية الأصول المعلوماتية والتقنية للجهة من الوصول المادي غير المصرح به والفقدان والسرقة والتخريب.
٢-١٤-٢	يجب تطبيق متطلبات الأمن السيبراني لحماية الأصول المعلوماتية والتقنية للجهة من الوصول المادي غير المصرح به والفقدان والسرقة والتخريب.
٢-١٤-٣	يجب أن تغطي متطلبات الأمن السيبراني لحماية الأصول المعلوماتية والتقنية للجهة من الوصول المادي غير المصرح به والفقدان والسرقة والتخريب بحد أدنى ما يلي: ٢-١٤-٣-١ الدخول المصرح به للأماكن الحساسة في الجهة (مثل: مركز بيانات الجهة، مركز التعافي من الكوارث، أماكن معالجة المعلومات الحساسة، مركز المراقبة الأمنية، غرف اتصالات الشبكة، مناطق الإمداد الخاصة بالأجهزة والعتاد التقنية، وغيرها). ٢-١٤-٣-٢ سجلات الدخول والمراقبة (CCTV). ٢-١٤-٣-٣ حماية معلومات سجلات الدخول والمراقبة. ٢-١٤-٣-٤ أمن إتلاف وإعادة استخدام الأصول المادية التي تحوي معلومات مصنفة (وتشمل: الوثائق الورقية ووسائط الحفظ والتخزين). ٢-١٤-٣-٥ أمن الأجهزة والمعدات داخل مباني الجهة وخارجها.
٢-١٤-٤	يجب مراجعة متطلبات الأمن السيبراني لحماية الأصول المعلوماتية والتقنية للجهة من الوصول المادي غير المصرح به والفقدان والسرقة والتخريب دورياً.
٢-١٥	حماية تطبيقات الويب (Web Application Security)
الهدف	ضمان حماية تطبيقات الويب الخارجية للجهة من المخاطر السيبرانية.
الضوابط	
٢-١٥-١	يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني لحماية تطبيقات الويب الخارجية للجهة من المخاطر السيبرانية.
٢-١٥-٢	يجب تطبيق متطلبات الأمن السيبراني لحماية تطبيقات الويب الخارجية للجهة.
٢-١٥-٣	يجب أن تغطي متطلبات الأمن السيبراني لحماية تطبيقات الويب الخارجية للجهة بحد أدنى ما يلي: ٢-١٥-٣-١ استخدام جدار الحماية لتطبيقات الويب (Web Application Firewall). ٢-١٥-٣-٢ استخدام مبدأ المعمارية متعددة المستويات (Multi-tier Architecture). ٢-١٥-٣-٣ استخدام بروتوكولات آمنة (مثل بروتوكول HTTPS). ٢-١٥-٣-٤ توضيح سياسة الاستخدام الآمن للمستخدمين. ٢-١٥-٣-٥ التحقق من الهوية متعدد العناصر (Multi-Factor Authentication) لعمليات دخول المستخدمين.
٢-١٥-٤	يجب مراجعة متطلبات الأمن السيبراني لحماية تطبيقات الويب للجهة من المخاطر السيبرانية دورياً.

٣ صمود الأمن السيبراني (Cybersecurity Resilience)

٣-١	جوانب صمود الأمن السيبراني في إدارة استمرارية الأعمال (Cybersecurity Resilience aspects of Business Continuity Management "BCM")
الهدف	ضمان توافر متطلبات صمود الأمن السيبراني في إدارة استمرارية أعمال الجهة. وضمان معالجة وتقليل الآثار المترتبة على الاضطرابات في الخدمات الإلكترونية الحرجة للجهة وأنظمة وأجهزة معالجة معلوماتها جراء الكوارث الناتجة عن المخاطر السيبرانية.
الضوابط	
٣-١-١	يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني ضمن إدارة استمرارية أعمال الجهة.
٣-١-٢	يجب تطبيق متطلبات الأمن السيبراني ضمن إدارة استمرارية أعمال الجهة.
٣-١-٣	يجب أن تغطي إدارة استمرارية الأعمال في الجهة بحد أدنى ما يلي: ٣-١-٣-١ التأكد من استمرارية الأنظمة والإجراءات المتعلقة بالأمن السيبراني. ٣-١-٣-٢ وضع خطط الاستجابة لحوداث الأمن السيبراني التي قد تؤثر على استمرارية أعمال الجهة. ٣-١-٣-٣ وضع خطط التعافي من الكوارث (Disaster Recovery Plan).
٣-١-٤	يجب مراجعة متطلبات الأمن السيبراني ضمن إدارة استمرارية أعمال الجهة دورياً.

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

٤-١	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"). وفقاً للسياسات والإجراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية ذات العلاقة.
الضوابط	
٤-١-١	يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني ضمن العقود والاتفاقيات مع الأطراف الخارجية للجهة.
٤-١-٢	يجب أن تغطي متطلبات الأمن السيبراني ضمن العقود والاتفاقيات (مثل اتفاقية مستوى الخدمة SLA) مع الأطراف الخارجية التي قد تتأثر بإصابتها بيانات الجهة أو الخدمات المقدمة لها بحد أدنى ما يلي: ٤-١-٢-١ بنود المحافظة على سرية المعلومات (Non-Disclosure Clauses) و الحذف الآمن من قِبَل الطرف الخارجي لبيانات الجهة عند انتهاء الخدمة. ٤-١-٢-٢ إجراءات التواصل في حال حدوث حادثة أمن سيبراني. ٤-١-٢-٣ إلزام الطرف الخارجي بتطبيق متطلبات وسياسات الأمن السيبراني للجهة والمتطلبات التشريعية والتنظيمية ذات العلاقة.
٤-١-٣	يجب أن تغطي متطلبات الأمن السيبراني مع الأطراف الخارجية التي تقدم خدمات إسناد لتقنية المعلومات، أو خدمات مدارة بحد أدنى مايلي: ٤-١-٣-١ إجراء تقييم لمخاطر الأمن السيبراني، والتأكد من وجود مايضمن السيطرة على تلك المخاطر، قبل توقيع العقود والاتفاقيات أو عند تغيير المتطلبات التشريعية والتنظيمية ذات العلاقة. ٤-١-٣-٢ أن تكون مراكز عمليات خدمات الأمن السيبراني المدارة للتشغيل والمراقبة، والتي تستخدم طريقة الوصول عن بعد، موجودة بالكامل داخل المملكة.
٤-١-٤	يجب مراجعة متطلبات الأمن السيبراني مع الأطراف الخارجية دورياً.
٤-٢	**الأمن السيبراني المتعلق بالحوسبة السحابية والاستضافة**
الهدف	ضمان معالجة المخاطر السيبرانية وتنفيذ متطلبات الأمن السيبراني للحوسبة السحابية والاستضافة بشكل ملائم وفعّال، وذلك وفقاً للسياسات والإجراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية والأوامر والقرارات ذات العلاقة. وضمان حماية الأصول المعلوماتية والتقنية للجهة على خدمات الحوسبة السحابية التي تتم استضافتها أو معالجتها أو إدارتها بواسطة أطراف خارجية.
الضوابط	
٤-٢-١	يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني الخاصة باستخدام خدمات الحوسبة السحابية والاستضافة.
٤-٢-٢	يجب تطبيق متطلبات الأمن السيبراني الخاصة بخدمات الحوسبة السحابية والاستضافة للجهة.

٤-٢-٣	بما يتوافق مع المتطلبات التشريعية والتنظيمية ذات العلاقة، وبالإضافة إلى ما ينطبق من الضوابط ضمن المكونات الرئيسية رقم (١) و (٢) و (٣) والمكون الفرعي رقم (٤-١) الضرورية لحماية بيانات الجهة أو الخدمات المقدمة لها، يجب أن تغطي متطلبات الأمن السيبراني الخاصة باستخدام خدمات الحوسبة السحابية والاستضافة بحد أدنى ما يلي: ٤-٢-٣-١ تصنيف البيانات قبل استضافتها لدى مقدمي خدمات الحوسبة السحابية والاستضافة، وإعادتها للجهة (بصيغة قابلة للاستخدام) عند إنتهاء الخدمة. ٤-٢-٣-٢ فصل البيئة الخاصة بالجهة (وخصوصاً الخوادم الافتراضية) عن غيرها من البيئات التابعة لجهات أخرى في خدمات الحوسبة السحابية. ٤-٢-٣-٣ موقع استضافة وتخزين معلومات الجهة يجب أن يكون داخل المملكة.
٤-٢-٤	يجب مراجعة متطلبات الأمن السيبراني الخاصة بخدمات الحوسبة السحابية والاستضافة دورياً.

0 الأمن السيبراني لأنظمة التحكم الصناعي (Industrial Control Systems Cybersecurity)

١-٥	حماية أجهزة وأنظمة التحكم الصناعي
الهدف	ضمان إدارة الأمن السيبراني بشكل سليم وفعال لحماية توافر وسلامة وسرية أصول الجهة المتعلقة بأجهزة وأنظمة التحكم الصناعي (OT/ICS) ضد الهجوم السيبراني (مثل الوصول غير المصرح به والتخريب والتجسس والتلاعب) بما يتماشى مع إستراتيجية الأمن السيبراني للجهة، وإدارة مخاطر الأمن السيبراني، والمتطلبات التشريعية والتنظيمية ذات العلاقة، وكذلك المتطلبات الدولية المقرّة تنظيمياً على الجهة والمتعلقة بالأمن السيبراني.
الضوابط	
١-١-٥	يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني لحماية أجهزة وأنظمة التحكم الصناعي (OT/ICS) للجهة.
٢-١-٥	يجب تطبيق متطلبات الأمن السيبراني لحماية أجهزة وأنظمة التحكم الصناعي (OT/ICS) للجهة.
٣-١-٥	بالإضافة إلى ما يمكن تطبيقه من الضوابط ضمن المكونات الرئيسية رقم (١) و (٢) و (٣) و (٤) الضرورية لحماية بيانات الجهة وخدماتها، فإن متطلبات الأمن السيبراني لحماية أجهزة وأنظمة التحكم الصناعي (OT/ICS) يجب أن تغطي بحد أدنى ما يلي: ١-٣-١-٥ التقييد الحازم والتقسيم المادي والمنطقي عند ربط شبكات الإنتاج الصناعية (OT/ICS) مع الشبكات الأخرى التابعة للجهة، مثل: شبكة الأعمال الداخلية للجهة "Corporate Network". ٢-٣-١-٥ التقييد الحازم والتقسيم المادي والمنطقي عند ربط الأنظمة أو الشبكات الصناعية مع شبكات خارجية، مثل: الإنترنت أو الدخول عن بعد أو الاتصال اللاسلكي. ٣-٣-١-٥ تفعيل سجلات الأحداث (Event logs) الخاصة بالأمن السيبراني للشبكة الصناعية والاتصالات المرتبطة بها ما أمكن ذلك، والمراقبة المستمرة لها. ٤-٣-١-٥ عزل أنظمة معدات السلامة ("Safety Instrumented System "SIS). ٥-٣-١-٥ التقييد الحازم لاستخدام وسائط التخزين الخارجية. ٦-٣-١-٥ التقييد الحازم لتوصيل الأجهزة المحمولة على شبكة الإنتاج الصناعية. ٧-٣-١-٥ مراجعة إعدادات وتحصين الأنظمة الصناعية، وأنظمة الدعم والأجهزة الآلية الصناعية (Secure Configuration and Hardening) دورياً. ٨-٣-١-٥ إدارة ثغرات الأنظمة الصناعية (OT/ICS Vulnerability Management). ٩-٣-١-٥ إدارة حزم التحديثات والإصلاحات الأمنية للأنظمة الصناعية (OT/ICS Patch Management). ١٠-٣-١-٥ إدارة البرامج الخاصة بالأمن السيبراني الصناعي للحماية من الفيروسات والبرمجيات المشبوهة والضارة.
٤-١-٥	يجب مراجعة متطلبات الأمن السيبراني لحماية أجهزة وأنظمة التحكم الصناعي (OT/ICS) للجهة دورياً.

ملاحق

ملحق (أ): مصطلحات وتعريفات

يوضح الجدول ٢ أدناه بعض المصطلحات وتعريفاتها التي ورد ذكرها في هذه الضوابط.

جدول ٢ :مصطلحات وتعريفات

المصطلح	التعريف
الحماية من التهديدات المتقدمة المستمرة Advanced Persistent Threat (APT) Protection	الحماية من التهديدات المتقدمة التي تستخدم أساليب خفية تهدف إلى الدخول غير المشروع على الأنظمة والشبكات التقنية ومحاولة البقاء فيها لأطول فترة ممكنة عن طريق تفادي أنظمة الكشف والحماية. وهذه الأساليب تستخدم عادة الفيروسات والبرمجيات الضارة غير المعروفة مسبقاً (Zero-Day Malware) لتحقيق هدفها.
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 أيضاً أشياء أقل وضوحاً، مثل: المعلومات والخصائص (مثل: سمعة الجهة وصورتها العامة، أو المهارة والمعرفة).
هجوم Attack	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 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 شرطاً أساسياً للسماح بالوصول إلى الموارد في النظام.
صلاحية المستخدم Authorization	خاصية تحديد والتأكد من حقوق/تراخيص المستخدم للوصول إلى الموارد والأصول المعلوماتية والتقنية للجهة والسماح له وفقاً لما حدد مسبقاً في حقوق/تراخيص المستخدم.
توافر Availability	ضمان الوصول إلى المعلومات والبيانات والأنظمة والتطبيقات واستخدامها في الوقت المناسب.
النسخ الإحتياطية Backup	الملفات والأجهزة والبيانات والإجراءات المتاحة للاستخدام في حالة الأعطال أو الفقدان، أو إذا حذف الأصل منها أو توقف عن الخدمة.

المصطلح	التعريف
أحضر الجهاز الخاص بك Bring Your Own Device (BYOD)	يشير هذا المصطلح إلى سياسة جهة تسمح (سواءً بشكل جزئي أو كلي) للعاملين فيها بجلب الأجهزة الشخصية الخاصة بهم (أجهزة الكمبيوتر المحمولة والأجهزة اللوحية والهواتف الذكية) إلى أماكن العمل في الجهة، واستخدام هذه الأجهزة للوصول إلى الشبكات والمعلومات والتطبيقات والأنظمة التابعة للجهة المقيدة بصلاحيات دخول.
الدائرة التلفزيونية المغلقة (CCTV)	يستخدم التليفزيون ذو الدائرة المغلقة، والمعروف أيضاً باسم المراقبة بالفيديو، كاميرات الفيديو لإرسال إشارة إلى مكان محدد على مجموعة محدودة من الشاشات. وغالباً ما يطلق هذا المصطلح على تلك التقنية المستخدمة للمراقبة في المناطق التي قد تحتاج إلى مراقبة حيث يشكل الأمن المادي مطلباً هاماً فيها.
إدارة التغيير Change Management	وهو نظام لإدارة الخدمة حيث يضمن منهجاً نظامياً واستباقياً باستخدام أساليب وإجراءات معيارية فعالة (على سبيل المثال: التغيير في البنية التحتية للجهة، وشبكاتها، ..إلخ). تساعد إدارة التغيير جميع الأطراف المعنيين، بما في ذلك الأفراد والفرق على حد سواء، على الانتقال من حالتهم الحالية إلى الحالة المرغوبة التالية، كما تساعد إدارة التغيير أيضاً على تقليل تأثير الحوادث ذات العلاقة على الخدمة.
الحوسبة السحابية Cloud Computing	نموذج لتمكين الوصول عند الطلب إلى مجموعة مشتركة من موارد تقنية المعلومات (مثل: الشبكات والخوادم والتخزين والتطبيقات والخدمات) التي يمكن توفيرها بسرعة وإطلاقها بالحد الأدنى من الجهد الإداري التشغيلي والتدخل/ التفاعل لإعداد الخدمة من مزود الخدمة. تسمح الحوسبة السحابية للمستخدمين بالوصول إلى الخدمات القائمة على التقنية من خلال شبكة الحوسبة السحابية دون الحاجة لوجود معرفة لديهم أو تحكم في البنية التحتية التقنية التي تدعمهم. يتألف نموذج الحوسبة السحابية من خمس خصائص أساسية: خدمة ذاتية حسب الطلب، ووصول إلى الشبكة بشكل واسع، ومجمع الموارد، ومرونة سريعة، والخدمة المقاسة. وهناك ثلاثة نماذج لتقديم خدمات الحوسبة السحابية وهي: البرمجيات السحابية كخدمة "Saas" Software-as-Service، والنظام أو المنصة السحابية كخدمة "PaaS" Platform-as-Service، والبنية التحتية السحابية كخدمة "IaaS" Infrastructure-as-Service. كما أن هناك أربعة نماذج للحوسبة السحابية حسب طبيعة الدخول: الحوسبة السحابية العامة، والحوسبة السحابية المجتمعية، والحوسبة السحابية الخاصة، والحوسبة السحابية الهجين.
انتهاك أمني Compromise	الإفصاح عن أو الحصول على معلومات لأشخاص غير مصرح تسريبها أو الحصول عليها، أو انتهاك السياسة الأمنية السيبرانية للجهة بالإفصاح عن أو تغيير أو تخريب أو فقد شيء سواءً بقصد أو بغير بقصد. ويقصد بالانتهاك الأمني الإفصاح عن أو الحصول على بيانات حساسة أو تسريبها أو تغييرها أو تبديلها أو استخدامها بدون تصريح (بما في ذلك مفاتيح تشفير النصوص وغيرها من المعايير الأمنية السيبرانية الحرجة).
السرية Confidentiality	الاحتفاظ بقيود مصرح بها على الوصول إلى المعلومات والإفصاح عنها بما في ذلك وسائل حماية معلومات الخصوصية والملكية الشخصية.

المصطلح	التعريف
المعلومات (أو البيانات) الحساسة Confidential Data/ Information	هي المعلومات (أو البيانات) التي تعتبر غاية في الحساسية والأهمية، حسب تصنيف الجهة، والمُعدة للاستخدام من قبل جهة أو جهات محددة. وأحد الطرق التي يمكن استخدامها في تصنيف هذا النوع من المعلومات هو قياس مدى الضرر عند الإفصاح عنها أو الاطلاع عليها بشكل غير مصرح به أو فقدها أو تخريبها، حيث قد يؤدي ذلك إلى أضرار مادية أو معنوية على الجهة أو المتعاملين معها، أو التأثير على حياة الأشخاص ذو العلاقة بتلك المعلومات، أو التأثير والضرر بأمن الدولة أو اقتصادها الوطني أو مقدراتها الوطنية. وتشمل المعلومات الحساسة كل المعلومات التي يترتب على الإفصاح عنها بشكل غير مصرح به أو فقدها أو تخريبها مساءلة أو عقوبات نظامية.
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 الكبيرة. • تأثير كبير على الأمن القومي و/أو الدفاع الوطني و/أو اقتصاد الدولة أو مقدراتها الوطنية.
التشفير Cryptography	(ويسمى أيضاً علم التشفير) وهي القواعد التي تشتمل مبادئ ووسائل وطرق تخزين ونقل البيانات أو المعلومات 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 Cyber-Attack	الاستغلال المتعمّد لأنظمة الحاسب الآلي والشبكات والجهات التي يعتمد عملها على تقنية المعلومات والاتصالات الرقمية بهدف إحداث أضرار.
المخاطر السيبرانية Cyber Risks	المخاطر التي تمس 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.
الصمود الأمني السيبراني Cybersecurity Resilience	القدرة الشاملة للجهة على الصمود أمام الأحداث السيبرانية، ومسببات الضرر، والتعافي منها.
الأمن السيبراني Cybersecurity	حسب ما نص عليه تنظيم الهيئة الصادر بالأمر الملكي رقم (٦٨٠١) وتاريخ (١١/ ١٤٣٩/٢هـ)، فإن الأمن السيبراني هو 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.

المصطلح	التعريف
الفضاء السيبراني Cyberspace	الشبكة المترابطة من البنية التحتية لتقنية المعلومات، والتي تشمل الإنترنت وشبكات الاتصالات وأنظمة الحاسب الآلي والأجهزة المتصلة بالإنترنت، إلى جانب المعالِجات وأجهزة التحكم المرتبطة بها. كما يمكن أن يشير المصطلح إلى عالم أو نطاق افتراضي كظاهرة مجربة أو مفهوم مجرّد.
تصنيف البيانات والمعلومات Data and Information Classification	تعيين مستوى الحساسية للبيانات والمعلومات التي ينتج عنها ضوابط أمنية لكل مستوى من مستويات التصنيف. يتم تعيين مستويات حساسية البيانات والمعلومات وفقاً لفئات محددة مسبقاً حيث يتم إنشاء البيانات والمعلومات أو تعديلها أو تحسينها أو تخزينها أو نقلها. مستوى التصنيف هو مؤشر على قيمة أو أهمية البيانات والمعلومات للجهة.
أرشفة البيانات Data Archiving	عملية نقل البيانات التي لم تعد مستخدمة بشكل فعال في جهاز تخزين منفصل للحفظ طويل الأجل. تتكون بيانات الأرشيف من بيانات قديمة لا تزال مهمة للجهة وقد تكون مطلوبة للرجوع إليها في المستقبل، وبيانات يجب الاحتفاظ بها للالتزام بالتشريعات والتنظيمات ذات العلاقة.
الدفاع الأمني متعدد المراحل Defense-in-Depth	هو مفهوم لتوكيد المعلومات (Information Assurance) حيث يتم وضع مستويات متعددة من الضوابط الأمنية (كدفاع) في نظام تقنية المعلومات (IT) أو تقنية التشغيل (OT).
التعافي من الكوارث Disaster Recovery	الأنشطة والبرامج والخطط المصممة لإرجاع وظائف وخدمات الأعمال الحيوية للجهة إلى حالة مقبولة، بعد التعرض إلى هجمات سيبرانية أو تعطل لهذه الخدمات والوظائف.
نظام أسماء النطاقات Domain Name System	نظام تقني يستخدم قاعدة بيانات يتم توزيعها عبر الشبكة و/أو الإنترنت تسمح بتحويل أسماء النطاقات إلى عناوين الشبكة (IP Addresses)، والعكس، لتحديد عناوين الخدمات مثل خوادم المواقع الإلكترونية والبريد الإلكتروني.
فعالية Effectiveness	تشير الفعالية إلى الدرجة التي يتم بها تحقيق تأثير مخطط له. وتعتبر الأنشطة المخططة فعالة إذا تم تنفيذ هذه الأنشطة بالفعل، وتعتبر النتائج المخطط لها فعالة إذا تم تحقيق هذه النتائج بالفعل. يمكن استخدام مؤشرات قياس الأداء "Key Performance Indicators "KPIs لقياس وتقييم مستوى الفعالية.
كفاءة Efficiency	العلاقة بين النتائج المحققة (المخرجات) والموارد المستخدمة (المدخلات). يمكن تعزيز كفاءة العملية أو النظام من خلال تحقيق نتائج أكثر باستخدام نفس الموارد (المدخلات) أو أقل.
حدث Event	شيء يحدث في مكان محدد (مثل الشبكة والأنظمة والتطبيقات وغيرها) وفي وقت محدد.
بروتوكول نقل النص التشعبي الآمن Hyper Text Transfer Protocol Secure (HTTPS)	بروتوكول يستخدم التشفير لتأمين صفحات وبيانات الويب عند انتقالها عبر الشبكة. وهو عبارة عن نسخة آمنة من نظام بروتوكول نقل النص التشعبي (HTTP).

المصطلح	التعريف
هوية Identification	وسيلة التحقق من هوية المستخدم أو العملية أو الجهاز، وهي عادة شرط أساسي لمنح حق الوصول إلى الموارد في النظام.
حادثة Incident	انتهاك أمني بمخالفة سياسات الأمن السيبراني أو سياسات الاستخدام المقبول أو ممارسات أو ضوابط أو متطلبات الأمن السيبراني.
سلامة المعلومة Integrity	الحماية ضد تعديل أو تخريب المعلومات بشكل غير مصرح به، وتتضمن ضمان عدم الإنكار للمعلومات (Non-Repudiation) والموثوقية.
المتطلبات الوطنية والدولية (Inter)National Requirements	المتطلبات الوطنية هي متطلبات طورتها جهة تشريعية في المملكة العربية السعودية للاستخدام بشكل تنظيمي (مثل: الضوابط الأساسية للأمن السيبراني "ECC-1:2018"). المتطلبات الدولية هي متطلبات طورتها جهة أو منظمة دولية عالمية للاستخدام بشكل تنظيمي في جميع أنحاء العالم (مثل: PCI، SWIFT، وغيرها).
نظام الحماية المتقدمة لاكتشاف ومنع الاختراقات Intrusion Prevention System (IPS)	نظام لديه قدرات كشف الاختراقات، بالإضافة إلى القدرة على منع وإيقاف محاولات الأنشطة والحوادث المشبوهة أو المحتملة.
مؤشر قياس الأداء Key Performance Indicator (KPI)	نوع من أدوات قياس مستوى الأداء يُقيّم مدى نجاح نشاط ما أو جهة تجاه تحقيق أهداف محددة.
ترميز أو علامة Labeling	عرض معلومات (بتسمية وترميز محدد وقياسي) توضع على أصول الجهة (مثل: الأجهزة والتطبيقات والمستندات وغيرها) ليستدل بها للإشارة إلى بعض المعلومات المتعلقة بتصنيف الأصل وملكيته ونوعه وغيرها من المعلومات المتعلقة بإدارة الأصول.
الحد الأدنى من الصلاحيات Least Privilege	مبدأ أساسي في الأمن السيبراني يهدف إلى منح المستخدمين صلاحيات الوصول التي يحتاجونها لتنفيذ مسؤولياتهم الرسمية فقط.
البرمجيات الضارة Malware	برنامج يُصيب الأنظمة بطريقة خفية (في الغالب) لانتهاك سرية أو سلامة ودقة أو توافر البيانات أو التطبيقات أو نظم التشغيل.
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. تتضمن آليات التحقق عدة عناصر: • المعرفة (شيء يعرفه المستخدم فقط "مثل كلمة المرور"). • الحيازة (شيء يملكه المستخدم فقط "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 فقط "مثل بصمة الإصبع").

المصطلح	التعريف
المعمارية متعددة المستويات Multi-tier Architecture	معمارية أو بنية تُطبق أسلوب عميل-خادم الذي يتم فيه تطوير وصيانة منطق العملية الوظيفية، والوصول إلى البيانات، وتخزين البيانات وواجهة المستخدم كوحدات مستقلة على منصات منفصلة.
الحاجة إلى المعرفة والحاجة إلى الاستخدام Need-to-know and Need-to-use	القيود المفروضة على البيانات، والتي تعتبر حساسة ما لم يكن لدى الشخص حاجة محددة للاطلاع على البيانات لغرض ما متعلق بأعمال ومهام رسمية.
النسخ الاحتياطي غير المتصل أو خارج الموقع Offline/Offsite Backup	نسخة احتياطية لقاعدة البيانات وإعدادات الأنظمة والتطبيقات والأجهزة عندما تكون النسخة غير متصلة وغير قابلة للتحديث. عادةً ما تستخدم أشرطة (Tapes) في حالة النسخة الاحتياطية خارج الموقع.
النسخ الاحتياطي المتصل Online Backup	طريقة للتخزين يتم فيها النسخ الاحتياطي بانتظام عبر شبكة على خادم بعيد، (إما داخل شبكة الجهة أو بالاستضافة لدى مزود خدمة).
العاملون في الجهة Organization Staff	الأشخاص الذين يعملون في الجهة (بما في ذلك الموظفون الرسميون والموظفون المؤقتون والمتعاقدون).
الاسناد 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.
اختبار الاختراق Penetration Testing	ممارسة اختبار على نظام حاسب آلي أو شبكة أو تطبيق موقع إلكتروني أو تطبيق هواتف ذكية للبحث عن ثغرات يمكن أن يستغلها المهاجم.
رسائل التصيّد الإلكتروني Phishing Emails	محاولة الحصول على معلومات حساسة مثل أسماء المستخدمين وكلمات المرور أو تفاصيل بطاقة الائتمان، غالباً لأسباب ونوايا ضارة وخبيثة، وذلك بالتنكر على هيئة جهة جديرة بالثقة في رسائل بريد إلكترونية.
الأمن المادي Physical Security	يصف الأمن المادي التدابير الأمنية التي تم 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). ينطوي الأمن المادي على استخدام طبقات متعددة من نظم مترابطة، تشمل الدوائر التلفزيونية المغلقة (CCTV)، وحراس الأمن، وحدود أمنية، والأقفال، وأنظمة التحكم في الوصول، والعديد من التقنيات الأخرى.

المصطلح	التعريف
سياسة Policy	وثيقة تحدد بنودها التزاماً عاماً أو توجيهاً أو نية ما كما تم التعبير عن ذلك رسمياً من قبل صاحب الصلاحية للجهة. سياسة 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.
الخصوصية Privacy	الحرية من التدخل غير المصرح به أو الكشف عن معلومات شخصية حول فرد.
إدارة الصلاحيات الهامة والحساسة Privileged Access Management	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 Procedure	وثيقة تحتوي على وصف تفصيلي للخطوات الضرورية لأداء عمليات أو أنشطة محددة في التوافق مع المعايير 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 أو التحكم في شيء منقطع أو تالف أو مسروق أو ضائع.
مدة الاحتفاظ Retention	هي المدة الزمنية التي يجب فيها الاحتفاظ بالمعلومات أو البيانات أو سجلات الأحداث أو النسخ الاحتياطية، بغض النظر عن الشكل (ورقي أو إلكتروني أو غير ذلك).
المعايير الأمنية لشفرة البرامج والتطبيقات Secure Coding Standards	ممارسة تطوير برمجيات وتطبيقات الحاسب الآلي بطريقة تحمي من التعرض غير المقصود لثغرات الأمن السيبراني المتعلقة بالبرمجيات والتطبيقات.
مراجعة الإعدادات والتحصين Secure Configuration and Hardening	حماية وتحصين وضبط إعدادات جهاز الحاسب الآلي، والنظام، والتطبيق، وجهاز الشبكة، والجهاز الأمني لمقاومة الهجمات السيبرانية. مثل: إيقاف أو تغيير الحسابات المصنعية والافتراضية، إيقاف الخدمات غير المستخدمة، إيقاف منافذ الشبكة غير المستخدمة.
نظام إدارة سجلات الأحداث ومراقبة الأمن السيبراني Security Information and Event Management (SIEM)	نظام يقوم بإدارة وتحليل بيانات سجلات الأحداث الأمنية في الوقت الفعلي لتوفير مراقبة للتهديدات، وتحليل نتائج القواعد المترابطة لسجلات الأحداث، والتقارير حول بيانات السجلات، والاستجابة للحوادث.

المصطلح	التعريف
الاختبار الأمني Security Testing	عملية تهدف إلى التأكد من أن النظام أوالتطبيق المعدّل أو الجديد يتضمن ضوابط وحمايات أمنية مناسبة ولا يحتوي على أي ثغرات أمنية قد تضر بالأنظمة أو التطبيقات الأخرى، أو تؤدي إلى سوء استخدام النظام أو التطبيق أو معلوماته، وكذلك للحفاظ على وظيفة النظام أو التطبيق على النحو المنشود.
الأمن من خلال التصميم Security-by-Design	منهجية لتطوير الأنظمة والتطبيقات وتصميم الشبكات التي تسعى إلى جعلها خالية من نقاط الضعف والثغرات الأمنية السيبرانية، والمقدرة على صد الهجوم السيبراني قدر الإمكان من خلال عدة تدابير على سبيل المثال: الاختبار المستمر، وحماية المصادقة والتمسك بأفضل ممارسات البرمجة والتصميم، وغيرها.
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.
إطار سياسة المرسل Sender Policy Framework	طريقة للتحقق من أن خادم البريد الإلكتروني المستخدم في إرسال رسائل البريد الإلكتروني يتبع المجال الخاص بالجهة المرسِلة.
طرف خارجي Third-Party	أي جهة تعمل كطرف في علاقة تعاقدية لتقديم السلع أو الخدمات (وهذا يشمل موردي ومزودي الخدمات).
تهديد Threat	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 مستغلاً 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 أحد نقاط الضعف الخاصة بنظام معلومات معين. وهذا التعريف يشمل التهديدات السيبرانية.
المعلومات الاستباقية Threat Intelligence	يوفر معلومات منظمة وتحليلها حول الهجمات الأخيرة والحالية والمحتملة التي يمكن أن تشكل تهديداً سيبرانياً للجهة.
الثغرة Vulnerability	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.
جدار الحماية لتطبيقات الويب Web Application Firewall	نظام حماية يوضع قبل تطبيقات الويب لتقليل المخاطر الناجمة من محاولات الهجوم الموجهة على تطبيقات الويب.
البرمجيات الضارة غير المعروفة مسبقاً Zero-Day Malware	عبارة عن برمجيات ضارة (Malware) غير معروفة مسبقاً، تم إنتاجها أو نشرها حديثاً. ويصعب في العادة اكتشافها بواسطة وسائل الحماية التي تعتمد على المعرفة المسبقة للبرمجيات الضارة (Signature-based Protection).

ملحق (ب): قائمة الاختصارات

يوضح الجدول ٣ أدناه معنى الاختصارات التي ورد ذكرها في هذه الضوابط.

جدول ٣ : قائمة الاختصارات

الاختصار	معناه
APT	Advanced Persistent Threat التهديدات المتقدمة المستمرة
BCM	Business Continuity Management إدارة استمرارية الأعمال
BYOD	Bring Your Own Device سياسة أحضر الجهاز الخاص بك
CCTV	Closed-circuit television الدائرة التلفزيونية المغلقة
CNI	Critical National Infrastructure البنية التحتية الحساسة
DNS	Domain Name System نظام أسماء النطاقات
ECC	Essential Cybersecurity Controls الضوابط الأساسية للأمن السيبراني
HTTPS	Hyper Text Transfer Protocol Secure بروتوكول نقل النص التشعبي الآمن
ICS	Industrial Control System نظام التحكم الصناعي
ICT	Information and Communication Technology تقنية المعلومات والاتصالات
IT	Information Technology تقنية المعلومات
MFA	Multi-Factor Authentication التحقق من الهوية متعدد العناصر
OT	Operational Technology التقنية التشغيلية
SIEM	Security Information and Event Management نظام إدارة سجلات الأحداث ومراقبة الأمن السيبراني
SIS	Safety Instrumented System نظام معدات السلامة
SLA	Service Level Agreement اتفاقية مستوى الخدمة

الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority