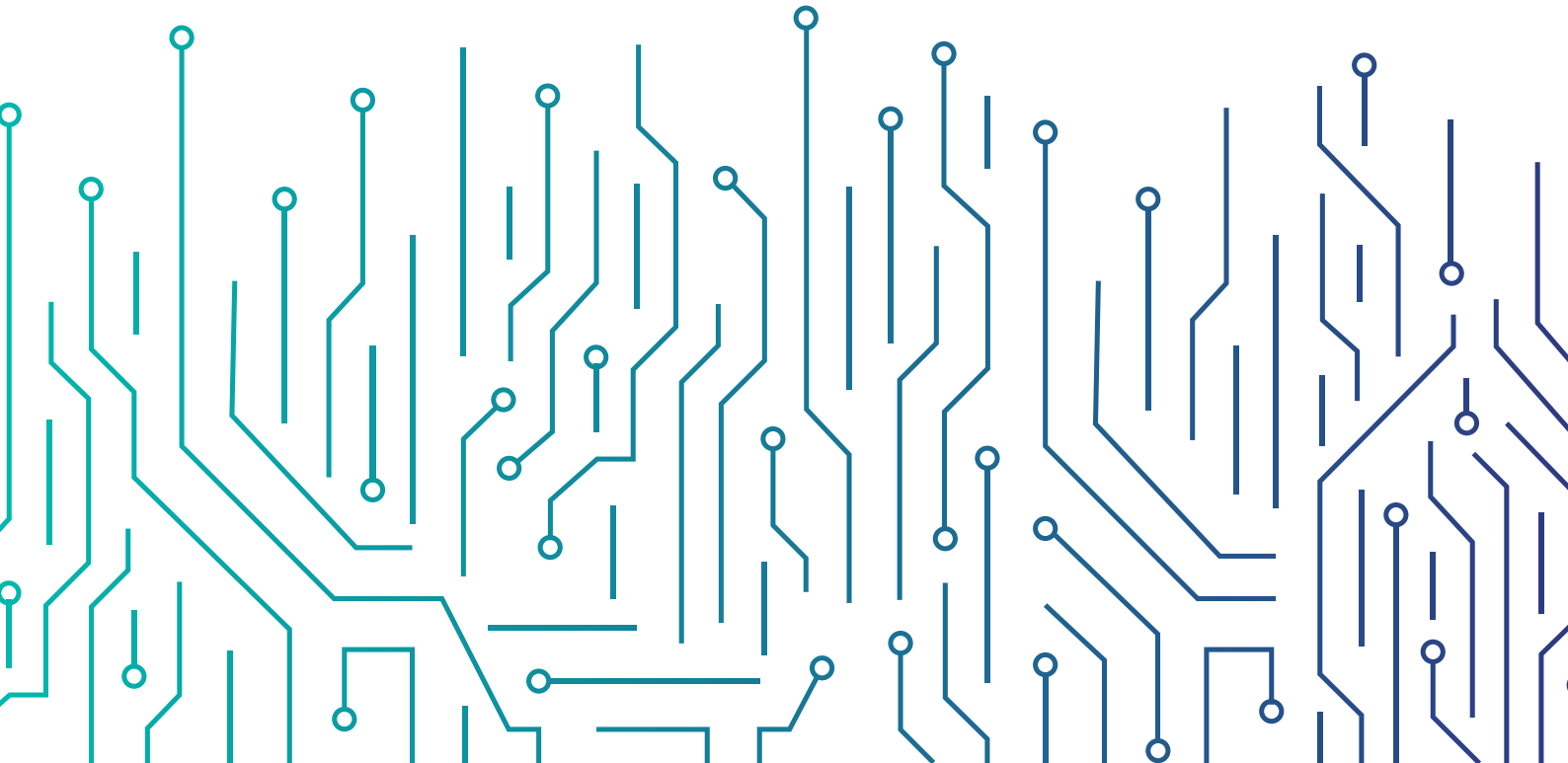
الهيئة الوطنية للأمن السيبـراني
National Cybersecurity Authority

ضوابط الأمن السيبراني
للأنظمة الحساسة

Critical Systems Cybersecurity Controls

(CSCC - 1 : 2019)

إشـــارة المـــشـــاركـــة: أبـيـض
تـصـنـيـف الـوثـيـقـة: مـتـــاح



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 ٦
المقدمة ٧
الأهداف ٧
تعريف ومعايير قياس الأنظمة الحساسة
تعريف الأنظمة الحساسة ٨
معايير قياس الأنظمة الحساسة ٨
مكونات الأنظمة الحساسة ٩
نطاق العمل وقابلية التطبيق
نطاق عمل الضوابط ١٠
قابلية التطبيق داخل الجهة (Statement of Applicability) ١٠
التنفيذ والالتزام ١١
التحديث والمراجعة ١١
مكونات وهيكلية ضوابط الأمن السيبراني للأنظمة الحساسة
المكونات الأساسية والفرعية لضوابط الأمن السيبراني للأنظمة الحساسة الهيكلية ١٢
ضوابط الأمن السيبراني للأنظمة الحساسة
١- حوكمة الأمن السيبراني (Cybersecurity Governance) ١٤
٢- تعزيز الأمن السيبراني (Cybersecurity Defense) ١٦
٣- صمود الأمن السيبراني (Cybersecurity Resilience) ٢٣
٤- الأمن السيبراني المتعلق بالأطراف الخارجية والحوسبة السحابية (Third-Party and Cloud Computing Cybersecurity) ٢٤
ملاحق
ملحق (أ): العلاقة مع الضوابط الأساسية للأمن السيبراني ٢٥
ملحق (ب): مصطلحات وتعريفات ٢٨
ملحق (ج): قائمة الاختصارات ٣٠
قائمة الجداول
جدول ١ : هيكلية ضوابط الأمن السيبراني للأنظمة الحساسة ١٣
جدول ٢ : مصطلحات وتعريفات ٢٨
جدول ٣ : قائمة الاختصارات ٣٠
قائمة الأشكال والرسوم التوضيحية
شكل ١: المكونات الأساسية والفرعية لضوابط الأمن السيبراني للأنظمة الحساسة ١٢
شكل ٢: معنى رموز ضوابط الأمن السيبراني للأنظمة الحساسة ١٣
شكل ٣: هيكلية ضوابط الأمن السيبراني للأنظمة الحساسة ١٣
شكل ٤: دليل ألوان المكونات الفرعية في الشكل ٥ ٢٥
شكل ٥: مكونات الضوابط الأساسية للأمن السيبراني، وضوابط الأمن السيبراني للأنظمة الحساسة ٢٧

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. على أن يتبع ذلك تنامي قدرات المعالجة الحاسوبية، وقدرات التخزين الهائلة للبيانات وتبادلها؛ بما 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. وقد تمت الموافقة على تنظيمها بموجب الأمر الملكي الكريم ذي الرقم ٦٨٠١ والتاريخ ١١ / ٢ / ١٤٣٩ هـ، وجعلها الجهة المختصة في المملكة بالأمن السيبراني، والمرجع الوطني في شؤونه.

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

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

وقد نص التنظيم الآنف الذكر على أن دور الهيئة التنظيمي لا يُخلي أي جهة عامة أو خاصة، أو غيرها من مسؤوليتها تجاه أمنها السيبراني؛ وهو ما أكده الأمر السامي الكريم ذو الرقم ٥٧٢٣١ والتاريخ ١٠ / ١١ / ١٤٣٩ هـ 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»، وكذلك ما أكده الأمر السامي الكريم ذو الرقم ٧٧٣٢ والتاريخ ١٢ / ٢ / ١٤٤٠ هـ.

ومن هذا المنطلق؛ قامت الهيئة الوطنية للأمن السيبراني بإعداد ضوابط الأمن السيبراني للأنظمة الحساسة (CSCC - 1 : 2019) لوضع الحد الأدنى من متطلبات الأمن السيبراني للأنظمة الحساسة في الجهات العامة، بالإضافة إلى الضوابط الأساسية للأمن السيبراني (ECC - 1 : 2018). وتوضح هذه الوثيقة تفاصيل ضوابط الأمن السيبراني للأنظمة الحساسة، وأهدافها، ونطاق العمل، وآلية الالتزام والمتابعة.

وعلى مختلف الجهات العامة التي تملك أنظمة حساسة أو تشغلها؛ تنفيذ ما يحقق الالتزام الدائم، والمستمر بهذه الضوابط على الأنظمة الحساسة؛ تحقيقاً لما ورد في الفقرة الثالثة من المادة العاشرة، في تنظيم الهيئة الوطنية للأمن السيبراني؛ وكذلك ما ورد في الأمر السامي الكريم ذي الرقم ٥٧٢٣١ والتاريخ ١٠ / ١١ / ١٤٣٩ هـ وما ورد في الأمر السامي الكريم ذي الرقم ٧٧٣٢ والتاريخ ١٢ / ٢ / ١٤٤٠ هـ.

المقدمة

قامت الهيئة الوطنية للأمن السيبراني، ويشار لها في هذه الوثيقة بـ (الهيئة)؛ بإصدار الضوابط الأساسية للأمن السيبراني (ECC - 1 : 2018)، وهي الضوابط التي وضعت الحد الأدنى من متطلبات الأمن السيبراني، الواجب الالتزام المستمر بها، من قبل الجهات العامة. وعلى هذا الأساس جاء تطوير هذه الوثيقة المتضمنة لضوابط الأمن السيبراني للأنظمة الحساسة (CSCC - 1 : 2019) التي تأتي امتداداً للضوابط الأساسية؛ ومكملة لها، و تكون أكثر ملاءمة لما هو حساس من الأنظمة الوطنية.

وقد شملت مراحل إعداد هذه الضوابط، دراسة عدد من المعايير، والأطر والضوابط، ذات الأهداف المماثلة لدى جهات ومنظمات دولية. وكذلك دراسة متطلبات التشريعات، والتنظيمات والقرارات الوطنية، ذات العلاقة؛ والاطلاع على أفضل الممارسات، والتجارب في مجال الأمن السيبراني، والاستفادة منها؛ إضافة إلى تحليل ما تم رصده من حوادث، وهجمات سيبرانية على مستوى الجهات العامة.

وقد حرصت الهيئة في إعدادها لضوابط الأمن السيبراني للأنظمة الحساسة، على مواءمة مكوناتها مع مكونات الضوابط الأساسية للأمن السيبراني إذ تعد متطلباً أساسياً لها؛ ولا يمكن تحقيق الالتزام بها إلا من خلال تحقيق الالتزام المستمر بالضوابط الأساسية للأمن السيبراني في المقام الأول كما هي مرتبطة مع المتطلبات التشريعية، والتنظيمية الوطنية والدولية، ذات العلاقة. وبناءً على ذلك فقد جاءت مكونات ضوابط الأمن السيبراني للأنظمة الحساسة على النحو الآتي:

- ٤ مكونات أساسية (4 Main Domains)
- ٢١ مكوناً فرعياً (21 Subdomains)
- ٣٢ ضابطاً أساسياً (32 Main Controls)
- ٧٣ ضابطاً فرعياً (73 Subcontrols)

الأهداف

امتداداً للضوابط الأساسية للأمن السيبراني؛ تهدف ضوابط الأمن السيبراني للأنظمة الحساسة إلى تمكين الجهات العامة؛ وتطوير قدرات الحماية، والصمود ضد الهجمات السيبرانية، والمحافظة على الأصول المعلوماتية والتقنية، للأنظمة الحساسة، المبنية على أفضل الممارسات والمعايير الدولية؛ وذلك بهدف تلبية الاحتياجات الحالية الأمنية، ورفع جاهزية الجهات، ضمن نطاق عمل هذه الضوابط، حيال المخاطر السيبرانية المتزايدة على أنظمتها الحساسة، التي قد ينجم عنها تأثيرات سلبية، وخسائر مكلفة على المستوى الوطني.

تعريف الأنظمة الحساسة ومعايير تحديدها

تعريف الأنظمة الحساسة

هي أي أنظمة أو شبكات، يؤدي تعطلها، أو التغيير غير المشروع لطريقة عملها، أو الدخول غير المصرح به لها، أو للبيانات والمعلومات التي تحفظها أو تعالجها؛ إلى التأثير السلبي على توافر الخدمات، أو أعمال الجهة العامة، أو إحداث آثار اقتصادية أو مالية أو أمنية، أو اجتماعية سلبية كبيرة، على المستوى الوطني.

معايير تحديد الأنظمة الحساسة

يعد النظام حساساً، إذا كان تعطله، أو التغيير غير المشروع لطريقة عمله، أو الدخول غير المصرح به له، أو للبيانات والمعلومات التي يحفظها أو يعالجها؛ يؤدي بشكل مباشر، أو غير مباشر إلى احتمالية تحقق واحد أو أكثر من المعايير الآتية (حسب تحديدها من الجهة المالكة للنظام):

١ . التأثير السلبي على الأمن الوطني.

٢ . التأثير السلبي على سمعة المملكة وصورتها العامة.

٣ . خسائر مالية كبيرة (مثال: أكثر من ٠,٠١ ٪ من إجمالي الناتج المحلي الوطني).

٤ . التأثير السلبي على خدمات مقدمة لعدد كبير من المستخدمين (مثال: أكثر من ٥٪ من التعداد السكاني).

٥ . خسائر في الأرواح.

٦ . الإفشاء غير المصرح به لبيانات يكون تصنيفها سري أو سري للغاية.

٧ . التأثير السلبي على أعمال قطاع حيوي (أو أكثر).

مكونات الأنظمة الحساسة

المكونات المعتمدة للأنظمة الحساسة هي (المكونات من ١ - ٨ هي المكونات التقنية):

١ . الشبكة؛ على سبيل المثال:

١-١ الأجهزة المرتبطة بالشبكة (Connecting Devices) مثل:

- الموجّه (Router).
- المبدلات (Switches).
- البوابات (Gateways).

١-٢ جدار الحماية (Firewall).

١-٣ أجهزة كشف التسلل ومنعه (IDS/IPS).

١-٤ أجهزة الحماية من التهديدات المتقدمة المستمرة (APT Protection).

٢ . قواعد البيانات (Databases).

٣ . وحدات الحفظ والتخزين (Storage Assets).

٤ . برمجيات التكامل الوسيطة (Middleware).

٥ . الخوادم وأنظمة التشغيل الخاصة بها (Servers and Operating Systems).

٦ . التطبيقات (Applications).

٧ . أجهزة التشفير (Encryption Devices).

٨ . الأجهزة الملحقة بالأنظمة الحساسة؛ على سبيل المثال: الطابعات والماسحات الضوئية.

٩ . الأشخاص العاملون في وظائف دعم الأنظمة الحساسة (مثل: المستخدمون، العاملون في الوظائف التقنية، ذات الصلاحيات الهامة، والحساسة، والمشغلون، مقدمو الخدمات).

١٠ . الوثائق المتعلقة بما سبق من المكونات.

نطاق العمل وقابلية التطبيق

نطاق عمل الضوابط

يجب تطبيق هذه الضوابط على الأنظمة الحساسة -وفقاً للمعايير المذكورة في هذه الوثيقة- من قبل الجهات العامة المالكة أو المشغلة لهذه الأنظمة، سواء أكانت جهات حكومية (مثل وزارات وهيئات ومؤسسات وسفارات وغيرها) داخل المملكة العربية السعودية؛ أو خارجها، أو جهات وشركات تابعة للجهات الحكومية، أو جهات القطاع الخاص ويشار لها جميعاً في هذا الوثيقة بـ (الجهة).

قابلية التطبيق داخل الجهة (Statement of Applicability)

يجب على كل جهة الالتزام بجميع الضوابط القابلة للتطبيق عليها، بعد قياس مدى التأثير، وإجراء الفحوصات اللازمة قبل التطبيق. ونشير هنا إلى مثال على الضوابط التي تتفاوت فيها قابلية التطبيق، من جهة إلى أخرى:

- الضوابط ضمن المكون الفرعي رقم (٤ - ٢) المتعلقة بالأمن السيبراني للحوسبة السحابية والاستضافة (Cloud Computing and Hosting Cybersecurity) تكون قابلة للتطبيق؛ وملزمة للجهة التي تستخدم حالياً خدمات الحوسبة السحابية، والاستضافة، 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 ذي الرقم ٥٧٢٣١ والتاريخ ١٠ / ١١ / ١٤٣٩ هـ وما ورد في الأمر السامي الكريم ذي الرقم ٧٧٣٢ والتاريخ ١٢ / ٢ / ١٤٤٠ هـ، يجب على جميع الجهات ضمن نطاق عمل هذه الضوابط ما يلي:

١ . تحديد أنظمتها الحساسة باستخدام (معايير تحديد الأنظمة الحساسة).

٢ . تنفيذ ما يحقق الالتزام بهذه الضوابط على الأنظمة الحساسة المحددة؛ خلال فترة تحقيق الالتزام التي تحددها الهيئة على أن يتم تقييم المخاطر السيبرانية وإدارتها، خلال هذه الفترة لتقليل المخاطر المحتملة.

٣ . العمل على تحقيق الالتزام الدائم والمستمر، بعد فترة تحقيق الالتزام.

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

التحديث والمراجعة

تتولى الهيئة مسؤولية التحديث، والمراجعة الدورية، لضوابط الأمن السيبراني للأنظمة الحساسة؛ حسب مستجدات الأمن السيبراني ذات العلاقة. كما تتولى الهيئة إعلان الإصدار المحدث من الضوابط لتطبيقه والالتزام به.

مكونات وهيكلية ضوابط الأمن السيبراني للأنظمة الحساسة

المكونات الأساسية والفرعية، لضوابط الأمن السيبراني للأنظمة الحساسة

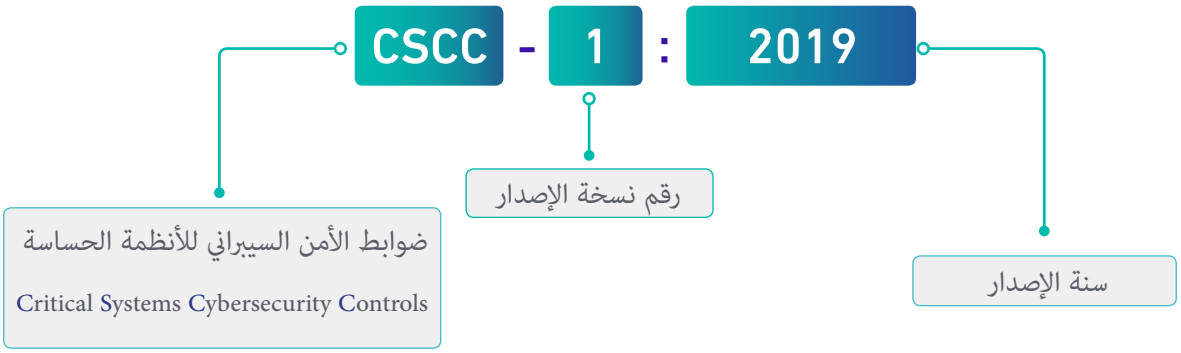
يوضح الشكل الآتي، المكونات الأساسية والفرعية، لضوابط الأمن السيبراني للأنظمة الحساسة. كما يوضح ملحق (أ) العلاقة مع الضوابط الأساسية للأمن السيبراني.

١ - حوكمة الأمن السيبراني Cybersecurity Governance	١ - ١	إستراتيجية الأمن السيبراني Cybersecurity Strategy	١ - ٢	إدارة مخاطر الأمن السيبراني Cybersecurity Risk Management
	١ - ٣	الأمن السيبراني ضمن إدارة المشاريع المعلوماتية والتقنية Cybersecurity in Information Technology Projects	١ - ٤	المراجعة والتدقيق الدوري للأمن السيبراني Cybersecurity Periodical Assessment and Audit
	١ - ٥	الأمن السيبراني المتعلق بالموارد البشرية Cybersecurity in Human Resources		
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	إدارة أمن الشبكات Networks Security Management
	٢ - ٥	أمن الأجهزة المحمولة Mobile Devices Security	٢ - ٦	حماية البيانات والمعلومات Data and Information Protection
	٢ - ٧	التشفير Cryptography	٢ - ٨	إدارة النسخ الاحتياطية Backup and Recovery Management
	٢ - ٩	إدارة الثغرات Vulnerabilities Management	٢ - ١٠	اختبار الاختراق Penetration Testing
	٢ - ١١	إدارة سجلات الأحداث ومراقبة الأمن السيبراني Cybersecurity Event Logs and Monitoring Management	٢ - ١٢	حماية تطبيقات الويب Web Application Security
	٢ - ١٣	حماية التطبيقات Application Security		
٣ - صمود الأمن السيبراني Cybersecurity Resilience	٣ - ١	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

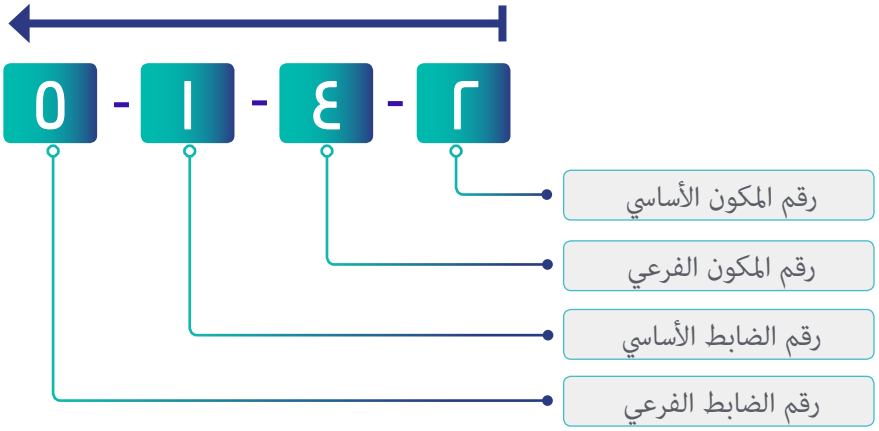
شكل ١: المكونات الأساسية والفرعية لضوابط الأمن السيبراني للأنظمة الحساسة

الهيكلية

يوضح الشكلان ٢ و ٣ أدناه معنى رموز ضوابط الأمن السيبراني للأنظمة الحساسة.



شكل ٢ : معنى رموز ضوابط الأمن السيبراني للأنظمة الحساسة



شكل ٣: هيكلية ضوابط الأمن السيبراني للأنظمة الحساسة

يرجى ملاحظة أن الأرقام بالأخضر (مثل: ١ - ٨ - ١)، هي عبارة عن إشارة مرجعية لمكون فرعي أو ضابط من الضوابط الأساسية للأمن السيبراني.

يوضح الجدول ١ طريقة هيكلية ضوابط الأمن السيبراني للأنظمة الحساسة.

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

جدول ١: هيكلية ضوابط الأمن السيبراني للأنظمة الحساسة

ضوابط الأمن السيبراني للأنظمة الحساسة

تفاصيل ضوابط الأمن السيبراني للأنظمة الحساسة

١ حوكمة الأمن السيبراني (Cybersecurity Governance)

١-١	إستراتيجية الأمن السيبراني (Cybersecurity Strategy)
الهدف	ضمان احتواء خطط العمل والأهداف والمبادرات والمشاريع داخل الجهة للأمن السيبراني وإسهامها في تحقيق المتطلبات التشريعية والتنظيمية ذات العلاقة.
الضوابط	
١-١-١	بالإضافة للضوابط ضمن المكون الفرعي ١ - ١ في الضوابط الأساسية للأمن السيبراني، يجب أن تضع إستراتيجية الأمـن السيبراني للجهة أولـويـة لدعم حماية الأنظمة الحساسة الخاصة بالجهة.
١-٢	إدارة مخاطر الأمن السيبراني (Cybersecurity Risk Management)
الهدف	ضمان إدارة مخاطر الأمن السيبراني؛ لحماية الأصول المعلوماتية والتقنية للجهة، على نحو ممنهج؛ وذلك وفقاً للسياسات والإجراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية ذات العلاقة.
الضوابط	
١-٢-١	بالإضافة للضوابط ضمن المكون الفرعي ١ - ٥ في الضوابط الأساسية للأمن السيبراني، يجب أن تشمل منهجية إدارة مخاطر الأمن السيبراني بحد أدنى ما يأتي: ١ - ٢ - ١ - ١ تنفيذ إجراء تقييم مخاطر الأمن السيبراني، على الأنظمة الحساسة، مرة واحدة سنوياً، على الأقل. ١ - ٢ - ١ - ٢ إنشاء سجل مخاطر الأمن السيبراني الخاص بالأنظمة الحساسة، ومتابعته مرة شهرياً على الأقل.
١-٣	الأمن السيبراني ضمن إدارة المشاريع المعلوماتية والتقنية (Cybersecurity in Information Technology Projects)
الهدف	التأكد من أن متطلبات الأمن السيبراني مضمنة في منهجية إدارة مشاريع الجهة وإجراءاتها؛ لحماية السرية، وسلامة الأصول المعلوماتية والتقنية للجهة، ودقتها وتوافرها؛ وذلك وفقاً للسياسات والإجراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية ذات العلاقة.
الضوابط	
١-٣-١	بالإضافة للضوابط الفرعية ضمن الضابط ١ - ٦ - ٢ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني، لإدارة المشاريع والتغييرات على الأصول المعلوماتية والتقنية للأنظمة الحساسة في الجهة، بحد أدنى؛ ما يلي: ١ - ٣ - ١ - ١ إجراء اختبار التحمل (Stress Testing) للتأكد من سعة المكونات المختلفة. ١ - ٣ - ١ - ٢ التأكد من تطبيق متطلبات استمرارية الأعمال.

١-٣-٢	بالإضافة للضوابط الفرعية ضمن الضابط ١ - ٦ - ٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني، لمشاريع تطوير التطبيقات، والبرمجيات الخاصة بالأنظمة الحساسة للجهة، بحد أدنى؛ ما يلي: ١ - ٣ - ٢ - ١ إجراء مراجعة أمنية للشفرة المصدرية، قبل إطلاقها (Security Source Code Review). ١ - ٣ - ٢ - ٢ تأمين الوصول، والتخزين، والتوثيق للشفرة المصدرية (Source Code) وإصداراتها. ١ - ٣ - ٢ - ٣ تأمين واجهة برمجة التطبيقات (Authenticated API). ١ - ٣ - ٢ - ٤ النقل الآمن والموثوق للتطبيقات من بيئات الاختبار (Testing Environment) إلى بيئات الإنتاج (Production Environment) مع حذف أي بيانات، أو هويات، أو كلمات مرور، متعلقة ببيئات الاختبار، قبل النقل.
٤-١	**المراجعة والتدقيق الدوري للأمن السيبراني (Cybersecurity Periodical Assessment and Audit)**
الهدف	ضمان التأكد من أن ضوابط الأمن السيبراني، لدى الجهة؛ مطبقة، وتعمل وفقاً للسياسات والإجراءات التنظيمية للجهة؛ وكذلك للمتطلبات التشريعية والتنظيمية الوطنية ذات العلاقة، والمتطلبات الدولية المقرّة تنظيمياً على الجهة.
الضوابط	
١-٤-١	رجوعاً للضابط ١ - ٨ - ١ في الضوابط الأساسية للأمن السيبراني، فإنه يجب على الإدارة المعنية بالأمن السيبراني؛ مراجعة تطبيق ضوابط الأمن السيبراني للأنظمة الحساسة، مرة واحدة سنوياً؛ على الأقل.
١-٤-٢	رجوعاً للضابط ١ - ٨ - ٢ في الضوابط الأساسية للأمن السيبراني، يجب أن تتم مراجعة تطبيق ضوابط الأمن السيبراني للأنظمة الحساسة؛ من قبل أطراف مستقلة عن الإدارة المعنية بالأمن السيبراني من داخل الجهة، مرة واحدة؛ كل ثلاث سنوات على الأقل.
٥-١	**الأمن السيبراني المتعلق بالموارد البشرية (Cybersecurity in Human Resources)**
الهدف	ضمان التأكد من أن مخاطر الأمن السيبراني ومتطلباته، المتعلقة بالعاملين (موظفين ومتعاقدين) في الجهة؛ تعالج بفعالية، قبل عملهم، وأثنائه، وعند انتهائه. وذلك وفقاً للسياسات والإجراءات التنظيمية للجهة؛ والمتطلبات التشريعية والتنظيمية ذات العلاقة.
الضوابط	
١-٥-١	بالإضافة للضوابط الفرعية ضمن الضابط ١ - ٩ - ٣ في الضوابط الأساسية للأمن السيبراني، فإنه يجب أن تغطي متطلبات الأمن السيبراني، قبل بدء علاقة العاملين المهنية بالجهة، بحد أدنى؛ ما يلي: ١ - ٥ - ١ - ١ إجراء المسح الأمني (Screening or Vetting) للعاملين على الأنظمة الحساسة. ١ - ٥ - ١ - ٢ أن يشغل وظائف الدعم، والتطوير التقني، للأنظمة الحساسة؛ مواطنون ذوو كفاءة عالية.

٢ تعزيز الأمن السيبراني (Cybersecurity Defense)

٢-١	إدارة الأصول (Asset Management)
الهدف	التأكد من أن الجهة لديها قائمة جرد دقيقة، وحديثة للأصول؛ تشمل التفاصيل ذات العلاقة، لجميع الأصول المعلوماتية، والتقنية المتاحة للجهة؛ وذلك من أجل دعم العمليات التشغيلية للجهة، ومتطلبات الأمن السيبراني، بهدف تحقيق سرية الأصول المعلوماتية والتقنية للجهة، وسلامتها ودقتها وتوافرها.
الضوابط	
٢ - ١ - ١	بالإضافة للضوابط ضمن المكون الفرعي ٢ - ١ في الضوابط الأساسية للأمن السيبراني، يجب أن تشمل متطلبات الأمن السيبراني لإدارة الأصول المعلوماتية والتقنية، بحد أدنى؛ مايلي: ٢ - ١ - ١ - ١ الاحتفاظ بقائمة محدثة سنوياً، لجميع الأصول التابعة للأنظمة الحساسة. ٢ - ١ - ١ - ٢ تحديد ملاك الأصول (Assets Owner) وإشراكهم في دورة حياة إدارة الأصول، التابعة للأنظمة الحساسة.
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	بالإضافة للضوابط الفرعية ضمن الضابط ٢ - ٢ - ٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني المتعلقة بإدارة هويات الدخول، والصلاحيات للأنظمة الحساسة في الجهة، بحد أدنى؛ ما يلي: ٢ - ٢ - ١ - ١ منع الدخول عن بعد من خارج المملكة. ٢ - ٢ - ١ - ٢ تقييد الدخول عن بعد من داخل المملكة؛ على أن يتم التأكد عن طريق مركز العمليات الأمنية الخاص بالجهة، عند كل عملية دخول؛ ومراقبة الأنشطة المتعلقة بالدخول عن بعد باستمرار. ٢ - ٢ - ١ - ٣ التحقق من الهوية متعدد العناصر (Multi-Factor Authentication «MFA») لجميع المستفيدين. ٢ - ٢ - ١ - ٤ التحقق من الهوية متعدد العناصر(Multi-Factor Authentication «MFA») للمستخدمين ذوي الصلاحيات الهامة، والحساسة؛ وعلى الأنظمة المستخدمة لإدارة الأنظمة الحساسة المذكورة في الضابط ٢ - ٣ - ١ - ٤ ومتابعتها. ٢ - ٢ - ١ - ٥ وضع سياسة آمنة لكلمة المرور ذات معايير عالية، وتطبيقها. ٢ - ٢ - ١ - ٦ استخدام الطرق والخوارزميات الآمنة لحفظ ومعالجة كلمات المرور مثل: استخدام دوال الاختزال (Hashing Functions). ٢ - ٢ - ١ - ٧ الإدارة الآمنة لحسابات الخدمات (Service Account) مابين التطبيقات والأنظمة؛ وتعطيل الدخول البشري التفاعلي (Interactive login) من خلالها. ٢ - ٢ - ١ - ٨ فيما عدا مشرفي قواعد البيانات (Database Administrators)، يمنع الوصول أو التعامل المباشر لأي مستخدم مع قواعد البيانات؛ ويتم ذلك من خلال التطبيقات فقط، وبناءً على الصلاحيات المخوّل بها؛ مع مراعاة تطبيق حلول أمنية تحد، أو تمنع من اطلاع مشرفي قواعد البيانات على البيانات المصنفة (Classified Data).

٢ - ٢ - ٢	رجوعاً للضابط ٢ - ٢ - ٣ - ٥ في الضوابط الأساسية للأمن السيبراني، يجب مراجعة هويات الدخول على الأنظمة الحساسة، مرة واحدة، كل ثلاثة أشهر، على الأقل.
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، والبنية التحتية للجهة، من المخاطر السيبرانية.
الضوابط	
٢ - ٣ - ١	بالإضافة للضوابط الفرعية ضمن الضابط ٢ - ٣ - ٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني لحماية الأنظمة الحساسة، وأجهزة معالجة المعلومات الخاصة بها، بحد أدنى؛ ما يلي: ٢ - ٣ - ١ - ١ السماح فقط بقائمة محددة من ملفات التشغيل (Whitelisting) للتطبيقات والبرامج؛ للعمل على الخوادم الخاصة بالأنظمة الحساسة. ٢ - ٣ - ١ - ٢ حماية الخوادم الخاصة بالأنظمة الحساسة بتقنيات حماية الأجهزة الطرفية (End-point Protection) المعتمدة لدى الجهة. ٢ - ٣ - ١ - ٣ تطبيق حزم التحديثات، والإصلاحات الأمنية، مرة واحدة شهرياً على الأقل، للأنظمة الحساسة الخارجية، والمتصلة بالإنترنت؛ وكل ثلاثة أشهر على الأقل، للأنظمة الحساسة الداخلية؛ مع اتباع آليات التغيير المعتمدة لدى الجهة. ٢ - ٣ - ١ - ٤ تخصيص أجهزة حاسب (Workstations) للعاملين في الوظائف التقنية، ذات الصلاحيات الهامة والحساسة؛ على أن تكون معزولة في شبكة خاصة، لإدارة الأنظمة (Management Network) وعلى أن لا ترتبط بأي شبكة، أو خدمة أخرى (مثل: خدمة البريد الإلكتروني، الإنترنت). ٢ - ٣ - ١ - ٥ تشفير أي وصول إشرافي عبر الشبكة (Non-console Administrative Access) لأي من المكونات التقنية للأنظمة الحساسة، باستخدام خوارزميات، وبروتوكولات التشفير الآمنة. ٢ - ٣ - ١ - ٦ مراجعة إعدادات الأنظمة الحساسة وتحصيناتها (Secure Configuration and Hardening) كل ستة أشهر على الأقل. ٢ - ٣ - ١ - ٧ مراجعة الإعدادات المصنعية (Default Configuration) وتعديلها والتأكد من عدم وجود كلمات مرور ثابتة، وخلفية، وإفتراضية (Hard-Coded, Backdoor and Default Passwords) ما أمكن تطبيقه. ٢ - ٣ - ١ - ٨ حماية السجلات، والملفات الحساسة للأنظمة، من الوصول غير المصرح به، أو العبث، أو التغيير، أو الحذف غير المشروع.

٢-٤	إدارة أمن الشبكات (Networks Security Management)
الهدف	ضمان حماية شبكات الجهة من المخاطر السيبرانية.
الضوابط	
٢ - ٤ - ١	بالإضافة للضوابط الفرعية ضمن الضابط ٢ - ٥ - ٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني لإدارة أمن شبكات الأنظمة الحساسة للجهة بحد أدنى ما يلي: ٢ - ٤ - ١ - ١ العزل والتقسيم المادي، أو المنطقي، لشبكات الأنظمة الحساسة. ٢ - ٤ - ١ - ٢ مراجعة إعدادات جدار الحماية (Firewall Rules) وقوائمه؛ كل ستة أشهر، على الأقل. ٢ - ٤ - ١ - ٣ منع التوصيل المباشر، لأي جهاز بالشبكة المحلية للأنظمة الحساسة؛ إلا بعد الفحص، والتأكد من توافر عناصر الحماية المحققة، للمستويات المقبولة للأنظمة الحساسة. ٢ - ٤ - ١ - ٤ منع الأنظمة الحساسة من الاتصال بالشبكة اللاسلكية. ٢ - ٤ - ١ - ٥ الحماية من التهديدات المتقدمة المستمرة على مستوى الشبكة (Network APT). ٢ - ٤ - ١ - ٦ منع الأنظمة الحساسة من الاتصال بالإنترنت في حال أن كانت تقدم خدمة داخلية للجهة؛ ولا توجد هناك حاجة ضرورية جداً، للدخول على الخدمة من خارج الجهة. ٢ - ٤ - ١ - ٧ تقديم خدمات الأنظمة الحساسة، من خلال شبكات مستقلة عن الإنترنت، في حال أن كانت خدمات تلك الأنظمة، موجهة لجهات محدودة؛ وليست للأفراد. ٢ - ٤ - ١ - ٨ الحماية من هجمات تعطيل الشبكات (Distrbuted Denial of Service Attack «DDoS») للحد من المخاطر الناتجة عن هجمات تعطيل الشبكات. ٢ - ٤ - ١ - ٩ السماح بقائمة محددة (Whitelisting) فقط، لقوائم جدار الحماية، الخاصة بالأنظمة الحساسة.

٢-٥	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 - ٥ - ١	بالإضافة للضوابط الفرعية ضمن الضابط ٢ - ٦ - ٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني، الخاصة بأمن الأجهزة المحمولة، وأجهزة (BYOD) للجهة، بحد أدنى؛ ما يلي: ٢ - ٥ - ١ - ١ منع الوصول من الأجهزة المحمولة للأنظمة الحساسة، إلا لفترة مؤقتة فقط؛ وذلك بعد إجراء تقييم المخاطر، وأخذ الموافقات اللازمة من الإدارة المعنية بالأمن السيبراني في الجهة. ٢ - ٥ - ١ - ٢ تشفير أقراص الأجهزة المحمولة، ذات صلاحية الوصول للأنظمة الحساسة، تشفيراً كاملاً (Full Disk Encryption).

٦-٢	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 - ٦ - ١	بالإضـــافة للـــضوابط الفرعية ضمن الـــضابط ٢ - ٧ - ٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني لحماية البيانات والمعلومات؛ بحد أدنى، ما يلي: ٢ - ٦ - ١ - ١ عدم استخـــدام بـــيانات الأنـــظمة الحساسة في غير بيئة الإنتاج (Production Environment) إلا بعد استخدام ضوابط مشددة لحماية تلك البيانات مثل: تقنيات تعتيم البيانات (Data Masking) أو تقنيات مزج البيانات (Data Scrambling). ٢ - ٦ - ١ - ٢ تصنيف جميع بيانات الأنظمة الحساسة. ٢ - ٦ - ١ - ٣ حماية البيانات المصنفة الخاصة بالأنظمة الحساسة من خلال تقنيات، منع تسريب البيانات (Data Leakage Prevention). ٢ - ٦ - ١ - ٤ تحديد مدة الاحتفاظ المطلوبة (Retention Period) لبيانات الأعمال المتعلقة بالأنظمة الحساسة؛ حسب التشريعات ذات العلاقة، ويتم الاحتفاظ بالبيانات المطلوبة فقط، في بيئات الإنتاج للأنظمة الحساسة. ٢ - ٦ - ١ - ٥ منع نقل أي من بيانات بيئة الإنتاج الخاصة بالأنظمة الحساسة إلى أي بيئة أخرى.
٧-٢	التشفير (Cryptography)
الهدف	ضمان الاستخدام السليم والفعال للتشفير؛ لحماية الأصول المعلوماتية الإلكترونية للجهة، وذلك وفقاً للسياسات، والإجـــراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية، ذات العلاقة.
الضوابط	
٢ - ٧ - ١	بالإضافة للضوابط الفرعية ضمن الضابط ٢ - ٨ - ٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني للتشفير، بحد أدنى، ما يلي: ٢ - ٧ - ١ - ١ تشفير جميع بيانات الأنظمة الحساسة؛ أثناء النقل (Data-In-Transit). ٢ - ٧ - ١ - ٢ تشفير جميع بيانات الأنظمة الحساسة؛ أثناء التخزين (Data-At-Rest) على مستوى الملفات، أو قاعدة البيانات، أو على مستوى أعمدة محددة، داخل قاعدة البيانات. ٢ - ٧ - ١ - ٣ استخدام طرق وخوارزميات ومفاتيح وأجهزة تشفير محدثة وآمنة وفقاً لما تصدره الهيئة بهذا الشأن.

٢-٨	إدارة النسخ الاحتياطية (Backup and Recovery Management)
الهدف	ضمان حماية بيانات الجهة ومعلوماتها، والإعدادات التقنية للأنظمة، والتطبيقات الخاصة بالجهة؛ من الأضرار الـــناجمة عن المخـــاطر السيـــبرانية، وذلك وفـــقاً للسيـــاسات، والإجراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية، ذات العلاقة.
الضوابط	
٢ - ٨ - ١	بالإضافة للضوابط الفرعية ضمن الضابط ٢ - ٩ - ٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني لإدارة النسخ الاحتياطية، بحد أدنى؛ ما يلي: ٢ - ٨ - ١ - ١ نطاق عمل النسخ الاحتياطي المتصل، وغير المتصل (Online and Offline Backup) ليشمل جميع الأنظمة الحساسة. ٢ - ٨ - ١ - ٢ عمل النسخ الاحتياطي على فترات زمنية مخطط لها؛ بناءً على تقييم المخاطر للجهة. وتوصي الهيئة بأن يتم عمل النسخ الاحتياطي، للأنظمة الحساسة، بشكل يومي. ٢ - ٨ - ١ - ٣ تأمين الوصول، والتخزين، والنقل لمحتوى النسخ الاحتياطية للأنظمة الحساسة ووسائطها، وحمايتها من الإتلاف، أو التعديل، أو الاطلاع غير المصرح به.
٢ - ٨ - ٢	رجوعاً للضابط ٢ - ٩ - ٣ - ٣ في الضوابط الأساسية للأمن السيبراني، يجب إجراء فحص دوري؛ كل ثلاثة أشهر على الأقل، لتحديد مدى فعالية استعادة النسخ الاحتياطية، الخاصة بالأنظمة الحساسة.
٢-٩	إدارة الثغرات (Vulnerabilities Management)
الهدف	ضمان اكتشاف الثغرات التقنية في الوقت المناسب، ومعالجتها بشكل فعال؛ وذلك لمنع احتمالية استغلال هذه الثغرات من قبل الهجمات السيبرانية أو تقليلها، وكذلك التقليل من الآثار المترتبة على أعمال الجهة.
الضوابط	
٢ - ٩ - ١	بالإضافة للضوابط الفرعية ضمن الضابط ٢ - ١٠ - ٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني لإدارة الثغرات للأنظمة الحساسة، بحد أدنى، ما يلي: ٢ - ٩ - ١ - ١ استخدام وسائل وأدوات موثوقة لإكتشاف الثغرات. ٢ - ٩ - ١ - ٢ تقييم الثغرات ومعالجتها (بتنصيب حزم التحديثات والإصلاحات) على المكونات التقنية للأنظمة الحساسة، مرة واحدة شهرياً، على الأقل، للأنظمة الحساسة الخارجية، والمتصلة بالإنترنت؛ وكل ثلاثة أشهر على الأقل، للأنظمة الحساسة الداخلية. ٢ - ٩ - ١ - ٣ معالجة فورية للثغرات الحرجة (Critical Vulnerabilities) المكتشفة حديثاً؛ مع اتباع آليات إدارة التغيير، المعتمدة لدى الجهة.
٢ - ٩ - ٢	رجوعاً للضابط ٢ - ١٠ - ٣ - ١ في الضوابط الأساسية للأمن السيبراني، يجب فحص الثغرات واكتشافها على المكونات التقنية، للأنظمة الحساسة، مرة واحدة شهرياً؛ على الأقل.

٢-١٠	اختبار الاختراق (Penetration Testing)
الهدف	تقييم مدى فعالية قدرات تعزيز الأمن السيبراني واختباره في الجهة؛ وذلك من خلال عمل محاكاة لتقنيات الهجوم السيبراني الفعلية وأساليبه. وكذلك اكتشاف نقاط الضعف الأمنية غير المعروفة، والتي قد تؤدي إلى الاختراق السيبراني للجهة؛ وذلك وفقاً للمتطلبات التشريعية والتنظيمية، ذات العلاقة.
الضوابط	
٢ - ١٠ - ١	بالإضافة للضوابط الفرعية ضمن الضابط ٢ - ١١ - ٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني لاختبار الاختراق للأنظمة الحساسة، بحد أدنى؛ ما يلي: ٢ - ١٠ - ١ - ١ نطاق عمل اختبار الاختراق، ليشمل جميع المكونات التقنية للأنظمة الحساسة، وجميع الخدمات المقدمة داخلياً وخارجياً. ٢ - ١٠ - ١ - ٢ عمل اختبار الاختراق من قبل فريق مؤهل.
٢ - ١٠ - ٢	رجوعاً للضابط ٢ - ١١ - ٣ - ٢ في الضوابط الأساسية للأمن السيبراني، يجب عمل اختبار الاختراق على الأنظمة الحساسة، كل ستة أشهر؛ على الأقل.
٢-١١	إدارة سجلات الأحداث ومراقبة الأمن السيبراني (Cybersecurity Event Logs and Monitoring Management)
الهدف	ضمان تجميع سجلات أحداث الأمن السيبراني وتحليلها ومراقبتها في الوقت المناسب؛ من أجل الاكتشاف الاستباقي للهجمات السيبرانية، وإدارة مخاطرها بفعالية؛ لمنع الآثار المترتبة على أعمال الجهة أو تقليلها.
الضوابط	
٢ - ١١ - ١	بالإضافة للضوابط الفرعية ضمن الضابط ٢ - ١٢ - ٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات إدارة سجلات الأحداث، ومراقبة الأمن السيبراني للأنظمة الحساسة، بحد أدنى؛ ما يلي: ٢ - ١١ - ١ - ١ تفعيل سجلات الأحداث (Event logs) الخاصة بالأمن السيبراني؛ على جميع المكونات التقنية للأنظمة الحساسة. ٢ - ١١ - ١ - ٢ تفعيل التنبيهات وسجلات الأحداث المتعلقة بإدارة تغييرات الملفات (File Integrity Management) ومراقبتها. ٢ - ١١ - ١ - ٣ مراقبة سلوك المستخدم (User Behavior Analytics «UBA») وتحليله. ٢ - ١١ - ١ - ٤ مراقبة سجلات الأحداث، الخاصة بالأنظمة الحساسة على مدار الساعة. ٢ - ١١ - ١ - ٥ الاحتفاظ بسجلات الأحداث، الخاصة بالأمن السيبراني، المتعلقة بالأنظمة الحساسة وحمايتها؛ على أن تكون شاملة، ومتضمنة للتفاصيل كاملة (مثل: الوقت، التاريخ، الهوية، النظام المتأثر).
٢ - ١١ - ٢	رجوعاً للضابط ٢ - ١٢ - ٣ - ٥ في الضوابط الأساسية للأمن السيبراني، يجب أن لا تقل مدة الاحتفاظ بسجلات الأحداث الخاصة بالأمن السيبراني، على الأنظمة الحساسة عن ١٨ شهراً؛ حسب المتطلبات التشريعية، والتنظيمية، ذات العلاقة.

٢-١٢	حماية تطبيقات الويب (Web Application Security)
الهدف	ضمان حماية تطبيقات الويب الخارجية (Internet-Facing Web Application Security) للجهة من المخاطر السيبرانية.
الضوابط	
٢ - ١٢ - ١	بالإضافة للضوابط الفرعية ضمن الـــضابط ٢ - ١٥ - ٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني، لحماية تطبيقات الويب الخارجية للأنظمة الحساسة للجهة، بحد أدنى؛ ما يلي: ٢ - ١٢ - ١ - ١ الإدارة الآمنة للجلسات (Secure Session Management)، ويشمل موثوقية الجلسات (Authenticity)، وإقفالها (Lockout)، وإنهاء مهلتها (Timeout). ٢ - ١٢ - ١ - ٢ تطبيق معايير أمن التطبيقات وحمايتها (OWASP Top Ten) في حدها الأدنى.
٢ - ١٢ - ٢	رجـــوعاً للضابط ٢ - ١٥ - ٣ - ٢ في الضوابط الأساســية للأمن السيبراني، يجب استخدام مبدأ المعمارية ذات المســـتويات المتعددة (Multi-tier Architecture) على أن لا يقـــل عدد المســـتويات عن ٣ (3-Tier Architecture).
٢-١٣	حماية التطبيقات (Application Security)
الهدف	ضمان حماية التطبيقات الداخلية، الخاصة بالأنظمة الحساسة للجهة، من المخاطر السيبرانية.
الضوابط	
٢ - ١٣ - ١	يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني لحماية التطبيقات الداخلية الخاصة بالأنظمة الحساسة للجهة من المخاطر السيبرانية.
٢ - ١٣ - ٢	يجب تطبيق متطلبات الأمن السيبراني؛ لحماية التطبيقات الداخلية، الخاصة بالأنظمة الحساسة للجهة.
٢ - ١٣ - ٣	يجب أن تغطي متطلبات الأمن السيبراني؛ لحماية التطبيقات الداخلية، الخاصة بالأنظمة الحساسة للجهة، بحد أدنى، ما يلي: ٢ - ١٣ - ٣ - ١ استخدام مبدأ المعمارية ذات المستويات المتعددة (Multi-tier Architecture) على أن لا يقل عدد المستويات عن ٣ (3-Tier Architecture). ٢ - ١٣ - ٣ - ٢ استخدام بروتوكولات آمنة (مثل بروتوكول HTTPS). ٢ - ١٣ - ٣ - ٣ توضيح سياسة الاستخدام الآمن للمستخدمين. ٢ - ١٣ - ٣ - ٤ الإدارة الآمنة للجلسات (Secure Session Management)، ويشمل موثوقية الجلسات (Authenticity)، وإقفالها (Lockout)، وإنهاء مهلتها (Timeout).
٢ - ١٣ - ٤	مراجعة متطلبات الأمن السيبراني لحماية التطبيقات الداخلية الخاصة بالأنظمة الحساسة للجهة 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 الآثار المترتبة على الاضطرابات وتقليلها في الخدمات الإلكترونية الحرجة، للجهة، وأجهزة معالجة معلوماتها وأنظمتها، وذلك عند وقوع الكوارث الناتجة عن المخاطر السيبرانية.
الضوابط	
٣ - ١ - ١	بالإضـــافة للـضوابط الفرعية ضمن الضـابط ٣ - ١ - ٣ في الضوابط الأســـاسية للأمن السيبراني، يجب أن تغطي إدارة استمرارية الأعمال في الجهة، بحد أدنى؛ ما يلي: ٣ - ١ - ١ - ١ وضع مركز للتعافي من الكوارث للأنظمة الحساسة. ٣ - ١ - ١ - ٢ إدراج الأنظمة الحساسة؛ ضمن خطط التعافي من الكوارث. ٣ - ١ - ١ - ٣ إجراء اختبارات دورية؛ للتأكد من فعالية خطط التعافي، من الكوارث للأنظمة الحساسة، مرة واحدة سنوياً؛ على الأقل. ٣ - ١ - ١ - ٤ توصي الهيئة بإجراء اختبار دوري حي؛ للتعافي من الكوارث (Live DR Test) للأنظمة الحساسة.

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

٤-١	الأمن السيبراني المتعلق بالأطراف الخارجية (Third-Party Cybersecurity)
الهدف	ضمان حماية أصول الجهة من مخاطر الأمن السيبراني، المتعلقة بالأطراف الخارجية؛ بما في ذلك خدمات الإسناد، لتقنية المعلومات (Outsourcing) والخدمات المدارة (Managed Services). وذلك وفقاً للسياسات والإجراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية ذات العلاقة.
الضوابط	
٤ - ١ - ١	بالإضافة للضوابط ضمن المكون الفرعي ٤ - ١ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني، المتعلقة بالأطراف الخارجية، بحد أدنى؛ ما يلي: ٤ - ١ - ١ - ١ إجراء المسح الأمني (Screening or Vetting) لشركات خدمات الإسناد، ولموظفي خدمات الإسناد، والخدمات المدارة العاملين على الأنظمة الحساسة. ٤ - ١ - ١ - ٢ أن تكون خدمات الإسناد، والخدمات المدارة على الأنظمة الحساسة؛ عن طريق شركات، وجهات وطنية؛ وفقاً للمتطلبات التشريعية، والتنظيمية ذات العلاقة.

٤-٢	الأمن السيبراني المتعلق بالحوسبة السحابية والاستضافة (Cloud Computing and Hosting Cybersecurity)
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	بالإضافة للضوابط الفرعية ضمن الضابط ٤ - ٢ - ٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني الخاصة باستخدام خدمات الحوسبة السحابية والاستضافة، بحد أدنى؛ ما يلي: ٤ - ٢ - ١ - ١ أن يكون موقع استضافة الأنظمة الحساسة، أو أي جزء من مكوناتها التقنية، داخل الجهة، أو في خدمات الحوسبة السحابية، المقدمة من قبل جهات حكومية، أو شركات وطنية محققة لضوابط الحوسبة السحابية الصادرة من الهيئة مع مراعاة تصنيف البيانات المستضافة.

ملاحق

ملحق (أ): العلاقة مع الضوابط الأساسية للأمن السيبراني

تعد ضوابط الأمن السيبراني للأنظمة الحساسة؛ امتداداً للضوابط الأساسية للأمن السيبراني (ECC - 1 : 2018) كما هو موضح في الشكلين ٤ و ٥، حيث تمت إضافة:

- مكون فرعي جديد، خاص بضوابط الأمن السيبراني للأنظمة الحساسة.
- عشرين مكوناً فرعياً، أضيف لها ضوابط خاصة بالأمن السيبراني للأنظمة الحساسة.

في حين أن هناك تسعة مكونات فرعية، لم يضف لها ضوابط خاصة بالأمن السيبراني للأنظمة الحساسة.

	مكونات فرعية خاصة بضوابط الأمن السيبراني للأنظمة الحساسة
	مكونات فرعية أضيف لها ضوابط خاصة بالأنظمة الحساسة
	مكونات فرعية لم يضف لها ضوابط خاصة بالأنظمة الحساسة

شكل ٤: دليل ألوان المكونات الفرعية في الشكل ٥

١ - حوكمة الأمن السيبراني Cybersecurity Governance	١ - ١	إستراتيجية الأمن السيبراني Cybersecurity Strategy	إدارة الأمن السيبراني Cybersecurity Management
		سياسات وإجراءات الأمن السيبراني Cybersecurity Policies and Procedures	أدوار ومسؤوليات الأمن السيبراني Cybersecurity Roles and Responsibilities
	١ - ٢	إدارة مخاطر الأمن السيبراني Cybersecurity Risk Management	١ - ٣ الأمن السيبراني ضمن إدارة المشاريع المعلوماتية والتقنية Cybersecurity in Information Technology Projects
		الالتزام بتشريعات وتنظيمات ومعايير الأمن السيبراني Cybersecurity Regulatory Compliance	١ - ٤ المراجعة والتدقيق الدوري للأمن السيبراني Cybersecurity Periodical Assessment and Audit
	١ - ٥	الأمن السيبراني المتعلق بالموارد البشرية Cybersecurity in Human Resources	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	حماية البريد الإلكتروني Email Protection
	٢ - ٤	إدارة أمن الشبكات Networks Security Management	٢ - ٥ أمن الأجهزة المحمولة Mobile Devices Security
	٢ - ٦	حماية البيانات والمعلومات Data and Information Protection	٢ - ٧ التشفير Cryptography
	٢ - ٨	إدارة النسخ الاحتياطية Backup and Recovery Management	٢ - ٩ إدارة الثغرات Vulnerabilities Management
		إدارة حوادث وتهديدات الأمن السيبراني Cybersecurity Incident and Threat Management	الأمن المادي Physical Security
	٢ - ١٠	اختبار الاختراق Penetration Testing	٢ - ١١ إدارة سجلات الأحداث ومراقبة الأمن السيبراني Cybersecurity Event Logs and Monitoring Management
	٢ - ١٢	حماية تطبيقات الويب Web Application Security	٢ - ١٣ حماية التطبيقات Application Security

٣ - صمود الأمن السيبراني Cybersecurity Resilience	١ - ٣	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	١ - ٤	الأمن السيبراني المتعلق بالأطراف الخارجية Third-Party Cybersecurity	٢ - ٤ الأمن السيبراني المتعلق بالحوسبة السحابية والاستضافة Cloud Computing and Hosting Cybersecurity
٥ - الأمن السيبراني لأنظمة التحكم الصناعي ICS Cybersecurity	حماية أجهزة وأنظمة التحكم الصناعي Industrial Control Systems (ICS) Protection		

شكل ٥: مكونات الضوابط الأساسية للأمن السيبراني، وضوابط الأمن السيبراني للأنظمة الحساسة

ملحق (ب) مصطلحات وتعريفات:

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

جدول ٢: مصطلحات وتعريفات

المصطلح	التعريف
المسح الأمني Screening or Vetting	هو عملية التحقق من هوية الأشخاص، قبل التوظيف، وذلك لارتباطهم بمهمة متعلقة بالأنظمة الحساسة.
واجهة برمجة التطبيقات Application Program Interface (API)	مجـموعة من الأوامـــر (Commands) والدوال (Functions) والـــكائنات (Objects) والبروتـــوكولات (Protocols) التي طوّرت ليتم استخدامها من قبل المبرمجين لتطوير البرمجيات، أو التفاعل مع أنظمة و/أو برمجيات أخرى.
اختبار التحمل Stress Testing	اختبار يجرى للبرمجيات (Software) والعتاد (Hardware) للتأكد من توافرها؛ وقياس مستوى فعاليتها في الظروف غير المتوقعة.
البيانات أثناء النقل Data-In-Transit	البيانات التي تنتقل من موقع إلى آخر، عن طريق أي نوع من الشبكات؛ مثل الإنترنت، شبكة خاصة... إلخ.
البيانات أثناء التخزين Data-At-Rest	هي البيانات المخزنة في وسائط التخزين الدائمة؛ مثل: الأشرطة (Tapes) والأقراص(Disk).
تحليل سلوك المستخدم User Behavior Analytics (UBA)	هي عملية تتبع لبيانات المستخدم وجمعها؛ والقيام بتحليلها، وتحديد أنماط أنشطة المستخدم؛ للكشف عن السلوكيات الضارة أو غير الإعتيادية.
تقنيات منع تسريب البيانات Data Leakage Prevention	هي إستراتيجية للحفاظ على البيانات المهمة، من الأشخاص غير المصرح لهم بالاطلاع عليها، ومنع تداولها خارج نطاق المنظمة في أي صورة تكون عليه هذه البيانات، ومكانها؛ سواء أكانت مخزنة على وحدات التخزين (In-Rest) أو أجهزة المستخدمين، والخوادم (In-Use) أو متنقلة من خلال الشبكة (In-Transit).
هجمات تعطيل الخدمات الموزعة Distributed Denial of Service Attack (DDoS)	هي محاولة لتعطيل النظام، وجعل خدماته غير متوافرة؛ عن طريق إرسال طلبات كثيرة، من أكثر من مصدر في الوقت نفسه.
الشفرة المصدرية Source Code	مجموعة من الأوامر، والتعليمات المكتوبة، بلغة من لغات البرمجة.
حسابات الخدمات Service Accounts	حساب يستخدم؛ لتشغيل خدمات أو برامج، ولديه صلاحية الوصول للبيانات والموارد.
تقنية حماية الأجهزة الطرفية End-point Protection	تقنية تستخدم لحماية الأجهزة أو الأصول من البرامج الضارة.
الثغرات الحرجة Critical Vulnerabilities	هي الثغرات التي قد يؤدي استغلالها إلى الوصول، غير المصرح به، إلى البيانات، أو المعلومات، أو الدخول للأجهزة والأنظمة.
برمجيات التكامل الوسيطة Middleware	برمجيات تلعب دور الوسيط وتسمح للتطبيقات والشبكات بالاتصال فيما بينها واستغلال طاقاتها المشتركة لمعالجة المعلومات.

المصطلح	التعريف
الدخول عن بعد Remote Access	دخول المستخدمين من خارج نطاق الشبكة الداخلية أو النظام المعلوماتي الداخلي.
تقنيات تعتيم البيانات Data Masking	تقنية تعتمد على إخفاء جزء من البيانات لحمايتها عن طريق استبدال بعض الأحرف أو القيم باستخدام رموز معينة.
تقنيات مزج البيانات Data Scrambling	تقنية تعتمد على إعادة ترتيب البيانات أو تبديلها في مجموعة بيانات بحيث تظل قيم البيانات موجودة ولكن لا تتوافق مع السجلات الأصلية ولا يمكن استردادها.
سري Secret	مستوى تصنيف يستخدم للبيانات التي يترتب على الكشف الغير مصرح به عنها ضرر جسيم بالأمن أو الاقتصاد الوطنيين أو بالعلاقات الخارجية للمملكة أو بالتحقيق في جرائم كبيرة.
سري للغاية Top Secret	مستوى تصنيف يستخدم للبيانات التي يترتب على الكشف الغير مصرح به عنها ضرر جسيم يصعب تداركه أو إصلاحه مرتبط بالأمن أو الاقتصاد الوطنيين أو بالعلاقات الخارجية للمملكة.
دوال الاختزال Hashing Functions	عملية تطبيق خوارزمية حسابية (ذات إتجاه واحد) على بيانات للحصول على قيمة عددية تعبر عن تلك البيانات بحيث يصعب (أو يكاد يكون مستحيلاً) الرجوع للبيانات الأصلية من القيمة العددية.

ملحق (ج): قائمة الاختصارات

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

جدول ٣: قائمة الاختصارات

الاختصار	معناه
APT	Advanced Persistent Threat التهديدات المتقدمة المستمرة
API	Application Program Interface واجهة برمجة التطبيقات
BCM	Business Continuity Management إدارة استمرارية الأعمال
BYOD	Bring Your Own Device سياسة أحضر الجهاز الخاص بك
CNI	Critical National Infrastructure البنية التحتية الحساسة
DDoS	Distributed Denial of Service Attack هجمات تعطيل الخدمات الموزعة
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
IDS	Intrusion Detection System نظام كشف التسلل
IPS	Intrusion Prevention System نظام منع التسلل
MFA	Multi-Factor Authentication التحقق من الهوية متعدد العناصر
TLP	Traffic Light Protocol بروتوكول الإشارة الضوئية
UBA	User Behavior Analytics تحليل سلوك المستخدم

الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority