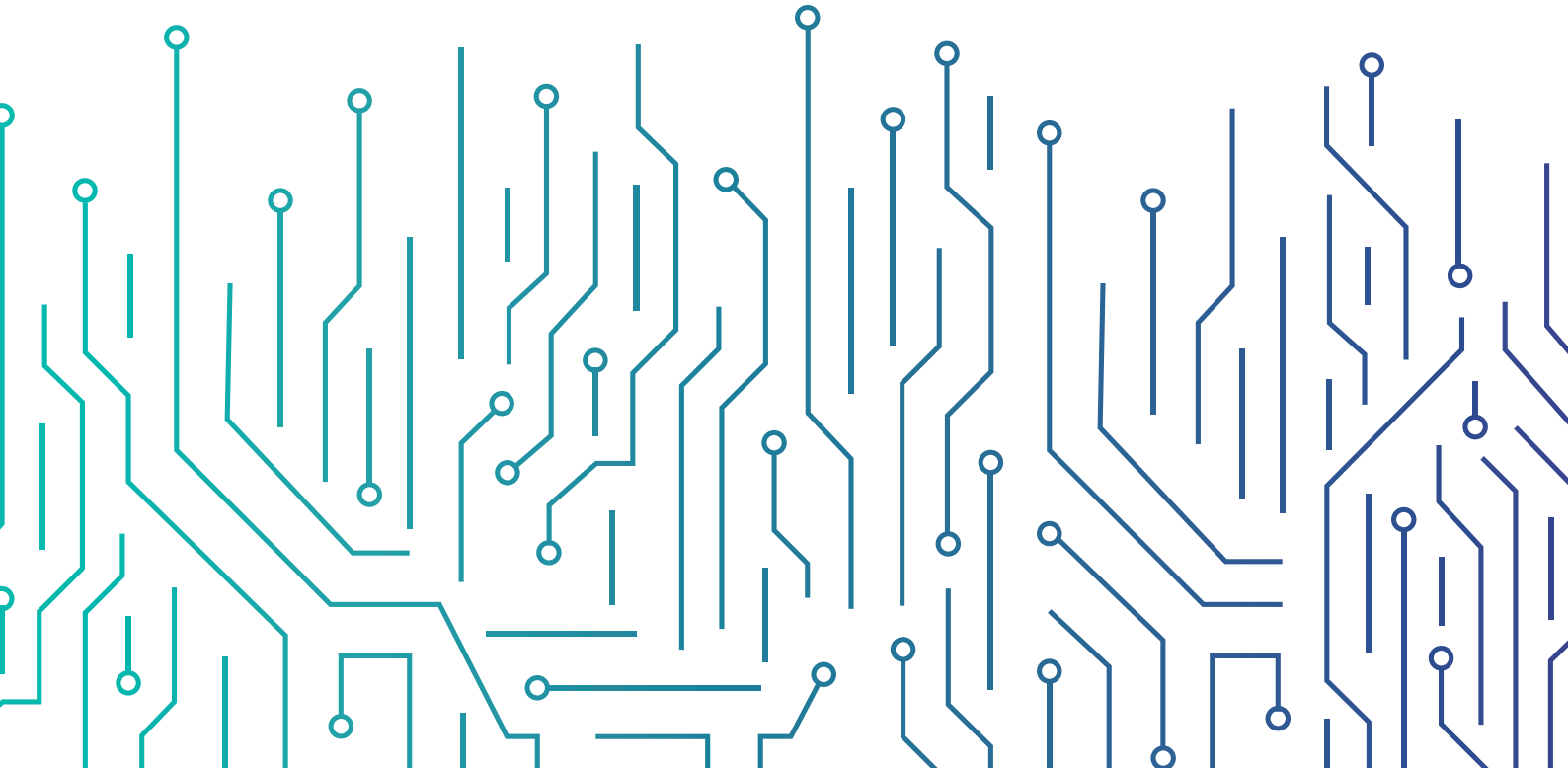
الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

ضوابط الأمن السيبراني
للحوسبة السحابية

Cloud Cybersecurity Controls

(CCC - 1 : 2020)

إشارة المشاركة: أبيض
تصنيف الوثيقة: متاح



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 أو 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

جدول المحتويات

قائمة الأشكال والرسوم التوضيحية

قائمة الجداول

١. الملخص التنفيذي

جاءت مهمات واختصاصات الهيئة الوطنية للأمن السيبراني ملبيةً لجوانب وضع السياسات وآليات الحوكمة والأطر والمعايير والضوابط والإرشادات المتعلقة بالأمن السيبراني وتعميمها على الجهات ذات العلاقة، بما يعزز دور الأمن السيبراني وأهميته والحاجة الملحة له مع ازدياد التهديدات والمخاطر الأمنية في الفضاء السيبراني أكثر من أي وقت مضى.

وحيث أصبح موضوع الحوسبة السحابية أكثر تداولًا عالميًا؛ ويتطور التوجه له والعمل به داخل المملكة بشكل متسارع، مما أظهر تحديات أو تهديدات أمن سيبرانية جديدة تستلزم وجود ضوابط للأمن السيبراني للتعامل مع خدمات الحوسبة السحابية على ضوء أفضل الممارسات العالمية في هذا المجال، وتكون امتدادًا للضوابط الأساسية للأمن السيبراني (ECC – 1: 2018).

وعليه تم تطوير وثيقة ضوابط الأمن السيبراني للحوسبة السحابية (CCC – 1 : 2020) والتي تهدف إلى تقليل المخاطر السيبرانية على مقدمي الخدمات والمشتركين. وتوضح هذه الوثيقة أهداف، ونطاق عمل، وقابلية تطبيق، وآلية الالتزام بهذه الضوابط.

وعلى مقدمي الخدمات و المشتركين اتخاذ ما يلزم لتحقيق الالتزام الدائم والمستمر بهذه الضوابط، تنفيذًا لما ورد في الفقرة الثالثة من المادة العاشرة في تنظيم الهيئة الوطنية للأمن السيبراني وكذلك ما ورد في الأمر السامي الكريم رقم ٥٧٢٣١ وتاريخ ١٠/ ١٤٣٩/١١ هـ.

٢. المقدمة

قامت الهيئة الوطنية للأمن السيبراني (ويشار لها في هذه الوثيقة بـ "الهيئة") بإصدار ضوابط الأمن السيبراني للحوسبة السحابية (CCC – 1 : 2020) بعد دراسة عدة معايير وأطر وضوابط أمن سيبراني تم إعدادها من قبل منظمات وجهات محلية ودولية، كما تم الاطلاع على أفضل الممارسات والتجارب ذات العلاقة في مجال الأمن السيبراني. وقد تم عمل دراسة مواءمة مع عدد من الضوابط والمعايير الدولية تشمل: المعيار الأمريكي FedRAMP والذي تتراوح عدد المتطلبات فيه بين ١٢٥ و ٤٢١ متطلبًا، ومعيار الأمن السحابي في سنغافورة (Multi-Tier Cloud Security Standard for Singapore (MTCS SS)) والذي يحتوي على ٥٣٥ متطلبًا، ومعيار Cloud Computing Compliance Control Catalogue (C5) والذي يحتوي على ١١٤ متطلبًا، وضوابط Cloud Controls Matrix (CCM) والتي تحتوي على ١٣٣ ضابطًا، ومعيار ISO/IEC 27001 والذي يحتوي على ١١٤ ضابطًا. وقد تم توضيح تفاصيل هذه المواءمة في وثيقة خاصة ملحقة بضوابط الأمن السيبراني للحوسبة السحابية.

مكونات ضوابط الأمن السيبراني للحوسبة السحابية

تتألف ضوابط الأمن السيبراني للحوسبة السحابية من المكونات التالية:

لمقدمي الخدمات	للمشتركين
٤ مكونات أساسية (4 Main Domains)	
٢٤ مكونًا فرعيًا (24 Subdomains)	
٣٧ ضابطًا أساسيًا (37 Main Controls)	١٨ ضابطًا أساسيًا (18 Main Controls)
٩٦ ضابطًا فرعيًّا (96 Subcontrols)	٢٦ ضابطًا فرعيًّا (26 Subcontrols)

شكل ١. مكونات ضوابط الأمن السيبراني للحوسبة السحابية

٣. الأهداف

امتدادًا للضوابط الأساسية للأمن السيبراني (ECC – 1: 2018)؛ تم تطوير هذه الوثيقة لتتضمن ضوابط الأمن السيبراني للحوسبة السحابية (CCC – 1:2020) ولتكون تابعة ومكملة لها.

تهدف هذه الوثيقة إلى تحقيق مستويات أعلى من الأهداف الوطنية للأمن السيبراني من خلال التركيز على خدمات الحوسبة السحابية من منظور مقدمي الخدمات والمشتركين وتحديد متطلبات الأمن السيبراني للحوسبة السحابية لهم، مع المساهمة في تمكينهم من تحديد المتطلبات الأمنية لخدمات الحوسبة السحابية والعمل على تحقيقها لتلبية الاحتياجات الأمنية ورفع جاهزيتها حيال المخاطر السيبرانية على كافة خدمات الحوسبة السحابية.

يتطلب الأمن السيبراني لخدمات الحوسبة السحابية من مقدمي الخدمات والمشتركين التركيز على ثلاثة مبادئ أساسية للأمن السيبراني تختص بالبيانات والمعلومات المستخدمة من قبلهم، وهي كالتالي:

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

وتأخذ هذه الضوابط بالاعتبار المحاور الأربعة الأساسية التي يرتكز عليها الأمن السيبراني، وهي:

- الاستراتيجية (Strategy)
- الأشخاص (People)
- الإجراء (Procedure)
- التقنية (Technology)

٤. نطاق العمل وقابلية التطبيق

نطاق عمل ضوابط الأمن السيبراني للحوسبة السحابية

تسري ضوابط الأمن السيبراني للحوسبة السحابية على مقدمي الخدمات والمشتركين، وتمثل هذه الضوابط الحد الأدنى من متطلبات الأمن السيبراني للحوسبة السحابية.

يقصد بمقدمي الخدمات أي مقدم خدمة يقدم خدمات الحوسبة السحابية إلى المشتركين ضمن نطاق العمل. ويقصد بالمشتركين أي جهة حكومية في المملكة العربية السعودية داخل المملكة أو خارجها (وتشمل الوزارات والهيئات والمؤسسات وغيرها) والجهات والشركات التابعة لها، وجهات القطاع الخاص التي تمتلك بنى تحتية وطنية حساسة أو تقوم بتشغيلها أو استضافتها الذين يستخدمون حاليًا أو يخططون لاستخدام أي من خدمات الحوسبة السحابية.

وتشجع الهيئة وبشدة الجهات الأخرى في المملكة على الاستفادة من هذه الضوابط لتطبيق أفضل الممارسات فيما يتعلق بتحسين وتطوير الأمن السيبراني للحوسبة السحابية.

أمثلة على مقدمي خدمات الحوسبة السحابية خارج نطاق العمل

- مقدمو الخدمات الذين يقدمون خدمات حوسبة سحابية لجهات غير سعودية خارج المملكة، ولا يقدمون خدمات للمشتركين ضمن نطاق العمل.
- مقدمو الخدمات الذين يقدمون خدمات حوسبة سحابية للأفراد، وجهات القطاع الخاص التي لا تمتلك بنى تحتية وطنية حساسة أو تقوم بتشغيلها أو استضافتها، ولا يقدمون خدمات للمشتركين ضمن نطاق العمل.

قابلية التطبيق على مقدمي الخدمات والمشتركين

تم إعداد الضوابط الأساسية للأمن السيبراني وضوابط الأمن السيبراني للحوسبة السحابية بحيث تكون ملائمة لمتطلبات الأمن السيبراني لمقدمي الخدمات والمشتركين بتنوع طبيعة أعمالهم، ويجب على مقدم الخدمة والمشترك الالتزام بجميع الضوابط القابلة للتطبيق عليهم.

٥. التنفيذ والالتزام

تحقيقًا لما ورد في الفقرة الثالثة من المادة العاشرة من تنظيم الهيئة، يجب على مقدمي الخدمات والمشتركين ضمن نطاق عمل هذه الضوابط تحقيق الالتزام الدائم والمستمر بضوابط الأمن السيبراني للحوسبة السحابية، وذلك حسب المستويات الموضحة في الجدول رقم (٢) والجدول رقم (٣) في قسم "الملحق (أ): مستويات ضوابط الأمن السيبراني للحوسبة السحابية" من هذه الوثيقة، مع الأخذ بالاعتبار القاعدتين أدناه:

- الضوابط التي تخص المشتركين في هذه الوثيقة مكملة للضوابط الواردة في وثيقة الضوابط الأساسية للأمن السيبراني وامتداد لها؛ وعليه فإن المشتركين ملزمون بالتطبيق الدائم والمستمر لجميع الضوابط الواردة في الوثيقتين.
- الضوابط التي تخص مقدمي الخدمة في هذه الوثيقة مكملة للضوابط الواردة في وثيقة الضوابط الأساسية للأمن السيبراني وامتداد لها؛ وعليه فإن مقدمي الخدمة، سواءً داخل أو خارج نطاق عمل الضوابط الأساسية للأمن السيبراني، ملزمون بالتطبيق الدائم والمستمر لجميع الضوابط الواردة في الوثيقتين.

ستقوم الهيئة بإعطاء فترة لالتزام مقدمي الخدمات والمشتركين داخل نطاق العمل بالضوابط (مع الأخذ بالاعتبار مقدمي الخدمات والمشتركين الذين ينتقلون من خارج نطاق العمل إلى داخل نطاق العمل) وفق ما تراه الهيئة مناسبًا، كما تقوم الهيئة بتقييم التزام مقدمي الخدمات و المشتركين بما ورد في هذه الوثيقة وفق الآلية التي تراها مناسبة لذلك، ومن هذه الآليات: التقييم الذاتي لمقدمي الخدمات والمشتركين و/أو تقييم الالتزام الخارجي من قبل الهيئة أو من تنيبه.

٦. ملحق المنهجية والمواءمة لضوابط الأمن السيبراني للحوسبة السحابية

قامت الهيئة بتطوير وثيقة ملحق المنهجية والمواءمة لضوابط الأمن السيبراني للحوسبة السحابية، والتي تعد جزءًا من وثيقة ضوابط الأمن السيبراني للحوسبة السحابية، وتحتوي هذه الوثيقة على:

- مبادئ تصميم ضوابط الأمن السيبراني للحوسبة السحابية.
- العلاقة بالمعايير الدولية الأخرى.
- منهجية تصميم ضوابط الأمن السيبراني للحوسبة السحابية.
- مكونات وهيكلية ضوابط الأمن السيبراني للحوسبة السحابية.
- مواءمة المكونات الفرعية مع المعايير الدولية.
- مواءمة الضوابط مع المعايير الدولية.
- مواءمة المكونات الفرعية للضوابط الأساسية للأمن السيبراني مع ضوابط الأمن السيبراني للحوسبة السحابية.
- قابلية تطبيق ضوابط الأمن السيبراني للحوسبة السحابية على نماذج الحوسبة السحابية الثلاثة (البرمجيات كخدمة "SaaS"، المنصة كخدمة "PaaS"، البنية التحتية كخدمة "IaaS").

٧. التحديث والمراجعة

تتولى الهيئة التحديث والمراجعة الدورية لضوابط الأمن السيبراني للحوسبة السحابية (والوثائق الإلحاقية الخاصة بها) حسب متطلبات الأمن السيبراني والمستجدات ذات العلاقة. كما تتولى الهيئة الإعلان عن الإصدار المحدث من الضوابط لتطبيقه والالتزام به.

٨. هيكلية المكونات الفرعية لضوابط الأمن السيبراني للحوسبة السحابية

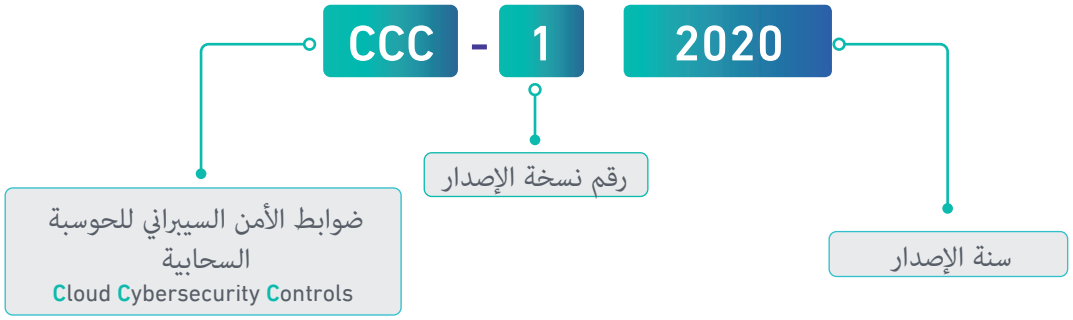
يوضح الشكل (٢) أدناه المكونات الأساسية والفرعية للضوابط.

١- حوكمة الأمن السيبراني Cybersecurity Governance	١-١	أدوار ومسؤوليات الأمن السيبراني Cybersecurity Roles and Responsibilities	٢-١	إدارة مخاطر الأمن السيبراني Cybersecurity Risk Management
	١-٣	الالتزام بتشريعات وتنظيمات ومعايير الأمن السيبراني Compliance with Cybersecurity Standards, Laws and Regulations	٤-١	الأمن السيبراني المتعلق بالموارد البشرية Cybersecurity in Human Resources
	١-٥	الأمن السيبراني ضمن إدارة التغيير Cybersecurity in Change Management		
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 Information Processing Facilities Protection	٤-٢	إدارة أمن الشبكات Networks Security Management
	٢-٥	أمن الأجهزة المحمولة Mobile Devices Security	٦-٢	حماية البيانات والمعلومات Data and Information Protection
	٢-٧	التشفير Cryptography	٨-٢	إدارة النسخ الاحتياطية Backup and Recovery Management
	٢-٩	إدارة الثغرات Vulnerabilities Management	١٠-٢	اختبار الاختراق Penetration Testing
	٢-١١	إدارة سجلات الأحداث ومراقبة الأمن السيبراني Cybersecurity Event Logs and Monitoring Management	١٢-٢	إدارة حوادث وتهديدات الأمن السيبراني Cybersecurity Incident and Threat Management
	٢-١٣	الأمن المادي Physical Security	١٤-٢	حماية تطبيقات الويب Web Application Security
	٢-١٥	إدارة المفاتيح Key Management	١٦-٢	أمن تطوير الأنظمة System Development Security
	٢-١٧	أمن وسائط التخزين Storage Media 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 Third-Party Cybersecurity	٤-١	الأمن السيبراني المتعلق بسلسلة الإمداد والأطراف الخارجية Supply Chain and Third-Party Cybersecurity		

شكل ٢: المكونات الأساسية والفرعية لضوابط الأمن السيبراني للحوسبة السحابية

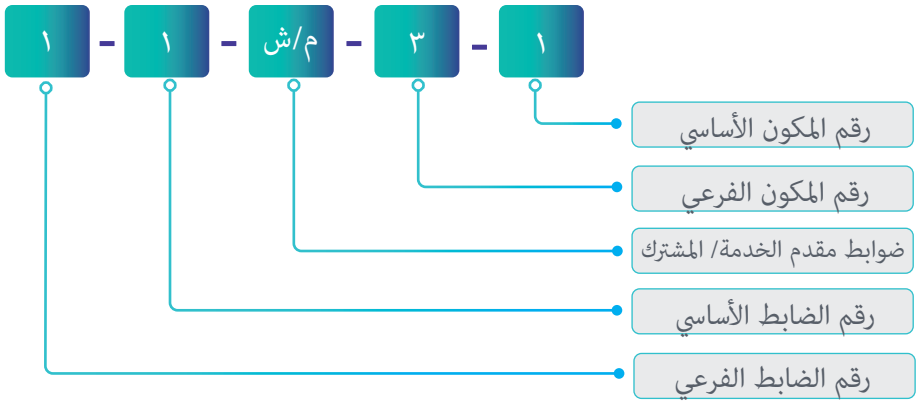
٩. هيكلية وثيقة ضوابط الأمن السيبراني للحوسبة السحابية

يُشار إلى وثيقة ضوابط الأمن السيبراني للحوسبة السحابية بالطريقة الموضحة في الشكل (٣).



شكل ٣: رموز تعريف ضوابط الأمن السيبراني للحوسبة السحابية

يتم استخدام الهيكلية الموضحة في الشكل (٤) لترقيم مكونات وضوابط الأمن السيبراني للحوسبة السحابية.



شكل ٤. هيكلية ضوابط الأمن السيبراني للحوسبة السحابية

تحتوي ضوابط الأمن السيبراني للحوسبة السحابية على ضوابط أساسية وفرعية لمقدمي الخدمات والمشتركين، وكما هو موضح في الشكل (٤) أعلاه، تم التفريق بينهما من خلال رمز الضابط، حيث تمت الإشارة إلى الضوابط الخاصة بمقدمي الخدمات والمشتركين كالتالي:

- تم استعمال الحرف (م) في رمز الضابط للإشارة إلى الضوابط الخاصة بمقدمي الخدمات.
- تم استعمال الحرف (ش) في رمز الضابط للإشارة إلى الضوابط الخاصة بالمشتركين.

فعلى سبيل المثال: ١-٣-م-١-١ يشير إلى أن الضابط خاص بمقدمي الخدمات، و ١-٣-ش-١-١ يشير إلى أن الضابط خاص بالمشتركين.

يرجى ملاحظة أن الأرقام التي تكون بخط عريض وباللون الأخضر (مثل: **١-٣-٢**) هي عبارة عن إشارة مرجعية لمكون فرعي أو ضابط من الضوابط الأساسية للأمن السيبراني.

طريقة هيكلية ضوابط الأمن السيبراني للحوسبة السحابية

يوضح جدول (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

١٠. ضوابط الأمن السيبراني للحوسبة السحابية

تفاصيل ضوابط الأمن السيبراني للحوسبة السحابية.

١ حوكمة الأمن السيبراني (Cybersecurity Governance)

١-١	**أدوار ومسؤوليات الأمن السيبراني (Cybersecurity Roles and Responsibilities)**
الهدف	ضمان تحديد أدوار ومسؤوليات واضحة لجميع الأطراف المشاركة في تطبيق ضوابط الأمن السيبراني للحوسبة السحابية، بما في ذلك أدوار ومسؤوليات منصب رئيس مقدم الخدمة أو المشترك، أو من ينيبه، ويشار له في هذه الضوابط باسم «صاحب الصلاحية».
الضوابط	
١-١-م-١	بالإضافة للضابط ١-٤-١ في الضوابط الأساسية للأمن السيبراني، يجب على صاحب الصلاحية تحديد وتوثيق واعتماد ما يلي: ١-١-م-١-١ أدوار الأمن السيبراني، وتكليفات المسؤولية والمحاسبة والاستشارة والتبليغ (RACI) لكل أصحاب العلاقة في خدمات الحوسبة السحابية، بما في ذلك أدوار ومسؤوليات صاحب الصلاحية.
١-١-ش-١	بالإضافة للضابط ١-٤-١ في الضوابط الأساسية للأمن السيبراني، يجب على صاحب الصلاحية تحديد وتوثيق واعتماد ما يلي: ١-١-ش-١-١ أدوار الأمن السيبراني، وتكليفات المسؤولية والمحاسبة والاستشارة والتبليغ (RACI) لكل أصحاب العلاقة في خدمات الحوسبة السحابية، بما في ذلك أدوار ومسؤوليات صاحب الصلاحية.
١-٢	**إدارة مخاطر الأمن السيبراني (Cybersecurity Risk Management)**
الهدف	ضمان إدارة مخاطر الأمن السيبراني على نحو ممنهج يهدف إلى حماية الأصول المعلوماتية والتقنية لدى مقدمي الخدمات والمشتركين، وذلك وفقًا للسياسات والإجراءات التنظيمية لديهم والمتطلبات التشريعية والتنظيمية ذات العلاقة.
الضوابط	
١-٢-م-١	يجب أن تتضمن منهجية إدارة مخاطر الأمن السيبراني المذكورة في المكون الفرعي ١-٥ في الضوابط الأساسية للأمن السيبراني لدى مقدمي الخدمات بحد أدنى ما يلي:

	١-٢-م-١-١ تحديد المستوى المقبول للمخاطر (Acceptable Risk Levels) فيما يتعلق بخدمات الحوسبة السحابية، وتوضيحها للمشترك إذا كانت المخاطر ذات علاقة به. ١-٢-م-١-٢ أخذ تصنيف البيانات والمعلومات بالاعتبار في منهجية إدارة مخاطر الأمن السيبراني. ١-٢-م-١-٣ إنشاء سجل لمخاطر الأمن السيبراني خاص بالعمليات وخدمات الحوسبة السحابية، ومتابعته دوريًا بما يتناسب مع طبيعة المخاطر.
١-٢-ش-١	يجب أن تتضمن منهجية إدارة مخاطر الأمن السيبراني المذكورة في المكون الفرعي ١-٥ في الضوابط الأساسية للأمن السيبراني لدى المشتركين بحد أدنى ما يلي: ١-٢-ش-١-١ تحديد المستوى المقبول للمخاطر (Acceptable Risk Levels) فيما يتعلق بخدمات الحوسبة السحابية. ١-٢-ش-١-٢ أخذ تصنيف البيانات والمعلومات بالاعتبار في منهجية إدارة مخاطر الأمن السيبراني. ١-٢-ش-١-٣ إنشاء سجل لمخاطر الأمن السيبراني خاص بالعمليات وخدمات الحوسبة السحابية، ومتابعته دوريًا بما يتناسب مع طبيعة المخاطر.
١-٣	**الالتزام بتشريعات وتنظيمات ومعايير الأمن السيبراني (Compliance with Cybersecurity Standards, Laws and Regulations)**
الهدف	ضمان التأكد من أن برنامج الأمن السيبراني لدى مقدمي الخدمات والمشتركين يتوافق مع المتطلبات التشريعية والتنظيمية ذات العلاقة.
الضوابط	
١-٣-م-١	بالإضافة للضابط ١-٧-١ في الضوابط الأساسية للأمن السيبراني، يجب أن يشتمل التزام مقدمي الخدمات بالمتطلبات التشريعية والتنظيمية بحد أدنى ما يلي: ١-٣-م-١-١ الالتزام الدائم والمستمر بجميع الأنظمة واللوائح والتعليمات والقرارات والأطر والضوابط التنظيمية المتعلقة بالأمن السيبراني والمعمول بها في المملكة.
١-٣-ش-١	بالإضافة للضابط ١-٧-١ في الضوابط الأساسية للأمن السيبراني، يجب أن يشتمل التزام المشتركين بالمتطلبات التشريعية والتنظيمية بحد أدنى ما يلي: ١-٣-ش-١-١ المراقبة الدائمة والمستمرة لمدى التزام مقدمي الخدمات بالتشريعات، وبنود العقود المتعلقة بالأمن السيبراني.
١-٤	**الأمن السيبراني المتعلق بالموارد البشرية (Cybersecurity in Human Resources)**
الهدف	ضمان التأكد من أن مخاطر الأمن السيبراني المتعلقة بالعاملين (موظفين ومتعاقدين) لدى مقدمي الخدمات والمشتركين، تعالج بفعالية قبل وأثناء وعند انتهاء/إنهاء عملهم، وذلك وفقًا للسياسات والإجراءات التنظيمية لديهم، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

الضوابط	
١-٤-م-١	بالإضافة للضوابط الفرعية ضمن الضابطين ١-٩-٣ و ١-٩-٤ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني قبل بدء وخلال العلاقة المهنية بين العاملين ومقدمي الخدمة بحد أدنى ما يلي: ١-٤-م-١-١ فيما يتعلق بمراكز البيانات التابعة لمقدم الخدمة داخل المملكة، يجب أن يشغل وظائف الأمن السيبراني مواطنون سعوديون مؤهلون. ١-٤-م-١-٢ إجراء المسح الأمني للعاملين داخل المملكة الذين لهم حق الوصول إلى الأنظمة التقنية السحابية (Cloud Technology Stack (CTS)) دوريًا. ١-٤-م-١-٣ إقرار وتوقيع العاملين على جميع سياسات الأمن السيبراني كشرط مسبق للوصول إلى الأنظمة التقنية السحابية (CTS).
١-٤-م-٢	بالإضافة للضوابط الفرعية ضمن الضابط ١-٩-٥ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني بعد انتهاء العلاقة المهنية بين العاملين ومقدمي الخدمة بحد أدنى ما يلي: ١-٤-م-٢-١ ضمان إعادة الأصول الخاصة بمقدمي الخدمات (لا سيما ذات الصلة بالأمن السيبراني) بمجرد إنهاء الخدمة مع العاملين.
١-٤-ش-١	بالإضافة للضوابط الفرعية ضمن الضابط ١-٩-٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني قبل بدء العلاقة المهنية بين العاملين والمشتركين، بحد أدنى ما يلي: ١-٤-ش-١-١ إجراء المسح الأمني للعاملين الذين لهم حق الوصول إلى المهام الحساسة لخدمات الحوسبة السحابية، مثل: إدارة المفاتيح، إدارة الخدمات، التحكم بالوصول (Access Control).
١-٥	**الأمن السيبراني ضمن إدارة التغيير (Cybersecurity in Change Management)**
الهدف	التأكد من أن متطلبات الأمن السيبراني مضمنة في منهجية وإجراءات إدارة التغيير لدى مقدمي الخدمات لحماية السرية وسلامة الأصول المعلوماتية والتقنية لديهم، ودقتها وتوافرها، وذلك وفقًا للسياسات والإجراءات التنظيمية لدى مقدمي الخدمات والمشتركين والمتطلبات التشريعية والتنظيمية ذات العلاقة.
الضوابط	
١-٥-م-١	يجب تحديد متطلبات الأمن السيبراني لإدارة التغيير لدى مقدمي الخدمات، وتوثيقها، واعتمادها.
١-٥-م-٢	يجب تطبيق متطلبات الأمن السيبراني، الخاصة بإدارة التغيير لدى مقدمي الخدمات.

١-٥-م-٣	يجب أن يغطي الأمن السيبراني لإدارة التغيير لدى مقدمي الخدمات بحد أدنى ما يلي: ١-٥-م-٣-١ إجراءات تنفيذ التغييرات (المخطط لها) بطرق آمنة، في أنظمة الإنتاج (Production Systems)، مع إعطاء أولوية للملاحظات المتعلقة بالأمن السيبراني. ١-٥-م-٣-٢ إجراءات تنفيذ التغييرات الاستثنائية ذات العلاقة بالأمن السيبراني (مثل التغييرات أثناء التعافي من الحوادث).
١-٥-م-٤	يجب مراجعة متطلبات الأمن السيبراني لإدارة التغيير لدى مقدمي الخدمات، ومراجعة تطبيقها، دوريًا.

٢ تعزيز الأمن السيبراني (Cybersecurity Defense)

٢-١	إدارة الأصول (Asset Management)
الهدف	التأكد من أن مقدمي الخدمات والمشتركين لديهم قائمة جرد دقيقة وحديثة للأصول تشمل التفاصيل ذات العلاقة لجميع الأصول المعلوماتية والتقنية، من أجل دعم العمليات التشغيلية لديهم ومتطلبات الأمن السيبراني، لتحقيق سرية وسلامة الأصول المعلوماتية والتقنية ودقتها وتوافرها.
الضوابط	
٢-١-م-١	بالإضافة للضوابط ضمن المكون الفرعي ٢-١ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني لإدارة الأصول المعلوماتية والتقنية لدى مقدمي الخدمات، بحد أدنى ما يلي: ٢-١-م-١-١ حصر جميع الأصول المعلوماتية والتقنية باستخدام التقنيات المناسبة كقاعدة بيانات إدارة الإعدادات (CMDB)، أو قدرة مماثلة، تتضمن جردًا لكل الأصول التقنية. ٢-١-م-١-٢ تحديد ملاك الأصول (Asset Owners) وإشراكهم في دورة حياة إدارة الأصول.
٢-١-ش-١	بالإضافة للضوابط ضمن المكون الفرعي ٢-١ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني لإدارة الأصول المعلوماتية والتقنية لدى المشتركين، بحد أدنى ما يلي: ٢-١-ش-١-١ حصر جميع الخدمات السحابية والأصول المعلوماتية والتقنية المتعلقة بها.
٢-٢	إدارة هويات الدخول والصلاحيات (Identity and Access Management)
الهدف	ضمان حماية الأمن السيبراني للوصول المنطقي (Logical Access) إلى الأصول المعلوماتية والتقنية الخاصة بمقدمي الخدمات والمشتركين من أجل منع الوصول غير المصرح به وتقييد الوصول إلى ماهو مطلوب لإنجاز الأعمال الخاصة بهم.
الضوابط	

٢-٢-م-١	بالإضافة للضوابط الفرعية ضمن الضابط ٢-٢-٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني الخاصة بإدارة هويات الدخول والصلاحيات لدى مقدمي الخدمات، بحد أدنى مايلي: ٢-٢-م-١-١ إدارة الحسابات العامة (Generic Accounts) التي لا يمكن إسناد مسؤوليتها إلى أشخاص محددين. ٢-٢-م-١-٢ الإدارة الآمنة للجلسات (Secure Session Management)، وتشمل موثوقية الجلسات (Authenticity)، وإقفالها (Lockout)، وإنهاء مهلتها (Timeout). ٢-٢-م-١-٣ التحقق من الهوية متعدد العناصر (Mulit-Factor Authentication) لحسابات المستخدمين ذوي الصلاحيات الهامة والحساسة، والذين لهم حق الوصول إلى الأنظمة التقنية السحابية (CTS). ٢-٢-م-١-٤ إجراءات لكشف محاولات الوصول غير المصرح به ومنعها مثل: (الحد الأقصى من محاولات عمليات الدخول غير الناجحة (Unsuccessful Login)). ٢-٢-م-١-٥ استخدام الطرق والخوارزميات الآمنة لحفظ ومعالجة كلمات المرور مثل: استخدام دوال اختزال آمنة (Secure Hashing Functions). ٢-٢-م-١-٦ الإدارة الآمنة للحسابات الخاصة بالعاملين التابعين للأطراف الخارجية (Third-party). ٢-٢-م-١-٧ التحكم في الوصول إلى الأنظمة الإدارية (Management Systsmes) والإشرافية (Administrative Consoles). ٢-٢-م-١-٨ إخفاء معلومات التحقق من الهوية، خاصةً كلمات المرور، عند عرضها للمستخدم؛ لحمايتها من اطلاع الآخرين عليها. ٢-٢-م-١-٩ الحصول على موافقة المشترك قبل عملية الوصول إلى أي من الأصول والبيانات الخاصة به، من قبل مقدم الخدمة أو الأطراف الخارجية لمقدم الخدمة. ٢-٢-م-١-١٠ القدرة على الإيقاف الفوري للجلسة (Session) لعمليات الدخول عن بعد ومنع المستخدم من الدخول مستقبلًا. ٢-٢-م-١-١١ تزويد المشتركين بخدمات التحقق من الهوية متعدد العناصر لكافة الحسابات السحابية للمستخدمين ذوي الصلاحيات الهامة والحساسة. ٢-٢-م-١-١٢ التحكم بالوصول لأنظمة ووسائل التخزين (مثل الشبكة الخاصة بالتخزين (Storage Area Network (SAN).)
٢-٢-ش-١	بالإضافة للضوابط الفرعية ضمن الضابط ٢-٢-٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني الخاصة بإدارة هويات الدخول والصلاحيات لدى المشتركين، بحد أدنى مايلي: ٢-٢-ش-١-١ إدارة هويات الدخول والصلاحيات لجميع الحسابات، التي لديها صلاحية الوصول إلى الخدمات السحابية، خلال دورة حياتها. ٢-٢-ش-١-٢ سرِّية هوية المستخدم والحسابات والصلاحيات، بما في ذلك الطلب من المستخدمين حفظ خصوصيتها (للعاملين، والأطراف الخارجية، والمستخدمين من جهة المشترك).

	٢-٢-ش-١-٣ الإدارة الآمنة للجلسات (Secure Session Management)، وتشمل موثوقية الجلسات (Authenticity)، وإقفالها (Lockout)، وإنهاء مهلتها (Timeout). ٢-٢-ش-١-٤ التحقق من الهوية متعدد العناصر لكافة الحسابات السحابية للمستخدمين ذوي الصلاحيات الهامة والحساسة. ٢-٢-ش-١-٥ إجراءات لكشف محاولات الوصول غير المصرح به ومنعها مثل: (الحد الأقصى من محاولات عمليات الدخول غير الناجحة (Unsuccessful Login)).
٢-٣	**حماية الأنظمة وأجهزة معالجة المعلومات (Information System and Information Processing Facilities Protection)**
الهدف	ضمان حماية الأنظمة وأجهزة معالجة المعلومات بما في ذلك أجهزة المستخدمين والبنى التحتية لدى مقدمي الخدمات والمشتركين من المخاطر السيبرانية.
الضوابط	
٢-٣-م-١	بالإضافة للضوابط الفرعية ضمن الضابط ٢-٣-٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني الخاصة بحماية الأنظمة وأجهزة معالجة المعلومات لدى مقدمي الخدمات، بحد أدنى مايلي: ٢-٣-م-١-١ التحقق من مدى التزام الإعدادات التقنية لمعايير الأمن السيبراني المعتمدة لدى مقدم الخدمة. ٢-٣-م-١-٢ وضع ضمانات لمنع اختلاط بيانات (Data Commingling) المشتركين. ٢-٣-م-١-٣ اتباع مبادئ الأمن السيبراني لتفعيل الحد الأدنى من الوظائف المطلوبة (Minimum Functionality Principle) لإعدادات الأنظمة (System Configurations). ٢-٣-م-١-٤ أن تكون الأنظمة التقنية السحابية (CTS) قادرة على التعامل بطرق آمنة مع: المدخلات والتحقق منها (Input Validation)، والاستثناءات (Exception)، والتوقف (Failure). ٢-٣-م-١-٥ عزل التطبيقات والوظائف الأمنية عن التطبيقات والوظائف الأخرى في الأنظمة التقنية السحابية (CTS). ٢-٣-م-١-٦ تبليغ المشترك بالمتطلبات المتعلقة بالأمن السيبراني التي يوفرها مقدم الخدمة والقابلة للاستخدام من قبل المشترك. ٢-٣-م-١-٧ اكتشاف ومنع التغييرات غير المصرح بها على البرامج والأنظمة. ٢-٣-م-١-٨ العزل بين بيئات الاستضافة الخاصة بالمشتركين (Guest Environments)، والحماية فيما بينها. ٢-٣-م-١-٩ أن تكون الحوسبة السحابية المشتركة المقدمة للمشتركين (الجهات الحكومية والجهات ذات البنية التحتية الحساسة) معزولة عن أي حوسبة سحابية أخرى مقدمة للجهات خارج نطاق العمل.

	٢-٣-م-١-١٠ تقديم خدمات الحوسبة السحابية من داخل المملكة، وتشمل الأنظمة المستخدمة بما في ذلك أنظمة التخزين، والمعالجة، ومراكز التعافي من الكوارث. ٢-٣-م-١-١١ تقديم خدمات الحوسبة السحابية من داخل المملكة، وتشمل الأنظمة المستخدمة بما في ذلك أنظمة المراقبة، والدعم. ٢-٣-م-١-١٢ استخدام التقنيات الحديثة، مثل تقنيات (Endpoint Detection and Response (EDR)) ، لضمان جاهزية خوادم وأجهزة المعلومات الخاصة بأنظمة وأجهزة معالجة المعلومات لدى مقدمي الخدمات، للاستجابة السريعة للحوادث.
٢-٣-ش-١	بالإضافة للضوابط الفرعية ضمن الضابط ٢-٣-٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني الخاصة بحماية الأنظمة وأجهزة معالجة المعلومات لدى المشتركين، بحد أدنى مايلي: ٢-٣-ش-١-١ التحقق من قيام مقدم الخدمة بعزل الحوسبة السحابية المشتركة المقدمة للمشتركين (الجهات الحكومية والجهات ذات البنية التحتية الحساسة) عن أي حوسبة سحابية أخرى مقدمة للجهات خارج نطاق العمل.
٢-٤	**إدارة أمن الشبكات (Networks Security Management)**
الهدف	ضمان حماية شبكات مقدمي الخدمات والمشتركين من المخاطر السيبرانية.
الضوابط	
٢-٤-م-١	بالإضافة للضوابط الفرعية ضمن الضابط ٢-٥-٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني الخاصة بإدارة أمن الشبكات لدى مقدمي الخدمات، بحد أدنى مايلي: ٢-٤-م-١-١ مراقبة الشبكات الداخلية والخارجية للكشف عن الأنشطة المشبوهة. ٢-٤-م-١-٢ عزل وحماية الشبكة الخاصة بالأنظمة التقنية السحابية (CTS) من الشبكات الأخرى الداخلية والخارجية. ٢-٤-م-١-٣ الحماية من هجمات تعطيل الخدمات (Denial of Service (DoS))، وهجمات تعطيل الخدمات الموزعة (Distributed Denial of Service (DDoS)). ٢-٤-م-١-٤ استخدام التشفير للبيانات المنتقلة عبر الشبكة من وإلى الشبكة الخاصة بالأنظمة التقنية السحابية (CTS) لعمليات الوصول الإشرافي والإداري (Management and Administrative Access). ٢-٤-م-١-٥ التحكم في الوصول (Access Control) بين أجزاء الشبكة (Network Segments) المختلفة. ٢-٤-م-١-٦ العزل بين شبكات الخدمات السحابية (Cloud Service Delivery) وشبكات الإدارة السحابية (Cloud Management) والشبكة الداخلية لمقدم الخدمة (Enterprise).

٢-٤-ش-١	بالإضافة للضوابط الفرعية ضمن الضابط ٢-٥-٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني الخاصة بإدارة أمن الشبكات لدى المشتركين، بحد أدنى مايلي: ٢-٤-ش-١-١ حماية القناة المستخدمة للاتصال الشبكي مع مقدم الخدمة.
٢-٥	**أمن الأجهزة المحمولة (Mobile Devices Security)**
الهدف	ضمان حماية الأجهزة المحمولة (بما في ذلك أجهزة الحاسب المحمول، والهواتف الذكية، والأجهزة اللوحية) من المخاطر السيبرانية، وضمان التعامل الآمن مع المعلومات والبيانات الحساسة التي ترتبط بأعمال مقدمي الخدمات والمشتركين، وحمايتها أثناء النقل والتخزين عند استخدام الأجهزة المحمولة.
الضوابط	
٢-٥-م-١	بالإضافة للضوابط الفرعية ضمن الضابط ٢-٦-٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني الخاصة بأمن الأجهزة المحمولة لدى مقدمي الخدمات، بحد أدنى مايلي: ٢-٥-م-١-١ الاحتفاظ بقائمة جرد محدثة (Inventory) للأجهزة المحمولة. ٢-٥-م-١-٢ الإدارة الأمنية للأجهزة المحمولة (Mobile Device Management) مركزيًا. ٢-٥-م-١-٣ قفل الشاشة لأجهزة المستخدمين (Screen Lock). ٢-٥-م-١-٤ قبل إعادة استخدام الأجهزة المحمولة أو التخلص منها، خصوصًا التي يتم استخدامها للدخول على الأنظمة التقنية السحابية (CTS)، يجب التأكد من عدم احتوائها على أية بيانات أو معلومات باستخدام وسائل آمنة.
٢-٥-ش-١	بالإضافة للضوابط الفرعية ضمن الضابط ٢-٦-٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني الخاصة بأمن الأجهزة المحمولة لدى المشتركين، بحد أدنى مايلي: ٢-٥-ش-١-١ قبل إعادة استخدام الأجهزة المحمولة أو التخلص منها، خصوصًا التي يتم استخدامها للدخول على الخدمات السحابية، يجب التأكد من عدم احتوائها على أية بيانات أو معلومات باستخدام وسائل آمنة.
٢-٦	**حماية البيانات والمعلومات (Data and Information Protection)**
الهدف	ضمان حماية بيانات مقدمي الخدمات والمشتركين، وسريتها، وسلامتها، ودقتها، وتوافرها وفقًا للسياسات والإجراءات التنظيمية لديهم، والمتطلبات التشريعية والتنظيمية ذات العلاقة.
الضوابط	
٢-٦-م-١	بالإضافة للضوابط الفرعية ضمن الضابط ٢-٧-٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني الخاصة بحماية البيانات والمعلومات لدى مقدمي الخدمة، بحد أدنى مايلي:

	٢-٦-م-١-١ عدم استخدام بيانات الأنظمة التقنية السحابية (CTS) 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-م-١-٢ تزويد المشتركين بعمليات وإجراءات وتقنيات آمنة لتخزين البيانات، مع الالتزام بالمتطلبات التشريعية والتنظيمية ذات العلاقة. ٢-٦-م-١-٣ حذف وإتلاف بيانات المشترك بطرق آمنة عند الانتهاء من العلاقة مع المشترك. ٢-٦-م-١-٤ الالتزام بالمحافظة على سرية بيانات ومعلومات المشترك، حسب المتطلبات التشريعية والتنظيمية ذات العلاقة. ٢-٦-م-١-٥ تزويد المشتركين بوسائل آمنة لتصدير ونقل البيانات والبنية التحتية الافتراضية.
٢-٦-ش-١	بالإضافة للضوابط الفرعية ضمن الضابط ٢-٧-٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني الخاصة بحماية بيانات و معلومات المشتركين في الحوسبة السحابية، بحد أدنى مايلي: ٢-٦-ش-١-١ وجود ضمانات للقدرة على حذف البيانات بطرق آمنة عند الانتهاء من العلاقة مع مقدم الخدمة (Exit Strategy). ٢-٦-ش-١-٢ استخدام وسائل آمنة لتصدير ونقل البيانات والبنية التحتية الافتراضية.
٢-٧	**التشفير (Cryptography)**
الهدف	ضمان استخدام التشفير بطريقة مناسبة وفعالة لحماية الأصول المعلوماتية الخاصة بمقدمي الخدمات والمشتركين وفقًا للسياسات والإجراءات التنظيمية والمتطلبات التشريعية والتنظيمية ذات العلاقة.
الضوابط	
٢-٧-م-١	بالإضافة للضوابط الفرعية ضمن الضابط ٢-٨-٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني الخاصة بالتشفير لدى مقدمي الخدمات، بحد أدنى مايلي: ٢-٧-م-١-١ الالتزام باستخدام طرق وخوارزميات ومفاتيح وأجهزة تشفير محدثة وآمنة، وفقًا للمستوى المتقدم (Advanced) ضمن المعايير الوطنية للتشفير (NCS-1:2020). ٢-٧-م-١-٢ القدرة على إصدار شهادات رقمية وإدارتها بطرق آمنة، أو استخدام شهادات رقمية صادرة من جهات موثوقة (Trusted Certification Authority).

٢-٧-ش-١	بالإضافة للضوابط الفرعية ضمن الضابط ٢-٨-٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني الخاصة بالتشفير لدى المشتركين، بحد أدنى مايلي: ٢-٧-ش-١-١ الالتزام باستخدام طرق وخوارزميات ومفاتيح وأجهزة تشفير محدثة وآمنة، وفقًا للمستوى المتقدم (Advanced) ضمن المعايير الوطنية للتشفير (NCS-1:2020). ٢-٧-ش-١-٢ تشفير البيانات والمعلومات المنقولة إلى الخدمات السحابية، أو المنقولة منها، بحسب المتطلبات التشريعية والتنظيمية ذات العلاقة.
٢-٨	**إدارة النسخ الاحتياطية (Backup and Recovery Management)**
الهدف	ضمان حماية بيانات ومعلومات مقدمي الخدمات والمشتركين والإعدادات التقنية للأنظمة والتطبيقات الخاصة بهم من الأضرار الناجمة عن المخاطر السيبرانية، وذلك وفقًا للسياسات والإجراءات التنظيمية لدى مقدمي الخدمات، والمتطلبات التشريعية والتنظيمية ذات العلاقة.
الضوابط	
٢-٨-م-١	بالإضافة للضوابط الفرعية ضمن الضابط ٢-٩-٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني الخاصة بإدارة النسخ الاحتياطية لدى مقدمي الخدمات، بحد أدنى مايلي: ٢-٨-م-١-١ تأمين الوصول، والتخزين، والنقل لمحتوى النسخ الاحتياطية لبيانات المشترك ووسائطها، وحمايتها من الإتلاف، أو التعديل، أو الاطلاع غير المصرح به. ٢-٨-م-١-٢ تأمين الوصول، والتخزين، والنقل لمحتوى النسخ الاحتياطية للأنظمة التقنية السحابية (CTS)، ووسائطها، وحمايتها من الإتلاف، أو التعديل، أو الاطلاع غير المصرح به.
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 الأعمال الخاصة بمقدمي الخدمات والمشتركين.
الضوابط	
٢-٩-م-١	بالإضافة للضوابط الفرعية ضمن الضابط ٢-١٠-٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني الخاصة بإدارة الثغرات لدى مقدمي الخدمات، بحد أدنى مايلي: ٢-٩-م-١-١ تقييم ومعالجة الثغرات لمكونات الأنظمة التقنية السحابية (CTS) الخارجية مرة واحدة شهريًا على الأقل، وكل ثلاثة أشهر على الأقل لمكونات الأنظمة التقنية السحابية (CTS) الداخلية. ٢-٩-م-١-٢ إشعار المشترك بالثغرات المكتشفة التي قد تؤثر عليه، وكيفية معالجتها.

٢-٩-ش-١	بالإضافة للضوابط الفرعية ضمن الضابط ٢-١٠-٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني الخاصة بإدارة الثغرات لدى المشتركين، بحد أدنى مايلي: ٢-٩-ش-١-١ تقييم ومعالجة الثغرات الخاصة بالخدمات السحابية مرة واحدة كل ثلاثة أشهر على الأقل. ٢-٩-ش-١-٢ إدارة الثغرات التي تم إشعار المشترك بها عن طريق مقدم الخدمة، ومعالجتها.
٢-١٠	**اختبار الاختراق (Penetration Testing)**
الهدف	تقييم واختبار مدى فعالية قدرات تعزيز الأمن السيبراني لدى مقدمي الخدمات، وذلك من خلال عمل محاكاة لتقنيات وأساليب الهجوم السيبراني الفعلية. ولاكتشاف نقاط الضعف الأمنية غير المعروفة والتي قد تؤدي إلى الاختراق السيبراني لمقدمي الخدمات. وذلك وفقاً للمتطلبات التشريعية والتنظيمية ذات العلاقة.
الضوابط	
٢-١٠-م-١	بالإضافة للضوابط الفرعية ضمن الضابط ٢-١١-٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني الخاصة باختبار الاختراق لدى مقدمي الخدمات، بحد أدنى مايلي: ٢-١٠-م-١-١ يجب أن يشمل نطاق عمل اختبار الاختراق الأنظمة التقنية السحابية (CTS)، وأن يتم عمل اختبار الاختراق كل ستة أشهر؛ على الأقل.
٢-١١	**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 مقدمي الخدمات والمشتركين.
الضوابط	
٢-١١-م-١	بالإضافة للضوابط الفرعية ضمن الضابط ٢-١٢-٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني لإدارة سجلات الأحداث ومراقبة الأمن السيبراني لدى مقدمي الخدمات، بحد أدنى مايلي: ٢-١١-م-١-١ تفعيل وحماية سجلات الأحداث (Event Logs) والتدقيق (Audit Trial) للأنظمة التقنية السحابية (CTS). ٢-١١-م-١-٢ تفعيل سجلات الأحداث الخاصة بمحاولات عمليات الدخول (Login) وجمعها. ٢-١١-م-١-٣ تفعيل وحماية سجلات الأحداث لجميع الأنشطة والعمليات التي يقوم بها مقدم الخدمة على أنظمة المشتركين، بهدف دعم عمليات التحليل الرقمي الجنائي (Digital Forensics).

	٢-١١-م-١-٤ حماية سجلات الأحداث (Event Logs) الخاصة بالأمن السيبراني، من الوصول غير المصرح به، أو العبث، أو التغيير، أو الحذف غير المشروع، وذلك وفقًا للمتطلبات التشريعية، أو التنظيمية. ٢-١١-م-١-٥ المراقبة الأمنية المستمرة لأحداث الأمن السيبراني (Cybersecurity Events) باستخدام تقنيات (SIEM) بحيث تشمل جميع الأحداث المتعلقة بالأنظمة التقنية السحابية (CTS). ٢-١١-م-١-٦ المراجعة الدورية لسجلات الأحداث (Event Logs) والتدقيق (Audit Trail) بحيث تشمل الأحداث والسجلات المتعلقة بالأنظمة التقنية السحابية (CTS)، التي تم تنفيذها من قبل مقدم الخدمة. ٢-١١-م-١-٧ استخدام وسائل آلية لمراقبة سجلات الأحداث الخاصة بعمليات الدخول عن بعد (Remote Access). ٢-١١-م-١-٨ التعامل الآمن مع بيانات المستخدمين المتواجدة في سجلات الأحداث (Event Logs) والتدقيق (Audit Trails) وسجلات أحداث الأمن السيبراني (Cybersecurity Events Logs).
٢-١١-ش-١	بالإضافة للضوابط الفرعية ضمن الضابط ٢-١٢-٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني لإدارة سجلات الأحداث ومراقبة الأمن السيبراني لدى المشتركين، بحد أدنى مايلي: ٢-١١-ش-١-١ تفعيل وجمع سجلات الأحداث الخاصة بعمليات الدخول (Login)، وسجلات الأحداث الخاصة بالأمن السيبراني على الأصول المتعلقة بالخدمات السحابية. ٢-١١-ش-١-٢ أن تشمل عملية المراقبة جميع الأحداث أحداث الأمن السيبراني المفعلة على الخدمات السحابية الخاصة بالمشترك.
٢-١٢	**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 استباقيًا من أجل منع أو تقليل الآثار المترتبة على أعمال مقدمي الخدمات.
الضوابط	
٢-١٢-م-١	بالإضافة للضوابط الفرعية ضمن الضابط ٢-١٣-٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني لإدارة حوادث وتهديدات الأمن السيبراني لدى مقدمي الخدمات، بحد أدنى مايلي: ٢-١٢-م-١-١ الاشتراك مع المجموعات والجهات المتخصصة والموثوقة للحصول على آخر التهديدات والمستجدات في مجال الأمن السيبراني. ٢-١٢-م-١-٢ تدريب العاملين (موظفين ومتعاقدين) على الاستجابة لحوادث الأمن السيبراني بما يتماشى مع الأدوار والمسؤوليات.

	٢-١٢-م-١-٣ اختبار قدرات الاستجابة لحوادث الأمن السيبراني دوريًا. ٢-١٢-م-١-٤ تحليل وتحديد الأسباب الجذرية (Root Cause Analysis) لحوادث الأمن السيبراني، ووضع الخطط الكفيلة بمعالجتها. ٢-١٢-م-١-٥ تقديم الدعم إلى المشتركين في حالات القضايا القانونية، والتحليل الرقمي الجنائي، والحفاظ على الأدلة الرقمية التي تقع تحت إدارة ومسؤولية مقدم الخدمة حسب المتطلبات التشريعية والتنظيمية ذات العلاقة. ٢-١٢-م-١-٦ تبليغ المشترك بشكل فوري عن حوادث الأمن السيبراني التي قد تؤثر عليه، في حال اكتشاف الحادثة. ٢-١٢-م-١-٧ دعم المشتركين للتعامل مع حوادث الأمن السيبراني حسب الاتفاقية مابين مقدم الخدمة والمشترك. ٢-١٢-م-١-٨ قياس ومراقبة مؤشرات الأداء الخاصة بإدارة حوادث الأمن السيبراني، ومراقبة مدى الالتزام بمتطلبات العقود والتشريعات.
٢-١٣	**الأمن المادي (Physical Security)**
الهدف	ضمان حماية الأصول المعلوماتية و التقنية الخاصة بمقدمي الخدمات من الوصول المادي غير المصرح به والفقدان والسرقة والتخريب.
الضوابط	
٢-١٣-م-١	بالإضافة للضوابط الفرعية ضمن الضابط ٢-١٤-٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني الخاصة بالأمن المادي لدى مقدمي الخدمات، بحد أدنى مايلي: ٢-١٣-م-١-١ المراقبة المستمرة لعمليات الدخول والخروج للمباني والمواقع لدى مقدم الخدمة. ٢-١٣-م-١-٢ منع الوصول غير المصرح به للأجهزة التي تتعامل مباشرة مع الأنظمة التقنية السحابية (CTS). ٢-١٣-م-١-٣ التخلص الآمن من أجهزة البنية التحتية (Infrastructure Hardware)، وبالأخص معدات التخزين (Storage Equipments) باتباع أفضل الممارسات والتشريعات ذات العلاقة.
٢-١٤	**حماية تطبيقات الويب (Web Application Security)**
الهدف	ضمان حماية تطبيقات الويب الخارجية لدى مقدمي الخدمات ضد المخاطر السيبرانية.
الضوابط	
٢-١٤-م-١	بالإضافة للضوابط الفرعية ضمن الضابط ٢-١٥-٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني الخاصة بحماية تطبيقات الويب لدى مقدمي الخدمات، بحد أدنى مايلي: ٢-١٤-م-١-١ حماية المعلومات المستخدمة في إجراء المعاملات عن طريق تطبيقات الويب من المخاطر المحتملة، مثل: انقطاع الاتصال (Incomplete Transmission)، التوجيه الخاطئ (Mis-routing)، التعديل غير المصرح به، الاطلاع غير المصرح به.

٢-١٥	إدارة المفاتيح (Key Management)
الهدف	ضمان الإدارة الآمنة لمفاتيح التشفير، لحماية السرية والسلامة والتوافر للأصول المعلوماتية والتقنية، لدى مقدمي الخدمات والمشتركين.
الضوابط	
٢-١٥-م-١	يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني، الخاصة بعملية إدارة المفاتيح لدى مقدمي الخدمات.
٢-١٥-م-٢	يجب تطبيق متطلبات الأمن السيبراني، الخاصة بعملية إدارة المفاتيح لدى مقدمي الخدمات.
٢-١٥-م-٣	بالإضافة للضابط ٢-٨-٣-٢ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني الخاصة بعملية إدارة المفاتيح لدى مقدمي الخدمات بحد أدنى ما يلي: ٢-١٥-م-٣-١ تحديد ملاك لمفاتيح التشفير (Key Owner). ٢-١٥-م-٣-٢ وجود آلية آمنة لاسترجاع مفاتيح التشفير في حال فقدانها مثل: (نسخها احتياطيًا وتخزينها بطرق آمنة خارج الأنظمة السحابية). ٢-١٥-م-٣-٣ تفعيل سجلات الأحداث المتعلقة بمفاتيح التشفير، ومراقبتها.
٢-١٥-م-٤	يجب مراجعة متطلبات الأمن السيبراني، الخاصة بإدارة المفاتيح لدى مقدمي الخدمات، ومراجعة تطبيقها دوريًا.
٢-١٥-ش-١	يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني، الخاصة بإدارة المفاتيح لدى المشتركين.
٢-١٥-ش-٢	يجب تطبيق متطلبات الأمن السيبراني، الخاصة بإدارة المفاتيح لدى المشتركين.
٢-١٥-ش-٣	بالإضافة للضابط ٢-٨-٣-٢ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني، الخاصة بعملية إدارة المفاتيح لدى المشتركين، بحد أدنى ما يلي: ٢-١٥-ش-٣-١ تحديد ملاك لمفاتيح التشفير (Key Owner). ٢-١٥-ش-٣-٢ وجود آلية آمنة لاسترجاع مفاتيح التشفير في حال فقدانها مثل: (نسخها احتياطيًا وتخزينها بطرق آمنة خارج الأنظمة السحابية).
٢-١٥-ش-٤	يجب مراجعة متطلبات الأمن السيبراني الخاصة بإدارة المفاتيح لدى المشتركين، ومراجعة تطبيقها، دوريًا.
٢-١٦	أمن تطوير الأنظمة (System Development Security)
الهدف	ضمان تطوير الأنظمة لدى مقدم الخدمة، وتكاملها، ونشرها بطريقة آمنة.
الضوابط	
٢-١٦-م-١	يجب تحديد متطلبات الأمن السيبراني لتطوير الأنظمة لدى مقدمي الخدمات، وتوثيقها واعتمادها.
٢-١٦-م-٢	يجب تطبيق متطلبات الأمن السيبراني لتطوير الأنظمة لدى مقدمي الخدمات.

٢-١٦-م-٣	يجب أن تغطي متطلبات الأمن السيبراني لتطوير الأنظمة لدى مقدمي الخدمات بحد أدنى الضوابط التالية خلال دورة حياة التطوير: ٢-١٦-م-٣-١ أخذ متطلبات الأمن السيبراني (للأنظمة التقنية السحابية (CTS)، والأنظمة ذات العلاقة) بالاعتبار عند تصميم وتطوير خدمات الحوسبة السحابية. ٢-١٦-م-٣-٢ حماية بيئات التطوير (Development Environments) والاختبار (Testing Environments) وماتحويه من بيانات، ومنصات التكامل (Integration Platforms).
٢-١٦-م-٤	يجب مراجعة متطلبات الأمن السيبراني لتطوير الأنظمة لدى مقدمي الخدمات، ومراجعة تطبيقها، دوريًا.
٢-١٧	**أمن وسائط التخزين (Storage Media Security)**
الهدف	ضمان التعامل الآمن مع المعلومات والبيانات عبر الوسائط المادية، لدى مقدم الخدمة.
الضوابط	
٢-١٧-م-١	يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني لاستخدام وسائط المعلومات والبيانات المادية لدى مقدمي الخدمات.
٢-١٧-م-٢	يجب تطبيق متطلبات الأمن السيبراني لاستخدام وسائط المعلومات والبيانات المادية لدى مقدمي الخدمات.
٢-١٧-م-٣	متطلبات الأمن السيبراني لاستخدام وسائط المعلومات والبيانات المادية لدى مقدمي الخدمات يجب أن تغطي بحد أدنى ما يلي: ٢-١٧-م-٣-١ يجب التأكد من عدم احتواء الوسائط على أية بيانات أو معلومات، قبل إعادة استخدام الوسائط أو التخلص منها. ٢-١٧-م-٣-٢ يجب استخدام وسائل آمنة عند التخلص من الوسائط. ٢-١٧-م-٣-٣ الحفاظ على سرية وسلامة البيانات على أجهزة وسائط التخزين الخارجية. ٢-١٧-م-٣-٤ وضع ترميز أو علامة (Labelling) مقروءة على الوسائط توضح تصنيفها ومدى حساسية المعلومات والبيانات التي تحتويها. ٢-١٧-م-٣-٥ الحفظ الآمن لأجهزة وسائط التخزين الخارجية. ٢-١٧-م-٣-٦ التقييد الحازم لاستخدام وسائط التخزين الخارجية على الأنظمة التقنية السحابية (CTS).
٢-١٧-م-٤	يجب مراجعة متطلبات الأمن السيبراني لاستخدام وسائط المعلومات والبيانات المادية لدى مقدمي الخدمات، ومراجعة تطبيقها، دوريًا.

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 مقدمي الخدمات والمشتركين، وضمان معالجة وتقليل الآثار المترتبة على الاضطرابات في الخدمات الإلكترونية الحرجة لمقدمي الخدمات والمشتركين وأنظمة وأجهزة معالجة معلوماتها جراء الكوارث الناتجة عن التهديدات السيبرانية.
الضوابط	
٣-١-م-١	بالإضافة للضوابط الفرعية ضمن الضابط ٣-١-٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني لجوانب صمود الأمن السيبراني في إدارة استمرارية الأعمال لدى مقدمي الخدمات، بحد أدنى مايلي: ٣-١-م-١-١ تطوير وتنفيذ إجراءات التعافي من الكوارث واستمرارية الأعمال بصورة آمنة. ٣-١-م-١-٢ تطوير وتنفيذ إجراءات لضمان صمود واستمرارية أنظمة الأمن السيبراني المخصصة لحماية الأنظمة التقنية السحابية (CTS).
٣-١-ش-١	بالإضافة للضوابط الفرعية ضمن الضابط ٣-١-٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني لجوانب صمود الأمن السيبراني في إدارة استمرارية الأعمال لدى المشتركين، بحد أدنى مايلي: ٣-١-ش-١-١ تطوير وتنفيذ إجراءات التعافي من الكوارث واستمرارية الأعمال، المتعلقة بالحوسبة السحابية، بصورة آمنة.

٤ الأمن السيبراني المتعلق بالأطراف الخارجية
Third-Party Cybersecurity

٤-١	الأمن المتعلق بسلسلة الإمداد والأطراف الخارجية (Supply Chain and Third-Party Cybersecurity)
الهدف	ضمان حماية أصول مقدمي الخدمات والمشتركين من مخاطر الأمن السيبراني المتعلقة بالأطراف الخارجية (بما في ذلك خدمات الإسناد "Outsourcing" والخدمات المُدارة "Managed Services") وفقًا للسياسات والإجراءات التنظيمية لديهم والمتطلبات التنظيمية والتشريعية ذات العلاقة.
الضوابط	
٤-١-م-١	بالإضافة إلى تطبيق الضابطين ٤-١-٢ و ٤-١-٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني المتعلق بالأطراف الخارجية لدى مقدمي الخدمات، بحد أدنى مايلي: ٤-١-م-١-١ ضمان تنفيذ مقدم الخدمة لطلبات الهيئة الوطنية للأمن السيبراني الخاصة بإزالة البرمجيات أو الخدمات المقدمة من أطراف خارجية التي قد تعتبر تهديدًا على الأمن السيبراني للجهات الوطنية، من السوق (Marketplace) المقدم للمشتركين. ٤-١-م-١-٢ طلب تقديم التوثيق (Documentation) اللازم، فيما يخص الأمن السيبراني، لأي معدات أو خدمات مقدمة من الموردين ومقدمي الخدمات من الأطراف الخارجية. ٤-١-م-١-٣ الزام الأطراف الخارجية بالمتطلبات التنظيمية، والتشريعية ذات الصلة بنطاق عملهم. ٤-١-م-١-٤ يجب على الطرف الخارجي إدارة مخاطر الأمن السيبراني الخاصة به.

١١. الملاحق

الملحق (أ): مستويات ضوابط الأمن السيبراني للحوسبة السحابية

تنقسم ضوابط الأمن السيبراني للحوسبة السحابية إلى أربع مستويات - تدرجًا من الأعلى (الأكثر تقييدًا) إلى الأقل -:

- المستوى ١: مستوى تصنيف يستخدم للبيانات المصنفة (سري للغاية) بحسب ما يصدر من الجهة المختصة.
- المستوى ٢: مستوى تصنيف يستخدم للبيانات المصنفة (سري) بحسب ما يصدر من الجهة المختصة.
- المستوى ٣: مستوى تصنيف يستخدم للبيانات المصنفة (مقيد) بحسب ما يصدر من الجهة المختصة.
- المستوى ٤: مستوى تصنيف يستخدم للبيانات المصنفة (عام) بحسب ما يصدر من الجهة المختصة.

تجدر الإشارة إلى أنه يتم اعتماد المستوى الأعلى من التصنيف عندما يتضمن محتوى مجموعة متكاملة من البيانات مستويات مختلفة.

ضوابط مقدم الخدمة:

يوضح الجدول (٢) أدناه التزام مقدم الخدمة بضوابط الأمن السيبراني للحوسبة السحابية (المذكورة في القسم رقم ١٠ "ضوابط الأمن السيبراني للحوسبة السحابية» من هذه الوثيقة" بحسب المستويات.

جدول ٢. التزام مقدم الخدمة بضوابط الأمن السيبراني للحوسبة السحابية

✣ اختياري (يوصى بتطبيقه) ✔ يجب تطبيقه

رمز المكون الفرعي أو الضابط	المستوى ١	المستوى ٢	المستوى ٣	المستوى ٤
الضوابط الأساسية للأمن السيبراني	✔	✔	✔	✔
١-١-م-١	✔	✔	✔	✔
١-٢-م-١	✔	✔	✔	✔
١-٣-م-١	✔	✔	✔	✣
١-٤-م-١	✔	✔	✔	✣
١-٤-م-٢	✔	✔	✔	✣
١-٥-م	✔	✔	✔	✔
٢-١-م-١	✔	✔	✔	✔
٢-٢-م-١	✔	✔	✔	✔[١]
٢-٣-م-١	✔	✔	✔[٢]	✔[٣]
٢-٤-م-١	✔	✔	✔	✔
٢-٥-م-١	✔	✔	✔	✔[٤]
٢-٦-م-١	✔	✔	✔	✔
٢-٧-م-١	✔	✔	✔	✔[٥]
٢-٨-م-١	✔	✔	✔	✔
٢-٩-م-١	✔	✔	✔	✔
٢-١٠-م-١	✔	✔	✔	✔
٢-١١-م-١	✔	✔	✔	✣
٢-١٢-م-١	✔	✔	✔	✔[٦]
٢-١٣-م-١	✔	✔	✔	✔
٢-١٤-م-١	✔	✔	✔	✔

[١] يستثنى من ذلك الضابط الفرعي ٢-٢-م-١-٩، والضابط الفرعي ٢-٢-م-١-١٠ حيث يعتبران اختياريين

[٢] يستثنى من ذلك الضابط الفرعي ٢-٣-م-١-١١ حيث يعتبر اختياريًا

[٣] يستثنى من ذلك الضابط الفرعي ٢-٣-م-١-٤، والضابط الفرعي ٢-٣-م-١-١١ حيث يعتبران اختياريان، وكذلك الضابط الفرعي ٢-٣-م-١-٩ حيث لا ينطبق.

[٤] يستثنى من ذلك الضابط الفرعي ٢-٥-م-١-٢ حيث يعتبر اختياريًا

[٥] يستثنى من ذلك الضابط الفرعي ٢-٧-م-١-١ حيث يعتبر اختياريًا

[٦] يستثنى من ذلك الضابط الفرعي ٢-١٢-م-١-٢، والضابط الفرعي ٢-١٢-م-١-٣، والضابط الفرعي ٢-١٢-م-١-٨ حيث تعتبر اختيارية

رمز المكون الفرعي أو الضابط	المستوى ١	المستوى ٢	المستوى ٣	المستوى ٤
٢-١٥-م	✔	✔	✔	✔[٧]
٢-١٦-م	✔	✔	✔	✔
٢-١٧-م	✔	✔	✔	✔
٣-١-م-١	✔	✔	✔	✔
٤-١-م-١	✔	✔	✔	✔[٨]

ضوابط المشترك:

يوضح الجدول (٣) أدناه التزام المشترك بضوابط الأمن السيبراني للحوسبة السحابية (المذكورة في القسم رقم ١٠ «ضوابط الأمن السيبراني للحوسبة السحابية» من هذه الوثيقة) بحسب المستويات.

جدول ٣. التزام المشترك بضوابط الأمن السيبراني للحوسبة السحابية

✤ اختياري (يوصى بتطبيقه)　　✔ يجب تطبيقه

رمز المكون الفرعي أو الضابط	المستوى ١	المستوى ٢	المستوى ٣	المستوى ٤
١-١-ش-١	✔	✔	✔	✔
١-٢-ش-١	✔	✔	✔	✔
١-٣-ش-١	✔	✔	✔	✔
١-٤-ش-١	✔	✔	✔	✤
٢-١-ش-١	✔	✔	✔	✔
٢-٢-ش-١	✔	✔	✔	✔
٢-٣-ش-١	✔	✔	✔	✔[٩]
٢-٤-ش-١	✔	✔	✔	✔
٢-٥-ش-١	✔	✔	✔	✤
٢-٦-ش-١	✔	✔	✔	✤
٢-٧-ش-١	✔	✔	✔	✔[١٠]
٢-٩-ش-١	✔	✔	✔	✔
٢-١١-ش-١	✔	✔	✔	✤
٢-١٥-ش	✔	✔	✔	✔
٣-١-ش-١	✔	✔	✔	✔

[٧] يستثنى من ذلك الضابط الفرعي ٢-١٥-م-٣-١ حيث يعتبر اختياريًا

[٨] يستثنى من ذلك الضابط الفرعي ٤-١-م-١-١ حيث يعتبر اختياريًا

[٩] يستثنى من ذلك الضابط الفرعي ٢-٣-ش-١-١ فهو لا ينطبق

[١٠] يستثنى من ذلك الضابط الفرعي ٢-٧-ش-١-١ حيث يعتبر اختياريًا

الملحق (ب): مصطلحات وتعريفات

يوضح الجدول (٤) أدناه بعض المصطلحات وتعريفاتها التي ورد ذكرها في هذه الضوابط.

جدول ٤. مصطلحات وتعريفات

المصطلح	التعريف
الأصل Asset	أي شيء ملموس أو غير ملموس له قيمة بالنسبة لمقدمي الخدمات والمشتركين. وهناك أنواع كثيرة من الأصول؛ بعض هذه الأصول تتضمن أشياء واضحة مثل: الأشخاص، والآلات، والمرافق، وبـراءات الاخـتراع، والبرمجيات والخدمات. ويمكن أن يشمل المصطلح أيضًا أشياء أقل وضوحًا، مثل: المعلومات والخصائص (مثل سمعة مقدمي الخدمات والمشتركين، وصورتهم 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، وغالبًا ما يكون هذا الأمر شرطًا أساسيًّا 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 وفقًا لما حدد مسبقًا في حقوق/تراخيص المستخدم.
توافر Availability	ضمان الوصول إلى المعلومات والبيانات والأنظمة والتطبيقات واستخدامها في الوقت المناسب.
النسخ الاحتياطية Backup	الملفات والأجهزة والبيانات والإجراءات المتاحة للاستخدام في حالة الأعطال أو الفقدان، أو إذا حذف الأصل منها أو توقف عن الخدمة.
الدائرة التلفزيونية المغلقة (CCTV)	يستخدم التلفزيون ذو الدائرة المغلقة، والمعروف أيضًا باسم المراقبة بالفيديو، كاميرات الفيديو لإرسال إشارة إلى مكان محدد على مجموعة محدودة من الشاشات. وغالبًا ما يطلق هذا المصطلح على تلك التقنية المستخدمة للمراقبة في المناطق التي قد تحتاج إلى مراقبة حيث يشكل الأمن المادي مطلبًا هامًّا فيها.

المصطلح	التعريف
إدارة التغيير Change Management	هو نظام لإدارة الخدمة حيث يضمن منهجًا نظاميًّا واستباقيًّا باستخدام أساليب وإجـراءات 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 أيضًا على تقليل تأثير الحوادث ذات العلاقة على الخدمة.
التصنيف Classification	تصنيف البيانات التي تقوم الجهات بإعدادها أو جمعها، أو تخزينها أو معالجتها، أو تبادلها؛ لتقديم الخدمات، أو تسيير الأعمال؛ بما في ذلك البيانات الواردة من أشخاص خارج الجهات، أو متبادلة معهم، أو التي تُعَد لمصلحة الجهات أو المتعلقة بالبنية التحتية الحساسة. وتُصنف البيانات المتعلقة بالجهات -تدرجاً من الأعلى إلى الأدنى- وفق المستويات: المستوى ١، المستوى ٢، المستوى ٣، المستوى ٤.
بيانات مصنفة Classified Data	أي بيانات مصنفة على أحد المستويات التالية: المستوى ١، أو المستوى ٢، أو المستوى ٣، أو المستوى ٤.
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 كخدمة "SaaS" Software-as-Service • المنصة كخدمة "PaaS" Platform-as-Service • البنية التحتية كخدمة "IaaS" Infrastructure-as-Service كما إن هناك أربعة نماذج للحوسبة السحابية حسب طبيعة الدخول: الحوسبة السحابية العامة، والحوسبة السحابية المجتمعية، والحوسبة السحابية الخاصة، والحوسبة السحابية الهجين.

المصطلح	التعريف
معيار Cloud Computing Compliance Catalogue (C5)	تم تطوير هذا المعايير من قبل المكتب الألماني الفيدرالي لأمن المعلومات (German Federal Office for Information Security (BSI))، لوضع الحد الأدنى من المتطلبات لحماية الخدمات السحابية لأجل تعزيز العلاقة ما بين مقدم الخدمة والمشترك.
خدمات الحوسبة السحابية Cloud Computing Services	هي تقديم العديد من الخدمات من خلال الإنترنت والتي يمكن الوصول لها من خلال منصات مختلفة (الأجهزة المكتبية، الأجهزة المحمولة، الهواتف المتنقلة .. إلخ). هذه الخدمات تشمل التطبيقات والبنية التحتية مثل الخوادم، وقواعد البيانات والشبكات لدعم الاتصالات، وتحليل البيانات ومعالجتها ومشاركتها وتخزينها.
معيار Cloud Controls Matrix (CCM)	تم تطوير هذا المعيار من قبل تحالف أمن الحوسبة السحابية (Cloud Security Alliance (CSA))، لوضع المبادئ الأمنية الأساسية لدعم المشتركين في عملية تقييم المخاطر الأمنية على الخدمات السحابية المقدمة من قبل مقدم الخدمة.
المشترك Cloud Customer	أي شخص طبيعي أو معنوي (مثل الشركات) يشترك في خدمات الحوسبة السحابية التي يوفرها مقدم الخدمة.
مقدم الخدمة Cloud Service Provider (CSP)	أي شخص طبيعي أو معنوي (مثل الشركات) يقدم خدمات الحوسبة السحابية إلى العموم، سواء بشكل مباشر أو غير مباشر من خلال مراكز بيانات (سواء كانت داخل المملكة أو خارجها) ويديرها بنفسه بشكل كلي أو جزئي.
قاعدة بيانات إدارة الإعدادات Configuration Management DataBase (CMDB)	تم تعريف مفهوم قاعدة بيانات إدارة الإعدادات في الأساس عن طريق معيار عمليات تشغيل مكتبة البنية التحتية لتقنية المعلومات (ITIL)، وهو يشمل استخدام قاعدة البيانات لتخزين سجلات التكوين الخاصة بالأنظمة طوال دورة حياتها.
الأنظمة التقنية السحابية Cloud Technology Stack (CTS)	بنية متعددة الطبقات من التقنيات الرئيسية لتنفيذ خدمات الحوسبة السحابية: (البنية التحتية لمركز البيانات، و الشبكة المحلية، و أجهزة التقارب الفائق للتخزين/الحوسبة، و مراقب الأجهزة الافتراضية، ومنصة الإدارة السحابية، والأجهزة الافتراضية، وأنظمة التشغيل، وبرمجيات التطبيق، ومنصات التشغيل والصيانة، وتقنيات حماية الحوسبة السحابية...إلخ).

المصطلح	التعريف
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 قصد. 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.
المعلومات (أو البيانات) الحساسة Confidential Data/ Information	هي المعلومات (أو البيانات) التي تعتبر غاية في الحساسية والأهمية، حسب تصنيف مقدمي الخدمات والمشتركين، والمعدة للاستخدام من قِبلهم. وإحدى الطرق التي يمكن استخدامها في تصنيف هذا النوع من المعلومات هي 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 مقدمي الخدمات والمشتركين أو المتعاملين معهم أو التأثير في حياة الأشخاص ذوي 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 في الأمن القومي و/أو الدفاع الوطني و/أو اقتصاد الدولة أو مقدراتها الوطنية.

المصطلح	التعريف
التشفير Cryptography	(ويسمى أيضًا علم التشفير) وهو القواعد التي تشمل 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 المتعمد لأنظمة الحاسب الآلي والشبكات ومقدمي الخدمات والمشتركين التي يعتمد عملهم على تقنية المعلومات والاتصالات الرقمية بهدف إحداث أضرار.
المخاطر السيبرانية Cyber Risks	المخاطر التي تمس عمليات أعمال مقدمي الخدمات والمشتركين (بما في ذلك الرؤية الخاصة بهم، أو رسالتهم، أو الإدارة لديهم، أو الصورة، أو السمعة الخاصة بهم) أو الأصول، أو الأفراد، أو الجهات، أو الدولة، بسبب إمكانية الوصول غير المصرح به، أو الاستخدام، أو الإفصاح، أو التعطيل، أو التعديل، أو التدمير للمعلومات و/أو نظم المعلومات.
صمود الأمن 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 (١٤٣٩/٢/١١هـ)، 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 الرقمي، ونحو ذلك.
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 مجرد.
البيانات Data	أي معلومات، أو سجلات، أو إحصاءات، أو وثائق مصورة، أو مسجلة ومخزنة بطريقة إلكترونية.
تصنيف البيانات والمعلومات Data and Information Classification	تعيين مستوى الحساسية للبيانات والمعلومات التي تنتج عنها ضوابط أمنية لكل مستوى من مستويات التصنيف. ويتم تعيين مستويات حساسية البيانات والمعلومات وفقًا لفئات محددة مسبقًا، حيث يتم إنشاء البيانات والمعلومات، أو تعديلها، أو تحسينها، أو تخزينها، أو نقلها. ومستوى التصنيف هو مؤشر على قيمة أو أهمية البيانات والمعلومات للجهة.

المصطلح	التعريف
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 (OS).
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.
الفعالية 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. ويمكن استخدام مؤشرات قياس الأداء Key Performance Indicators (KPIs) لقياس وتقييم مستوى الفاعلية.
حدث Event	شيء يحدث في مكان محدد (مثل الشبكة، والأنظمة، والتطبيقات، وغيرها) وفي وقت محدد.
المعيار الأمريكي الفيدرالي FedRAMP	هو عملية التقييم والتفويض للوكالات الفيدرالية الأمريكية من جانب حكومة الولايات المتحدة، وهي مصممة لضمان تفعيل الأمن عند الوصول إلى منتجات الحوسبة السحابية وخدماتها. ويقوم هذا البرنامج باعتماد مقدمي الخدمات السحابية للتعامل مع البيانات على مستوى واحد من ثلاثة مستويات للأثر: • التصنيف المنخفض في البرنامج - سوف ينتج عن فقد السرية والسلامة والتوافر آثار سلبية محدودة على عمليات الوكالة، أو أصولها، أو أفرادها. • التصنيف المتوسط في البرنامج - سوف ينتج عن فقد السرية والسلامة والتوافر آثار سلبية خطيرة على عمليات الوكالة، أو أصولها، أو أفرادها. • التصنيف المرتفع في البرنامج - نظم إنفاذ القانون وخدمات الطوارئ، والنظم المالية، ونظم الصحة، وغيرها من النظم، حيث قد يتوقع من فقد السرية والسلامة والتوافر آثار سلبية حادة أو كارثية على عمليات الوكالة، أو أصولها، أو أفرادها.
هوية Identification	وسيلة التحقق من هوية المستخدم أو العملية أو الجهاز، وهي عادة شرط أساسي لمنح حق الوصول إلى الموارد في النظام.

المصطلح	التعريف
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: SWIFT، PCI، وغيرها).
معيار ISO/IEC 27000	تم تطوير هذه السلسة من قبل: • المنظمة الدولية للمعايير (International Organizatio for Standardization (ISO)) • اللجنة الكهروتقنية الدولية (International Electrotechnical Commission (IEC)) لتقديم توصيات بناءً على أفضل الممارسات لإعداد نظام لإدارة أمن المعلومات والعمل على تطبيقه ومتابعته والتحسين المستمر له.
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 Labelling	عرض معلومات (بتسمية وترميز محدد وقياسي) توضع على أصول مقدمي الخدمات والمشتركين (مثل: الأجهزة والتطبيقات والمستندات وغيرها) ليستدل بها للإشارة إلى بعض المعلومات المتعلقة بتصنيف الأصل وملكيته ونوعه وغيرها من المعلومات المتعلقة بإدارة الأصول.
المستوى ١ Level 1	مستوى تصنيف يستخدم للبيانات المصنفة (سري للغاية) بحسب ما يصدر من الجهة المختصة.
المستوى ٢ Level 2	مستوى تصنيف يستخدم للبيانات المصنفة (سري) بحسب ما يصدر من الجهة المختصة.

المصطلح	التعريف
المستوى ٣ Level 3	مستوى تصنيف يستخدم للبيانات المصنفة (مقيد) بحسب ما يصدر من الجهة المختصة.
المستوى ٤ Level 4	مستوى تصنيف يستخدم للبيانات المصنفة (عام) بحسب ما يصدر من الجهة المختصة.
التحقق من الهوية متعدد العناصر Multi-Factor Authentication (MFA)	نظام أمني يتحقق من هوية المستخدم، ويتطلب 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 لعمليات الدخول، ويُطلق عليها: "One-Time-Password"). • الملازمة (صفة أو سمة حيوية متعلقة بالمستخدم نفسه فقط «مثل بصمة الإصبع»).
معيار الأمن السحابي في سنغافورة Multi-Tier Cloud Security Standard for Singapore (MTCS SS)	يهدف هذا المعيار إلى إدارة المخاطر المتعلقة بالحوسبة السحابية بشكل آمن. ويتكون من ثلاثة مستويات –المستوى الأول هو المستوى الأساسي، والمستوى الثالث هو الأكثر تقييدًا-: • المستوى الأول: يتعلق بالبيانات والأنظة الغير خاصة بالأعمال، وقد تم وضع ضوابط أساسية للتعامل مع المخاطر والتهديدات على خدمات الحوسبة السحابية التي قد تؤثر بشكل منخفض على البيانات والأنظمة. • المستوى الثاني: يتعلق بتلبية احتياجات الجهات التي تعمل على أنظمة وبيانات حساسة من خلال عدة ضوابط أكثر تقييدًا عن المستوى الأول للتعامل مع المخاطر والتهديدات على خدمات الحوسبة السحابية التي قد تؤثر بشكل متوسط على البيانات والأنظمة. • المستوى الثالث: يتعلق بالجهات المنظمة من خلال إضافة ضوابط أكثر تقييدًا عن المستوى الأول والمستوى الثاني، للتعامل مع المخاطر والتهديدات على خدمات الحوسبة السحابية التي قد تؤثر بشكل كبير على البيانات والأنظمة.

المصطلح	التعريف
العاملون Staff	الأشخاص الذي يعملون لدى مقدمي الخدمة أو المشتركين (بما في ذلك الموظفون الرسميون، والموظفون المؤقتون، والمتعاقدون).
الإسناد الخارجي Outsourcing	الحصول على (السلع أو الخدمات) عن طريق التعاقد مع مورد أو مقدم خدمة.
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.
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، والحدود الأمنية، والأقفال، وأنظمة التحكم في الوصول، والعديد من التقنيات الأخرى.
سياسة Policy	وثيقة تحدد بنودها التزامًا عامًّا أو توجيهًا أو نية كما تم التعبير عن ذلك رسميًّا من قِبَل صاحب الصلاحية للجهة. سياسة الأمن السيبراني هي وثيقة تعبر بنودها عن الالتزام الرسمي للإدارة العليا للجهة بتنفيذ وتحسين برنامج الأمن السيبراني بالجهة، وتشتمل السياسة على الأهداف الخاصة بمقدمي الخدمات والمشتركين فيما يتعلق ببرنامج الأمن السيبراني، وضوابطه، ومتطلباته، وآلية تحسينه وتطويره.
إدارة الصلاحيات الهامة والحساسة Privileged Access Management	عملية إدارة الصلاحيات ذات الخطورة العالية على أنظمة الجهة 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 تحوِّل المدخلات إلى مخرجات. وهذه الأنشطة متأثرة بالسياسات الخاصة بمقدمي الخدمات والمشتركين.

المصطلح	التعريف
مصفوفة توزيع المسؤوليات RACI Matrix	هي مصفوفة يتم فيها توضيح وتحديد أدوار الأعضاء المعنيين بإتمام أي عملية أو مشروع.
الاستعادة Recovery	إجراء أو عملية لاستعادة أو التحكم في شيء منقطع، أو تالف، أو مسروق، أو ضائع، أو التحكم فيه.
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.
أمن تطوير الأنظمة System Development Security	أي تطبيق أو منصة أو برنامج وسيط أو نظام تشغيل أو مراقب أجهزة افتراضية أو مجموعة شبكات أو أي برمجيات أخرى تمثل جزءًا من الأنظمة التقنية السحابية (CTS).
طرف خارجي Third-Party	أي جهة تعمل كطرف في علاقة تعاقدية لتقديم السلع أو الخدمات (وهذا يشمل موردي ومقدمي الخدمات).
تهديد Threat	أي ظرف أو حدث من المحتمل أن يؤثر سلبًا على أعمال مقدمي الخدمات والمشتركين (بما في ذلك مهمتهم، أو وظائفهم، أو مصداقيتهم، أو سمعتهم) أو الأصول الخاصة بهم، أو المنسوبين لديهم، مستغلًا أحد أنظمة المعلومات عن طريق الوصول غير المصرح به إلى المعلومات، أو تدميرها، أو كشفها، أو تغييرها، أو حجب الخدمة. وأيضًا قدرة مصدر التهديد على النجاح في استغلال إحدى نقاط الضعف الخاصة بنظام معلومات معين، وهذا التعريف يشمل التهديدات السيبرانية.
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.

الملحق (ج): قائمة الاختصارات

يوضح الجدول (٥) أدناه معنى الاختصارات التي ورد ذكرها في هذه الضوابط.

جدول ٥. قائمة الاختصارات

الاختصار	معناه
BCM	Business Continuity Management إدارة استمرارية الأعمال
CCC	Cloud Cybersecurity Controls ضوابط الأمن السيبراني للحوسبة السحابية
CCTV	Closed-Circuit Television الدائرة التلفزيونية المغلقة
CMDB	Configuration Management DataBase قاعدة بيانات إدارة الإعدادات
CNI	Critical National Infrastructure البنية التحتية الحساسة
CSP	Cloud Service Provider مقدم الخدمة
CST	Cloud Service Tenant المشترك
CTS	Cloud Technology Stack الأنظمة التقنية السحابية
DDoS	Distributed Denial of Service هجمات تعطيل الخدمات الموزعة
ECC	Essential Cybersecurity Controls الضوابط الأساسية للأمن السيبراني
IaaS	البنية التحتية كخدمة Infrastructure as a Service

الاختصار	معناه
MFA	Multi-Factor Authentication التحقق من الهوية متعدد العناصر
PaaS	المنصة كخدمة Platform as a Service
SAN	الشبكة الخاصة بالتخزين Storage Area Netwoek
SaaS	البرمجيات كخدمة Software as a Service
SIEM	Security Information and Event Management نظام سجلات الأحداث ومراقبة الأمن السيبراني

الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority