الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

ضوابط الأمن السيبراني للحوسبة السحابية

Cloud Cybersecurity Controls

(CCC - 1 : 2020)

مسودة

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 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

جدول المحتويات

١. الملخص التنفيذي

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

كما جاءت ملبية لجوانب التحديث ومتابعة الالتزام من قبل الجهات 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 بشكل سريع جدًا مع المستجدات العصرية والثورة الصناعية الرابعة وذلك بالاعتماد على القدرات الهائلة والفائقة لمقدمي الخدمة لتقديم خدمات سريعة وقليلة التكلفة وتوفير نسخ احتياطية لا تتأثر بأي عوامل خارجية، وذلك للأفراد والجهات على حد سواء ومن تلك الخدمات التخزين وقواعد البيانات والبرمجيات عبر شبكة الإنترنت؛ مما يجعل الحاجة قائمة وملحة لوجود ضوابط للأمن السيبراني للتعامل مع خدمات الحوسبة لتكون امتدادًا للضوابط الأساسية للأمن السيبراني (ECC – 1: 2018) وأهم الممارسات الدولية في هذا المجال.

تهدف ضوابط الأمن السيبراني للحوسبة السحابية (CCC – 1 : 2020) إلى تقليل المخاطر السيبرانية على المشتركين ومقدمي الخدمات.

كما توضح هذه الوثيقة تفاصيل اشتراطات وضوابط الأمن السيبراني للحوسبة السحابية، وأهدافها، ونطاق العمل، وقابلية التطبيق، وآلية الالتزام بها.

وعلى مقدمي الخدمات و المشتركين تنفيذ ما يحقق الالتزام الدائم والمستمر بهذه الاشتراطات والضوابط، تحقيقاً لما ورد في الفقرة الثالثة من المادة العاشرة في تنظيم الهيئة الوطنية للأمن السيبراني وكذلك ما ورد في الأمر السامي الكريم رقم ٥٧٢٣١ وتاريخ 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 للأمن السيبراني قامت بإعدادها سابقًا عدة منظمات وجهات محلية ودولية، والاطلاع على أفضل الممارسات والتجارب في مجال الأمن السيبراني. وقد تم عمل دراسة مواءمة مع ضوابط منظمات دولية مثل المعيار الأمريكي الفيدرالي (FedRAMP)، معيار الأمن السحابي في سنغافورة (MTCS)، معيار الحكومة الألمانية (C5) ، معيار Cloud Controls Matrix (CCM)، ومعايير (ISO/IEC 27000)، حيث تم توضيح هذه المواءمة في وثيقة خاصة ملحقة بضوابط الأمن السيبراني للحوسبة السحابية للتسهيل على شركات مقدمي الخدمات الوطنية والدولية المواءمة والالتزام. وتتألف ضوابط الأمن السيبراني للحوسبة السحابية من المكونات التالية:

لمقدمي الخدمات	للمشتركين
٤ مكونات أساسية (4 Main Domains)	
٢٦ مكونًا فرعيًا (26 Subdomains)	
٤٦ ضابطًا أساسيًا (46 Main Controls)	٣٣ ضابطًا أساسيًا (33 Main Controls)
١٨٩ ضابطًا فرعيًّا (189 Subcontrols)	٤٧ ضابطًا فرعيًّا (47 Subcontrols)

شكل ١: مكونات ضوابط الأمن السيبراني للحوسبة السحابية

٣. الأهداف

امتدادًا للضوابط الأساسية للأمن السيبراني؛ تهدف هذه الوثيقة إلى تحديد متطلبات الأمن السيبراني للحوسبة السحابية من منظور مقدمي الخدمات و المشتركين. كما تهدف إلى تمكينهم من تحديد المتطلبات الأمنية لخدمات الحوسبة السحابية والعمل على تحقيقها بما يتناسب مع المتطلبات التشريعية، والتنظيمية الوطنية والدولية، ذات العلاقة، لتلبية الاحتياجات الحالية الأمنية ورفع جاهزيتها حيال المخاطر السيبرانية على كافة خدمات الحوسبة السحابية.

تم تطوير هذه الوثيقة المتضمنة اشتراطات وضوابط الأمن السيبراني للحوسبة السحابية (CCC – 1 : 2020) لتكون امتدادًا للضوابط الأساسية ومكملة لها، بهدف تحقيق مستويات أعلى من أهداف الأمن السيبراني الوطنية من خلال التركيز على خدمات الحوسبة السحابية من منظور مقدمي الخدمات و المشتركين.

يتطلب الأمن السيبراني لخدمات الحوسبة السحابية (لكل من المشتركين ومقدمي الخدمات) التركيز على ثلاثة مبادئ أساسية للأمن السيبراني الخاصة بالبيانات والمعلومات المستخدمة من قِبل مقدمي الخدمات والمشتركين، وهي:

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

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

- الأشخاص
- الإجراء
- التقنية
- الإستراتيجية، وهي ليست مخصصة فقط للحوسبة السحابية، وقد تم ذكرها في الضوابط الأساسية للأمن السيبراني.

٤. نطاق العمل وقابلية التطبيق

نطاق عمل ضوابط الأمن السيبراني للحوسبة السحابية

تسري اشتراطات الأمن السيبراني وضوابط الأمن السيبراني للحوسبة السحابية على مقدمي الخدمات والمشتركين.

المشتركون ضمن نطاق العمل يشملون أي جهة (حسب التعريف المذكور في الملحق (أ)) تستخدم حاليًا أو تخطط لاستخدام أي من خدمات الحوسبة السحابية من أحد مقدمي الخدمات

مقدمي الخدمات ضمن نطاق العمل يشملون أي مقدم خدمة داخل أو خارج المملكة يقدم خدمات الحوسبة السحابية إلى المشتركين ضمن نطاق العمل.

كما تشجع الهيئة مقدمي الخدمات في المملكة وبشدة على الاستفادة من هذه الضوابط لتطبيق أفضل الممارسات فيما يتعلق بتحسين الأمن السيبراني وتطويره.

أمثلة لمقدمي خدمات الحوسبة السحابية خارج نطاق العمل:

- مقدمي الخدمات الذين يقدمون خدمات حوسبة سحابية لجهات غير سعودية خارج المملكة.
- مقدمي الخدمات الذين يقدمون خدمات حوسبة سحابية للأفراد، والمنشآت الصغيرة والمتوسطة، وجهات القطاع الخاص التي لا تمتلك بنى تحتية وطنية حساسة أو تقوم بتشغيلها أو استضافتها.

٥. التنفيذ والالتزام

تحقيقاً لما ورد في الفقرة الثالثة من المادة العاشرة في تنظيم الهيئة وكذلك ما ورد في الأمر السامي الكريم رقم ٥٧٢٣١ وتاريخ ١٤٣٩/١١/١٠ هـ يجب على مقدمي الخدمات و المشتركين ضمن نطاق عمل هذه الضوابط تنفيذ ما يحقق الالتزام الدائم والمستمر بهذه الضوابط والاشتراطات.

لا يمكن للمشتركين ومقدمي الخدمات تحقيق الالتزام المستمر بضوابط واشتراطات الأمن السيبراني للحوسبة السحابية إلا من خلال تحقيق الالتزام المستمر بالضوابط الأساسية للأمن السيبراني في المقام الأول، كما أنها مرتبطة مع المتطلبات التشريعية، والتنظيمية الوطنية والدولية ذات العلاقة.

تقوم الهيئة بتقييم التزام مقدمي الخدمات و المشتركين بما ورد في هذه الوثيقة بطرق متعددة، منها: التقييم الذاتي لمقدمي الخدمات والمشتركين و/أو الزيارات الميدانية للتدقيق من قبل الهيئة أو من تنيبه، وفق الآلية التي تراها الهيئة مناسبة لذلك.

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.

٧. التحديث والمراجعة

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

٨. اشتراطات الأمن السيبراني للحوسبة السحابية

تنقسم اشتراطات الأمن السيبراني للحوسبة السحابية إلى أربع مستويات - تدرجًا من 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، والمستوى ٣ هو المستوى الأدنى لاستضافة الأنظمة الحساسة وما تحويه من بيانات.
- **المستوى ٤:** مستوى تصنيف يستخدم للبيانات المصنفة (متاح) بحسب ما يصدر من الجهة المختصة.

١.٨ يلتزم مقدم الخدمة بتحقيق الالتزام الدائم والمستمر باشتراطات الأمن السيبراني للحوسبة السحابية المذكورة أدناه، وبضوابط الأمن السيبراني للحوسبة السحابية (المذكورة في القسم رقم ١١ «ضوابط الأمن السيبراني للحوسبة السحابية» من هذه الوثيقة) حسب المستويات كما هو موضح في الجدول (١).

جدول ١: التزام مقدم الخدمة بضوابط الأمن السيبراني للحوسبة السحابية

رمز المكون الفرعي أو الضابط	المستوى ٤	المستوى ٣	المستوى ٢	المستوى ١
١-١-م-١	✓	✓	✓	✓
١-٢-م-١	✓	✓	✓	✓
١-٣-م-١	✣	✓	✓	✓
١-٤-م-١	✓	✓	✓	✓
١-٤-م-٢	✓	✓	✓	✓
١-٥-م-١	✣	✓	✓	✓
١-٥-م-٢	✣	✓	✓	✓
١-٦-م	✓	✓	✓	✓
٢-١-م-١	✓	✓	✓	✓
٢-٢-م	✓	✓	✓	✓

٢-٣-م-١	✣	✔	✔	✔
٢-٤-م	✔	✔	✔	✔
٢-٥-م-١	✔	✔	✔	✔
٢-٦-م-١	✔	✔	✔	✔
٢-٧-م-١	✔ [1]	✔	✔	✔
٢-٨-م-١	✔	✔	✔	✔
٢-٩-م-١	✔	✔	✔	✔
٢-١٠-م-١	✔	✔	✔	✔
٢-١١-م	✔	✔	✔	✔
٢-١٢-م-١	✔	✔	✔	✔
٢-١٣-م-١	✔	✔	✔	✔
٢-١٤-م-١	✔	✔	✔	✔
٢-١٥-م	✔	✔	✔	✔
٢-١٦-م-١	✔	✔	✔	✔
٢-١٧-م	✔	✔	✔	✔
٢-١٨-م-١	✔	✔	✔	✔
٣-١-م-١	✔	✔	✔	✔
٤-١-م-١	✔	✔	✔	✔

✔ يجب تطبيقه
✣ اختياري (يُنصح بتطبيقه)

[1] يستثنى من ذلك الضابطين الفرعيين ٢-٧-م-١-١٥ و ٢-٧-م-١-١٦ حيث يعتبران اختياريان

٢.٨ يلتزم المشترك بتحقيق الالتزام الدائم والمستمر باشتراطات الأمن السيبراني للحوسبة السحابية المذكورة أدناه، وبضوابط الأمن السيبراني للحوسبة السحابية (المذكورة في القسم رقم ١١ «ضوابط الأمن السيبراني للحوسبة السحابية» من هذه الوثيقة) حسب تصنيف البيانات كما هو موضح في الجدول (٢).

جدول ٢: التزامات المشترك بضوابط الأمن السيبراني للحوسبة السحابية

رمز المكون الفرعي أو الضابط	المستوى ٤	المستوى ٣	المستوى ٢	المستوى ١
١-٢-ش-١	✔	✔	✔	✔
١-٣-ش-١	✔	✔	✔	✔
١-٤-ش-١	✔	✔	✔	✔
١-٥-ش-١	✣	✔	✔	✔
١-٦-ش	✔	✔	✔	✔
٢-٢-ش	✔	✔	✔	✔
٢-٥-ش-١	✣	✔	✔	✔
٢-٦-ش-١	✣	✔	✔	✔
٢-٧-ش-١	✔	✔	✔	✔
٢-٨-ش-١	✔	✔	✔	✔
٢-١٣-ش-١	✣	✔	✔	✔
٢-١٥-ش	✔	✔	✔	✔
٢-١٦-ش-١	✔	✔	✔	✔
٢-١٧-ش	✔	✔	✔	✔
٣-١-ش-١	✔	✔	✔	✔
٤-١-ش-١	✔	✔	✔	✔

✔ يجب تطبيقه

✣ اختياري (يُنصح بتطبيقه)

٣.٨ اشتراطات الأمن السيبراني للمستوى ٤:

١.٣.٨ يجب على المشترك، الالتزام بالاشتراطات الآتية:

١.١.٣.٨ يجب التقيد بما يصدر من مكتب إدارة البيانات الوطنية أو الأنظمة ذات العلاقة بخصوص تصنيف البيانات، وفي حال وجود استفسار يتم الرجوع إلى المكتب.

٢.١.٣.٨ أن يقتصر التعاقد مع مقدم خدمة مرخص له.

٣.١.٣.٨ أن تحكم الأنظمة واللوائح والأطر التنظيمية والقرارات الصادرة في المملكة جميع الخدمات السحابية المقدمة للمشترك.

٤.١.٣.٨ التحقق من أن مقدم الخدمة متقيد بكل الضوابط، والإرشادات، والأطر، واللوائح الخاصة بالأمن السيبراني في المستوى ٤.

٢.٣.٨ يجب على مقدم الخدمة، الالتزام بالاشتراطات الآتية:

١.٢.٣.٨ مراعاة جميع الأنظمة واللوائح والأطر والضوابط التنظيمية المعمول بها والمتعلقة بالأمن السيبراني في المملكة.

٢.٢.٣.٨ استخدام البنية التحتية للاتصالات؛ بما فيها الاتصالات الدولية، من خلال المشغلين المرخصين في المملكة؛ وذلك إلى الحد المطلوب بموجب أنظمة المملكة.

٣.٢.٣.٨ فيما يتعلق بالإجراءات المتخذة من قبل مقدم الخدمة أو نيابة عنه في المملكة:

١.٣.٢.٣.٨ عدم نسخ أي بيانات خاصة بالمشترك أو الاحتفاظ بها، إلا في حال موافقة المشترك (مالك البيانات)، أو بناء على طلب نظامي من السلطات المعنية في المملكة.

٢.٣.٢.٣.٨ عدم الالتزام بأي قوانين أخرى غير قوانين المملكة؛ قد يؤدي الالتزام بها إلى مخالفة للمتطلبات المحددة في هذه الوثيقة أو أي تعديل لاحق لها. فيما يتعلق بالإجراءات المتخذة من قبل مقدم الخدمة أو من ينوب عنه خارج المملكة والتي من شأنها أن تؤدي إلى الوصول إلى بيانات داخل المملكة، لا يجوز لمقدم الخدمة أن ينتهك أي أنظمة أو لوائح أو أطر أو ضوابط تتعلق بالأمن السيبراني معمول بها في المملكة إلا إذا ألزم قانوناً بذلك، وفي هذه الحال، بعد أن يبذل جميع الجهود المعقولة لمعارضة هذا الإلزام. فإنه يجب إشعار الجهات المعنية في المملكة - ودون تأخير غير مبرر وإلى أقصى حد يسمح به القانون- بأي تعارض مع تلك الأنظمة واللوائح.

٤.٢.٣.٨ أن يقدم ما يأتي إلى الهيئة:

١.٤.٢.٣.٨ الإفصاح (عن طريق تقديم تقرير تفصيلي مرة واحدة في السنة على الأقل) عن التقنيات والميزات وضوابط التحكم ووسائل التخفيف المتاحة المتعلقة بقدرة مقدم

الخدمة على الوصول إلى أي بيانات تم تخزينها أو معالجتها أو نقلها في المملكة أو عبرها، أو فك تشفير تلك البيانات أو مساعدة طرف ثالث أو السماح له بالوصول إلى تلك البيانات أو فك تشفيرها.

٢.٤.٢.٣.٨ القيام دون تأخير غير مبرر، بتحديث تلك التقارير المشار إليها في الفقرة السابقة، بعد أي تغيير جوهري سلبي لأمن البيانات الحكومية السعودية المخزنة أو المعالجة أو المنقولة في المملكة أو من خلالها، وذلك نتيجة لتغييرات أو تحديثات لقدرة مقدم الخدمة الموضحة في هذه الفقرة.

٥.٢.٣.٨ تقديم خدمات الحوسبة السحابية من داخل المملكة، وتشمل جميع الأنظمة المستخدمة بما في ذلك أنظمة التخزين، والمعالجة، والمراقبة، والدعم، ومراكز التعافي من الكوارث.

٦.٢.٣.٨ أن تحكم الأنظمة واللوائح والأطر التنظيمية والقرارات الصادرة في المملكة جميع الخدمات السحابية المقدمة للجهات في المملكة.

٧.٢.٣.٨ التقيد بكل الضوابط، والإرشادات، والأطر، واللوائح الخاصة بالأمن السيبراني في المستوى ٤.

٤.٨ اشتراطات الأمن السيبراني للمستوى ٣:

يجب على المشترك و مقدم الخدمة، الالتزام بالاشتراطات الخاصة بالأمن السيبراني في المستوى ٤ المذكورة في الفقرة ٣.٨، ويستثنى من ذلك الفقرة (٢.٣.٢.٣.٨)، بالإضافة الى الاشتراطات الآتية:

١.٤.٨ يجب على المشترك، التحقق من أن مقدم الخدمة متقيد بكل الضوابط، والإرشادات، والأطر، واللوائح الخاصة بالأمن السيبراني في المستوى ٣.

٢.٤.٨ يجب على مقدم الخدمة، الالتزام بالاشتراطات الآتية:

١.٢.٤.٨ فيما يتعلق بمراكز البيانات التابعة لمقدم الخدمة داخل المملكة؛ يلتزم مقدم الخدمة بتقديم خطة زمنية معقولة متفق عليها تبين إحلال جميع الوظائف الفنية والتشغيلية الهامة داخل تلك المراكز - بما في ذلك وظائف الأمن السيبراني - بمواطنين سعوديين مؤهلين.

٢.٢.٤.٨ تزويد الجهات المختصة بالوصف العام والموقع والسمات الرئيسية للربط الشبكي، سواء كانت سلكية أو لاسلكية، بين البنية التحتية للاتصالات والنظام البيئي السحابي[٢] الخاص بمقدم الخدمة داخل المملكة.

٣.٢.٤.٨ العمل مع الجهات المختصة في المملكة، لتطوير الحل التقني؛ للتحقق من أن أي طرف ثالث، من مقدمي الخدمات، في النظام البيئي السحابي لمقدم الخدمة، سوف يمتثل لجميع الاشتراطات والضوابط المذكورة في هذه الوثيقة. وأن يعمل مع السلطات السعودية المختصة على تطوير حل تقني يسمح لها بإدراج الموردين ممن يرغبون في تقديم خدماتهم إلى جهات حكومية سعودية في قائمة بيضاء ضمن ذلك النظام البيئي.

[٢] Cloud Ecosystem

٤.٢.٤.٨ فيما يتعلق بالإجراءات المتخذة من قبل مقدم الخدمة أو من ينوب عنه في المملكة.

١.٤.٢.٤.٨ عدم تطبيق أي قوانين أو لوائح أو طلبات قد تتعارض مع القوانين أو المتطلبات الأمنية المعمول بها في المملكة، ويلتزم مقدم الخدمة في هذا الشأن بأن يستخدم جميع الإمكانيات القانونية المتوفرة لديه؛ لإشعار الجهات المختصة في المملكة بأي تعارض قد يظهر.

٢.٤.٢.٤.٨ أن يفصح (بموجب وثيقة مفصلة خاصة بذلك) عن أي إمكانيات تتوفر لديه للاطلاع على أي بيانات مخزنة لديه في المملكة أو تم معالجتها أو نقلها في المملكة أو عبرها، أو لفك شفرة تلك البيانات، أو لمساعدته أي طرف ثالث أو سماحه له بالاطلاع على تلك البيانات أو فك شفرتها. وعدم تنفيذ أي إمكانيات جديدة في هذا الصدد دون موافقة خطية صريحة ومسبقة من الهيئة.

٥.٢.٤.٨ التقيد بكل الضوابط، والإرشادات، والأطر، واللوائح الخاصة بالأمن السيبراني في المستوى ٣.

٥.٨ اشتراطات الأمن السيبراني للمستوى ٢ والمستوى ١:

يجب على مقدم الخدمة و المشترك، الالتزام بالاشتراطات الخاصة بالأمن السيبراني في المستوى ٣ المذكورة في الفقرة ٤.٨ ؛ بالإضافة الى الاشتراطات الآتية:

١.٥.٨ يجب على المشترك، الالتزام بالاشتراطات الآتية:

١.١.٥.٨ التحقق من مقدم الخدمة بقيامه بعزل السحابة المخصصة لهذا المستوى عن أي مستوى أقل منه.
٢.١.٥.٨ التحقق من أن مقدم الخدمة متقيد بكل الضوابط، والإرشادات، والأطر، واللوائح الخاصة بالأمن السيبراني في المستوى ٢ والمستوى ١.

٢.٥.٨ يجب على مقدم الخدمة، الالتزام بالاشتراطات الآتية:

١.٢.٥.٨ عزل السحابة المخصصة لهذا المستوى عن أي مستوى أقل منه.

٢.٢.٥.٨ يجب التأكد من أن الأطراف الخارجية تطبق جميع الاشتراطات والضوابط القابلة للتطبيق عليها.

٣.٢.٥.٨ التقيد بكل الضوابط، والإرشادات، والأطر، واللوائح الخاصة بالأمن السيبراني في المستوى ٢ والمستوى ١.

٩. هيكلية المكونات الفرعية لضوابط الأمن السيبراني للحوسبة السحابية

يوضح الشكل (٢) أدناه المكونات الأساسية والفرعية للضوابط.

١- حوكمة الأمن السيبراني Cybersecurity Governance	١-١	سياسات وإجراءات الأمن السيبراني Cybersecurity Policies and Procedures	١-٤	أدوار ومسؤوليات الأمن السيبراني Cybersecurity Roles and Responsibilities
	١-٢	إدارة مخاطر الأمن السيبراني Cybersecurity Risk Management	١-٥	الأمن السيبراني المتعلق بالموارد البشرية Cybersecurity in Human Resources
	١-٣	الالتزام بتشريعات وتنظيمات ومعايير الأمن السيبراني Compliance with Cybersecurity Standards, Laws and Regulations	١-٦	إدارة التغيير Change Management
٢- تعزيز الأمن السيبراني Cybersecurity Defense	٢-١	إدارة الأصول Asset Management	٢-١٠	إدارة أمن الشبكات Networks Security Management
	٢-٢	الأمن السيبراني لإدارة العمليات والخدمات Operations and Service Management Cybersecurity	٢-١١	أمن الوسائط Storage Media Cybersecurity
	٢-٣	إدارة سجلات الأحداث ومراقبة الأمن السيبراني Cybersecurity Event Logs and Monitoring Management	٢-١٢	حماية تطبيقات الويب Web Application Security
	٢-٤	أمن تطوير الأنظمة System Development Security	٢-١٣	أمن الأجهزة المحمولة Mobile Devices Security
	٢-٥	إدارة حوادث وتهديدات الأمن السيبراني Cybersecurity Incident and Threat Management	٢-١٤	إدارة النسخ الاحتياطية Backup and Recovery Management
	٢-٦	حماية البيانات والمعلومات Data and Information Protection	٢-١٥	إدارة المفاتيح Key Management
	٢-٧	إدارة هويات الدخول والصلاحيات Identity and Access Management	٢-١٦	التشفير Cryptography
	٢-٨	إدارة الثغرات Vulnerabilities Management	٢-١٧	مرونة التنقل Interoperability
	٢-٩	حماية الأنظمة وأجهزة معالجة المعلومات Information System and Processing Facilities Protection	٢-١٨	الأمن المادي Physical Security

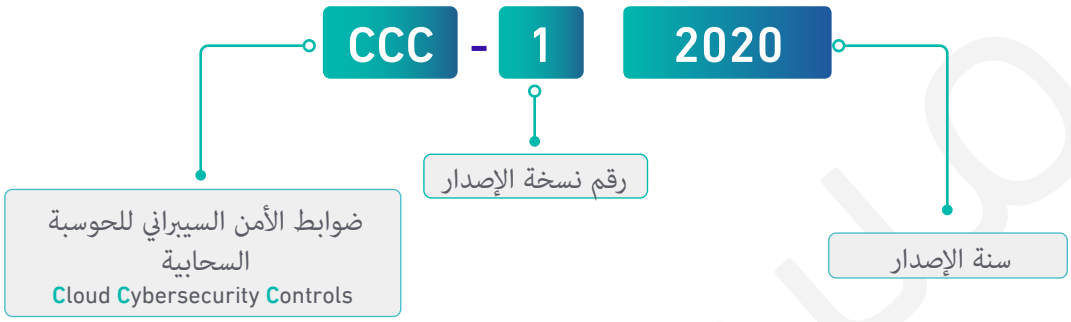
٣- صمود الأمن السيبراني Cybersecurity Resilience	١-٣	جوانب صمود الأمن السيبراني في إدارة استمرارية الأعمال Cybersecurity Resilience aspects of Business Continuity Management (BCM)
٤- الأمن السيبراني المتعلق بالأطراف الخارجية Third-Party Cybersecurity	١-٤	الأمن السيبراني المتعلق بسلسلة الإمداد والأطراف الخارجية Supply Chanin & Third-Party Cybersecurity

شكل ٢: المكونات الأساسية والفرعية لضوابط الأمن السيبراني للحوسبة السحابية

١٠. هيكلية وثيقة ضوابط الأمن السيبراني للحوسبة السحابية

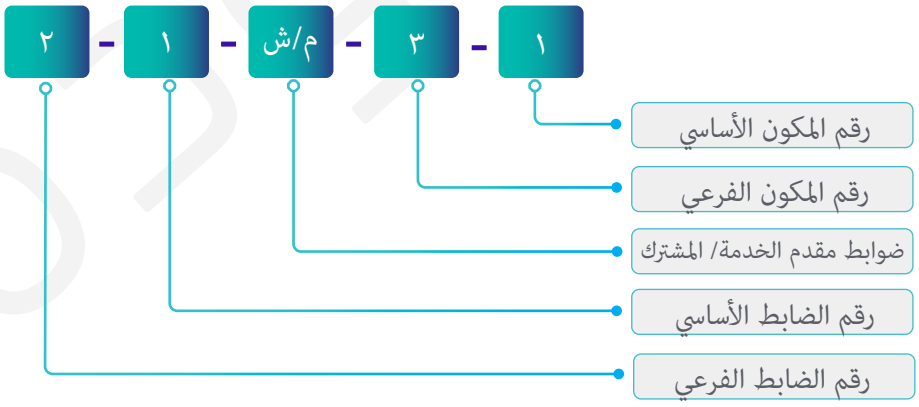
رموز ضوابط الأمن السيبراني للحوسبة السحابية

يشار إلى وثيقة ضوابط الأمن السيبراني للحوسبة السحابية (CCC) بالطريقة الموضحه في الشكل (٣)



شكل ٣: رموز تعريف ضوابط الأمن السيبراني للحوسبة السحابية

يتم استخدام الهيكلية الموضحة في الشكل (٤) لترقيم أي جزء من أجزاء هذه الوثيقة من مكونات وضوابط.



شكل٤: 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 تم 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-١-٣ تعني أن الضابط خاص بمقدمي الخدمات، والضابط ١-٣-ش-١-٢ خاص بالمشتركين.

يرجى ملاحظة أن الأرقام 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 (٣) أدناه طريقة هيكلية الضوابط.

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

١١. ضوابط الأمن السيبراني للحوسبة السحابية

تفاصيل ضوابط الأمن السيبراني للحوسبة السحابية.

١ حوكمة الأمن السيبراني
Cybersecurity Governance

١-١	**سياسات وإجراءات الأمن السيبراني (Cybersecurity Policies and Procedures)**
الهدف	ضمان توثيق ونشر متطلبات الأمن السيبراني والتزام مقدمي الخدمات والمشتركين بها، وذلك وفقًا لمتطلبات الأعمال التنظيمية لدى مقدمي الخدمات والمشتركين، والمتطلبات التشريعية والتنظيمية ذات العلاقة.
الضوابط	
١-١-م-١	رجوعًا للضابط ١-٣-٢ في الضوابط الأساسية للأمن السيبراني بشأن تطبيق سياسات الأمن السيبراني، يلتزم مقدم الخدمات أيضًا بتطبيق ما يلي: ١-١-م-١-١ الحصول على اعتماد صاحب الصلاحية وذلك حسب الهيكل التنظيمي للحوكمة والأدوار والمسؤوليات الخاصة بالأمن السيبراني، بالنسبة للأعمال والممارسات التي لا تتماشى مع سياسات أو إجراءات أو عمليات الأمن السيبراني المعتمدة لدى مقدم الخدمة.
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. 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.

	١-٢-م-١-٤ تحديث سياسات الأمن السيبراني حسب نتائج تقييم مخاطر الأمن السيبراني لخدمات الحوسبة السحابية.
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 مايلي: ١-٢-ش-١-١ المستوى المقبول للمخاطر (Acceptable Risk Levels) فيما يتعلق بخدمات الحوسبة السحابية. ١-٢-ش-١-٢ أخذ تنصيف 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. ١-٢-ش-١-٤ تحديث سياسات الأمن السيبراني حسب نتائج تقييم مخاطر الأمن السيبراني لخدمات الحوسبة السحابية.
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 تحديد بنود التشريعات واللوائح والعقود التي قد تفرض التزامات وواجبات تشريعية أو قانونية ومراقبتها باستمرار. ١-٣-م-١-٢ حماية السجلات، من الوصول غير المصرح به، أو العبث، أو التغيير، أو الحذف غير المشروع، وذلك وفقًا للمتطلبات القانونية، أو التشريعية، أو التعاقدية. ١-٣-م-١-٣ الالتزام بالمحافظة على سرِّية البيانات الشخصية وحمايتها حسب المتطلبات القانونية، والتشريعية، والتعاقدية. ١-٣-م-١-٤ الالتزام بالتشفير حسب المتطلبات القانونية، والتشريعية، واتفاقيات مستوى الخصوصية، وأفضل الممارسات ذات الصلة. ١-٣-م-١-٥ التزام الأطراف الخارجية بالمتطلبات القانونية، والتشريعية ذات الصلة بنطاق عملهم.
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 إجراءات لضمان الالتزام بالأنظمة والتشريعات ذات العلاقة عند استخدام خدمات الحوسبة السحابية. ١-٣-ش-١-٢ المراقبة الدائمة والمستمرة لمدى التزام مقدمي الخدمات بالتشريعات ذات العلاقة.
١-٤	**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	
١-٤-م-١	بالإضافة للضابط ١-٤-١ في الضوابط الأساسية للأمن السيبراني، يجب على صاحب الصلاحية تحديد وتوثيق واعتماد ما يلي: ١-٤-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.
١-٤-م-٢	بالإضافة إلى الأدوار والمسؤوليات الداخلية لدى مقدمي الخدمات والمحددة في الضابط ١-٤-١ في الضوابط الأساسية للأمن السيبراني، يجب على صاحب الصلاحية أيضًا تحديد العلاقات الخارجية التالية: ١-٤-م-٢-١ الاشتراك مع المجموعات والجهات المتخصصة و الموثوقة للحصول على آخر المعلومات والمستجدات في مجال الأمن السيبراني. ١-٤-م-٢-٢ التواصل مع الجهات التنظيمية.
١-٤-ش-١	بالإضافة للضابط ١-٤-١ في الضوابط الأساسية للأمن السيبراني، يجب على صاحب الصلاحية تحديد وتوثيق واعتماد ما يلي: ١-٤-ش-١-١ أدوار الأمن السيبراني، وتكليفات المسؤولية والمحاسبة والاستشارة والتبليغ (RACI) لكل أصحاب العلاقة في خدمات الحوسبة السحابية.
١-٥	**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	

١-٥-م-١	بالإضافة للضوابط الفرعية ضمن الضابط ١-٩-٤ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني خلال العلاقة المهنية بين العاملين ومقدم الخدمة بحد أدنى ما يلي: ١-٥-م-١-١ يجب تحديد درجة المخاطر (Risk Designation) لكل منصب (أو مسمى) وظيفي، وتحديد مواصفات الموظفين المطلوبة لكل درجة. ١-٥-م-١-٢ إجراء المسح الأمني للعاملين الذين لهم حق الوصول إلى أنظمة CTS دوريًا. ١-٥-م-١-٣ الإجراءات التأديبية للعاملين الذين ينتهكون سياسات أو إجراءات الأمن السيبراني. ١-٥-م-١-٤ توقيع واعتماد اتفاقيات صلاحية الوصول كشرط مسبق للوصول إلى أنظمة CTS.
١-٥-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: ١-٥-م-٢-١ أفضل ممارسات الأمن السيبراني عند إنهاء عقود العاملين، بما في ذلك: • إجراء مقابلات انتهاء الخدمة (Exit Interviews) مع العاملين الرئيسيين في مجال الأمن السيبراني. • التأكد من قدرة مقدم الخدمة على الاستمرار بأداء المهام والصلاحيات المناطة بالعاملين المنتهية خدماتهم. • إشعار كافة العاملين بانتهاء خدمة العاملين في مجال الأمن السيبراني. ١-٥-م-٢-٢ ضمان إعادة الأصول الخاصة بمقدمي الخدمات (لا سيما ذات الصلة بالأمن السيبراني) بمجرد إنهاء الخدمة مع العاملين.
١-٥-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: ١-٥-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).
١-٦	**إدارة التغيير (Change Management)**

الهدف	التأكد من أن متطلبات الأمن السيبراني مضمنة في منهجية وإجراءات إدارة التغيير لدى مقدمي الخدمات والمشتركين لحماية السرية وسلامة الأصول المعلوماتية والتقنية لديهم، ودقتها وتوافرها، وذلك وفقًا للسياسات والإجراءات التنظيمية لدى مقدمي الخدمات والمشتركين والمتطلبات التشريعية والتنظيمية ذات العلاقة.
الضوابط	
١-٦-م-١	يجب تحديد متطلبات الأمن السيبراني لإدارة التغيير لدى مقدمي الخدمات، وتوثيقها، واعتمادها.
١-٦-م-٢	يجب تطبيق متطلبات الأمن السيبراني، الخاصة بإدارة التغيير لدى مقدمي الخدمات.
١-٦-م-٣	يجب أن يغطي الأمن السيبراني لإدارة التغيير لدى مقدمي الخدمات بحد أدنى ما يلي: ١-٦-م-٣-١ إجراءات تنفيذ التغييرات (المخطط لها) بشكل منظم في أنظمة الإنتاج (Production Systems). ١-٦-م-٣-٢ أفضل الممارسات لإجراءات الاختبار والتراجع (Rollback) للتغييرات المخطط لها. ١-٦-م-٣-٣ إجراءات تنفيذ التغييرات الاستثنائية (مثل التغييرات أثناء التعافي من الحوادث). ١-٦-م-٣-٤ تحليل التأثير الأمني لكل طلبات التغيير المخططة على أنظمة CTS. ١-٦-م-٣-٥ اتباع مبدأ تفعيل الحد الأدنى من الوظائف المطلوبة (Minimum Functionality Principle) لإعدادات الأنظمة (System Configurations). ١-٦-م-٣-٦ السماح فقط بقائمة محددة من ملفات التشغيل (Whitelisting) للتطبيقات والبرامج.
١-٦-م-٤	يجب مراجعة متطلبات الأمن السيبراني لإدارة التغيير لدى مقدمي الخدمات، ومراجعة تطبيقها، دوريًا.
١-٦-ش-١	يجب تحديد متطلبات الأمن السيبراني لإدارة التغيير لدى المشتركين، وتوثيقها، واعتمادها.
١-٦-ش-٢	يجب تطبيق متطلبات الأمن السيبراني الخاصة بإدارة التغيير لدى المشتركين.
١-٦-ش-٣	يجب أن يغطي الأمن السيبراني لإدارة التغيير لدى المشتركين بحد أدنى ما يلي: ١-٦-ش-٣-١ تحليل التأثير الأمني لكل طلبات التغيير المخططة على أنظمة CTS.
١-٦-ش-٤	يجب مراجعة متطلبات الأمن السيبراني لإدارة التغيير لدى المشتركين، 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 ١-٢ 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.

٢-٢	الأمن السيبراني لإدارة العمليات والخدمات (Operations and Service Management Cybersecurity)
الهدف	ضمان إجراء كل العمليات على نحو يحفظ سرية الأصول المعلوماتية والتقنية، وسلامتها، وتوافرها لدى مقدمي الخدمات و المشتركين.
الضوابط	
٢-٢-م-١	يجب تحديد متطلبات الأمن السيبراني لإدارة العمليات والخدمات لدى مقدمي الخدمات، وتوثيقها واعتمادها.
٢-٢-م-٢	يجب تطبيق متطلبات الأمن السيبراني الخاصة بإدارة العمليات والخدمات لدى مقدمي الخدمات.
٢-٢-م-٣	يجب أن يغطي الأمن السيبراني لإدارة العمليات والخدمات لدى مقدمي الخدمات بحد أدنى ما يلي: ٢-٢-م-٣-١ إجراءات لمراقبة مدى استخدام (Load Utilization) الموارد التقنية، والتخطيط لزيادة السعة عند الاحتياج (Capacity Planning). ٢-٢-م-٣-٢ الإجراءات الخاصة بأنظمة CTS والتصنيف الأمني لها. ٢-٢-م-٣-٣ إدارة وصيانة إعدادات أنظمة CTS.

	٢-٢-م-٣-٤ المراقبة المستمرة لمدى الالتزام ببنود اتفاقية مستوى الخدمة المبرمة بين مقدم الخدمة والمشترك. ٢-٢-م-٣-٥ معمارية الأمن السيبراني (Cybersecurity Architecture) لخدمات الحوسبة السحابية تأخذ بالاعتبار كل من الآتي: المنهجية، التصنيف الأمني، المعمارية الشاملة للجهة (Enterprise Architecture)، ضوابط الأمن السيبراني، النموذج التشغيلي (Operating Model).
٢-٢-م-٤	يجب مراجعة متطلبات الأمن السيبراني الخاصة بإدارة العمليات والخدمات لدى مقدمي الخدمات، ومراجعة تطبيقها، دوريًا.
٢-٢-ش-١	يجب تحديد متطلبات الأمن السيبراني لإدارة العمليات والخدمات لدى المشتركين، وتوثيقها، واعتمادها.
٢-٢-ش-٢	يجب تطبيق متطلبات الأمن السيبراني الخاصة بإدارة العمليات والخدمات لدى المشتركين.
٢-٢-ش-٣	يجب أن يغطي الأمن السيبراني لإدارة العمليات والخدمات لدى المشتركين بحد أدنى مايلي: ٢-٢-ش-٣-١ توثيق الإجراءات الخاصة بأنظمة CTS والتصنيف الأمني لها.
٢-٢-ش-٤	يجب مراجعة متطلبات الأمن السيبراني الخاصة بإدارة العمليات والخدمات لدى المشتركين، ومراجعة تطبيقها، دوريًا.
٢-٣	**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	
٢-٣-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: ٢-٣-م-١-١ تفعيل سجلات الأحداث والتدقيق (Audit Trial) لأنظمة CTS. ٢-٣-م-١-٢ حماية سجلات الأحداث والتدقيق (Audit Trial) لأنظمة CTS. ٢-٣-م-١-٣ تفعيل وحماية سجلات الأحداث لجميع الأنشطة والعمليات على أنظمة المشتركين، بهدف دعم عمليات التحليل الرقمي الجنائي (Digital Forensics).

	٢-٣-م-١-٤ رجوعًا للضابط ٢-١٢-٣-٥ في الضوابط الأساسية للأمن السيبراني، يجب أن يتم الاحتفاظ بسجلات الأحداث (لمدة لا تقل عن ١٨ شهر)، ونسخها احتياطيًا. ٢-٣-م-١-٥ المراقبة الأمنية المستمرة لأحداث الأمن السيبراني (Cybersecurity Events) باستخدام تقنيات (SIEM) بحيث تشمل جميع الأحداث المتعلقة بأنظمة CTS. ٢-٣-م-١-٦ المراجعة الدورية لسجلات الأحداث والتدقيق (Audit Trail) وسجلات الأمن السيبراني (Cybersecurity Events) بحيث تشمل الأحداث والسجلات المتعلقة بأنظمة CTS. ٢-٣-م-١-٧ إنفاذ اتفاقيات مستوى الخدمة (SLAs) الخاصة بتوافر تقنيات (SIEM). ٢-٣-م-١-٨ المتطلبات التقنية والتنظيمية للتعامل الآمن مع بيانات المستخدمين المتواجدة في سجلات الأحداث والتدقيق (Audit Trails) وسجلات أحداث الأمن السيبراني (Cybersecurity Events Logs). ٢-٣-م-١-٩ مراقبة آلية لسجلات الأحداث الخاصة بعمليات الدخول عن بعد (Remote Access). ٢-٣-م-١-١٠ تفعيل وجمع سجلات الأحداث الخاصة بعمليات الدخول (Login).
٢-٣-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: ٢-٣-ش-١-١ التأكد من تفعيل مقدم الخدمة لسجلات الأحداث لجميع الأنشطة والعمليات على أنظمة المشتركين. ٢-٣-ش-١-٢ أن تشمل عملية المراقبة جميع الأحداث المفعلة على الخدمة السحابية الخاصة بالمشترك. ٢-٣-ش-١-٣ تفعيل وجمع سجلات الأحداث الخاصة بعمليات الدخول (Login).
٢-٤	**أمن تطوير الأنظمة (System Development Security)**
الهدف	ضمان تطوير الأنظمة، وتكاملها، ونشرها بطريقة آمنة.
الضوابط	
٢-٤-م-١	يجب تحديد متطلبات الأمن السيبراني لتطوير البرمجيات والتطبيقات والأنظمة لدى مقدمي الخدمات، وتوثيقها واعتمادها.

٢-٤-م-٢	يجب تطبيق متطلبات الأمن السيبراني لتطوير البرمجيات والتطبيقات والأنظمة لدى مقدمي الخدمات.
٢-٤-م-٣	يجب أن تغطي متطلبات الأمن السيبراني لتطوير البرمجيات والتطبيقات والأنظمة لدى مقدمي الخدمات بحد أدنى الضوابط التالية خلال دورة حياة التطوير: ٢-٤-م-٣-١ التأكد من تطبيق ضوابط الأمن السيبراني خلال دورة حياة تطوير التطبيقات (SDLC) المعرفة لدى مقدم الخدمة، لتكون عبارة عن دورة آمنة لتطوير التطبيقات (Secure SDLC). ٢-٤-م-٣-٢ المتطلبات التقنية والتنظيمية لنشر التطبيقات وتكاملها. ٢-٤-م-٣-٣ أخذ متطلبات الأمن السيبراني (لأنظمة CTS والأنظمة ذات العلاقة) بالاعتبار عند تصميم خدمات الحوسبة السحابية. ٢-٤-م-٣-٤ مرحلة اختبار التطبيقات يجب أن تشمل الاختبارات الأمنية لأنظمة CTS واستخدام حالات اختبار (Test Cases) محددة ومعرفة مسبقًا. ٢-٤-م-٣-٥ احتواء الوثائق التقنية (Technical Documentation) لمختلف التطبيقات والأنظمة على الجوانب المتعلقة بالأمن السيبراني. ٢-٤-م-٣-٦ حماية بيئات التطوير (Development Environments) والاختبار (Testing Environments) ومنصات التكامل (Integration Platforms). ٢-٤-م-٣-٧ تأمين الوصول، والتخزين، والتوثيق للشفرة المصدرية (Source Code) وإصداراتها. ٢-٤-م-٣-٨ إلزام المطورين من الأطراف الخارجية (Third-party) باتباع معايير الأمن السيبراني الخاصة بمقدم الخدمة. ٢-٤-م-٣-٩ حماية ومراقبة التطبيقات المطورة من قبل أطراف خارجية. ٢-٤-م-٣-١٠ حماية بيانات عمليات اختبار الأنظمة.
٢-٤-م-٤	يجب مراجعة متطلبات الأمن السيبراني لتطوير البرمجيات والتطبيقات والأنظمة لدى مقدمي الخدمات، ومراجعة تطبيقها، دوريًا.
٢-٤-ش-١	يجب تحديد متطلبات الأمن السيبراني لتطوير البرمجيات والتطبيقات والأنظمة لدى المشتركين، فيما يتعلق بالخدمات السحابية، وتوثيقها، واعتمادها.
٢-٤-ش-٢	يجب تطبيق متطلبات الأمن السيبراني لتطوير البرمجيات والتطبيقات والأنظمة لدى المشتركين فيما يتعلق بالخدمات السحابية.

٢-٤-ش-٣	يجب أن تغطي متطلبات الأمن السيبراني لتطوير البرمجيات والتطبيقات والأنظمة لدى المشتركين فيما يتعلق بالخدمات السحابية بحد أدنى الضوابط التالية طوال دورة التطوير (Development Cycle): ٢-٤-ش-٣-١ أخذ متطلبات الأمن السيبراني بالاعتبار لكل خدمات الحوسبة السحابية التي يستهلكها المشترك. ٢-٤-ش-٣-٢ مرحلة اختبار التطبيقات يجب أن تشمل الاختبارات الأمنية، واستخدام حالات اختبار (Test Cases) محددة ومعرفة مسبقًا لكل خدمات الحوسبة السحابية التي يستخدمها المشترك.
٢-٤-ش-٤	يجب مراجعة متطلبات الأمن السيبراني لتطوير البرمجيات والتطبيقات لدى المشتركين، ومراجعة تطبيقها، دوريًا.
٢-٥	**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 والمشتركين، مع مراعاة ما ورد في الأمر السامي الكريم رقم ٣٧١٤٠ وتاريخ ١٤٣٨/٨/١٤ هـ.
الضوابط	
٢-٥-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: ٢-٥-م-١-١ وجود الإجراءات اللازمة للاستجابة لحوادث الأمن السيبراني بالكفاءة والوقت المناسبين. ٢-٥-م-١-٢ تدريب العاملين (موظفين ومتعاقدين) على الاستجابة لحوادث الأمن السيبراني بما يتماشى مع الأدوار والمسؤوليات. ٢-٥-م-١-٣ الاستجابة لحوادث تسريب المعلومات (واحتوائها). ٢-٥-م-١-٤ تحليل وتحديد الأسباب الجذرية (Root Cause Analysis) لحوادث الأمن السيبراني. ٢-٥-م-١-٥ تقديم الدعم إلى المشتركين في حالات القضايا القانونية، والتحليل الرقمي الجنائي، والحفاظ على الأدلة الرقمية. ٢-٥-م-١-٦ إلزام العاملين (موظفين ومتعاقدين) بالتبليغ عن حوادث الأمن السيبراني التي تصل إلى عملهم. ٢-٥-م-١-٧ دعم المشتركين للتعامل مع حوادث الأمن السيبراني..

	٢-٥-م-١-٨ قياس مؤشرات الأداء الخاصة بإدارة حوادث الأمن السيبراني، ومراقبة مدى الالتزام بمتطلبات العقود والتشريعات.
	٢-٥-م-١-٩ اختبار قدرات الاستجابة لحوادث الأمن السيبراني دوريًا. ٢-٥-م-١-١٠ التبليغ الفوري لحوادث الأمن السيبراني للمشترك.
٢-٥-ش-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 المشتركين، بحد أدنى مايلي: ٢-٥-ش-١-١ التعامل مع حوادث الأمن السيبراني التي يُبلِغ عنها مقدم الخدمة. ٢-٥-ش-١-٢ التواصل مع مقدم الخدمة للحصول على الدعم بشأن إدارة الحوادث ذات الصلة بالخدمات السحابية، عند الضرورة. ٢-٥-ش-١-٣ قياس مؤشرات الأداء الخاصة بإدارة حوادث الأمن السيبراني ومراقبة الالتزام باتفاقيات مستوى الخدمة والعقود والتشريعات. ٢-٥-ش-١-٤ إلزام العاملين (موظفين ومتعاقدين) بالتبليغ عن حوادث الأمن السيبراني التي تصل إلى عملهم. ٢-٥-ش-١-٥ اختبار قدرات الاستجابة لحوادث الأمن السيبراني دوريًا لدى كل من مقدم الخدمة والمشترك.
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 ضمان احتواء نقل ومعالجة البيانات ضمن الحدود الموضحة، في العقود والتشريعات. ٢-٦-م-١-٢ تزويد المستخدمين ذوي الصلاحيات الهامة والحساسة (Administrators) والمشتركين، بقدرات تحديد الموقع المادي والجغرافي لكافة البيانات. ٢-٦-م-١-٣ عدم استخدام بيانات الأنظمة 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-م-١-٤	تزويد المشتركين بعمليات وإجراءات وتقنيات تخزين البيانات، مع الالتزام بالمتطلبات التعاقدية والمتطلبات التشريعية والتنظيمية ذات العلاقة.
	٢-٦-م-١-٥	تزويد المشتركين بآليات لإدارة خصوصية وأمن البيانات الوصفية (Metadata).
	٢-٦-م-١-٦	توفير آلية لترميز البيانات الوصفية (Metadata Labelling) للالتزام بالمتطلبات التشريعية والتنظيمية ذات العلاقة بخصوصية البيانات وسيادتها وحمايتها.
	٢-٦-م-١-٧	وضع قيود على الموقع الجغرافي لمعالجة البيانات وفقاً للمتطلبات التنظيمية والتشريعية ذات العلاقة بخصوصية البيانات وسيادتها وحمايتها.
	٢-٦-م-١-٨	عند إتلاف أو حذف بيانات المشترك يجب التأكد من عدم إمكانية استرجاعها.
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 البيانات والمعلومات لدى المشتركين، بحد أدنى مايلي:
	٢-٦-ش-١-١	ضمان احتواء نقل ومعالجة البيانات ضمن الحدود الموضحة، في العقود والتشريعات.
	٢-٦-ش-١-٢	التأكد من توفير مقدم الخدمة لقدرات تحديد الموقع المادي والجغرافي لكافة البيانات.
	٢-٦-ش-١-٣	استخدام آلية لترميز البيانات الوصفية (Metadata labelling) للالتزام بالمتطلبات التشريعية والتنظيمية ذات العلاقة بخصوصية البيانات وسيادتها وحمايتها.
	٢-٦-ش-١-٤	وجود ضمانات للقدرة على حذف البيانات بطرق آمنة عند الانتهاء من العلاقة مع مقدم الخدمة (Exit Strategy).
٢-٧		**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		
٢-٧-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:
	٢-٧-م-١-١	إدارة الحسابات العامة (Generic Accounts) التي لا يمكن إنشاء حساب مخصص لها (Personalized Account).

	٢-٧-م-١-٢	إدارة هويات الدخول والصلاحيات لجميع الحسابات خلال دورة حياتها.
	٢-٧-م-١-٣	سرِّية هوية المستخدم والحسابات والصلاحيات، بما في ذلك الطلب من المستخدمين حفظ سريتها (للموظفين، والأطراف الخارجية، والمستخدمين من جهة المشترك).
	٢-٧-م-١-٤	الإدارة الآمنة للجلسات (Secure Session Management)، وتشمل موثوقية الجلسات (Authenticity)، وإقفالها (Lockout)، وإنهاء مهلتها (Timeout).
	٢-٧-م-١-٥	التحقق من الهوية متعدد العناصر لكافة الحسابات.
	٢-٧-م-١-٦	إجراءات لكشف محاولات الوصول غير المصرح به ومنعه (مثلًا الحد الأقصى من محاولات عمليات الدخول غير الناجحة (Unsuccessful Login).
	٢-٧-م-١-٧	منع الوصول من شبكات لاسلكية إلى الشبكة الخاصة بأنظمة CTS.
	٢-٧-م-١-٨	الإدارة الآمنة للحسابات الخاصة بالعاملين التابعين للأطراف الخارجية (Third-party).
	٢-٧-م-١-٩	استخدام تقنيات التحقق من الموقع (Location-aware) لعمليات الدخول إلى أنظمة CTS.
	٢-٧-م-١-١٠	التحكم في الوصول إلى الأنظمة الإدارية التقنية والإشرافية (Management and Administrative Access).
	٢-٧-م-١-١١	إخفاء معلومات التحقق من الهوية، خاصةً كلمات المرور، عند عرضها للمستخدم؛ لحمايتها من اطلاع الآخرين عليها.
	٢-٧-م-١-١٢	إشعار المستخدم عند إجراء عملية الدخول إلى نظام خاضع للرقابة، بأنه يمكن مراقبة هذه الجلسة (Session)، وأن إمكانية الدخول محصورة على المستخدمين المصرح لهم، وأن هناك التزامات قانونية عند استخدام النظام.
	٢-٧-م-١-١٣	القدرة على الإيقاف الفوري للجلسة (Session) لعمليات الدخول عن بعد ومنع المستخدم من الدخول مستقبلًا.
	٢-٧-م-١-١٤	القدرة على التحقق من الهوية باستخدام شهادات رقمية (Digital Certificate) صادرة من جهات موثوقة (Trusted Certification Authority)، بالاعتماد على البنية التحتية للمفاتيح العامة (PKI)؛ للتحقق من ملكية الفرد للهوية.
	٢-٧-م-١-١٥	إشعار المشترك عند عملية الوصول إلى أي من الأصول والبيانات الخاصة به.
	٢-٧-م-١-١٦	الحصول على الموافقة من المشترك قبل عملية الوصول إلى أي من الأصول والبيانات الخاصة به.

	٢-٧-م-١-١٧	استخدام الطرق والخوارزميات الآمنة لحفظ ومعالجة كلمات المرور مثل: استخدام دوال الاختزال (Hashing Functions).
٢-٧-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:
	٢-٧-ش-١-١	إدارة هويات الدخول والصلاحيات لجميع الحسابات طوال دورة حياتها.
	٢-٧-ش-١-٢	سرِّية هوية المستخدم والحسابات والصلاحيات، بما في ذلك الطلب من المستخدمين حفظ خصوصيتها (للموظفين، والأطراف الخارجية، والمستخدمين من جهة المشترك).
	٢-٧-ش-١-٣	الإدارة الآمنة للجلسات (Secure Session Management)، وتشمل موثوقية الجلسات (Authenticity)، وإقفالها (Lockout)، وإنهاء مهلتها (Timeout).
	٢-٧-ش-١-٤	التحقق من الهوية متعدد العناصر لكافة الحسابات السحابية للمستخدمين ذوي الصلاحيات الهامة والحساسة.
	٢-٧-ش-١-٥	إجراءات لكشف محاولات الوصول غير المصرح به ومنعه (مثلًا الحد الأقصى من محاولات عمليات الدخول غير الناجحة (Unsuccessful Login)).
٢-٨		**إدارة الثغرات (Vlunerabilities 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		
٢-٨-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:
	٢-٨-م-١-١	الحرص على عدم التأثير على الخدمات المقدمة للمشتركين عند معالجة الثغرات.
	٢-٨-م-١-٢	معالجة فورية للثغرات الحرجة (Critical Vulnerabilities) المكتشفة حديثًا على أنظمة CTS.
	٢-٨-م-١-٣	تقييم الثغرات لأنظمة CTS.
	٢-٨-م-١-٤	تقييم ومعالجة الثغرات الخارجية مرة واحدة شهريًا على الأقل، وكل ثلاثة أشهر على الأقل للأنظمة الداخلية.

	٢-٨-م-١-٥ إشعار المشترك بالثغرات المكتشفة وكيفية معالجتها.
٢-٨-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: ٢-٨-ش-١-١ تقييم ومعالجة الثغرات الخاصة بالخدمات السحابية مرة واحدة كل ثلاثة أشهر على الأقل. ٢-٨-ش-١-٢ إدارة الثغرات التي يُبلغ عنها مقدم الخدمة ومعالجتها.
٢-٩	**حماية الأنظمة وأجهزة معالجة المعلومات (Information System and Processing Facilities Protection)**
الهدف	ضمان حماية الأنظمة وأجهزة معالجة المعلومات بما في ذلك أجهزة المستخدمين والبنى التحتية لدى مقدمي الخدمات والمشتركين من المخاطر السيبرانية.
الضوابط	
٢-٩-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: ٢-٩-م-١-١ توفير خدمة حماية سلامة (Integrity) أنظمة CTS. ٢-٩-م-١-٢ حماية السلامة (Integrity) الخاصة بالأجهزة الافتراضية (Virtual Machines). ٢-٩-م-١-٣ التحقق من مدى التزام الإعدادات التقنية للمعايير المعتمدة لدى مقدم الخدمة. ٢-٩-م-١-٤ عزل التطبيقات والوظائف المتعلقة بالمستخدمين، عن التطبيقات والوظائف الخاصة بالأنظمة. ٢-٩-م-١-٥ اتباع مبدأ تفعيل الحد الأدنى من الوظائف المطلوبة (Minimum Functionality Principle) عند تطبيق وسائل الحماية. ٢-٩-م-١-٦ أن تكون أنظمة CTS قادرة على التعامل بطرق آمنة مع: المدخلات والتحقق منها (Input Validation)، والإستثناءات (Exception)، والتوقف (Failure). ٢-٩-م-١-٧ التوثيق التفصيلي لمعمارية (Architecture) أنظمة CTS، مع توضيح التصاميم والوسائل المتبعة للوفرة (Redundancy) والسعة (Capacity). ٢-٩-م-١-٨ تطبيق المستوى المناسب للوفرة (Redundancy) والسعة (Capacity) والتوافر (Availability) لأنظمة CTS؛ لتلبية متطلبات اتفاقيات مستوى الخدمة. ٢-٩-م-١-٩ آلية موثقة لإدارة الموارد التقنية (Technical Resource Management) بطريقة مرنة. ٢-٩-م-١-١٠ عزل التطبيقات والوظائف الأمنية عن التطبيقات والوظائف الأخرى في أنظمة CTS.

	٢-٩-م-١-١١ استخدام القياس (والتبليغ) الآلي، ما أمكن، لمؤشرات قياس الأداء (KPIs) الخاصة بالأمن السيبراني. ٢-٩-م-١-١٢ منع تنفيذ البرامج غير المصرح بها بأنواعها، مثل البرمجيات (Scripts). ٢-٩-م-١-١٣ اكتشاف ومنع التغييرات غير المصرح بها على البرامج والأنظمة. ٢-٩-م-١-١٤ العزل بين بيئات الإستضافة الخاصة بالمشتركين (Guest Environments)، والحماية فيما بينها. ٢-٩-م-١-١٥ تفعيل العزل بين العمليات (Process Isolation) في أنظمة CTS. ٢-٩-م-١-١٦ الالتزام بالحد الأدنى المحدَّد مسبقًا من الموارد للمشتركين. ٢-٩-م-١-١٧ ضمان فصل وعزل البيانات على مستوى بيئات المشتركين؛ لمنع اختلاط البيانات (Data Commingling). ٢-٩-م-١-١٨ التحكم بالوصول المنطقي (Access Control) لأنظمة ووسائل التخزين والعزل بين البيئات الخاصة بالمشتركين (Guest Environments) في الشبكة الخاصة بالتخزين + (Storage Area Network (SAN)).
٢-١٠	**إدارة أمن الشبكات (Networks Security Management)**
الهدف	ضمان حماية شبكات مقدمي الخدمات والمشتركين من المخاطر السيبرانية.
الضوابط	
٢-١٠-م-١	بالإضافة للضوابط الفرعية ضمن الضابط ٢-٥-٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني الخاصة بإدارة أمن المعلومات لدى مقدمي الخدمات، بحد أدنى مايلي: ٢-١٠-م-١-١ توثيق معمارية الشبكات (Network Architecture) مع توضيح طرق ووسائل الحماية. ٢-١٠-م-١-٢ عزل وحماية الشبكة الخاصة بأنظمة CTS من الشبكات الأخرى الداخلية والخارجية. ٢-١٠-م-١-٣ الحماية من هجمات تعطيل الخدمات (DoS). ٢-١٠-م-١-٤ استخدام التشفير للبيانات المنتقلة عبر الشبكة من وإلى الشبكة الخاصة بأنظمة CTS. ٢-١٠-م-١-٥ التحكم في الوصول (Access Control) بين أجزاء الشبكة (Network Segments) المختلفة. ٢-١٠-م-١-٦ الالتزام بالحد الأدنى المحدد مسبقًا من موارد الشبكة (Bandwidth,Latency).

	٢-١٠-م-١-٧ عزل الشبكات اللاسلكية عن الشبكة الخاصة بأنظمة CTS. ٢-١٠-م-١-٨ فصل وعزل بيانات المشتركين عن بعضها البعض على مستوى الشبكات. ٢-١٠-م-١-٩ العزل بين شبكات الخدمات السحابية (Cloud Service Delivery) وشبكات الإدارة السحابية (Cloud Management) والشبكة الداخلية لمقدم الخدمة (Enterprise). ٢-١٠-م-١-١٠ مراقبة الشبكات الداخلية والخارجية للكشف عن الأنشطة المشبوهة. ٢-١٠-م-١-١١ أنظمة كشف ومنع التسلل (IDS/IPS) على أنظمة CTS وجميع المكونات التقنية لمقدم الخدمة.
٢-١١	**أمن الوسائط (Storage Media Security)**
الهدف	ضمان التعامل الآمن مع المعلومات والبيانات عبر الوسائط المادية.
الضوابط	
٢-١١-م-١	يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني لاستخدام وسائط المعلومات والبيانات المادية لدى مقدمي الخدمات.
٢-١١-م-٢	يجب تطبيق متطلبات الأمن السيبراني لاستخدام وسائط المعلومات والبيانات المادية لدى مقدمي الخدمات.
٢-١١-م-٣	متطلبات الأمن السيبراني لاستخدام وسائط المعلومات والبيانات المادية لدى مقدمي الخدمات يجب أن تغطي بحد أدنى ما يلي: ٢-١١-م-٣-١ يجب التأكد من عدم احتواء الوسائط على أية بيانات أو معلومات، قبل إعادة استخدام الوسائط أو التخلص منها. ٢-١١-م-٣-٢ يجب استخدام وسائل آمنة عند التخلص من الوسائط. ٢-١١-م-٣-٣ الحفاظ على سرية وسلامة البيانات على أجهزة وسائط التخزين الخارجية. ٢-١١-م-٣-٤ وضع علامات مقروءة على الوسائط توضح مدى حساسيتها. ٢-١١-م-٣-٥ الحفظ الآمن لأجهزة وسائط التخزين الخارجية. ٢-١١-م-٣-٦ التقييد الحازم لاستخدام وسائط التخزين الخارجية على أنظمة CTS.
٢-١١-م-٤	يجب مراجعة متطلبات الأمن السيبراني لاستخدام وسائط المعلومات والبيانات المادية لدى مقدمي الخدمات، ومراجعة تطبيقها، دوريًا.
٢-١٢	**حماية تطبيقات الويب (Web Application Security)**

الهدف	ضمان حماية تطبيقات الويب الخارجية لدى مقدمي الخدمات والمشتركين ضد المخاطر السيبرانية.
الضوابط	
٢-١٢-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: ٢-١٢-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 الغير مصرح به، الاطلاع غير المصرح به.
٢-١٣	**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 الشخصية الخاصة بمقدمي الخدمات والمشتركين (مبدأ "BYOD").
الضوابط	
٢-١٣-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: ٢-١٣-م-١-١ الاحتفاظ بقائمة جرد محدثة (Inventory) للأجهزة المحمولة. ٢-١٣-م-١-٢ إدارة الأجهزة المحمولة (Mobile Device Management) مركزيًا. ٢-١٣-م-١-٣ قفل الشاشة لأجهزة المستخدمين (Screen Lock). ٢-١٣-م-١-٤ تطبيق التحديثات الأمنية (Patching) على الأجهزة المحمولة. ٢-١٣-م-١-٥ استخدام أنظمة حماية متقدمة (IDS/IPS) على أجهزة المستخدمين. ٢-١٣-م-١-٦ إعادة الأصول التي لدى العاملين، خصوصًا التي يتم استخدامها للدخول على أنظمة CTS. ٢-١٣-م-١-٧ قبل إعادة استخدام الأجهزة المحمولة أو التخلص منها، خصوصًا التي يتم استخدامها للدخول على أنظمة CTS، يجب التأكد من عدم احتوائها على أية بيانات أو معلومات باستخدام وسائل آمنة.

	٢-١٣-م-١-٨ تعطيل الكاميرات ومكبرات الصوت والوسائط الأخرى على الأجهزة المحمولة التي قد تُستخدم للدخول على أنظمة CTS. ٢-١٣-م-١-٩ الإدارة الآمنة لأدوات الصيانة المحمولة التي يمكنها الوصول إلى أنظمة CTS.
٢-١٣-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: ٢-١٣-ش-١-١ إعادة الأصول التي لدى العاملين، خصوصًا التي يتم استخدامها للدخول على الخدمات السحابية. ٢-١٣-ش-١-٢ 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.
٢-١٤	**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 والمشتركين، والمتطلبات التشريعية والتنظيمية ذات العلاقة.
الضوابط	
٢-١٤-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: ٢-١٤-م-١-١ عمل النسخ الاحتياطي المتصل وغير المتصل (Online and Offline backup) للبيانات الخاصة بالمشترك على فترات زمنية مخطط لها، مع القدرة على استعادتها بجميع صورها حسب اتفاقية مستوى الخدمة. ٢-١٤-م-١-٢ نطاق عمل النسخ الاحتياطي المتصل وغير المتصل (Online and Offline backup) ليشمل أنظمة CTS. ٢-١٤-م-١-٣ تأمين الوصول، والتخزين، والنقل لمحتوى النسخ الاحتياطية لبيانات المشترك ووسائطها، وحمايتها من الإتلاف، أو التعديل، أو الاطلاع غير المصرح به. ٢-١٤-م-١-٤ تأمين الوصول، والتخزين، والنقل لمحتوى النسخ الاحتياطية لأنظمة CTS ووسائطها، وحمايتها من الإتلاف، أو التعديل، أو الاطلاع غير المصرح به.
٢-١٥	**إدارة المفاتيح (Key Management)**

الهدف	ضمان الإدارة الآمنة لمفاتيح التشفير، لحماية السرية والسلامة والتوافر للأصول المعلوماتية والتقنية.
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 أخذ نسخ احتياطية من مفاتيح التشفير وتخزينها بطرق آمنة خارج الأنظمة السحابية. ٢-١٥-م-٣-٣ القدرة على إلغاء مفاتيح التشفير والشهادات الرقمية من المستخدمين ونظم المعلومات بطرق آمنة. ٢-١٥-م-٣-٤ وجود آلية لاسترجاع البيانات، بطرق آمنة، في حالة فقدان مفاتيح التشفير. ٢-١٥-م-٣-٥ تفعيل سجلات الأحداث المتعلقة بفاتيح 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 تخزين مفاتيح التشفير بطرق آمنة خارج الأنظمة السحابية. ٢-١٥-ش-٣-٣ القدرة على إلغاء مفاتيح التشفير والشهادات الرقمية من المستخدمين ونظم المعلومات. ٢-١٥-ش-٣-٤ وجود آلية لاسترجاع البيانات، بطرق آمنة، في حالة فقدان مفاتيح التشفير.
٢-١٥-ش-٤	يجب مراجعة متطلبات الأمن السيبراني الخاصة بإدارة المفاتيح لدى المشتركين، ومراجعة تطبيقها، دوريًا.
٢-١٦	التشفير (Cryptography)

الهدف	ضمان استخدام التشفير بطريقة مناسبة وفعالة لحماية الأصول المعلوماتية الإلكترونية الخاصة بمقدمي الخدمات والمشتركين وفقًا للسياسات والإجراءات التنظيمية لديهم والمتطلبات التشريعية والتنظيمية ذات العلاقة.
الضوابط	
٢-١٦-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:
	٢-١٦-م-١-١ استخدام طرق وخوارزميات ومفاتيح وأجهزة تشفير محدثة وآمنة. ٢-١٦-م-١-٢ القدرة على إصدار شهادات رقمية، أو استخدام شهادات رقمية صادرة من جهات موثوقة (Trusted Certification Authority).
٢-١٦-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: ٢-١٦-ش-١-١ استخدام طرق وخوارزميات ومفاتيح وأجهزة تشفير محدثة وآمنة. ٢-١٦-ش-١-٢ تشفير البيانات والمعلومات المنقولة إلى الخدمات السحابية، أو المخزَّنة فيها، أو المنقولة منها.
٢-١٧	**مرونة التنقل (Interoperability)**
الهدف	ضمان وجود الحد الأدنى من القيود التشغيلية والاقتصادية الناتجة عن استخدام أصول تقنية (Technical Assets) وأساليب تخزين (Storage Formats) خاصة (Proprietary) أو غير قابلة للنقل (Non-interoperable).
الضوابط	
٢-١٧-م-١	يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني، الخاصة بمرونة التنقل (Interoperability) لدى مقدمي الخدمات.
٢-١٧-م-٢	يجب تطبيق متطلبات الأمن السيبراني، الخاصة بمرونة التنقل (Interoperability) لدى مقدمي الخدمات.
٢-١٧-م-٣	يجب أن تغطي متطلبات الأمن السيبراني، الخاصة بمرونة التنقل (Interoperability) لدى مقدمي الخدمات، بحد أدنى ما يلي:
	٢-١٧-م-٣-١ إتاحة الخدمات القابلة للتنقل (Interoperable) للمشترك. ٢-١٧-م-٣-٢ تقديم واجهات برمجة تطبيقات مفتوحة ومنشورة (Open and Published APIs) للمشتركين لضمان مرونة التنقل (Interoperability).

	٢-١٧-م-٣-٣ توفير بروتوكولات شبكة معيارية (Standard Network Protocols) للمشتركين. ٢-١٧-م-٣-٤ تزويد المشتركين بتنسيقات بيانات معيارية (Standard Data Formats). ٢-١٧-م-٣-٥ توفير تنسيقات معيارية (Standard Formats) لأجهزة التخزين الافتراضية (Virtual Storage Appliances) وصور الأجهزة الافتراضية (Virtual Machines Images)، مثل: تنسيق OVF للمشتركين.
٢-١٧-م-٤	يجب مراجعة متطلبات الأمن السيبراني الخاصة بمرونة التنقل (Interoperability) لدى مقدمي الخدمات، ومراجعة تطبيقها، دوريًا.
٢-١٧-ش-١	يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني، الخاصة بمرونة التنقل (Interoperability) لدى المشتركين.
٢-١٧-ش-٢	يجب تطبيق متطلبات الأمن السيبراني، الخاصة بمرونة التنقل(Interoperability) لدى المشتركين.
٢-١٧-ش-٣	يجب أن تغطي متطلبات الأمن السيبراني، الخاصة بمرونة التنقل(Interoperability) لدى المشتركين بحد أدنى ما يلي: ٢-١٧-ش-٣-١ خدمات قابلة للنقل في العقد المبرم بين المشترك ومقدم الخدمة. ٢-١٧-ش-٣-٢ من الأفضل استخدام واجهات برمجة تطبيقات قياسية ومنشورة (Open and Published APIs) لضمان مرونة التنقل (Interoperability). ٢-١٧-ش-٣-٣ من الأفضل استخدام بروتوكولات شبكة معيارية (Standard Network Protocols). ٢-١٧-ش-٣-٤ من الأفضل استخدام تنسيقات بيانات معيارية (Standard Data Formats). ٢-١٧-ش-٣-٥ وجود ضمانات للقدرة على تصدير ونقل البيانات عند الإنتهاء من العلاقة مع مقدم الخدمة (Exit Strategy).
٢-١٧-ش-٤	يجب مراجعة متطلبات الأمن السيبراني الخاصة بمرونة التنقل (Interoperability) لدى المشتركين، ومراجعة تطبيقها، دوريًا.
٢-١٨	**الأمن المادي (Physical Security)**
الهدف	ضمان حماية الأصول المعلوماتية و التقنية الخاصة بمقدمي الخدمات والمشتركين من الوصول المادي غير المصرح به و الفقدان و السرقة و التخريب.
الضوابط	
٢-١٨-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:

٢-١٨-م-١-١	المراقبة المستمرة لعمليات الدخول والخروج للمباني والمواقع لدى مقدم الخدمة.
٢-١٨-م-١-٢	السماح للعاملين المصرح لهم فقط بالوصول إلى مركز البيانات (DC) لدى مقدم الخدمة.
٢-١٨-م-١-٣	الحماية المادية لوسائط نقل البيانات (Transmission Media)، مثل خطوط نقل الشبكات (Network Cables).
٢-١٨-م-١-٤	منع الوصول غير المصرح به للأجهزة التي تتعامل مباشرة مع أنظمة CTS.
٢-١٨-م-١-٥	تطبيق وسائل السلامة والأمان في مراكز البيانات (DCs).
٢-١٨-م-١-٦	إضاءة مراكز البيانات (DCs) ومسارات ومخارج الطوارئ في حالات انقطاع مصدر الطاقة الكهربائية.
٢-١٨-م-١-٧	القدرة على إيقاف تشغيل نظم المعلومات أو مكوناتها فورًا بطرق آمنة في حالات الطوارئ.
٢-١٨-م-١-٨	أنظمة لاكتشاف وإخماد الحرائق تعمل بمصدر طاقة مستقل.
٢-١٨-م-١-٩	تدابير وقائية لحماية البنية التحتية للمرافق الخاصة بأنظمة CTS من الزلازل والانفجارات والاضطرابات المدنية وغيرها من أشكال التهديدات الطبيعية والتهديدات البشرية.
٢-١٨-م-١-١٠	الحماية من تسرب المياه.
٢-١٨-م-١-١١	الحماية من الأعطال التي تسببها حالات انقطاع مصدر الطاقة أو الأعطال الكهربائية.
٢-١٨-م-١-١٢	الإستعانة بخدمات المرافق (مثل خدمات الطاقة، خدمات المياه، .. إلخ) من عدة مصادر، والتأكد من استمراريتها في حال الانقطاع، وعمل الاختبارات الدورية لها.
٢-١٨-م-١-١٣	الاستعانة بشبكتين مختلفتين من شبكات الاتصالات المُستخدمة بين المشتركين والخدمات السحابية والإنترنت.
٢-١٨-م-١-١٤	منع تجميع معدات أنظمة المعلومات في مناطق البناء، حيث تكون الأخطار مرجحة.
٢-١٨-م-١-١٥	تنفيذ أعمال الصيانة الروتينية للمعدات دوريًا.
٢-١٨-م-١-١٦	أن تشمل قائمة الخدمات (Service Portofolio) المقدمة للمشتركين خدمة توفير بنية تحتية خاصة مؤمنة (Caged Infrastructure).
٢-١٨-م-١-١٧	تصنيف الأصول المادية من الناحية الأمنية والتشغيلية وترميزها (Labelling).
٢-١٨-م-١-١٨	ضمان نقل المعدات المصرح بها فقط بطرق آمنة داخل الموقع أو خارجه.

	٢-١٨-م-١-١٩	مناطق التحميل والنقل (Loading Areas) يجب أن تكون معزولة عن بقية المناطق.
	٢-١٨-م-١-٢٠	التخلص الآمن من أجهزة البنية التحتية (Infrastructure Hardware)، وبالأخص معدات التخزين (Storage Equipments).
	٢-١٨-م-١-٢١	الضبط التلقائي لدرجة الحرارة والتهوية والرطوبة في مركز البيانات (DC).
	٢-١٨-م-١-٢٢	وجود خطوط كابلات كهربائية توفر مصادر طاقة احتياطية في مركز البيانات(DC).

٣ صمود الأمن السيبراني
Cybersecurity Resilience

١-٣	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 للجهة 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 استئناف الخدمات خلال فترة زمنية محددة معرفة باتفاقية مستوى الخدمة (SLA).
	٣-١-م-١-٢ تقييم مخاطر الأعطال أو الكوارث المحتملة، والتعامل معها.
	٣-١-م-١-٣ توعية العاملين وتدريبهم من خلال خطط تجريبية وتدريبية للتعافي من الكوارث.
	٣-١-م-١-٤ اختبار ومحاكاة خطة التعافي من الكوارث.
	٣-١-م-١-٥ مركز بيانات بديل في موقع جغرافي آخر (منعزل بمسافة ٥٠ كم أو أكثر) لتولّي أعمال الحوسبة والمعالجة في حالة وقوع كارثة أو حادثة تؤدي إلى إيقاف عمل الموقع الرئيسي، بشرط ألا يشترك الموقعان في نفس المخاطر المحتملة.
	٣-١-م-١-٦ مركز بيانات بديل في موقع جغرافي آخر (منعزل بمسافة ٥٠ كم أو أكثر) لحفظ البيانات في حالة وقوع كارثة أو حادثة تؤدي إلى إيقاف عمل الموقع الرئيسي، بشرط ألا يشترك الموقعان في نفس المخاطر المحتملة.

	٣-١-م-١-٧	موقع بديل في موقع جغرافي آخر (منعزل بمسافة ١٠٠ كم أو أكثر) لاستضافة أعمال مركز القيادة والقوى العاملة (Command Center) لضمان استمراريتها في حالة وقوع كارثة أو حادثة تؤدي إلى إيقاف عمل الموقع الرئيسي، بشرط ألا يشترك الموقعان في نفس المخاطر المحتملة.
	٣-١-م-١-٨	تحديد الأدوار والمسؤوليات ذات العلاقة بإدارة استمرارية الأعمال والتعافي من الكوارث.
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	تحديد اتفاقيات مستوى الخدمة في الاتفاق مع مقدم الخدمة من أجل استئناف الخدمات.
	٣-١-ش-١-٢	أحكام لاستمرارية أساليب التعامل والتواصل مع مقدم الخدمة في حالات الكوارث، وتدريب العاملين عليها.

٤ الأمن السيبراني المتعلق بالأطراف الخارجية
Third-Party Cybersecurity

١-٤	الأمن المتعلق بسلسلة الإمداد والأطراف الخارجية (Supply Chain & 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	
١-١-٤-م	بالإضافة للضوابط الفرعية ضمن الضابط 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 تقييم الأمن السيبراني والتدقيق الدوري للأطراف الخارجية، والتعامل مع الملاحظات التي تم رصدها بصورة مناسبة. 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 إدارة سلامة المعلومات لدى الأطراف الخارجية. ٤-١-م-١-٤ المراقبة الأمنية المستمرة على الخدمات المقدمة من الأطراف الخارجية. ٤-١-م-١-٥ يجب على الطرف الخارجي إدارة مخاطر الأمن السيبراني الخاصة به. ٤-١-م-١-٦ إجراء المسح الأمني (screening or vetting) لشركات خدمات الإسناد، ولموظفي خدمات الإسناد، والخدمات المدارة ذات العلاقة بأنظمة CTS.
١-١-٤-ش	بالإضافة للضوابط الفرعية ضمن الضابط 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-ش-١-١ إدارة سلامة المعلومات مع الأطراف الخارجية.

١٢. الملاحق

الملحق (أ): مصطلحات وتعريفات

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

جدول ٤: مصطلحات وتعريفات

المصطلح	التعريف
الحماية من التهديدات المتقدمة المستمرة Advanced Persistent Threat (APT) Protection	الحماية من التهديدات المتقدمة التي تستخدم أساليب خفية تهدف إلى الدخول غير المشروع على الأنظمة والشبكات التقنية ومحاولة البقاء فيها لأطول فترة ممكنة عن طريق تفادي أنظمة الكشف والحماية. وهذه الأساليب تستخدم عادة الفيروسات والبرمجيات الضارة غير المعروفة مسبقًا (Zero-Day Malware) لتحقيق هدفها.
الأصل Asset	أي شيء ملموس أو غير ملموس له قيمة بالنسبة لمقدمي الخدمات والمشتركين. هناك أنواع كثيرة من الأصول؛ بعض هذه الأصول تتضمن أشياء واضحة مثل: الأشخاص، والآلات، والمرافق، وبراءات الاختراع، والبرمجيات والخدمات. ويمكن أن يشمل المصطلح أيضًا أشياء أقل وضوحًا، مثل: المعلومات والخصائص (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.
أحضِر الجهاز الخاص بك Bring Your Own Device (BYOD)	يشير هذا المصطلح إلى سياسة مقدمي الخدمات والمشتركين التي تسمح (سواء بشكل جزئي أو كلي) للعاملين لديهم بجلب الأجهزة الشخصية الخاصة بهم (أجهزة الكمبيوتر المحمولة والأجهزة اللوحية والهواتف الذكية) إلى أماكن العمل، واستخدام هذه الأجهزة للوصول إلى الشبكات والمعلومات والتطبيقات والأنظمة التابعة للجهة المقيدة بصلاحيات دخول.
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.
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.
مصفوفة توزيع المسؤوليات RACI Matrix	هي مصفوفة يتم فيها توضيح وتحديد أدوار الأعضاء المعنيين بإتمام أي عملية أو مشروع.
قاعدة بيانات إدارة الإعدادات (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.
أنظمة CTS Cloud Technology Stack (CTS)	بنية متعددة الطبقات من التقنيات التي تنفذ خدمات الحوسبة السحابية: (البنية التحتية لمركز البيانات، و الشبكة المحلية، و أجهزة التقارب الفائق للتخزين/الحوسبة، و مراقب الأجهزة الافتراضية، و منصة الإدارة السحابية، و الأجهزة الافتراضية، و أنظمة التشغيل، و برمجيات التطبيق، و منصات التشغيل والصيانة...إلخ).

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.
منطقة الشبكة المراقبة Controlled Area Network	هو منطقة من الشبكة تدعم أنظمة CTS، وهي منفصلة عن بقية المنشأة بإمكانية وصول متحكم فيه.
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.

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.
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. مستوى التصنيف هو مؤشر على قيمة أو أهمية البيانات والمعلومات للجهة.

أرشفة البيانات Data Archiving	عملية نقل البيانات التي لم تعد مستخدمة بشكل فعال في جهاز تخزين منفصل للحفظ طويل الأجل. تتكون بيانات الأرشيف من بيانات قديمة لا تزال مهمة للجهة، وقد تكون مطلوبة للرجوع إليها في المستقبل، وبيانات يجب الاحتفاظ بها للالتزام بالتشريعات والتنظيمات ذات العلاقة.
الدفاع الأمني متعدد المراحل Defense-in-Depth	هو مفهوم لتوكيد المعلومات (information assurance)، حيث يتم وضع مستويات متعددة من الضوابط الأمنية (كدفاع) في نظام تقنية المعلومات (IT) أو تقنية التشغيل(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.
نظام اسماء النطاقات Domain Name System	نظام تقني يستخدم قاعدة بيانات يتم توزيعها عبر الشبكة و/أو الإنترنت تسمح بتحويل أسماء النطاقات إلى عناوين الشبكة (IP addresses)، والعكس، لتحديد عناوين الخدمات مثل خوادم المواقع الإلكترونية والبريد الإلكتروني.
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.
كفاءة Efficiency	العلاقة بين النتائج المحققة (المخرجات) والموارد المستخدمة (المدخلات). يمكن تعزيز كفاءة العملية أو النظام من خلال تحقيق نتائج أكثر باستخدام نفس الموارد (المدخلات) أو أقل.
حدث Event	شيء يحدث في مكان محدد (مثل الشبكة، والأنظمة، والتطبيقات، وغيرها) وفي وقت محدد.

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.
بروتوكول نقل النص التشعبي الآمن Hyper Text Transfer Protocol Secure (HTTPS)	بروتوكول يستخدم التشفير لتأمين صفحات وبيانات الويب عند انتقالها عبر الشبكة. وهو عبارة عن نسخة آمنة من بروتوكول نقل النص التشعبي (HTTP).
هوية Identification	وسيلة التحقق من هوية المستخدم أو العملية أو الجهاز، وهي عادة شرط أساسي لمنح حق الوصول إلى الموارد في النظام.
حادثة Incident	انتهاك أمني بمخالفة سياسات الأمن السيبراني، أو سياسات الاستخدام المقبول، أو ممارسات، أو ضوابط أو متطلبات الأمن السيبراني.
تسرب المعلومات Information Spillage	يشير تسرب المعلومات إلى مواقف توضع فيها إما المعلومات المصنّفة أو الحساسة دون قصد على نظم المعلومات الغير مصرح لها بمعالجتها. ويحدث هذا التسرب للمعلومات في الغالب عندما يتم نقل معلومات يُظَن للوهلة الأولى أنها منخفضة الحساسية إلى نظام للمعلومات ثم يتحدد فيما بعد أنها عالية الحساسية. وعند الوصول إلى هذه النقطة، يجب اتخاذ إجراء تصحيحي.
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).
نظام الحماية المتقدمة لاكتشاف ومنع الاختراقات Intrusion Prevention System (IPS)	نظام لديه قدرات كشف الاختراقات، بالإضافة إلى القدرة على منع وإيقاف الحوادث المشبوهة أو المحتملة.
مؤشر قياس الأداء Key Performance Indicator (KPI)	نوع من أدوات قياس مستوى الأداء يُقيّم مدى نجاح نشاط ما أو جهة تجاه تحقيق أهداف محددة.
ترميز أو علامة 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.
الحد الأدنى من الصلاحيات Least Privilege	مبدأ أساسي في الأمن السيبراني يهدف إلى منح المستخدمين صلاحيات الوصول التي يحتاجونها لتنفيذ مسؤولياتهم الرسمية فقط.
البرمجيات الضارة Malware	برنامج يصيب الأنظمة بطريقة خفية (في الغالب) لانتهاك سرية أو دقة أو توافر البيانات أو التطبيقات أو نظم التشغيل.
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»).

المعمارية متعددة المستويات Multi-tier Architecture	معمارية أو بنية تطبق أسلوب عميل-خادم الذي يتم فيه تطوير وصيانة منطق العملية الوظيفية، والوصول إلى البيانات، وتخزين البيانات وواجهة المستخدم كوحدات مستقلة على منصات منفصلة.
الحاجة إلى المعرفة والحاجة إلى الاستخدام Need-to-Know and Need-to-Use	القيود المفروضة على البيانات، والتي تعتبر حساسة ما لم يكن لدى الشخص حاجة محددة إلى الاطلاع على البيانات لغرض ما متعلق بأعمال ومهام رسمية.
النسخ الاحتياطي غير المتصل أو خارج الموقع Offline/Offsite Backup	نسخة احتياطية لقاعدة البيانات وإعدادات الأنظمة والتطبيقات والأجهزة عندما تكون النسخة غير متصلة وغير قابلة للتحديث. عادة ما تُستخدم أشرطة (Tapes) في حالة النسخة الاحتياطية خارج الموقع.
النسخ الاحتياطي المتصل Online Backup	طريقة للتخزين يتم فيها النسخ الاحتياطي بانتظام عبر شبكة على خادم بعيد (إما داخل شبكة خاصة بمقدمي الخدمات والمشتركين أو بالاستضافة لدى مقدم خدمة).
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.
حزم التحديثات والإصلاحات Patch	حزم بيانات داعمة لتحديث أو إصلاح أو تحسين نظام التشغيل للحاسب الآلي أو لتطبيقاته أو برامجه. وهذا يشمل إصلاح الثغرات الأمنية وغيرها من الأخطاء، حيث تسمى هذه الحزم عادةً إصلاحات، أو إصلاح الأخطاء، وتحسين إمكانية الاستخدام أو الأداء.
اختبار الاختراق Penetration Testing	ممارسة اختبار على نظام حاسب آلي أو شبكة أو تطبيق موقع إلكتروني أو تطبيق هواتف ذكية للبحث عن ثغرات يمكن أن يستغلها المهاجم.
رسائل التصيد الإلكتروني Phishing Emails	محاولة الحصول على معلومات حساسة مثل أسماء المستخدمين، وكلمات المرور، أو تفاصيل بطاقة الائتمان، غالبًا لأسباب ونوايا ضارة وخبيثة، وذلك بالتنكر على هيئة جهة جديرة بالثقة في رسائل بريد إلكترونية.
الأمن المادي Physical Security	يصف الأمن المادي التدابير الأمنية التي تم تصميمها لمنع الوصول غير المصرح به إلى المرافق والمعدات والموارد التابعة للجهة، وحماية الأفراد والممتلكات من التلف أو الضرر (مثل التجسس أو السرقة، أو الهجمات الإرهابية). ينطوي الأمن المادي على استخدام طبقات متعددة من نظم مترابطة، تشمل الدوائر التلفزيونية المغلقة (CCTV))، وحراس الأمن، 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.
الخصوصية Privacy	الحرية من التدخل غير المصرح به أو الكشف عن معلومات شخصية حول الفرد.
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.
الاستعادة Recovery	إجراء أو عملية لاستعادة أو التحكم في شيء منقطع، أو تالف، أو مسروق، أو ضائع.
مدة الاحتفاظ Retention	هي المدة الزمنية التي يجب فيها الاحتفاظ بالمعلومات، أو البيانات، أو سجلات الأحداث، أو النسخ الاحتياطية، بغض النظر عن الشكل (ورقي، أو إلكتروني، أو غير ذلك).
المعايير الأمنية لشفرة البرامج والتطبيقات Secure Coding Standards	ممارسة تطوير برمجيات وتطبيقات الحاسب الآلي بطريقة تحمي من التعرض غير المقصود لثغرات الأمن السيبراني المتعلقة بالبرمجيات والتطبيقات.
مراجعة الإعدادات والتحصين Secure Configuration and Hindering	حماية وتحصين وتعديل إعدادات جهاز الحاسب الآلي، والنظام، والتطبيق، وجهاز الشبكة، والجهاز الأمني لمقاومة الهجمات السيبرانية، مثل: إيقاف أو تغيير الحسابات المصنعية والافتراضية، وإيقاف الخدمات غير المستخدمة، وإيقاف منافذ الشبكة غير المستخدمة.
نظام إدارة سجلات الأحداث ومراقبة الأمن السيبراني Security Information and Event Management (SIEM)	نظام يقوم بإدارة وتحليل بيانات سجلات الأحداث الأمنية في الوقت الفعلي لتوفير مراقبة للتهديدات، وتحليل نتائج القواعد المترابطة لسجلات الأحداث، والتقارير حول بيانات السجلات، والاستجابة للحوادث.

الاختبار الأمني Security Testing	عملية تهدف إلى التأكد من أن النظام أو التطبيق المعدّل أو الجديد يتضمن ضوابط وحمايات أمنية مناسبة، ولا يحتوي على أي ثغرات أمنية قد تضر بالأنظمة أو التطبيقات الأخرى، أو تؤدي إلى سوء استخدام النظام أو التطبيق أو معلوماته، وكذلك للحفاظ على وظيفة النظام أو التطبيق على النحو المنشود.
الأمن من خلال التصميم Security-by-Design	منهجية لتطوير الأنظمة والتطبيقات وتصميم الشبكات التي تسعى إلى جعلها خالية من نقاط الضعف والثغرات الأمنية السيبرانية، والمقدرة على صد الهجوم السيبراني قدر الإمكان من خلال عدة تدابير على سبيل المثال: الاختبار المستمر، وحماية المصادقة، والتمسك بأفضل ممارسات البرمجة والتصميم، وغيرها.
فصل المهام Segregation of Duties	مبدأ أساسي في الأمن السيبراني يهدف إلى تقليل الأخطاء والاحتيال خلال مراحل تنفيذ عملية محددة؛ عن طريق التأكد من ضرورة وجود أكثر من شخص لإكمال هذه المراحل وبصلاحيات مختلفة.
إطار سياسة المرسل Sender Policy Framework	طريقة للتحقق من أن خادم البريد الإلكتروني المستخدم في إرسال رسائل البريد الإلكتروني يتبع مجال المرسل الخاص بمقدمي الخدمات والمشتركين.
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 أنظمة 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.
المعلومات الاستباقية Threat Intelligence	يوفر معلومات منظمة وتحليلها حول الهجمات الأخيرة والحالية والمحتملة التي يمكن أن تشكل تهديدًا سيبرانيًا للجهة.
الثغرة Vulnerability	أي نوع من نقاط الضعف في نظام الحاسب الآلي، أو برامجه أو تطبيقاته، أو في مجموعة من الإجراءات، أو في أي شيء يجعل الأمن السيبراني عرضة للتهديد.

جدار الحماية لتطبيقات الويب Web Application Firewall	نظام حماية يوضع قبل تطبيقات الويب لتقليل المخاطر الناجمة عن محاولات الهجوم الموجهة إلى تطبيقات الويب.
البرمجيات الضارة غير المعروفة مسبقًا Zero-Day Malware	عبارة عن برمجيات ضارة (Malware) غير معروفة مسبقًا، تم إنتاجها أو نشرها حديثًا، ويصعب في العادة اكتشافها بواسطة وسائل الحماية التي تعتمد على المعرفة المسبقة للبرمجيات الضارة (Signature-based Protection).
شخص Person	الشخص الطبيعي، أو المعنوي (مثل: الشركات) بحسب الحال.
جهة Organization	أي جهة حكومية في المملكة العربية السعودية (وتشمل الوزارات والهيئات والمؤسسات وغيرها) والجهات والشركات التابعة لها، وجهات القطاع الخاص التي تمتلك بنى تحتية وطنية حساسة أو تقوم بتشغيلها أو استضافتها.
المشترك Cloud Customer	أي شخص يشترك في خدمات الحوسبة السحابية التي يوفرها مقدم الخدمة.
مقدم الخدمة Cloud Service Provider (CSP)	أي شخص 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.
البيانات Data	أي معلومات، أو سجلات، أو إحصاءات، أو وثائق مصورة، أو مسجلة ومخزنة بطريقة إلكترونية.

الحوسبة السحابية Cloud Computing	نموذج لتمكين الوصول عند الطلب إلى مجموعة مشتركة من موارد تقنية المعلومات (مثل: الشبكات والخوادم والتخزين والتطبيقات والخدمات) التي يمكن توفيرها بسرعة وإطلاقها بالحد الأدنى من الجهد الإداري التشغيلي والتدخل/التفاعل لإعداد الخدمة من مزود الخدمة. تسمح الحوسبة السحابية للمستخدمين بالوصول إلى الخدمات القائمة على التقنية من خلال شبكة الحوسبة السحابية دون الحاجة لوجود معرفة لديهم أو تحكم في البنية التحتية التقنية التي تدعمهم. يتألف نموذج الحوسبة السحابية من خمس خصائص أساسية: خدمة ذاتية حسب الطلب، ووصول إلى الشبكة بشكل واسع، ومجمع الموارد، ومرونة سريعة، والخدمة المقاسة. وهناك ثلاثة نماذج لتقديم خدمات الحوسبة السحابية وهي: البرمجيات السحابية كخدمة "Software-as-Service "Saas ، والنظام أو المنصة السحابية كخدمة "Platform-as-Service "PaaS ، والبنية التحتية السحابية كخدمة"Infrastructure-as-Service "IaaS. كما أن هناك أربعة نماذج للحوسبة السحابية حسب طبيعة الدخول: الحوسبة السحابية العامة، والحوسبة السحابية المجتمعية، والحوسبة السحابية الخاصة، والحوسبة السحابية الهجين.
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.
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.
المستوى ٣ Level 3	مستوى تصنيف يستخدم للبيانات المصنفة (مقيد) بحسب ما يصدر من الجهة المختصة، والمستوى ٣ هو المستوى الأدنى لاستضافة الأنظمة الحساسة وما تحويه من بيانات.
المستوى ٤ Level 4	مستوى تصنيف يستخدم للبيانات المصنفة (متاح) بحسب ما يصدر من الجهة المختصة.
بيانات مصنفة Classified Data	أي بيانات مصنفة على أحد المستويات التالية: المستوى ١، أو المستوى ٢، أو المستوى ٣، أو المستوى ٤.

الملحق (ب): 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
BYOD	Bring Your Own Device أحضِرْ الجهاز الخاص بك
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
DNS	Domain Name System نظام أسماء النطاقات
ECC	Essential Cybersecurity Controls الضوابط الأساسية للأمن السيبراني
HTTPS	Hyper Text Transfer Protocol Secure برتوكول نقل النص التشعبي الآمن
ICS	Industrial Control System نظام التحكم الصناعي
ICT	Information and Communication Technology تقنية المعلومات والاتصالات

IT	Information Technology تقنية المعلومات
MFA	Multi-Factor Authentication التحقق من الهوية متعدد العناصر
OT	Operational Technology التقنية التشغيلية
SIEM	Security Information and Event Management نظام سجلات الأحداث ومراقبة الأمن السيبراني
SIS	Safety Instrumented System نظام معدات السلامة
SLA	Service Level Agreement اتفاقية مستوى الخدمة
CTS	Cloud Technology Stack أنظمة CTS


الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority