الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

الدليل الإرشادي لتطبيق ضوابط الأمن السيبراني للحوسبة السحابية للمشتركين

Guide to Cloud Cybersecurity Controls For Service Tenants Implementation
(GCCC-CST – 1 : 2023)

إشارة المشاركة: أبيض
تصنيف الوثيقة: عام

إخلاء مسؤولية: طُور هذا الدليل الإرشادي عن طريق الهيئة الوطنية للأمن السيبراني لتمكين الجهات من تطبيق ضوابط الأمن السيبراني للحوسبة السحابية للمشتركين، كما تخلي الهيئة الوطنية للأمن السيبراني مسؤوليتها من الاعتماد على هذه الوثيقة فقط؛ وتؤكد على ضرورة الأخذ بعين الاعتبار المتطلبات الخاصة بالجهة وبيئتها؛ وتؤكد الهيئة الوطنية للأمن السيبراني بأن هذه الوثيقة ماهي إلا دليل إرشادي يمكن استخدامه كمثال ولا تعني بالضرورة أن تكون الطريقة الوحيدة لتطبيق الضوابط على ألا تتعارض الطرق الأخرى مع متطلبات الهيئة الوطنية للأمن السيبراني. تحتوي هذه الوثيقة على بعض الأمثلة للمخرجات ذات العلاقة بتطبيق الضوابط، ويحق للمقيم أو المدقق أن يطلب أدلة أخرى حسب ما يراه المقيم أو المدقق لضمان التأكد من تطبيق جميع الضوابط.

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 للإستلام.

برتقالي – مشاركة محدودة

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

أخضر – مشاركة في نفس المجتمع

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

أبيض – غير محدود

قائمة المحتويات

مقدمة..... ٥
الهدف..... ٥
نطاق العمل..... ٥
مكونات وهيكلية ضوابط الأمن السيبراني للحوسبة السحابية..... ٦
هيكلية الدليل الإرشادي..... ٧
إرشادات عامة لتطبيق ضوابط الأمن السيبراني للحوسبة السحابية..... ٨
إرشادات تطبيق ضوابط الأمن السيبراني للحوسبة السحابية للمشتركين ٩

قائمة الأشكال

شكل ١: المكونات الأساسية والفرعية لضوابط الأمن السيبراني للحوسبة السحابية ٦
شكل ٢: هيكلية الدليل الإرشادي لتطبيق ضوابط الأمن السيبراني للحوسبة السحابية..... ٧

مقدمة

طورت الهيئة الوطنية للأمن السيبراني (ويشار لها في هذه الوثيقة بـ "الهيئة") الدليل الإرشادي لتطبيق ضوابط الأمن السيبراني المنصوص عليها في ضوابط الأمن السيبراني للحوسبة السحابية (CCC - 1: 2020) المتعلقة بالمشتركين (ويشار لها في هذه الوثيقة بـ "الضوابط")، وذلك للمساهمة في تمكين الجهات الوطنية من تطبيق متطلبات الالتزام بضوابط الأمن السيبراني للحوسبة السحابية. حيث تم بناء هذا الدليل الإرشادي بالاعتماد على المعلومات والخبرات التي قامت الهيئة بجمعها وتحليلها منذ نشر الضوابط ومواءمة هذا الدليل الإرشادي مع أفضل الممارسات الرائدة في الأمن السيبراني لتسهيل تطبيق الضوابط في الجهات الوطنية.

الهدف

الهدف الرئيسي من هذا الدليل الإرشادي هو المساهمة في تمكين الجهات الوطنية لتحقيق متطلبات الالتزام بتطبيق ضوابط الأمن السيبراني للحوسبة السحابية للمشتركين في الجهة، وذلك بهدف رفع وتعزيز مستوى الأمن السيبراني لديها، وتقليل مخاطر الأمن السيبراني المتعلقة بالحوسبة السحابية التي تنشأ من التهديدات السيبرانية الداخلية والخارجية.

نطاق العمل

نطاق العمل لهذا الدليل ينطبق على المشتركين كما هو مذكور في ضوابط الأمن السيبراني للحوسبة السحابية (CCC - 1: 2020) وهو:

- 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.
- يقصد 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 بنية تحتية وطنية حساسة أو تقوم بتشغيلها أو استضافتها الذين يستخدمون حاليًا أو يخططون لاستخدام أي من خدمات الحوسبة السحابية.
- تشجع الهيئة الجهات الأخرى في المملكة وبشدة على الاستفادة من هذه الضوابط لتطبيق أفضل الممارسات في ما يتعلق بتحسن الأمن السيبراني وتطويره داخل الجهة.

مكونات وهيكلية ضوابط الأمن السيبراني للحوسبة السحابية

يوضح الشكل رقم (١) أدناه المكونات الأساسية والفرعية لضوابط الأمن السيبراني للحوسبة السحابية.

١	حوكمة الأمن السيبراني Cybersecurity Governance	١-١	أدوار ومسؤوليات الأمن السيبراني Cybersecurity Roles and Responsibilities	١-٢	إدارة مخاطر الأمن السيبراني Cybersecurity Risk Management
		١-٣	الالتزام بتشريعات وتنظيمات ومعايير الأمن السيبراني Compliance with Cybersecurity Standards, Laws and Regulations	١-٤	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	٢-٤	إدارة أمن الشبكات Networks Security Management
		٢-٥	أمن الأجهزة المحمولة Mobile Devices Security	٢-٦	حماية البيانات والمعلومات Data and Information Protection
		٢-٧	التشفير Cryptography	٢-٨	إدارة النسخ الاحتياطية Backup and Recovery Management
		٢-٩	إدارة الثغرات Vulnerability Management	٢-١٠	اختبار الاختراق Penetration Testing
		٢-١١	إدارة سجلات الأحداث ومراقبة الأمن السيبراني Cybersecurity Event Logs and Monitoring Management	٢-١٢	إدارة حوادث وتهديدات الأمن السيبراني Cybersecurity Incident and Threat Management
		٢-١٣	الأمن المادي Physical Security	٢-١٤	حماية تطبيقات الويب Web Application Security
		٢-١٥	إدارة المفاتيح Key Management	٢-١٦	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 ١: المكونات الأساسية والفرعية لضوابط الأمن السيبراني للحوسبة السحابية

هيكلية الدليل الإرشادي

يوضح الشكل رقم (٢) أدناه هيكلية الدليل الإرشادي لتطبيق ضوابط الأمن السيبراني للحوسبة السحابية.

	١	اسم المكون الأساسي
	الرقم المرجعي للمكون الأساسي	
	الرقم المرجعي للمكون الفرعي	اسم المكون الفرعي
	الهدف	
	الضوابط	
الرقم المرجعي للضابط	بنود الضابط	
	إرشادات تطبيق الضوابط:	
	المخرجات المتوقعة:	

شكل ٢: هيكلية الدليل الإرشادي لتطبيق ضوابط الأمن السيبراني للحوسبة السحابية

إرشادات تطبيق ضوابط الأمن السيبراني للحوسبة السحابية

إرشادات عامة
• تحديد خدمات الحوسبة السحابية التي تستفيد منها الجهة، وتحديد مستوى تصنيف البيانات التي تخزنها أو تعاجلها الخدمات بما يتواءم مع ما هو مذكور في وثيقة ضوابط الأمن السيبراني للحوسبة السحابية (CCC-1:2020)، مع الأخذ بالاعتبار المتطلبات التشريعية والتنظيمية ذات العلاقة. • حصر الأصول المتعلقة بالخدمات السحابية، ومراجعتها وتحديثها بشكل سنوي. • حصر حسابات المستخدمين ذوي الصلاحيات الهامة والحساسة (Privileged Accounts) والذين لديهم القدرة على إدارة الخدمات السحابية في الجهة، ومراجعتها بشكل دوري. • تحديد وتوثيق متطلبات الأمن السيبراني للحوسبة السحابية والأدوار والمسؤوليات المتعلقة بها، واعتمادها من قبل صاحب الصلاحية ومراجعتها بشكل دوري. • مراجعة الدليل الإرشادي لتطبيق الضوابط الأساسية للأمن السيبراني والعمل على تطبيق الضوابط ذات العلاقة بضوابط الأمن السيبراني للحوسبة السحابية للمشتركين. • وضع خطة لتطبيق ضوابط الأمن السيبراني للحوسبة السحابية للمشتركين، ومتابعتها بشكل مستمر.

إرشادات تطبيق ضوابط الأمن السيبراني للحوسبة السحابية للمشتركين

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-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.
		أدوات الأمن السيبراني ذات العلاقة: • نموذج أدوار ومسؤوليات الأمن السيبراني **إرشادات تطبيق الضوابط:** • العمل على تحديد الخدمات السحابية المستخدمة وأصحاب المصلحة المعنيين بالأمن السيبراني على الصعيدين الداخلي والخارجي (على سبيل المثال: مزود الخدمة ووحدات الأمن السيبراني الخاصة بهم ، وعمليات الأمن السيبراني للشركات السحابية ، وممثلي الخدمات المُدارة لحماية الحوسبة السحابية ، وممثلي أمن الحوسبة السحابية كخدمة (SaaS) ، ومكتب المشاريع ، والمستفيدين من الخدمة).
		المخرجات المتوقعة: • وثيقة أدوار ومسؤوليات الأمن السيبراني في خدمة الحوسبة السحابية ومصفوفة (RACI) واعتمادها وتوثيقها ضمن اتفاقيات مستوى الخدمة ذات الصلة (SLAs) بين مزود الخدمة والمشترك.

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-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.
		أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة إدارة مخاطر الأمن السيبراني **إرشادات تطبيق الضوابط:** بالإضافة إلى إرشادات تطبيق الضابط ١-٥ في الدليل الإرشادي لتطبيق الضوابط الأساسية للأمن السيبراني: • العمل على تحديد الخدمات السحابية قيد الاستخدام وتحليل تأثيرها على الأعمال اليومية التي تستعمل خدمات الحوسبة السحابية داخل المنشأة (على سبيل المثال: تحليل تأثير الخدمة السحابية المقدمة في عملية رفع الوثائق) لفهم وتقييم الأثر في حال تعطل الخدمة ، وتسرب البيانات، ومخاطر الوصول غير المصرح به ، ونطاق الضرر الذي قد يتسبب فيه أحد مشكلات الحوسبة السحابية. • العمل على تحديد مستويات المخاطر للخدمات السحابية (على سبيل المثال: حرجة ، عالية ، متوسطة ، منخفضة) بناءً على منهجية ادارة مخاطر الامن السيبراني في الجهة والعمل على تطبيق الاجراءات اللازمة حسب مستوى الخطر.
		المخرجات المتوقعة: • سجل الخدمات السحابية مع تحديد مستوى المخاطر المقبولة.
	١-٢-ش-١-٢	أخذ تصنيف البيانات والمعلومات بالاعتبار في منهجية إدارة مخاطر الأمن السيبراني.
		أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة إدارة مخاطر الأمن السيبراني

		• نماذج عمليات إدارة المخاطر السيبرانية **إرشادات تطبيق الضوابط:** • العمل على تحديد البيانات التي تمت معالجتها ، وتخزينها ، ونقلها ، واستخدامها ، والتخلص منها في الجهة وتصنيفها إلى فئات متفق عليها (على سبيل المثال: عامة ، مقيدة ، سرية ، سرية للغاية) بناءً على قيمة وحساسية البيانات التي تعود على الجهة ، وتضمينها في منهجية إدارة مخاطر الأمن السيبراني.
		المخرجات المتوقعة: • منهجية إدارة مخاطر الأمن السيبراني مع نهج محدد لتصنيف البيانات.
	١-٢-ش-١-٣	إنشاء سجل لمخاطر الأمن السيبراني خاص بالعمليات وخدمات الحوسبة السحابية، ومتابعته دورياً بما يتناسب مع طبيعة المخاطر.
		أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة إدارة مخاطر الأمن السيبراني • نموذج سجل مخاطر الأمن السيبراني **إرشادات تطبيق الضوابط:** • العمل على تحديد المخاطر المتعلقة بالخدمات السحابية ومقدمي خدمات الحوسبة السحابية - استخدام المعلومات الاستباقية للتهديدات وسجلات الاستجابة للحوادث لتحليل المخاطر المطبقة على الخدمات السحابية (على سبيل المثال: تسرب البيانات بسبب سوء تهيئة خدمة التخزين السحابي العامة أو بسبب المصادقة الضعيفة) ومتابعتها دورياً بما يتناسب مع طبيعة وتصنيف الخطر حتى يتم معالجتها بالاولية.
		المخرجات المتوقعة: • سجل مخاطر الأمن السيبراني لخدمات الحوسبة السحابية. • خطة مراجعة سجل 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-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.
		أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الالتزام بتشريعات وتنظيمات الأمن السيبراني • نموذج سياسة مراجعة وتدقيق الأمن السيبراني • نموذج سياسة مراجعة وتدقيق الأمن السيبراني • نموذج سجل خطة تدقيق الأمن السيبراني **إرشادات تطبيق الضوابط:** • العمل على تحديد التشريعات واللوائح الوطنية المتعلقة بالأمن السيبراني للخدمات السحابية ومقدمي الخدمات السحابية. • العمل على مراجعة العقد المقرر قبل وبعد الاتفاق مع مزود الخدمة السحابية فيما يتعلق بالتزامات الأمن السيبراني. التحقق منها بانتظام وضمان المراقبة الدائمة والمستمرة لمدى التزام مقدم الخدمة السحابية بالتشريعات، وبنود العقد المقرر المتعلقة بالأمن السيبراني (على سبيل المثال: يمكن التحقق من التزام مزود الخدمة السحابية بالإبلاغ عن ثغرات المشترك إذا تم تسليم هذه التقارير أو تبريرها). • التأكد من طلب تقارير الامتثال الخاصة بمقدم الخدمة السحابية (على سبيل المثال: بجعلها مطلباً تعاقدياً). • التأكد من مراقبة امتثال مقدم الخدمة السحابية بطريقة مستمرة (مثل التحقق اليومي أو الأسبوعي) باستخدام أدوات تقنية مؤتمتة أو في الوقت الفعلي (مثل الفحوصات الآلية).	
		المخرجات المتوقعة: • تقارير أو إثبات متابعة التزام مقدم الخدمة بشكل دوري (و ما اذا يتم اتمتة ذلك). • تقارير أو إثبات يوضح متابعة الالتزام ضمن العقود.
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-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).
		أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للموارد البشرية **إرشادات تطبيق الضوابط:** • مراجعة المسميات والأوصاف الوظيفية للواجبات في مجالات إدارة المفاتيح (بما في ذلك التشفير) ، وإدارة الخدمات السحابية التقنية ، وإدارة هويات الدخول والصلاحيات والتحكم بالوصول والتأكد من أن المرشحين لهذه الوظائف يخضعون للمسح الأمني والتدقيق (على سبيل المثال: مهندس الوصول إلى خدمات الحوسبة السحابية ، مسؤول الخدمة السحابية ، مهندس أمان Key Vault).
		المخرجات المتوقعة: • سجل أدوار المستخدمين ذوي الصلاحيات (بما في ذلك إدارة المفاتيح وإدارة الخدمة والتحكم في الوصول). • وثيقة أو إثبات عملية المسح الأمني للمرشحين الذين لهم حق الوصول إلى المهام الحساسة لخدمات الحوسبة السحابية.

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 للجهة ودقتها وتوافرها.	
الضوابط		
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.
		أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة إدارة الأصول **إرشادات تطبيق الضوابط:** • العمل على تحديد الخدمات السحابية المستخدمة (على سبيل المثال: من خلال مراجعة العقد ، ومراجعة البنية التحتية للحلول ، ومراقبة اتصالات الشبكة النشطة) • العمل على تحديد البيانات المخزنة أو المعالجة في الخدمات السحابية (مثل: مراجعة الخدمات السحابية لتدفقات البيانات ومخازن البيانات). • العمل على تحديد أصول التقنية السحابية أو مجموعة الأصول (على سبيل المثال: مراجعة الخدمات السحابية للمكونات التقنية قيد الاستخدام). مع الأخذ بالاعتبار مكونات البنية التحتية كخدمة (IaaS) ووظائف قابلية التوسع التلقائي. • التأكد من الاحتفاظ بقوائم جرد للخدمات السحابية والبيانات والأصول التقنية (على سبيل المثال: إنشاء قاعدة بيانات للخدمات السحابية والبيانات المخزنة، و الأصول المعالجة، والتقنية المشاركة في هذه العمليات).
		المخرجات المتوقعة: • سجل حصر الخدمات السحابية والبيانات والأصول ذات الصلة.
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-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.
		أدوات الأمن السيبراني ذات العلاقة: • نموذج معيار إدارة هويات الدخول والصلاحيات، بحيث يشمل إدارة كلمات المرور • نموذج سياسة إدارة هويات الدخول والصلاحيات **إرشادات تطبيق الضوابط:** بالإضافة إلى الضوابط الفرعية في الدليل الإرشادي لتطبيق الضوابط الأساسية للأمن السيبراني في ECC 2-2-3: • تحليل وموائمة نموذج هويات الدخول والصلاحيات لجميع الحسابات ذي الصلة بالخدمات السحابية مع الادوار والمسؤوليات (على سبيل المثال: RBAC ، ومبادئ الخدمة ، والسياسات ، والموارد). • الادارة الامنة والفعالة لهويات الدخول والصلاحيات. • الاستفادة من المصادقة الموحدة. • تفعيل التحقق من الهوية متعدد العناصر.
		المخرجات المتوقعة: • وثيقة عملية دورة حياة هويات الدخول والصلاحيات الى الخدمات السحابية.
	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).
		أدوات الأمن السيبراني ذات العلاقة: • نموذج معيار إدارة هويات الدخول والصلاحيات، بحيث يشمل إدارة كلمات المرور • نموذج سياسة إدارة هويات الدخول والصلاحيات

		إرشادات تطبيق الضوابط: • العمل على تقييد الوصول إلى إدارة الهوية وأنظمة إدارة الوصول للموظفين المخصصين (على سبيل المثال: موظفو عمليات IAM , استخدام مبدأ الحاجة للمعرفة "Need to Know"). • العمل على جعل طرق المصادقة التقنية مشفرة (على سبيل المثال: TLS للوصول الى الخدمة السحابية, إغلاق الجلسة بناء على أفضل الممارسات). **المخرجات المتوقعة:** • إثبات يؤكد على تطبيق تسجيل الدخول فقط عبر القنوات المشفرة (مثل TLS).
	٢-٢-ش-١-٣	الإدارة الآمنة للجلسات (Secure Session Management)، وتشمل موثوقية الجلسات (Authenticity)، وإقفالها (Lockout)، وإنهاء مهلتها (Timeout). **أدوات الأمن السيبراني ذات العلاقة:** • نموذج معيار إدارة هويات الدخول والصلاحيات، بحيث يشمل إدارة كلمات المرور • نموذج سياسة إدارة هويات الدخول والصلاحيات • نموذج سياسة الإعدادات والتحصين • نموذج معيار الإعدادات والتحصين الآمن **إرشادات تطبيق الضوابط:** • العمل على ربط الجلسات من خلال الوكلاء المعتمدين (Authenticated Proxies) مع إمكانية إنهاء الجلسات. • التأكد من تكوين نظام إدارة الجلسة لإغلاق الجلسات ومهلة الجلسة (على سبيل المثال: إغلاق الجلسة بعد ٥ دقائق والمهلة بعد ١٠ دقائق من عدم تنشيط الجلسة). **المخرجات المتوقعة:** • نظام إدارة الجلسات وتشمل موثوقية الجلسات وإقفالها وإنهاء مهلتها.
	٢-٢-ش-١-٤	التحقق من الهوية متعدد العناصر لكافة الحسابات السحابية للمستخدمين ذوي الصلاحيات الهامة والحساسة.

		أدوات الأمن السيبراني ذات العلاقة: • نموذج معيار إدارة هويات الدخول والصلاحيات، بحيث يشمل إدارة كلمات المرور • نموذج سياسة إدارة هويات الدخول والصلاحيات **إرشادات تطبيق الضوابط:** • العمل على تحديد المهام الحساسة لخدمات الحوسبة السحابية (على سبيل المثال: التعديلات في الوظائف: الإدارة الرئيسية ، وإدارة الهوية والوصول ، وإدارة الخدمة). • العمل على تحديد الأدوار والهويات ذات الصلاحيات الهامة التي تستخدم هذه الصلاحيات (مثل: دور مهندس نظام إدارة هويات الدخول(IAM) للحلول السحابية). • إنشاء سياسة التحقق من الهوية متعدد العناصر (على سبيل المثال: استخدام مصادقة البرامج ، و استخدام الهاتف المحمول) وتعيينها إلى مستخدمين ذوي الصلاحيات أو مجموعات من المستخدمين.
		المخرجات المتوقعة: • سياسة التحقق من الهوية متعدد العناصر للمستخدمين ذوي الصلاحيات أو مجموعات المستخدمين. • إثبات يوضح قائمة مستخدمي السحابة 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)).
		أدوات الأمن السيبراني ذات العلاقة: • نموذج معيار إدارة هويات الدخول والصلاحيات، بحيث يشمل إدارة كلمات المرور • نموذج سياسة إدارة هويات الدخول والصلاحيات **إرشادات تطبيق الضوابط:** بالإضافة إلى الضوابط الفرعية في الدليل الإرشادي لتطبيق الضوابط الأساسية للأمن السيبراني في ECC 2-2-3: • تمكين كلمة مرور الخدمة الذاتية لإعادة التعيين وإدارة كلمة المرور. • إنشاء إشعارات البريد الإلكتروني و الهاتف المحمول لمصادقة الحساب السحابي للتأكد من أن مالك الحساب قد تم إشعاره بشأن مصادقة الحساب.

		• حظر استخدام نفس الحساب من مواقع مختلفة. • إعداد التنبيهات والإشعارات لمحاولات عمليات الدخول غير الناجحة (Unsuccessful Login) ومراقبتها ضمن أعمال مراقبة الأحداث. • تقييد المستخدم عند تجاوز الحد الأقصى من محاولات عمليات الدخول غير الناجحة (Unsuccessful Login).
		المخرجات المتوقعة: • وثائق توضح إجراءات لكشف محاولات الوصول غير المصرح به ومنعها.
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-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.
		أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة مراجعة وتدقيق الأمن السيبراني • نموذج سياسة مراجعة وتدقيق الأمن السيبراني • نموذج سجل خطة تدقيق الأمن السيبراني • نموذج معيار امن الخوادم **إرشادات تطبيق الضوابط:** • العمل على مراجعة عمليات التدقيق المستقلة لمزود الخدمة والتأكد من العزل الفعال للحوسبة السحابية المشتركة عن السحب العامة وغيرها من السحابات المشتركة (على سبيل المثال: مراجعة ضوابط العزل المادي ، وضوابط العزل المنطقية).

		المخرجات المتوقعة: • إثبات يوضح التحقق من عزل الحوسبة السحابية المشتركة بالوسائل المتفق عليها بين مقدم الخدمة والمشترك دوريا.
٢-٤	إدارة أمن الشبكات (Networks Security Management)	
الهدف	ضمان حماية شبكات مقدمي الخدمات والمشتركين من المخاطر السيبرانية.	
الضوابط		
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.
		أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة امن الشبكات • نموذج معيار امن الشبكات **إرشادات تطبيق الضوابط:** • العمل على تحديد متطلبات الأمان للاتصال بموفري خدمات الحوسبة السحابية من حيث السرية والتكامل وتوافر البيانات المنقولة من خلال هذه الاتصالات (على سبيل المثال: جدار الحماية، التشفير أثناء النقل ، وتكرار الاتصال ، والاتصال الفاشل ، والحماية من هجمات حجب الخدمة ، ومصادقة الشبكة الافتراضية الخاصة). • العمل على تصميم وتنفيذ اتصال الشبكة وفقًا لذلك (على سبيل المثال: استخدام مزود خدمة إنترنت منفصلين لمنطقتين حيث يعمل مقدم الخدمة الحوسبة السحابية باستخدم شبكة الافتراضية الخاصة). • العمل على تحديد خطة التعافي من الكوارث للاتصال السحابي.
		المخرجات المتوقعة: • إثبات يوضح خطة التعافي من الكوارث للاتصال الشبكي للمشترك إلى مقدم الخدمة. • وثيقة مخطط الشبكة الذي يوضح تطبيق ممارسات الأمن السيبراني لحماية الاتصال الشبكي بين المشترك ومقدم 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-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. **أدوات الأمن السيبراني ذات العلاقة:** • نموذج سياسة أمن أجهزة المستخدمين والأجهزة المحمولة والأجهزة الشخصية • نموذج معيار امن أجهزة المستخدمين • نموذج معيار امن الأجهزة المحمولة **إرشادات تطبيق الضوابط:** • العمل على تحديد أجهزة المستخدم النهائي التي لديها إمكانية الوصول إلى الخدمات السحابية (على سبيل المثال: الهواتف والأجهزة المكتبية والأجهزة المحمولة). • العمل على تحديد طرق فعالة لإعادة الاستخدام والتخلص منها والتقنيات ذات الصلة (مثل: الجهاز الذي سيتم مسحه باستخدام نظام إدارة الأجهزة المحمولة). • بناء العمليات والحلول لتأمين الأجهزة (على سبيل المثال: استخدام نظام إدارة الأجهزة المحمولة مع ميزات مسح البيانات للجهاز المطلوب). **المخرجات المتوقعة:** • وثيقة معتمدة تحدد تنفيذ أدوات وإجراءات إعادة استخدام والتخلص من الأجهزة .
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-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 مقدمي الخدمة، 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).
		أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للبيانات • نموذج معيار الأمن السيبراني للبيانات **إرشادات تطبيق الضوابط:** • العمل على تحليل القدرات التقنية السحابية للتخلص الآمن من البيانات المخزنة في التخزين السحابي (على سبيل المثال: تشفير البيانات باستخدام مفتاح المشترك المُدار بما في ذلك التخلص من المفتاح). • العمل على تحديد استراتيجية الخروج من السحابة بما في ذلك التخلص من مفتاح التشفير لجعل بيانات المشترك مشفرة في البنية التحتية لمقدم الخدمة بعد المغادرة.
		المخرجات المتوقعة: • وثيقة توضح إستراتيجية الخروج من السحابة. • إثبات يؤكد وجود خدمة مقدمة من مقدم الخدمة تسمح للمشترك بالتخلص من البيانات بصورة آمنة أو على الأقل أن يكون ضمن العقد بين المشترك ومقدم الخدمة إعطاء المشترك القدرة على التخلص من البيانات.
	٢-٦-ش-١-٢	استخدام وسائل آمنة لتصدير ونقل البيانات والبنية التحتية الافتراضية.
		إرشادات تطبيق الضوابط: • العمل على تحليل قابلية نقل الحلول التي تم نشرها إلى مقدم الخدمة (على سبيل المثال: الاعتماد على الخدمات والميزات والتقنيات الأصلية لمقدم الخدمة). • التأكد من تنسيق البيانات وتصدير القدرات التقنية للبيانات في الخدمات السحابية (على سبيل المثال: استخدام تنسيقات وبروتوكولات البيانات الموحدة).

		• التأكد من ضمان إمكانية نقل الأصول والبيانات الافتراضية بأمان (على سبيل المثال: من خلال القنوات المشفرة) عند الطلب.
		المخرجات المتوقعة: • وثيقة توضح تحديد وتوثيق المتطلبات المحددة والحلول الأمنية المطبقة ذات الصلة بتصدير 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-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).
		أدوات الأمن السيبراني ذات العلاقة: • نموذج معيار التشفير • نموذج معيار إدارة مفاتيح التشفير • نموذج سياسة التشفير **إرشادات تطبيق الضوابط:** • العمل على تطوير معيار تشفير وفقًا للمستوى المتقدم (Advanced) بما يتماشى مع معايير التشفير الوطنية (NCS-1: 2020).
		المخرجات المتوقعة • وثائق تؤكد تطبيق معيار التشفير.
	٢-٧-ش-١-٢	تشفير البيانات والمعلومات المنقولة إلى الخدمات السحابية، أو المنقولة منها، بحسب المتطلبات التشريعية والتنظيمية ذات العلاقة.

		أدوات الأمن السيبراني ذات العلاقة: • نموذج معيار التشفير • نموذج سياسة التشفير • نموذج معيار إدارة مفاتيح التشفير **إرشادات تطبيق الضوابط:** • العمل على تحديد الضوابط والاجراءات المتعلقة بنقل ومشاركة البيانات السحابية (على سبيل المثال: معايير التشفير الوطنية) والتحقق من الامتثال لهذه اللوائح.
		المخرجات المتوقعة: • وثيقة تؤكد تشفير منافذ الاتصال السحابي عند عملية النقل والمشاركة وتمرير البيانات.
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-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.
		أدوات الأمن السيبراني ذات العلاقة: • نموذج إجراء تقييم الثغرات الأمنية • نموذج سياسة إدارة الثغرات • نموذج معيار إدارة الثغرات • نموذج سجل الثغرات **إرشادات تطبيق الضوابط:**

		• العمل على تحديد وتنفيذ سياسة إدارة الثغرات التي تتضمن القصد والغرض والحوكمة لكيفية معالجة المشترك للثغرات الخاصة بالخدمات السحابية، وكحد أدنى يجب أن تحدد السياسة: ○ التقييمات الدورية (مثل التقييمات ربع السنوية) ، ○ الفترات المقبولة لمعالجة التهديدات والثغرات - ثلاثة أشهر. ○ أدوات لاكتشاف الثغرات (مثل ادوات فحص ثغرات الويب). ○ المكونات التي سيتم تغطيتها ضمن النطاق مع مراعاة القوانين واللوائح المعمول بها والمتطلبات التعاقدية. ○ مستويات الثغرات ذات الصلة بالجهة. ○ آليات الإبلاغ عن الثغرات (الكيفية ولمن يجب الإبلاغ) ومراجعتها ، لا سيما نقاط الضعف الهامة. ○ كيف يتم تتبع إجراءات المعالجة.
		المخرجات المتوقعة: • وثيقة توضح إنشاء وضمان تنفيذ سياسة إدارة الثغرات تتضمن الحوسبة السحابية. • تقرير 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.
		أدوات الأمن السيبراني ذات العلاقة: • نموذج إجراء تقييم الثغرات الأمنية • نموذج سياسة إدارة الثغرات • نموذج معيار إدارة الثغرات • نموذج سجل الثغرات **إرشادات تطبيق الضوابط:** • العمل على تحديد وتنفيذ سياسة إدارة الثغرات التي تتضمن القصد والغرض والحوكمة لكيفية معالجة المشترك للثغرات الخاصة بالخدمات السحابية، وكحد أدنى يجب أن تحدد السياسة: ○ كيف يتم إشعار المشترك بشأن الثغرات الأمنية التي اكتشفها مقدم الخدمة. ○ طرق تقييم الثغرات. ○ كيف يتم تتبع إجراءات المعالجة.

		المخرجات المتوقعة: • وثيقة توضح إنشاء وضمان تنفيذ سياسة إدارة الثغرات تتضمن الحوسبة السحابية. • تقرير إدارة الثغرات التي تم إشعار المشترك بها عن طريق مقدم الخدمة، ومعالجتها.
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-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.
		أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة إدارة سجلات الأحداث ومراقبة الأمن السيبراني • نموذج معيار إدارة سجلات الأحداث ومراقبة الأمن السيبراني **إرشادات تطبيق الضوابط:** • التأكد من تمكين تسجيل مصادقة الحساب وأحداث الأمن السيبراني الأخرى في الخدمات السحابية (على سبيل المثال: استخدام خدمة التسجيل الأصلية السحابية والوكلاء المرتبطين بها).
		المخرجات المتوقعة: • وثائق توضح سجل أحداث الأمن السيبراني للخدمات السحابية.
	٢-١١-ش-١-٢	أن تشمل عملية المراقبة جميع الأحداث أحداث الأمن السيبراني المفعلة على الخدمات السحابية الخاصة بالمشترك.
		أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة إدارة سجلات الأحداث ومراقبة الأمن السيبراني

	• نموذج معيار إدارة سجلات الأحداث ومراقبة الأمن السيبراني **إرشادات تطبيق الضوابط:** • العمل على تحديد حالات استخدام المراقبة ذات الصلة بالخدمات السحابية (على سبيل المثال: مراقبة تعديلات وصول المستخدم). • العمل على جمع سجلات الأمن السيبراني ذات الصلة بحالات استخدام المراقبة المحددة عبر الخدمات السحابية (على سبيل المثال: استدعاءات واجهة برمجة التطبيقات ذات الصلة بوصول المستخدم يتم التقاط التعديلات). • التأكد من مراقبة سجلات الأمن السيبراني للخدمات السحابية (على سبيل المثال: استخدام تقنيات السحابة الأصلية أو تقنيات النظام المركزي لجمع سجلات الأحداث (SIEM) الداخلية لتحليل السجلات لاكتشاف الحوادث الأمنية).
	المخرجات المتوقعة: • وثيقة تؤكد رصد سجلات أحداث الأمن السيبراني.
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-ش-١	يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني، الخاصة بعملية إدارة المفاتيح لدى المشتركين.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني المتعلق بالحوسبة السحابية والاستضافة • نموذج إجراء تطوير وثائق الأمن السيبراني **إرشادات تطبيق الضوابط:** • العمل على تحديد متطلبات الأمن السيبراني لجوانب الإدارة الرئيسية (على سبيل المثال: تبادل المفاتيح والتخزين والاستخدام والملكية) - استخدام الاستبيانات وعقد ورش العمل مع أصحاب المصلحة المعنيين. • العمل على تحديد واعتماد ومراجعة بانتظام (على سبيل المثال سنوياً) معيار الإدارة الرئيسية لتحديد متطلبات الأمن السيبراني.
	المخرجات المتوقعة: • وثيقة توضح متطلبات الأمن السيبراني لإدارة مفاتيح التشفير موثقة ومعتمدة بشكل رسمي. • نتائج المراجعة الدورية.
٢-١٥-ش-٢	يجب تطبيق متطلبات الأمن السيبراني، الخاصة بإدارة المفاتيح لدى المشتركين.

		إرشادات تطبيق الضوابط: • العمل على فرض معيار إدارة المفاتيح المحدد (مثل تقوية خدمة إدارة المفاتيح ، وتقييد التحكم في الوصول ، والمراقبة). • التأكد من التحكم في التنفيذ الفعال للمعيار. • العمل على الإبلاغ عن الانتهاكات للمعيار. • العمل على توثيق وإدارة الاستثناءات.
		المخرجات المتوقعة: • وثيقة لاعتماد تطبيق متطلبات الأمن السيبراني لإدارة مفاتيح التشفير. • وثيقة توضح إجراءات الابلاغ عن الانتهاكات للمعيار.
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).
		أدوات الأمن السيبراني ذات العلاقة: • نموذج معيار إدارة مفاتيح التشفير **إرشادات تطبيق الضوابط:** • العمل على تحديد المسؤوليات التي تأتي مع ملكية مفاتيح التشفير خلال دورة حياة المفتاح بالكامل (على سبيل المثال: إنشاء مفتاح ، والسماح باستخدام المفتاح ، والتخلص من المفتاح). • التأكد من تعيين ملكية مفاتيح التشفير لموظفي المشتركين. • العمل على مراجعة مفاتيح التشفير بانتظام (يجب أن يكون لكل مفتاح مالك نشط معين). • العمل على تعيين مالكي مفاتيح التشفير الجديدة كخطوة إلزامية عند إنشاء المفاتيح.
		المخرجات المتوقعة: • وثيقة تؤكد على تحديد مفاتيح التشفير وملاكها و مسؤولياتهم. • نتائج المراجعة الدورية.
	٢-١٥-ش-٣-٢	وجود آلية آمنة لاسترجاع مفاتيح التشفير في حال فقدانها مثل: (نسخها احتياطيًا وتخزينها بطرق آمنة خارج الأنظمة السحابية).

		أدوات الأمن السيبراني ذات العلاقة: • نموذج معيار إدارة مفاتيح التشفير **إرشادات تطبيق الضوابط:** • العمل على تطوير واختبار خطط استرداد مفتاح التشفير لفقدان مفتاح التشفير أو تلفها (على سبيل المثال: طباعة مفاتيح التشفير ووضعها في مظاريف ذات علامات وتخزينها في خزائن مادية في مواقع خارجية موثوقة وآمنة مثل صناديق الإيداع أو حاويات آمنة في البنوك). **المخرجات المتوقعة:** • وثيقة توضح خطة استرجاع مفتاح التشفير.
٢-١٥-ش-٤	يجب مراجعة متطلبات الأمن السيبراني، الخاصة بإدارة المفاتيح لدى المشتركين ، ومراجعة تطبيقها دورياً.	**أدوات الأمن السيبراني ذات العلاقة:** • نموذج يشرح دورة حياة عملية إدارة الإجراءات والسياسات ومعايير الأمن السيبراني، بما في ذلك البناء والتطوير والاعتمادات والمراجعات الدورية **إرشادات تطبيق الضوابط:** • العمل على مراجعة متطلبات الأمن السيبراني بشكل دوري للإدارة الرئيسية ، على الأقل سنوياً. • التأكد من الاحتفاظ بسجلات المراجعات الدورية (على سبيل المثال: من ومتى تمت مراجعتها وسجل التغيير). **المخرجات المتوقعة:** • وثيقة تؤكد على مراجعة متطلبات الأمن السيبراني لإدارة المفاتيح بشكل دوري.

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-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.
		أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني ضمن استمرارية الأعمال **إرشادات تطبيق الضوابط:** • العمل على تحديد متطلبات التعافي من الكوارث وإجراءات استمرارية الأعمال ، مع مراعاة المخاطر المحددة المتعلقة بالحوسبة السحابية (مثل: تسرب البيانات أو التعرض غير المقصود) • العمل على تطوير واعتماد وتنفيذ إجراءات / خطط التعافي من الكوارث واستمرارية الأعمال للحوسبة السحابية على أساس المتطلبات. • العمل على اختبار الإجراءات بانتظام وعلى التغييرات الهامة للتأكد من قابليتها للتطبيق.
		المخرجات المتوقعة: • وثيقة توضح إجراءات خطة التعافي من الكوارث للحوسبة السحابية. • وثيقة توضح إجراءات خطة استمرارية الأعمال للحوسبة السحابية.

الهيئة الوطنية
للأمن السيبراني
National Cybersecurity Authority