الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

الدليل الإرشادي لتطبيق ضوابط الأمن السيبراني للحوسبة السحابية لمقدمي الخدمات

Guide to Cloud Cybersecurity Controls for Service Providers Implementation

(GCCC-CSP – ٢ : ٢٠٢٦)

إشارة المشاركة: شفاف
تصنيف الوثيقة: عام

تنويه: لمواكبة المتغيرات بشأن تحديثات الوثائق الصادرة عن الهيئة الوطنية للأمن السيبراني، تود الهيئة الوطنية للأمن السيبراني التنويه على أهمية الاعتماد الدائم على نسخ الوثائق المنشورة في الموقع الإلكتروني للهيئة https://nca.gov.sa

إخلاء مسؤولية: طُور هذا الدليل الإرشادي لتمكين الجهات من تطبيق ضوابط الأمن السيبراني للحوسبة السحابية لمقدمي الخدمات، ومن الضروري عدم الاعتماد على هذه الوثيقة فقط؛ والأخذ 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. تحتوي هذه الوثيقة على بعض الأمثلة للمخرجات والأدلة ذات العلاقة بتطبيق الضوابط، ويحق للمقيم أو المدقق أن يطلب أدلة أخرى حسب ما يراه المقيم أو المدقق لضمان التأكد من تطبيق الضوابط بالشكل المناسب.

بسم الله الرحمن الرحيم

بروتوكول الإشارة الضوئية (TLP):

يستخدم هذا البروتوكول 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 أكان ذلك من داخل الجهة أم خارجها؛ خارج النطاق المحدد للاستلام.

برتقالي + مشدد (مشاركة في نفس الجهة)

المستلم يمكنه مشاركة المعلومات في الجهة نفسها مع الأشخاص المعنيين فحسب.

برتقالي (مشاركة محدودة)

المستلم يمكنه مشاركة المعلومات في الجهة نفسها مع الأشخاص المعنيين فحسب. ومن يتطلب الأمر منه اتخاذ إجراء يخص المعلومة.

أخضر (مشاركة في نفس المجتمع)

المستلم يمكنه مشاركة المعلومات مع آخرين في الجهة نفسها، أو جهة أخرى على علاقة معهم أو في القطاع نفسه؛ ولا يسمح بتبادلها أو نشرها من خلال القنوات العامة.

شفاف (غير محدود)

قائمة المحتويات

قائمة الأشكال

مقدمة

حدثت 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 - ٢: ٢٠٢٤) المتعلقة بمقدمي الخدمات (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 لمقدمي الخدمات في الجهة، وذلك بهدف رفع وتعزيز مستوى الأمن السيبراني لديها، وتقليل مخاطر الأمن السيبراني التي تنشأ من التهديدات السيبرانية الداخلية والخارجية.

نطاق العمل

نطاق العمل لهذا الدليل ينطبق على مقدمي الخدمات كما هو مذكور في ضوابط الأمن السيبراني للحوسبة السحابية (CCC - ٢: ٢٠٢٤) 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 بنى تحتية وطنية حساسة أو تقوم بتشغيلها أو استضافتها الذين يستخدمون حاليًا أو يخططون لاستخدام أي من خدمات الحوسبة السحابية.
- تشجع الهيئة وبشدة الجهات الأخرى في المملكة على الاستفادة من هذه الضوابط لتطبيق أفضل الممارسات فيما يتعلق بتحسين وتطوير الأمن السيبراني للحوسبة السحابية.

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.

<table>
<tr><td colspan="2">١</td><td>اسم المكون الأساسي</td></tr>
<tr><td colspan="2">الرقم المرجعي للمكون الأساسي</td><td></td></tr>
<tr><td colspan="2">الرقم المرجعي للمكون الفرعي</td><td>اسم المكون الفرعي</td></tr>
<tr><td colspan="3">الهدف</td></tr>
<tr><td colspan="3">الضوابط</td></tr>
<tr><td rowspan="3">الرقم المرجعي للضابط</td><td colspan="2">بنود الضابط</td></tr>
<tr><td colspan="2">إرشادات تطبيق الضوابط:</td></tr>
<tr><td colspan="2">المخرجات المتوقعة:</td></tr>
</table>

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

إرشادات تطبيق ضوابط الأمن السيبراني للحوسبة السحابية لمقدمي الخدمات

إرشادات عامة
• تحديد خدمات الحوسبة السحابية التي تقدمها الجهة، وتحديد مستوى تصنيف البيانات التي تخزنها أو تعالجها الخدمات بما يتوائم مع ما هو مذكور في وثيقة ضوابط الأمن السيبراني للحوسبة السحابية (CCC-٢:٢٠٢٤)، مع الأخذ بالاعتبار المتطلبات التشريعية والتنظيمية ذات العلاقة. • حصر الأصول والأنظمة التقنية السحابية لدى الجهة، 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 لمقدمي الخدمات. • وضع خطة لتطبيق ضوابط الأمن السيبراني للحوسبة السحابية لمقدمي الخدمات، ومتابعتها بشكل مستمر.

إرشادات تطبيق ضوابط الأمن السيبراني للحوسبة السحابية لمقدمي الخدمات

١ حوكمة الأمن السيبراني (Cybersecurity Governance)

١-١	أدوار ومسؤوليات الأمن السيبراني (Cybersecurity Roles and Responsibilities)	
الهدف	ضمان تحديد أدوار ومسؤوليات واضحة لجميع الأطراف المشاركة في تطبيق ضوابط الأمن السيبراني للحوسبة السحابية، بما في ذلك أدوار ومسؤوليات منصب رئيس مقدم الخدمة أو المشترك، أو من ينيبه، ويشار له في هذه الضوابط باسم «صاحب الصلاحية».	
الضوابط		
١-١-م-١	بالإضافة للضابط ١-٤-١ في الضوابط الأساسية للأمن السيبراني، يجب على صاحب الصلاحية تحديد وتوثيق واعتماد ما يلي:	
	١-١-م-١-١	أدوار الأمن السيبراني، وتكليفات المسؤولية والمحاسبة والاستشارة والتبليغ (RACI) لكل أصحاب العلاقة في خدمات الحوسبة السحابية، بما في ذلك أدوار ومسؤوليات صاحب الصلاحية.
		أدوات الأمن السيبراني ذات العلاقة: • نموذج أدوار ومسؤوليات الأمن السيبراني. • نموذج الهيكل التنظيمي للأمن السيبراني. **إرشادات تطبيق الضوابط:** • العمل على تحديد خدمات الحوسبة السحابية (على سبيل المثال: بناءً على منشورة دليل خدمات الحوسبة السحابية المقدمة) المقدمة والأطراف المعنيين بالأمن السيبراني الخاص بها داخل وخارج الجهة (على سبيل المثال: فرق معماري وهندسة وعمليات الأمن السيبراني للحوسبة السحابية، الأطراف الخارجية للخدمات المدارة المتعلقة بأمن الحوسبة السحابية، الأقسام ذات الصلاحية، مشتركي خدمات الحوسبة السحابية، إلخ).
		المخرجات المتوقعة: • وثيقة توضح مصفوفة الصلاحيات (RACI) والأدوار والمسؤوليات المتعلقة بالأمن السيبراني لخدمات الحوسبة السحابية موثقة ومعتمدة ومضمنة ضمن الاتفاقيات بين مقدم خدمات الحوسبة السحابية والمشتركين.

٢-١	إدارة مخاطر الأمن السيبراني (Cybersecurity Risk Management)	
الهدف	ضمان إدارة مخاطر الأمن السيبراني على نحو ممنهج يهدف إلى حماية الأصول المعلوماتية والتقنية لدى مقدمي الخدمات والمشتركين، وذلك وفقًا للسياسات والإجراءات التنظيمية لديهم والمتطلبات التشريعية والتنظيمية ذات العلاقة.	
الضوابط		
١-٢-م-١	يجب أن تتضمن منهجية إدارة مخاطر الأمن السيبراني المذكورة في المكون الفرعي ١- ٥ في الضوابط الأساسية للأمن السيبراني لدى مقدمي الخدمات بحد أدنى ما يلي:	
	١-٢-م-١-١	تحديد المستوى المقبول للمخاطر (Acceptable Risk Levels) فيما يتعلق بخدمات الحوسبة السحابية، وتوضيحها للمشترك إذا كانت المخاطر ذات علاقة به.
		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 خدمات الحوسبة السحابية المقدمة وتحليل تأثير الأعمال بناءً على إجراءات محددة لفهم وتقييم المخاطر (على سبيل المثال: انقطاع الخدمة، تسرب البيانات، الوصول غير المصرح به، إلخ) والأضرار التي قد تحدثها خدمات الحوسبة على غيرها. • العمل على تحديد مستويات المخاطر لخدمات الحوسبة السحابية (على سبيل المثال: حرج، عالي، متوسط، منخفض) وتحديد مستويات المخاطر المقبولة. • مشاركة مستويات المخاطر المقبولة مع المشتركين للخدمة المقدمة (على سبيل المثال: مشاركة تحليل تقييم المخاطر والتهديدات لخدمات الحوسبة السحابية المقدمة للمشتركين) .
		المخرجات المتوقعة: • وثائق توضح مستويات المخاطر المقبولة محددة وموثقة وتم مشاركتها مع الأطراف المعنية وأصحاب المصلحة ومنهم المشتركين.
	١-٢-م-١-٢	أخذ تصنيف البيانات والمعلومات بالاعتبار في منهجية إدارة مخاطر الأمن السيبراني.
		أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة إدارة مخاطر الأمن السيبراني.

		• نموذج إجراء إدارة مخاطر الأمن السيبراني. • نموذج سجل مخاطر الأمن السيبراني. **إرشادات تطبيق الضوابط:** • العمل على تحديد أنواع البيانات والمعلومات التي يتم معالجتها أو تخزينها باستخدام خدمات الحوسبة السحابية وتصنيفها إلى فئات متفق عليها مع المشترك (على سبيل المثال: عام، مقيد، سري، وسري للغاية) بناءً على حساسيتها وقيمتها بالنسبة للمشترك وتضمينها في منهجية إدارة مخاطر الأمن السيبراني عند التعامل مع المخاطر المتعلقة بخدمات الحوسبة السحابية. **المخرجات المتوقعة:** • منهجية إدارة مخاطر الأمن السيبراني تتضمن إجراءات واضحة للتعامل مع البيانات بناءً على مستويات تصنيفها.
	١-٢-م-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 إجراء إدارة مخاطر الأمن السيبراني. • نموذج سجل المخاطر السيبرانية. **إرشادات تطبيق الضوابط:** • العمل على تحديد مخاطر الأمن السيبراني المتعلقة بخدمات الحوسبة السحابية والمشتركين وتقييمها بناءً على المنهجية المعتمدة. • إنشاء سجل لمخاطر الأمن السيبراني يشمل مكونات خدمات الحوسبة السحابية، بحيث يحتوي على المعلومات المهمة التي تساعد على اتخاذ القرارات عن كيفية الاستجابة للمخاطر السيبرانية ومتابعة الإجراءات المتخذة بخصوصها. • التأكد من مراجعة سجل المخاطر بشكل دوري، بناءً على خطة معتمدة، مع الأخذ بعين الاعتبار المخاطر المحددة وحساسيتها (على سبيل المثال: مستوى الخطر حرج، عالي، متوسط، منخفض). **المخرجات المتوقعة:** • وثائق توضح سجل مخاطر الأمن السيبراني المتعلقة بخدمات الحوسبة السحابية. • وثيقة خطة مراجعة سجل مخاطر الأمن السيبراني المتعلقة بخدمات الحوسبة السحابية.

		• وثائق تقارير مراجعة سجل مخاطر الأمن السيبراني المتعلقة بخدمات 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	الالتزام الدائم والمستمر بجميع الأنظمة واللوائح والتعليمات والقرارات والأطر والضوابط التنظيمية المتعلقة بالأمن السيبراني والمعمول بها في المملكة.
		أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الالتزام بتشريعات وتنظيمات الأمن السيبراني. • نموذج سياسة مراجعة وتدقيق الأمن السيبراني. • نموذج سجل خطة تدقيق الأمن السيبراني. **إرشادات تطبيق الضوابط:** • العمل على تحديد بشكل دوري (على سبيل المثال: سنوي أو عند حدوث تغيير) جميع الأنظمة واللوائح والتعليمات والقرارات والأطر والضوابط التنظيمية المتعلقة بالأمن السيبراني المعمول بها في المملكة والمنطبقة على مزود الخدمة. • مراقبة التزام مقدم خدمة الحوسبة السحابية بهذه المتطلبات بشكل مستمر (على سبيل المثال: الاستفادة من أدوات لإجراء التحقق اليومي أو الأسبوعي).
		المخرجات المتوقعة: • قائمة الأنظمة واللوائح والتعليمات والقرارات والأطر والضوابط التنظيمية المتعلقة بالأمن السيبراني والمعمول بها في المملكة والمنطبقة على مقدم خدمات الحوسبة السحابية. • وثائق توضح تقارير حالة الالتزام بهذه المتطلبات. • وثائق توضح خطط دورية لمتابعة الالتزام.
١-٤	الأمن السيبراني المتعلق بالموارد البشرية (Cybersecurity in Human Resources)	

الهدف	ضمان التأكد من أن مخاطر الأمن السيبراني المتعلقة بالعاملين (موظفين ومتعاقدين) لدى مقدمي الخدمات والمشتركين، تعالج بفعالية قبل وأثناء وعند انتهاء/إنهاء عملهم، وذلك وفقًا للسياسات والإجراءات التنظيمية لديهم، والمتطلبات التشريعية والتنظيمية ذات العلاقة.	
الضوابط		
١-٤-م-١	بالإضافة للضوابط الفرعية ضمن الضابطين ١-٩-٣ و١-٩-٤ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني قبل بدء وخلال العلاقة المهنية بين العاملين ومقدمي الخدمة بحد أدنى ما يلي:	
	١-٤-م-١-١	فيما يتعلق بمراكز البيانات التابعة لمقدم الخدمة داخل المملكة، يجب أن يشغل وظائف الأمن السيبراني مواطنون سعوديون مؤهلون.
		أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للموارد البشرية. **إرشادات تطبيق الضوابط:** • العمل على تحديد أدوار ومناصب ووظائف الأمن السيبراني وفق المرجع فيما يتعلق بالوظائف ذات العلاقة بالأمن السيبراني (الإطار السعودي لكوادر الأمن السيبراني – سيوف) والمتعلقة بمراكز البيانات في المملكة العربية السعودية (على سبيل المثال: مهندس أمن الحوسبة السحابية، فريق مراقبة الأمن السيبراني، إلخ). • العمل على توظيف مواطنين سعوديين لشغل هذه المناصب على أن يكونوا حائزين على خبرات وشهادات في مجال الأمن السيبراني متعلقة بالمناصب المرشحين لها. • العمل على تضمين العاملين في مراكز البيانات ضمن برنامج تدريب الأمن السيبراني لتطوير مهاراتهم ومؤهلاتهم.
		المخرجات المتوقعة: • قائمة مناصب الأمن السيبراني المتعلقة بمراكز البيانات داخل المملكة العربية السعودية ومتطلبات كلًا من هذه المناصب. • قائمة الموظفين الذين يشغلون هذه المناصب بالإضافة إلى مؤهلاتهم. • وثيقة توضح برنامج الأمن السيبراني وشهادات التدريب المقدمة بناءً عليه.
	١-٤-م-١-٢	إجراء المسح الأمني للعاملين داخل المملكة الذين لهم حق الوصول إلى الأنظمة التقنية السحابية (Cloud Technology Stack (CTS)) دوريًا.
		أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للموارد البشرية. **إرشادات تطبيق الضوابط:**

		• التأكد من مراجعة المناصب الوظيفية ومسمياتها والوصف الوظيفي لتحديد المهام المتعلقة بالحاجة إلى الوصول إلى الأنظمة التقنية السحابية لضمان إجراء المسح الأمني قبل التوظيف وبشكل دوري على من يشغل هذه المناصب (على سبيل المثال: مهندس الحوسبة السحابية، مشرف خدمات الحوسبة السحابية، مهندس أمن مخزن المفاتيح).
		المخرجات المتوقعة: • وثائق تؤكد إجراءات المسح الأمني محددة لشاغلي ومرشحي الوظائف التي تتطلب حق الوصول إلى الأنظمة التقنية السحابية وتتضمن خطة للمسح الأمني بشكل دوري. • وثائق توضح تقارير المسح الأمني لشاغلي ومرشحي الوظائف التي تتطلب حق الوصول إلى الأنظمة التقنية السحابية. يجب أن تؤخذ خصوصية وحساسية والمعلومات بعين الاعتبار عند التعامل مع هذه التقارير.
	١-٤-م-١-٣	إقرار وتوقيع العاملين على جميع سياسات الأمن السيبراني كشرط مسبق للوصول إلى الأنظمة التقنية السحابية (CTS).
		أدوات الأمن السيبراني ذات العلاقة: • نموذج تعهد الالتزام بسياسات الأمن السيبراني. • نموذج سياسة الأمن السيبراني للموارد البشرية. **إرشادات تطبيق الضوابط:** • العمل على الزام المنظمين للجهة والعاملين على الاطلاع على سياسات الأمن السيبراني للجهة قبل إعطاؤهم صلاحيات الوصول للأنظمة التقنية السحابية (CTS) من خلال التوقيع على نموذج إقرار رسمي.
		المخرجات المتوقعة: • وثيقة توضح نموذج الإقرار والالتزام بسياسات الأمن السيبراني للجهة موقع من قبل جميع العاملين على الأنظمة التقنية السحابية (CTS) قبل الحصول على صلاحيات الوصول لها.
١-٤-م-٢		بالإضافة للضوابط الفرعية ضمن الضابط ١- ٩- ٥ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني بعد انتهاء العلاقة المهنية بين العاملين ومقدمي الخدمة بحد أدنى ما يلي:
	١-٤-م-٢-١	ضمان إعادة الأصول الخاصة بمقدمي الخدمات (لا سيما ذات الصلة بالأمن السيبراني) بمجرد إنهاء الخدمة مع العاملين.
		أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للموارد البشرية. **إرشادات تطبيق الضوابط:**

		• العمل على تضمين خطوات للتحقق من إعادة جميع الأصول الخاصة بمقدمي الخدمات التي بحوزة العاملين ضمن إجراءات إخلاء الطرف عند إنهاء الخدمة. • التأكد من توثيق عمليات التحقق من خلال نموذج رسمي (على سبيل المثال: نموذج إخلاء الطرف) والزام العاملين بالتوقيع عليه. **المخرجات المتوقعة:** • وثائق تؤكد نماذج إخلاء الطرف موقعة تتضمن إقرار العاملين بإعادة جميع الأصول الخاصة بالجهة مع التحقق من ذلك من قبل الإدارة المعنية.
١-٥	**الأمن السيبراني ضمن إدارة التغيير (Cybersecurity in Change Management)**	
الهدف	التأكد من أن متطلبات الأمن السيبراني مضمنة في منهجية وإجراءات إدارة التغيير لدى مقدمي الخدمات لحماية السرية وسلامة الأصول المعلوماتية والتقنية لديهم، ودقتها وتوافرها، وذلك وفقًا للسياسات والإجراءات التنظيمية لدى مقدمي الخدمات والمشتركين والمتطلبات التشريعية والتنظيمية ذات العلاقة.	
الضوابط		
١-٥-م-١	يجب تحديد متطلبات الأمن السيبراني لإدارة التغيير لدى مقدمي الخدمات، وتوثيقها، واعتمادها.	
	أدوات الأمن السيبراني ذات العلاقة: • نموذج قائمة التحقق من متطلبات الأمن السيبراني لمشاريع تقنية المعلومات وإدارة التغيير. **إرشادات تطبيق الضوابط:** • العمل على تطوير وتوثيق سياسة الأمن السيبراني لإدارة التغيير (تتضمن التغييرات المخطط لها والاستثنائية) بحيث تتضمن على سبيل المثال متطلبات لكلٍ من: ○ إعطاء الأولوية للتغييرات المتعلقة بالأمن السيبراني. ○ إجراء اختبار مرحلة ما قبل الانتاج وما قبل التطوير قبل تطبيق التغييرات على بيئة الإنتاج. ○ تحديد الأدوار والمسؤوليات. ○ تحديد آلية التراجع في حال عدم نجاح التغيير. ○ حصر التغيير للمستخدمين ذوي العلاقة. ○ رفع طلبات لصلاحيات تنفيذ التغيير والموافقة عليها. ○ تفعيل سجلات التدقيق لتنفيذ التغيير. ○ مراقبة أنشطة المستخدم عند تنفيذ التغيير. • التأكد من توثيق متطلبات الأمن السيبراني لإدارة التغيير. • العمل على ضمان الموافقة على متطلبات الأمن السيبراني لإدارة التغيير من قبل ممثلي إدارة الأمن السيبراني وإدارة التغيير.	

		• العمل على أن تكون السياسة في الجهة مدعومة من قبل الإدارة التنفيذية. وذلك من خلال اعتماد وموافقة صاحب الصلاحية.
		المخرجات المتوقعة: • وثيقة سياسة الأمن السيبراني لإدارة التغيير المعتمدة من قبل الجهة (مثال: نسخة إلكترونية أو نسخة ورقية رسمية). • وثيقة موافقة رسمية من قبل رئيس الجهة أو من ينيبه على السياسة (مثال: عن طريق البريد الإلكتروني الرسمي للجهة، أو التوقيع الورقي أو الإلكتروني).
١-٥-م-٢		يجب تطبيق متطلبات الأمن السيبراني، الخاصة بإدارة التغيير لدى مقدمي الخدمات.
		إرشادات تطبيق الضوابط: • العمل على تطبيق كافة متطلبات الأمن السيبراني لإدارة التغيير للجهة وتشمل الآتي على الأقل: ○ تنفيذ متطلبات الأمن السيبراني المعتمدة لإدارة التغيير في الجهة وعلى سبيل المثال لا الحصر: إجراءات تنفيذ التغييرات (المخطط لها) بطرق آمنة، في أنظمة الإنتاج وإجراءات تنفيذ التغييرات الاستثنائية ذات العلاقة بالأمن السيبراني.
		المخرجات المتوقعة: • وثائق تؤكد تطبيق متطلبات الأمن السيبراني لإدارة التغيير والتي تم توثيقها في وثيقة السياسات. • وثيقة توضح خطة عمل لتطبيق متطلبات الأمن السيبراني لإدارة التغيير.
١-٥-م-٣		يجب أن يغطي الأمن السيبراني لإدارة التغيير لدى مقدمي الخدمات بحد أدنى ما يلي:
	١-٥-م-٣-١	إجراءات تنفيذ التغييرات (المخطط لها) بطرق آمنة، في أنظمة الإنتاج (Production Systems)، مع إعطاء أولوية للملاحظات المتعلقة بالأمن السيبراني.
		أدوات الأمن السيبراني ذات العلاقة: • نموذج قائمة التحقق من متطلبات الأمن السيبراني لمشاريع تقنية المعلومات وإدارة التغيير. **إرشادات تطبيق الضوابط:**

		• العمل على تطوير وتوثيق إجراءات لتنفيذ التغييرات المخطط لها بطرق آمنة بحيث تتضمن التأكد من تنفيذ متطلباتها والحصول على الموافقات اللازمة بحسب الأدوار والمسؤوليات المحددة. • التأكد من أن الإجراءات تعطي أولوية للتغييرات التي تخص ملاحظات متعلقة بالأمن السيبراني.
		المخرجات المتوقعة: • وثائق توضح إجراءات إدارة التغييرات تشمل تحديد أولوية تطبيق التغييرات المتعلقة بالأمن السيبراني. • إثبات يوضح التأكد من إجراءات آمنة أثناء تنفيذ التغيرات.
	١-٥-م-٣-٢	إجراءات تنفيذ التغييرات الاستثنائية ذات العلاقة بالأمن السيبراني (مثل التغييرات أثناء التعافي من الحوادث).
		أدوات الأمن السيبراني ذات العلاقة: • نموذج قائمة التحقق من متطلبات الأمن السيبراني لمشاريع تقنية المعلومات وإدارة التغيير. **إرشادات تطبيق الضوابط:** • العمل على تطوير وتوثيق إجراءات لتنفيذ التغييرات الاستثنائية ذات العلاقة بالأمن السيبراني بطرق آمنة بحيث تتضمن التأكد من تنفيذ متطلباتها والحصول على الموافقات اللازمة بحسب الأدوار والمسؤوليات المحددة. • العمل على تضمين مبادئ وإجراءات للتغييرات الاستثنائية (على سبيل المثال: مراقبة نشاط المستخدم وتطبيق مبدأ الموافقات "four-eyes principle") لضمان عدم إجراء أي تغييرات دون الحصول على الموافقات اللازمة. • العمل على تحديد إجراءات تقنية للوصول السريع (على سبيل المثال: عمليات تخطي الوصول "Break Glass") بناءً على المتطلبات المعتمدة (على سبيل المثال يتم منح الوصول المميز المؤقت تلقائيًا في ظل ظروف محددة عندما يكون نطاق التغيير مرتبطًا بحادثة أمن سيبراني). • التأكد من بناء القدرات التقنية لهذه العملية (على سبيل المثال: الجلسات التفاعلية المميزة المتاحة فقط من خلال القنوات المخصصة).
		المخرجات المتوقعة: • وثيقة توضح إجراءات محددة لتطبيق التغييرات الاستثنائية. • إثبات يوضح بناء القدرات التقنية لمراقبة التغييرات والتحكم بها.

١-٥-م-٤	يجب مراجعة متطلبات الأمن السيبراني لإدارة التغيير لدى مقدمي الخدمات، ومراجعة تطبيقها، دورياً.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة مراجعة وتدقيق الأمن السيبراني. **إرشادات تطبيق الضوابط:** • التأكد من مراجعة وتحديث متطلبات الأمن السيبراني الخاصة بإدارة التغيير للجهة بشكل دوري حسب خطة موثقة ومعتمدة للمراجعة بناءً على فترة زمنية محددة، سنوياً على الأقل، أو في حالة حدوث تغييرات في المتطلبات التشريعية والتنظيمية ذات العلاقة. • العمل على توثيق المراجعة والتغييرات التي تتم على متطلبات الأمن السيبراني الخاصة بإدارة التغيير للجهة واعتمادها من قبل رئيس الجهة أو من ينيبه.
	المخرجات المتوقعة: • وثائق توضح سجل التحديثات والتغييرات التي تمت على متطلبات الأمن السيبراني الخاصة بإدارة التغيير. • وثيقة معتمدة تحدد جدول المراجعة للسياسة. • وثيقة السياسة بما يوضح أنه تم مراجعتها وتحديثها وتم توثيق التغييرات واعتمادها من قبل رئيس الجهة أو من ينيبه. • إثبات يؤكد الموافقة الرسمية والاعتماد من قبل رئيس الجهة أو من ينيبه على السياسة المحدثة (مثال: عن طريق البريد الإلكتروني الرسمي للجهة، أو التوقيع الورقي أو الإلكتروني).

٢ تعزيز الأمن السيبراني (Cybersecurity Defense)

٢-١	إدارة الأصول (Asset Management)	
الهدف	التأكد من أن مقدمي الخدمات والمشتركين لديهم قائمة جرد دقيقة وحديثة للأصول تشمل التفاصيل ذات العلاقة لجميع الأصول المعلوماتية والتقنية، من أجل دعم العمليات التشغيلية لديهم ومتطلبات الأمن السيبراني، لتحقيق سرية وسلامة الأصول المعلوماتية والتقنية ودقتها وتوافرها.	
الضوابط		
٢-١-م-١	بالإضافة للضوابط ضمن المكون الفرعي ٢-١ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني لإدارة الأصول المعلوماتية والتقنية لدى مقدمي الخدمات، بحد أدنى ما يلي:	
	٢-١-م-١-١	حصر جميع الأصول المعلوماتية والتقنية باستخدام التقنيات المناسبة كقاعدة بيانات إدارة الإعدادات (CMDB)، أو قدرة مماثلة، تتضمن جرداً لكل الأصول التقنية.
		أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة إدارة الأصول. • نموذج إدارة الأصول بحيث يشمل إرشادات التصنيف. **إرشادات تطبيق الضوابط:** • العمل على تحديد أنواع الأصول المعلومات والتقنية المستخدمة في الجهة باستخدام الطرق المناسبة والموثوقة (على سبيل المثال: استخدام تقنيات اكتشاف الأصول، والمسح التقني، إلخ). • العمل على تحديد أنواع الأصول المعلومات والتقنية المستخدمة في الاصول الخاصة للأنظمة التقنية السحابية (على سبيل المثال: الخوادم الافتراضية، ووسائط التخزين السحابية، وجدار حماية تطبيق الويب، إلخ). • العمل على استخدام تقنيات على مستوى تقنيات قاعدة بيانات إدارة الإعدادات (CMDB) لتسجيل جميع الأصول المعلومات والتقنية والمعلومات الخاصة بها. • التأكد من تحديث سجل الأصول تلقائيًا لتسجيل التغييرات الطفيفة على مستوى الأصول التقنية السحابية.

		المخرجات المتوقعة: • إثبات يوضح تقنيات لجرد الأصول محددة ومستخدمة. • وثيقة توضح حصر الاصول التقنية الخاصة للأنظمة السحابية. • وثيقة توضح سجل الأصول (مثل CMDB) تحتوي على جميع أصول الجهة المعلوماتية والتقنية والمعلومات المتعلقة بها.
	٢-١-م-١-٢	تحديد ملاك الأصول (Asset Owners) وإشراكهم في دورة حياة إدارة الأصول.
		أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة إدارة الأصول. **إرشادات تطبيق الضوابط:** • العمل على تحديد الواجبات والالتزامات التنظيمية والتعاقدية المتعلقة بالأصول (على سبيل المثال: الموافقة على التغييرات أو الوصول لكافة الأصول التقنية والمعلوماتية والسحابية وإدارتها). • العمل على تحديد وتوثيق الأدوار والمسؤوليات المتعلقة بالأصول خلال دورة حياة إدارة الأصول (على سبيل المثال: الإنشاء والنشر والإدارة والاتلاف) ومشاركتها مع ملاك الأصول. • العمل على تعيين ملاك للأصول المعلوماتية والتقنية بحيث يكون لكل أصل معلوماتي أو تقني مالك محدد.
		المخرجات المتوقعة: • وثيقة توضح سجل الأصول التقنية والمعلوماتية يحتوي على معلومات ملاك لكل الأصول. • إثبات يؤكد تحديد الأدوار والمسؤوليات فيما يتعلق بإدارة الأصول ومشاركة ملاك الأصول.
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 ما هو مطلوب لإنجاز الأعمال الخاصة بهم.	
الضوابط		
٢-٢-م-١	بالإضافة للضوابط الفرعية ضمن الضابط ٢-٢-٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني الخاصة بإدارة هويات الدخول والصلاحيات لدى مقدمي الخدمات، بحد أدنى ما يلي:	

	٢-٢-م-١-١	إدارة الحسابات العامة (Generic Accounts) التي لا يمكن إسناد مسؤوليتها إلى أشخاص محددين.
		أدوات الأمن السيبراني ذات العلاقة: • نموذج معيار إدارة هويات الدخول والصلاحيات، بحيث يشمل إدارة كلمات المرور. • نموذج سياسة إدارة هويات الدخول والصلاحيات. • نموذج معيار أجهزة المستخدمين ذات الصلاحيات الهامة والحساسة. **إرشادات تطبيق الضوابط:** • العمل على تحديد كلاً من الحسابات العامة ذات الصلاحيات الخاصة الهامة والحساسة وذات الصلاحيات الافتراضية (على سبيل المثال: حسابات الخدمة والحسابات الفنية والحسابات غير الشخصية). • العمل على تطبيق قيود تقنية لحساب المستخدم بناءً على الصلاحيات المسندة له (على سبيل المثال: تغيير بيانات الاعتماد المرتبطة بالحساب بانتظام، تحديد سياسة للاستخدام المقبول للحساب بما في ذلك من يمكنه الوصول إليه ومتى يجب استخدامه والاجراءات المسموح بها).
		المخرجات المتوقعة: • وثيقة توضح قائمة محددة لمستخدمي الحسابات العامة (حسابات الخدمة، الحسابات الفنية، إلخ). • إثبات يؤكد القيود التقنية المطبقة على استخدام وإدارة الحسابات العامة.
	٢-٢-م-١-٢	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 معيار أجهزة المستخدمين ذات الصلاحيات الهامة والحساسة. **إرشادات تطبيق الضوابط:** • العمل على استخدام جلسات (Tunnel sessions) من خلال خوادم وكيل (Proxies) موثقة مع القدرة على إنهاء الجلسات في حال عدم وجود نشاط.

		• التأكد من إعداد نظام إدارة الجلسة لإغلاق الجلسات وإنهاء مهلتها (على سبيل المثال: إغلاق الجلسة بعد ١٥ دقيقة والمهلة بعد ١٠ دقائق من عدم النشاط).
		المخرجات المتوقعة: • إثبات يوضح الإعدادات المطبقة لإدارة الجلسات بما يشمل موثوقيتها وإقفالها وإنهاء مهلتها.
	٢-٢-م-١-٣	التحقق من الهوية متعدد العناصر (Mulit-Factor Authentication) لحسابات المستخدمين ذوي الصلاحيات الهامة والحساسة، والذين لهم حق الوصول إلى الأنظمة التقنية السحابية (CTS).
		أدوات الأمن السيبراني ذات العلاقة: • نموذج معيار إدارة هويات الدخول والصلاحيات، بحيث يشمل إدارة كلمات المرور. • نموذج سياسة إدارة هويات الدخول والصلاحيات. • نموذج معيار أجهزة المستخدمين ذات الصلاحيات الهامة والحساسة. **إرشادات تطبيق الضوابط:** • العمل على تحديد وحصر حسابات المستخدمين ذوي الصلاحيات الهامة والحساسة، والذين لهم حق الوصول إلى الأنظمة التقنية السحابية (CTS) في قائمة محدثة. • التأكد من استخدام التقنيات اللازمة للتحقق من الهوية متعدد العناصر لعمليات دخول هذه الحسابات إلى الأنظمة التقنية السحابية (CTS) (على سبيل المثال استخدام رمز مصادقة البرامج، رسائل نصية "SMS").
		المخرجات المتوقعة: • إثبات يوضح حسابات المستخدمين ذوي الصلاحيات الهامة والحساسة، والذين لهم حق الوصول إلى الأنظمة التقنية السحابية (CTS). • إثبات يوضح تقنيات التحقق من الهوية متعدد العناصر لعمليات الدخول لحسابات المستخدمين ذوي الصلاحيات الهامة والحساسة، والذين لهم حق الوصول إلى الأنظمة التقنية السحابية (CTS).
	٢-٢-م-١-٤	إجراءات لكشف محاولات الوصول غير المصرح به ومنعها مثل: (الحد الأقصى من محاولات عمليات الدخول غير الناجحة (Unsuccessful Login)).

		أدوات الأمن السيبراني ذات العلاقة: ● نموذج معيار إدارة هويات الدخول والصلاحيات، بحيث يشمل إدارة كلمات المرور. ● نموذج سياسة إدارة هويات الدخول والصلاحيات. ● نموذج معيار أجهزة المستخدمين ذات الصلاحيات الهامة والحساسة. **إرشادات تطبيق الضوابط:** ● العمل على تحديد وتطبيق عملية إدارة الهوية والوصول (IAM) التي تتضمن حوكمة كيفية تعامل المشترك (CSP) مع تهديد الوصول غير المصرح به بحسب النطاق المحدد. يحتوي وصف العملية كحد أدنى على: ○ طرق مصادقة المستخدم المقبولة والحد الأدنى للإعدادات (مثل سياسة تعقيد كلمة المرور واستخدام التحق من الهوية متعدد العناصر "MFA"). ○ يتطلب الوصول المشروط استيفاء معايير معينة قبل منح حق الوصول. ○ مراقبة مصادقة المستخدم بحثًا عن الأنشطة المشبوهة والسلوك غير الاعتيادي (على سبيل المثال العديد من عمليات تسجيل الدخول غير الناجحة على التوالي، والسفر غير الممكن). ○ تمكين إعادة تعيين وإدارة كلمة المرور ذاتيًا. ○ إعداد إشعارات البريد الإلكتروني / الهاتف المحمول لتوثيق الحساب السحابي للتأكد من أن مالك الحساب قد تم إخطاره بشأن توثيق الحساب.
		المخرجات المتوقعة: ● إثبات يوضح عمليات الوصول ومراقبتها. ● إثبات يوضح عدد محاولة الوصول المسموحة محدد ويتم إغلاق الحساب مؤقتا عند تجاوز الحد. ● إثبات يوضح إعدادات النظام وتقارير المراقبة. ● إثبات يوضح تنبيهات محاولات الدخول.
	٢-٢-م-١-٥	استخدام الطرق والخوارزميات الآمنة لحفظ ومعالجة كلمات المرور مثل: استخدام دوال اختزال آمنة (Secure Hashing Functions).
		أدوات الأمن السيبراني ذات العلاقة: ● نموذج معيار إدارة هويات الدخول والصلاحيات، بحيث يشمل إدارة كلمات المرور.

		• نموذج سياسة إدارة هويات الدخول والصلاحيات. • نموذج معيار أجهزة المستخدمين ذات الصلاحيات الهامة والحساسة. **إرشادات تطبيق الضوابط:** • العمل على تخزين كلمات المرور (محليًا ومركزيًا) بشكل يضمن عدم القدرة على معرفتها (على سبيل المثال: استخدام دوال اختزال آمنة "Secure Hashing Functions"). • العمل على استخدم دوال اختزال المعتمدة. • التأكد من مراجعة هذه الدوال بشكل دوري لمنع استخدام الدوال المخترقة أو غير ذات كفاءة. • العمل على استخدم زوائد التشفير (Cryptographic Salt) لإنشاء دوال اختزال فريدة لكلمات المرور حتى في حال قام المستخدمون باستخدام نفس كلمات المرور. • العمل على استخدام الخوارزميات والدوال المذكورة في معايير التشفير الوطنية (المستوى المتقدم). **المخرجات المتوقعة:** • إثبات يوضح عينة من كلمات المرور المخزنة. • وثيقة توضح المعايير المطبقة على تخزين كلمات المرور.
	٢-٢-م-١-٦	الإدارة الآمنة للحسابات الخاصة بالعاملين التابعين للأطراف الخارجية (Third-party). **أدوات الأمن السيبراني ذات العلاقة:** • نموذج معيار إدارة هويات الدخول والصلاحيات، بحيث يشمل إدارة كلمات المرور. • نموذج سياسة إدارة هويات الدخول والصلاحيات. • نموذج معيار أجهزة المستخدمين ذات الصلاحيات الهامة والحساسة. **إرشادات تطبيق الضوابط:** • العمل على تحديد وتطبيق قيود لإدارة الهوية والوصول (IAM) لحسابات الأطراف الخارجية من مقدمي خدمات ومتعاقدين ونحو ذلك. • العمل على تحديد وتطبيق إجراءات لإدارة حسابات الأطراف الخارجية بما يشمل إنشاءها ومراقبتها وإلغاءها والحصول على الموافقات اللازمة لكلًا من ذلك.

		• العمل على تفعيل سجلات الأحداث الخاصة بحسابات الأطراف الخارجية ومراقبة الأنشطة المتعلقة بها. • العمل على استخدام ترميز واضح لحسابات الأطراف الخارجية. • العمل على استخدام خدمات وهويات الدخول والمصادقة الموحدة (على سبيل المثال ADFS، SAML٢، oAuth٢) لحسابات الأطراف الخارجية. • التأكد من المراجعة الدورية للحسابات والصلاحيات بحسب خطة مراجعة محددة.
		المخرجات المتوقعة: • إثبات يوضح القيود المطبقة على حسابات الأطراف الخارجية بناءً على المعايير المعتمدة. • وثائق توضح الإجراءات المعتمدة لإدارة حسابات الأطراف الخارجية خلال دورة حياتها. • إثبات يوضح طلبات حسابات الأطراف الخارجية للحصول على الموافقات اللازمة. • إثبات يوضح سجلات مراقبة أنشطة حسابات الأطراف الخارجية. • إثبات يوضح الترميز المحدد لحسابات الأطراف الخارجية. • إثبات يوضح خدمات وهويات الدخول والمصادقة الموحدة المستخدمة. • وثيقة توضح خطة مراجعة حسابات وصلاحيات الأطراف الخارجية وتقارير المراجعة المنفذة.
	٢-٢-م-١-٧	التحكم في الوصول إلى الأنظمة الإدارية (Management Systems) والإشرافية (Administrative Consoles).
		أدوات الأمن السيبراني ذات العلاقة: • نموذج معيار إدارة هويات الدخول والصلاحيات، بحيث يشمل إدارة كلمات المرور. • نموذج سياسة إدارة هويات الدخول والصلاحيات. • نموذج معيار أجهزة المستخدمين ذات الصلاحيات الهامة والحساسة. **إرشادات تطبيق الضوابط:** • العمل على تحديد وحصر الأنظمة الإدارية (Management Systems) والإشرافية (Administrative Consoles) ومراجعتها بشكل دوري. • العمل على الحصول على الموافقات اللازمة قبل إعطاء صلاحيات الوصول إلى الأنظمة الإدارية والإشرافية.

		• التأكد من مراجعة صلاحيات الوصول إلى الأنظمة الإدارية والإشرافية بشكل دوري. • العمل على استخدام حلول إدارة الصلاحيات الهامة والحساسة (PAM) للتحكم بالوصول إلى الأنظمة الإدارية والإشرافية وتشفير الاتصالات المتعلقة بها عبر الشبكة. • العمل على تفعيل التحقق متعدد العناصر (MFA) لعمليات الوصول إلى الأنظمة الإدارية والإشرافية. • العمل على تفعيل سجلات مراقبة الأحداث على الأنشطة المتعلقة بالوصول إلى الأنظمة الإدارية والإشرافية ومراقبتها وتسجيل جلسات الوصول.
		المخرجات المتوقعة: • وثيقة توضح قائمة الأنظمة الإدارية والإشرافية. • إثبات يؤكد عملية طلبات الوصول إلى الأنظمة الإدارية والإشرافية. • وثيقة توضح خطة مراجعة صلاحيات الوصول إلى الأنظمة الإدارية والإشرافية وتقارير المراجعة. • اثبات من تطبيق نظام إدارة الصلاحيات الهامة والحساسة (PAM) للوصول إلى الأنظمة الإدارية والإشرافية. • اثبات تفعيل تشفير اتصالات الوصول عبر الشبكة للأنظمة الإدارية والإشرافية وقائمة خوارزميات التشفير المفعلة. • اثبات تفعيل التحقق متعدد العناصر. • إثبات يوضح سجلات مراقبة الأحداث والتنبيهات المتعلقة بها من خلال نظام مراقبة سجلات الأحداث (SIEM). • إثبات يوضح تسجيلات جلسات الوصول.
	٢-٢-م-١-٨	إخفاء معلومات التحقق من الهوية، خاصةً كلمات المرور، عند عرضها للمستخدم؛ لحمايتها من اطلاع الآخرين عليها.
		أدوات الأمن السيبراني ذات العلاقة: • نموذج معيار إدارة هويات الدخول والصلاحيات، بحيث يشمل إدارة كلمات المرور. • نموذج سياسة إدارة هويات الدخول والصلاحيات. • نموذج معيار أجهزة المستخدمين ذات الصلاحيات الهامة والحساسة. **إرشادات تطبيق الضوابط:**

		• العمل على تفعيل خصائص لتعتيم البيانات عند عرضها للمستخدمين مثل: البيانات الحساسة، كلمة المرور والبيانات الشخصية، رقم الجوال والبريد الإلكتروني في حال طلب استعادة/تغيير كلمة المرور.
		المخرجات المتوقعة: • إثبات يؤكد تطبيق التعتيم والإخفاء للمعلومات الحساسة والشخصية.
	٢-٢-م-١-٩	الحصول على موافقة المشترك قبل عملية الوصول إلى أي من الأصول والبيانات الخاصة به، من قبل مقدم الخدمة أو الأطراف الخارجية لمقدم الخدمة.
		أدوات الأمن السيبراني ذات العلاقة: • نموذج معيار إدارة هويات الدخول والصلاحيات، بحيث يشمل إدارة كلمات المرور. • نموذج سياسة إدارة هويات الدخول والصلاحيات. • نموذج معيار أجهزة المستخدمين ذات الصلاحيات الهامة والحساسة. **إرشادات تطبيق الضوابط:** • العمل على جعل موافقة المشترك (CST) شرط أساسي قبل الوصول إلى أي من الأصول المرتبطة أو البيانات الخاصة به من قبل أي طرف من جهة مقدم الخدمة (CSP)، على أن يكون الحصول على الموافقة من خلال قنوات معتمدة بين المشترك ومقدمة الخدمة.
		المخرجات المتوقعة: • وثيقة توضح إجراءات طلب الموافقة للوصول إلى الأصول والبيانات الخاص بالمشترك المعتمدة والموافقة عليه من قبل المشترك. • إثبات يوضح طلبات الموافقة.
	٢-٢-م-١-١٠	القدرة على الإيقاف الفوري للجلسة (Session) لعمليات الدخول عن بعد ومنع المستخدم من الدخول مستقبلًا.
		أدوات الأمن السيبراني ذات العلاقة: • نموذج معيار إدارة هويات الدخول والصلاحيات، بحيث يشمل إدارة كلمات المرور. • نموذج سياسة إدارة هويات الدخول والصلاحيات. • نموذج معيار أجهزة المستخدمين ذات الصلاحيات الهامة والحساسة.

		إرشادات تطبيق الضوابط: • استخدام خادم وكيل (Proxy) موثق للجلسات عن بعد. • إعداد الخادم الوكيل (Proxy) لإنهاء الجلسة على الفور في ظل ظروف محددة (على سبيل المثال: انتهاك السياسة). • إعداد الخادم الوكيل (Proxy) لإيقاف قبول الاتصالات من مصادر أو مستخدمين محددين. **المخرجات المتوقعة:** • إثبات يوضح إنشاء جلسات الوصول عن بعد التي يتم التحكم فيها. • إثبات يوضح عينة من تكوينات النظام / الوكيل.
	٢-٢-م-١-١١	تزويد المشتركين بخدمات 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. • نموذج معيار أجهزة المستخدمين ذات الصلاحيات الهامة والحساسة. • نموذج معيار الكشف عن تهديدات الشبكات والاستجابة لها (NDR). **إرشادات تطبيق الضوابط:** • العمل على تحديد الأدوار ذات الصلاحيات الهامة والحساسة وتفعيل التحقق من الهوية متعدد العناصر (MFA) لعمليات دخول العاملين لها. **المخرجات المتوقعة:** • إثبات يؤكد تفعيل التحقق متعدد العناصر (MFA) لعمليات دخول المستخدمين ذوي الصلاحيات الهامة والحساسة لكافة الحسابات السحابية.
	٢-٢-م-١-١٢	التحكم بالوصول لأنظمة ووسائل التخزين (مثل الشبكة الخاصة بالتخزين (Storage Area Network (SAN)). **أدوات الأمن السيبراني ذات العلاقة:** • نموذج معيار إدارة هويات الدخول والصلاحيات، بحيث يشمل إدارة كلمات المرور.

		• نموذج سياسة إدارة هويات الدخول والصلاحيات. • نموذج معيار أجهزة المستخدمين ذات الصلاحيات الهامة والحساسة. • نموذج سياسة أمن وسائط التخزين. **إرشادات تطبيق الضوابط:** • العمل على تحديد متطلبات الأمن السيبراني المتعلقة بالوصول إلى أنظمة التخزين. • العمل على تحديد وحصر أنظمة التخزين وأنواعها وملاكها ومن لديهم صلاحيات الوصول لها. • العمل على تحديد وتنفيذ سياسة الوصول المتعلقة بالوصول إلى أنظمة التخزين التي تشمل الغرض والحوكمة لكيفية معالجة المشترك (CSP) لتهديدات الوصول غير المصرح بها إلى هذه الأنظمة. • العمل على فصل أنظمة التخزين والحوسبة ماديًا ومنطقيًا عن الأنظمة الأخرى. • التأكد من تقييد الوصول إلى هذه الأنظمة وعدم السماح بالوصول إلا بعد الحصول على الموافقات اللازمة.
		المخرجات المتوقعة: • وثيقة توضح سياسة الوصول لأنظمة التخزين. • وثيقة توضح سجل الأصول الذي يحتوي على أنظمة التخزين. • إثبات يوضح تطبيق سياسة الوصول لأنظمة التخزين. • وثائق توضح تصميم معمارية لأنظمة التخزين. • إثبات يوضح طلبات الوصول لأنظمة التخزين.
٢-٣	حماية الأنظمة وأجهزة معالجة المعلومات (Information System and Information Processing Facilities Protection)	
الهدف	ضمان حماية الأنظمة وأجهزة معالجة المعلومات بما في ذلك أجهزة المستخدمين والبنى التحتية لدى مقدمي الخدمات والمشتركين من المخاطر السيبرانية.	
الضوابط		
٢-٣-م-١	بالإضافة للضوابط الفرعية ضمن الضابط ٢-٣-٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني الخاصة بحماية الأنظمة وأجهزة معالجة المعلومات لدى مقدمي الخدمات، بحد أدنى ما يلي:	
	٢-٣-م-١-١	التحقق من مدى التزام الإعدادات التقنية لمعايير الأمن السيبراني المعتمدة لدى مقدم الخدمة.

		أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة أمن الخوادم. • نموذج معيار أمن الخوادم. • نموذج معيار أمن الأنظمة الافتراضية. • نموذج معيار نظام الخادم الوكيل. • نموذج سياسة الإعدادات والتحصين. **إرشادات تطبيق الضوابط:** • العمل على توثيق واعتماد معايير الأمن السيبراني لأنظمة المعلومات. • العمل على إعداد أنظمة المعلومات بناءً على المعايير المتعمدة قبل إطلاق وقبل تطبيق التغييرات. • التأكد من مراجعة إعدادات أنظمة المعلومات بشكل دوري للتأكد من التزامها بمعايير الأمن السيبراني المعتمدة. • العمل على مراقبة التغييرات التي تتم على الإعدادات. • العمل على تقييد صلاحيات تعديل الإعدادات وحصرها بحسب الأدوار المعتمدة. • العمل على إدارة طلبات تعديل الإعدادات على أن تكون ضمن عملية إدارة التغيير المعتمدة لدى الجهة. **المخرجات المتوقعة:** • وثائق توضح معايير الأمن السيبراني لأنظمة المعلومات المعتمدة. • وثيقة توضح قائمة التحقق من تطبيق المعايير على الإعدادات قبل الإطلاق وقبل تطبيق التغييرات. • وثيقة توضح خطة مراجعة إعدادات أنظمة المعلومات وتقارير المراجعة. • إثبات من سجلات أحداث مراقبة التغييرات على الإعدادات. • وثائق تؤكد القيود المطبقة على تعديل الإعدادات وقائمة العاملين ذوي صلاحيات تغيير الإعدادات. • إثبات يؤكد طلبات تغيير الإعدادات.
	٢-٣-م-١-٢	وضع ضمانات لمنع اختلاط بيانات (Data Commingling) المشتركين.

		أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة أمن الخوادم. • نموذج معيار أمن الخوادم. • نموذج معيار أمن الأنظمة الافتراضية. • نموذج معيار نظام الخادم المفوض. • نموذج سياسة الإعدادات والتحصين. • نموذج سياسة الأمن السيبراني للبيانات. • نموذج معيار الأمن السيبراني للبيانات. **إرشادات تطبيق الضوابط:** • العمل على تنفيذ آليات موثوقة للفصل والعزل بين بيانات المشتركين (CSTs) باستخدام أجهزة المعالجة الافتراضية على مستوى البيئات والخوادم والشبكات وأنظمة معالجة المعلومات (على سبيل المثال: شبكات معرفة بالبرمجيات "Software Defined Network"). • التأكد من تنفيذ اختبار آليات العزل بشكل دوري (على سبيل المثال: اختبارات الاختراق).
		المخرجات المتوقعة: • وثيقة توضح الآليات المعتمدة للفصل والعزل بين بيانات المشتركين لضمان منع اختلاط البيانات. • تقارير الاختبارات المنفذة لتحقق من منع اختلاط البيانات.
	٢-٣-م-١-٣	اتباع مبادئ الأمن السيبراني لتفعيل الحد الأدنى من الوظائف المطلوبة (Minimum Functionality Principle) لإعدادات الأنظمة (System Configurations).
		أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة أمن الخوادم. • نموذج معيار أمن الخوادم. • نموذج معيار أمن الأنظمة الافتراضية. • نموذج معيار نظام الخادم الوكيل. • نموذج سياسة الإعدادات والتحصين. **إرشادات تطبيق الضوابط:**

		• العمل على تفعيل "مبدأ الحد الأدنى من الوظائف" على مستوى معمارية الحلول والأنظمة بناءً على الحاجة الوظيفية وتوصيات مزودي الخدمة. • العمل على تحديد وتطبيق متطلبات الحد الأدنى للإعدادات والوظائف للتقنيات والأنظمة والبرمجيات والخدمات. • التأكد من مراجعة الإعدادات بشكل دوري للتحقق من عدم تفعيل وظائف زائدة عن حاجة العمل. **المخرجات المتوقعة:** • وثيقة متطلبات الحد الأدنى من الوظائف المحددة على مستوى الإعدادات والوظائف للتقنيات والأنظمة والبرمجيات والخدمات، إلخ. • تقارير مراجعة الإعدادات لغرض الالتزام مع المتطلبات المحددة.
	٢-٣-م-١-٤	أن تكون الأنظمة التقنية السحابية (CTS) قادرة على التعامل بطرق آمنة مع: المدخلات والتحقق منها (Input Validation)، والاستثناءات (Exception)، والتوقف (Failure). **أدوات الأمن السيبراني ذات العلاقة:** • نموذج سياسة أمن الخوادم. • نموذج معيار أمن الخوادم. • نموذج معيار أمن الأنظمة الافتراضية. • نموذج معيار نظام الخادم الوكيل. • نموذج سياسة الإعدادات والتحصين. **إرشادات تطبيق الضوابط:** • العمل على تنفيذ إطار عمل فني موحد للتحقق من صحة المدخلات على مستوى الأنظمة التقنية السحابية (CTS) (على سبيل المثال: الأحرف الخاصة والطول ومجموعات الأحرف إلخ). • العمل على إعداد الأنظمة التقنية السحابية (CTS) للتحقق من صحة المدخلات. • التأكد من مراقبة ومتابعة المدخلات لاكتشاف محاولات الاستثناءات والفشل. **المخرجات المتوقعة:** • إثبات يوضح إعدادات التحقق من صحة المدخلات. • إثبات يؤكد تمكين المراقبة التلقائية لاكتشاف حالات الاستثناءات والفشل. • إثبات يؤكد تسجيل ومراقبة تنبيهات/تقارير التحقق.

	٢-٣-م-١-٥	عزل التطبيقات والوظائف الأمنية عن التطبيقات والوظائف الأخرى في الأنظمة التقنية السحابية (CTS).
		أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة أمن الخوادم. • نموذج معيار أمن الخوادم. • نموذج معيار أمن الأنظمة الافتراضية. • نموذج معيار نظام الخادم المفوض. **إرشادات تطبيق الضوابط:** • العمل على تثبيت الحلول/الأدوات والتطبيقات الأمنية في بيئات مادية أو منطقية مخصصة.
		المخرجات المتوقعة: • إثبات يوضح وظائف وتطبيقات الأمان معزولة عن الوظائف والتطبيقات الأخرى في الأنظمة التقنية السحابية (CTS). • وثيقة التصميم المعماري للتطبيقات والوظائف الأمنية.
	٢-٣-م-١-٦	تبليغ المشترك بالمتطلبات المتعلقة بالأمن السيبراني التي يوفرها مقدم الخدمة والقابلة للاستخدام من قبل المشترك.
		أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة أمن الخوادم. • نموذج معيار أمن الخوادم. • نموذج معيار أمن الأنظمة الافتراضية. • نموذج معيار نظام الخادم الوكيل. **إرشادات تطبيق الضوابط:** • العمل على تحديد متطلبات الأمن السيبراني للمشتركين (على سبيل المثال: الاتصال الآمن، بروتوكولات التكامل الآمن). • العمل على إرسال التنبيهات إلى المشتركين حول متطلبات الأمن السيبراني التي يوفرها مقدم الخدمة وطرق تفعليها على الخدمات المستخدمة من قبل المشتركين.

		المخرجات المتوقعة: • وثيقة متطلبات الأمن السيبراني التي يوفرها مقدم الخدمة وطرق تفعليها على الخدمات المستخدمة من قبل المشتركين. • إثبات يوضح مشاركة المتطلبات التي يمكن تفعيلها بحسب طلب المشتركين والتي تمت مشاركتها معهم.
	٢-٣-م-١-٧	اكتشاف ومنع التغييرات غير المصرح بها على البرامج والأنظمة.
		أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة أمن الخوادم. • نموذج معيار أمن الخوادم. • نموذج معيار أمن الأنظمة الافتراضية. • نموذج معيار نظام الخادم الوكيل. **إرشادات تطبيق الضوابط:** • العمل على تحديد وتوثيق متطلبات الأمن السيبراني لإدارة التغيير والتحكم في الوصول والتسجيل والمراقبة لاكتشاف ومنع التغييرات غير المصرح بها (على سبيل المثال: تحديد الأدوار والمسؤوليات لتصميم واعتماد وتطبيق التغيير، السماح للمستخدمين ذوي الصلاحيات المحددة فقط بتطبيق التغييرات، رفع طلب الصلاحيات لإجراء التغييرات، تفعيل سجلات التدقيق لتطبيق التغييرات، مراقبة أنشطة المستخدم عند تطبيق التغييرات). • العمل على تنفيذ كل من الضوابط الإدارية والتقنية لفرض هذه المتطلبات (مثل: إدارة التغيير، وأنظمة إدارة الوصول ذو الصلاحيات الهامة والحساسة، وأنظمة التسجيل والمراقبة).
		المخرجات المتوقعة: • إثبات يوضح متطلبات الأمن السيبراني لإدارة التغييرات. • إثبات يؤكد القيود المطبقة لمنع التغييرات غير المصرح بها واكتشافها وإعادتها. • إثبات يوضح إعدادات الأنظمة لأدوات منع التغييرات. • وثيقة توضح تقرير / تنبيهات مراقبة التغييرات.
	٢-٣-م-١-٨	العزل بين بيئات الاستضافة الخاصة بالمشتركين (Guest Environments)، والحماية فيما بينها.

		أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة أمن الخوادم. • نموذج معيار أمن الخوادم. • نموذج معيار أمن الأنظمة الافتراضية. • نموذج معيار نظام الخادم الوكيل. **إرشادات تطبيق الضوابط:** • العمل على بناء ومراجعة نموذج التهديدات لتقنية البيئات الافتراضية. • العمل على تحديد مشكلات تقنية البيئات الافتراضية والاستجابة لها (على سبيل المثال: تسرب الذاكرة، تبديل المضيف في حال الفشل). • العمل على إعداد البيئات الافتراضية لعزل كل بيئات المستضيفين عن بعضها. • التأكد من اختبار البيئات الافتراضية للتحقق من تطبيق متطلبات عزل بيئات المستضيفين وحمايتها.
		المخرجات المتوقعة: • إثبات يؤكد عزل بيئات المستضيفين. • وثيقة التصميم المعماري لبيئات المستضيفين توضح العزل. • عينة من نموذج تهديدات البيئات الافتراضية. • عينة من تقارير الاختبار.
	٢-٣-م-١-٩	أن تكون الحوسبة السحابية المشتركة المقدمة للمشتركين (الجهات الحكومية والجهات ذات البنية التحتية الحساسة) معزولة عن أي حوسبة سحابية أخرى مقدمة للجهات خارج نطاق العمل.
		أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة أمن الخوادم. • نموذج معيار أمن الخوادم. • نموذج معيار أمن الأنظمة الافتراضية. • نموذج معيار نظام الخادم الوكيل. **إرشادات تطبيق الضوابط:** • العمل على تحديد الإجراءات اللازمة لضمان العزل المادي وفصل الخدمات السحابية المقدمة إلى الجهات الحكومية والجهات ذات البنية التحتية الحساسة عن أي حوسبة سحابية أخرى مقدمة إلى الجهات خارج نطاق العمل.

		• العمل على تطبيق آليات العزل المحددة والمتفق عليها بين الخدمات السحابية المقدمة الجهات الحكومية والجهات ذات البنية التحتية الحساسة (على سبيل المثال: تطبيق الحواجز المادية والمنطقية).
		المخرجات المتوقعة: • وثيقة التصميم المعماري. • عينة من آليات العزل المطبقة بين الخدمات السحابية المقدمة إلى الجهات الحكومية والجهات ذات البنية التحتية الحساسة عن أي حوسبة سحابية أخرى مقدمة إلى الجهات خارج نطاق العمل.
	٢-٣-م-١-١٠	استخدام التقنيات الحديثة، مثل تقنيات (Endpoint Detection and Response (EDR))، لضمان جاهزية خوادم وأجهزة المعلومات الخاصة بأنظمة وأجهزة معالجة المعلومات لدى مقدمي الخدمات، للاستجابة السريعة للحوادث.
		أدوات الأمن السيبراني ذات العلاقة: • نموذج الكشف عن تهديدات النقاط النهائية والاستجابة لها (EDR). • نموذج معيار الحماية من التهديدات المستمرة المتقدمة (APT). • نموذج معيار أنظمة الحماية من التهديدات المتقدمة المستمرة. • نموذج سياسة الحماية من البرمجيات الضارة. • نموذج معيار الحماية من البرمجيات الضارة. • نموذج سياسة أمن الخوادم. • نموذج معيار أمن الخوادم. • نموذج معيار أمن الأنظمة الافتراضية. • نموذج معيار نظام الخادم لوكيل. **إرشادات تطبيق الضوابط:** • العمل على توفير تقنيات وآليات من فئة التقنية لاكتشاف والاستجابة للتهديدات المتقدمة وللحماية من الفيروسات والبرامج والأنشطة المشبوهة والبرامج الضارة. • العمل على تحديث التقنيات المتوفرة وتحتوي على خصائص الحماية من الهجمات المتقدمة والمستمرة (APT). • التأكد من مراجعة نظام الحماية بشكل دوري للتأكد من أن نطاق نظام الحماية شامل لجميع أجهزة المستخدمين والخوادم من خلال وحدة التحكم في نظام الحماية.

		• العمل على وضع وتنفيذ خطة عمل تصحيحية (عند الحاجة) لتثبيت نظام الحماية على جميع الأجهزة. • التأكد من متابعة نظام الحماية بشكل دوري للتأكد من تطبيق التحديثات على جميع أجهزة المستخدمين والخوادم.
		المخرجات المتوقعة: • إثبات يوضح أنظمة الحماية من التهديدات المتقدمة والمستمرة مطبقة على مستوى جميع الأجهزة والخوادم. • وثيقة توضح خطة مراجعة إعدادات أنظمة الحماية وتقارير المراجعة. • وثيقة توضح خطة تحديثات أنظمة الحماية وتقارير تطبيق التحديثات.
٢-٤	إدارة أمن الشبكات (Networks Security Management)	
الهدف	ضمان حماية شبكات مقدمي الخدمات والمشتركين من المخاطر السيبرانية.	
الضوابط		
٢-٤-م-١	بالإضافة للضوابط الفرعية ضمن الضابط ٢-٥-٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني الخاصة بإدارة أمن الشبكات لدى مقدمي الخدمات، بحد أدنى ما يلي:	
	٢-٤-م-١-١	مراقبة الشبكات الداخلية والخارجية للكشف عن الأنشطة المشبوهة.
		أدوات الأمن السيبراني ذات العلاقة: • نموذج معيار امن الشبكات. • نموذج سياسة امن الشبكات. **إرشادات تطبيق الضوابط:** • العمل على تحديد نطاق اكتشاف الأنشطة المشبوهة على الشبكات الداخلية والخارجية. • العمل على تحديد جميع الشبكات الداخلية والخارجية ومسارات الشبكة. • العمل على إنشاء طرق وحدود للاكتشاف الفعال للأنشطة المشبوهة مع الأخذ في الاعتبار معدلات الاكتشافات غير الصحيحة. • العمل على تطبيق حلول مراقبة تتناسب مع حجم حركة اتصالات الشبكة. • العمل على ربط أحداث الشبكة بأحداث أمنية أخرى للمقارنة والربط. • التأكد من مراجعة قواعد الارتباط بشكل دوري.

		• العمل على النظر في طرق الكشف عن الأنشطة المشبوهة المبنية على الذكاء الاصطناعي.
		المخرجات المتوقعة: • قائمة لتقارير مسارات الشبكة. • إثبات يؤكد قواعد كشف الأنشطة المشبوهة على الشبكة الداخلية والخارجية مُعرفة على مستوى الحلول الأمنية.
	٢-٤-م-١-٢	عزل وحماية الشبكة الخاصة بالأنظمة التقنية السحابية (CTS) من الشبكات الأخرى الداخلية والخارجية.
		أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة أمن الشبكات. • نموذج معيار أمن الشبكات. **إرشادات تطبيق الضوابط:** • العمل على تحديد المخاطر المحتملة المتعلقة بشبكة الأنظمة التقنية السحابية (CTS) وتطبيق حلول الحماية ذات الصلة. • العمل على عزل مادياً أو منطقياً (على سبيل المثال: الشبكات المعرفة بالبرمجيات) لشبكات الأنظمة التقنية السحابية (CTS) والشبكات الداخلية والخارجية.
		المخرجات المتوقعة: • نموذج التهديدات لشبكة الأنظمة التقنية السحابية (CTS). • إثبات يؤكد تطبيق الضوابط على مستوى الشبكة لضمان العزل والحماية. • وثيقة التصميم المعماري.
	٢-٤-م-١-٣	الحماية من هجمات تعطيل الخدمات (Denial of Service (DoS))، وهجمات تعطيل الخدمات الموزعة (Distributed Denial of Service (DDoS)).
		أدوات الأمن السيبراني ذات العلاقة: • نموذج معيار الحماية من هجمات حجب الخدمة الموزعة (DDoS Attacks) • نموذج سياسة أمن الشبكات. • نموذج معيار أمن الشبكات.

		إرشادات تطبيق الضوابط: • العمل على تحديد الشبكات المعرضة لهجمات تعطيل الخدمات وهجمات تعطيل الخدمات الموزعة. • العمل على إنشاء عمليات لمراقبة الشبكة لاكتشاف الهجمات الحجمية. • العمل على إجراء تحليل عميق للحزم (Deep packet analysis) لاكتشاف حركة الشبكة التي تم إنشاؤها بواسطة الأجهزة المستغلة لغرض التعمية. • العمل على استخدم التقنيات والطرق المناسبة لإيقاف ومنع هجمات تعطيل الخدمات وهجمات تعطيل الخدمات الموزعة. **المخرجات المتوقعة:** • وثائق أو تقارير توضح الحلول والطرق المطبقة لاكتشاف ومنع هجمات تعطيل الخدمات وهجمات تعطيل الخدمات الموزعة.
	٢-٤-م-١-٤	استخدام التشفير للبيانات المنتقلة عبر الشبكة من وإلى الشبكة الخاصة بالأنظمة التقنية السحابية (CTS) لعمليات الوصول الإشرافي والإداري (Management and Administrative Access). **أدوات الأمن السيبراني ذات العلاقة:** • نموذج سياسة أمن الشبكات. • نموذج معيار أمن الشبكات. **إرشادات تطبيق الضوابط:** • العمل على تشفير شبكات الأنظمة التقنية السحابية (CTS) الإدارية والإشرافية (التفاعلية وغير التفاعلية - API) باستخدام آليات تشفير قوية تستخدم الخوارزميات والدوال المذكورة في معايير التشفير الوطنية (المستوى المتقدم). **المخرجات المتوقعة:** • إثبات يؤكد شبكات الأنظمة التقنية السحابية (CTS) مشفرة باستخدام لخوارزميات والدوال المذكورة في معايير التشفير الوطنية (المستوى المتقدم).
	٢-٤-م-١-٥	التحكم في الوصول (Access Control) بين أجزاء الشبكة (Network Segments) المختلفة. **أدوات الأمن السيبراني ذات العلاقة:** • نموذج سياسة أمن الشبكات.

		• نموذج معيار أمن الشبكات. **إرشادات تطبيق الضوابط:** • العمل على السماح فقط بحركة المرور المصادق عليها بين أجزاء الشبكة المختلفة. • العمل على تعيين اتصال الشبكة لمستخدم/هوية بحيث يكون مسؤولاً عن عمليات نقل البيانات بين أجزاء الشبكة. • العمل على إدارة التراخيص لإنشاء اتصالات عبر أجزاء الشبكة.
		المخرجات المتوقعة: • إثبات يوضح اتصالات الشبكة معينة على مستخدمين/هويات مصادق عليها. • قائمة التحكم بالوصول والقيود المطبقة.
	٢-٤-م-١-٦	العزل بين شبكات الخدمات السحابية (Cloud Service Delivery) وشبكات الإدارة السحابية (Cloud Management) والشبكة الداخلية لمقدم الخدمة (Enterprise).
		أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة أمن الشبكات. • نموذج معيار أمن الشبكات. **إرشادات تطبيق الضوابط:** • العمل على الفصل مادياً أو منطقيًا بين شبكات الجهة والشبكات المتعلقة بالخدمات السحابية وإدارة السحابة وبناء آليات عزل (على سبيل المثال: الشبكات المعرفة بالبرمجيات) لهذه الشبكات.
		المخرجات المتوقعة: • إثبات يؤكد آليات عزل الشبكات. • وثيقة التصميم المعماري.

٢-٥	أمن الأجهزة المحمولة (Mobile Devices Security)

الهدف	ضمان حماية الأجهزة المحمولة (بما في ذلك أجهزة الحاسب المحمول، والهواتف الذكية، والأجهزة اللوحية) من المخاطر السيبرانية، وضمان التعامل الآمن مع المعلومات والبيانات الحساسة التي ترتبط بأعمال مقدمي الخدمات والمشتركين، وحمايتها أثناء النقل والتخزين عند استخدام الأجهزة المحمولة.	
الضوابط		
٢-٥-م-١	بالإضافة للضوابط الفرعية ضمن الضابط ٢-٦-٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني الخاصة بأمن الأجهزة المحمولة لدى مقدمي الخدمات، بحد أدنى ما يلي:	
٢-٥-م-١-١	الاحتفاظ بقائمة جرد محدثة (Inventory) للأجهزة المحمولة.	
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة أمن أجهزة المستخدمين والأجهزة المحمولة والأجهزة الشخصية. • نموذج معيار أمن أجهزة المستخدمين. • نموذج معيار أمن الأجهزة المحمولة. **إرشادات تطبيق الضوابط:** • العمل على الحفاظ على جرد جميع أجهزة المستخدم النهائي مثل الأجهزة المحمولة والأجهزة اللوحية (على سبيل المثال: الهواتف الذكية، والساعات الذكية) ومالكيها ومستخدميها. وتشمل الأجهزة المملوكة لمزود خدمة الحوسبة السحابية (CSP) وأجهزة العاملين الشخصيةBYOD)). • التأكد من مراجعة الجرد بشكل دوري (على سبيل المثال، سنوياً).	
	المخرجات المتوقعة: • قائمة محدثة لجرد أجهزة المستخدمين والأجهزة المحمولة. • وثائق المراجعة الدورية.	
٢-٥-م-١-٢	الإدارة الأمنية للأجهزة المحمولة (Mobile Device Management) مركزياً.	
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة أمن أجهزة المستخدمين والأجهزة المحمولة والأجهزة الشخصية. • نموذج معيار أمن أجهزة المستخدمين. • نموذج معيار أمن الأجهزة المحمولة. **إرشادات تطبيق الضوابط:**	

		• العمل على تحديد المتطلبات اللازمة لإدارة أمن الأجهزة المحمولة مركزياً على سبيل المثال: تطبيق سياسة الأمان، فرض رمز (PIN) لفتح الجهاز، ومحو البيانات من الجهاز. • العمل على اختيار وتثبيت وتفعيل منصة/نظام إدارة الأجهزة المحمولة. • العمل على ربط وإضافة جميع الأجهزة المحمولة المستخدمة لغرض العمل بمنصة/نظام إدارة الأجهزة المحمولة. **المخرجات المتوقعة:** • إثبات يؤكد إدارة جميع الأجهزة المحمولة بشكل مركزي من حيث الأمان. • عيّنة من إعدادات النظام.
	٢-٥-م-١-٣	قفل الشاشة لأجهزة المستخدمين (Screen Lock). **أدوات الأمن السيبراني ذات العلاقة:** • نموذج سياسة الإعدادات والتحصين. • نموذج سياسة امن أجهزة المستخدمين والأجهزة المحمولة والأجهزة الشخصية. • نموذج معيار امن أجهزة المستخدمين. • نموذج معيار امن الأجهزة المحمولة. • خطة برنامج التوعية بالأمن السيبراني. **إرشادات تطبيق الضوابط:** • العمل على تحديد وتفعيل سياسة قفل الشاشة والخصائص ذات العلاقة (مثل: وقت الخمول (Timeout)، وطرق الفتح (Unlock Methods). • العمل على فرض هذه السياسة من خلال تفعيلها في إعدادات أجهزة المستخدمين (عبر استخدام (Active Directory GPO) أو عن طريق (End-Point Agents) أو أنظمة الإدارة عن بعد للأجهزة المحمولة (MDM). • العمل على توعية المستخدمين بقفل الشاشة يدوياً عندما لا يكونون بالقرب من أجهزتهم. • تفعيل خاصية القفل التلقائي لشاشات المستخدمين بعد مدة زمنية محددة بناءً على أفضل الممارسات. **المخرجات المتوقعة:** • إثبات يوضح فرض وتفعيل سياسة قفل الشاشة على أجهزة المستخدمين.

		• وثائق توضح وسائل توعية المستخدمين بقفل الشاشة يدويا عندما لا يكونون بالقرب من أجهزتهم.
	٢-٥-م-١-٤	قبل إعادة استخدام الأجهزة المحمولة أو التخلص منها، خصوصًا التي يتم استخدامها للدخول على الأنظمة التقنية السحابية (CTS)، يجب التأكد من عدم احتوائها على أية بيانات أو معلومات باستخدام وسائل آمنة.
		أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة امن أجهزة المستخدمين والأجهزة المحمولة والأجهزة الشخصية. • نموذج معيار امن أجهزة المستخدمين. • نموذج معيار امن الأجهزة المحمولة. **إرشادات تطبيق الضوابط:** • العمل على تحديد أجهزة المستخدمين والتقنيات المستضافة على الأنظمة التقنية السحابية على سبيل المثال: نظام التشغيل (MS Windows) و(Linux) و (Apple iOS). • العمل على اختيار وتحديد أساليب فعالة لإزالة البيانات الحساسة (Data-Sanitation) وآليات الحذف الآمن الخاصة بهذه الأنظمة. • العمل على التخلص بأمان من هذه الأجهزة والبيانات عند الضرورة.
		المخرجات المتوقعة: • قائمة معتمدة ومطبقة لأدوات وطرق إزالة البيانات الحساسة والتخلص من أجهزة المستخدمين المتعلقة بأنظمة التقنية السحابية.
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 ما يلي:	
	٢-٦-م-١-١	عدم استخدام بيانات الأنظمة التقنية السحابية (CTS) في غير بيئة الإنتاج (Production Environment) إلا بعد استخدام ضوابط مشددة لحماية تلك البيانات

		مثل: تقنيات تعتيم البيانات (Data Masking) أو تقنيات مزج البيانات (Data Scrambling).
		إرشادات تطبيق الضوابط: • العمل على فصل بيئات الإنتاج عن بيئات غير الإنتاج (التطوير) مادياً ومنطقيًا. • العمل على استخدام بيانات اصطناعية (Synthetic Data) في بيئات غير الإنتاج. • العمل على بناء حواجز منطقية لنقل البيانات من/إلى بيئة الإنتاج. • العمل على استخدام قناة/وسيلة (Channel/Gateway) مرخصة لتبادل البيانات بين البيئات التي يتم التحقق فيها من أن البيانات ذات الصلة بالأنظمة التقنية السحابية مشفرة باستخدام تقنيات تعتيم البيانات أو تقنيات مزج البيانات (Masked/Tokenized/Scrambled) بطريقة تضمن عدم إمكانية عكس هذه العملية.
		المخرجات المتوقعة: • وثيقة تؤكد فصل بيانات بيئة الإنتاج عن بيانات بيئة الاختبار. • وثائق تصميم البنية التحتية.
	٢-٦-م-١-٢	تزويد المشتركين بعمليات وإجراءات وتقنيات آمنة لتخزين البيانات، مع الالتزام بالمتطلبات التشريعية والتنظيمية ذات العلاقة.
		إرشادات تطبيق الضوابط: • العمل على تحديد المتطلبات التشريعية والتنظيمية المتعلقة بتخزين البيانات في السحابة (مثل: تشفير المعلومات الشخصية). • التأكد من تمكين الوظائف والخصائص والتقنيات (والعمليات ذات الصلة) للسماح لمشتركي خدمة الحوسبة السحابية بالامتثال لهذه الالتزامات (مثل: آليات التشفير المدمجة في خدمات السحابة). • العمل على التواصل مع مشتركي خدمة الحوسبة السحابية بشأن هذه الوظائف والخصائص.
		المخرجات المتوقعة: • قائمة بالمتطلبات القانونية والتنظيمية المعمول بها. • وثيقة توضح تقنيات وإجراءات تخزين البيانات المتوائمة مع المتطلبات القانونية.

	٢-٦-م-١-٣	حذف وإتلاف بيانات المشترك بطرق آمنة عند الانتهاء من العلاقة مع المشترك.
		إرشادات تطبيق الضوابط: • التأكد من مراقبة تاريخ انتهاء أو إنهاء عقود مشتركي خدمة الحوسبة السحابية. • العمل على التخلص من بيانات مشتركي خدمة الحوسبة السحابية في أسرع وقت ممكن عند عدم وجود عقد ساري المفعول. • العمل على التخلص من بيانات مشتركي خدمة الحوسبة السحابية وحذفها باستخدام أساليب معتمدة لضمان عدم قابلية عكس عملية الحذف، مع الأخذ في الاعتبار الأساليب التقنية المستخدمة لتخزين البيانات وقدرات استعادة البيانات التقنية المتاحة.
		المخرجات المتوقعة: • إثبات يؤكد مراقبة حالات العقود وسريان مفعولها. • سجلات بيانات مشتركي خدمة الحوسبة السحابية التي تم التخلص منها مع تحديد الأساليب المستخدمة في عملية التخلص منها.
	٢-٦-م-١-٤	الالتزام بالمحافظة على سرية بيانات ومعلومات المشترك، حسب المتطلبات التشريعية والتنظيمية ذات العلاقة.
		إرشادات تطبيق الضوابط: • العمل على تحديد وتحليل المتطلبات التشريعية والتنظيمية لتخزين ومعالجة بيانات المشترك (مثل: تشفير البيانات).
		المخرجات المتوقعة: • إثبات يؤكد أن تخزين ومعالجة بيانات المشترك تخضع للتشريعات القانونية والتنظيمية المعمول بها.
	٢-٦-م-١-٥	تزويد المشتركين بوسائل آمنة لتصدير ونقل البيانات والبنية التحتية الافتراضية.
		إرشادات تطبيق الضوابط: • العمل على بناء خدمات سحابية مع وظائف مدمجة لاستخراج ونقل البيانات والبنية التحتية الافتراضية عبر قناة أو اتصال مشفر وآمن.

		المخرجات المتوقعة: • إثبات يؤكد تأمين خصائص استخراج البيانات / الأصول عبر قناة أو اتصال مشفر وآمن.
٢-٧	**التشفير (Cryptography)**	
الهدف	ضمان استخدام التشفير بطريقة مناسبة وفعالة لحماية الأصول المعلوماتية الخاصة بمقدمي الخدمات والمشتركين وفقًا للسياسات والإجراءات التنظيمية والمتطلبات التشريعية والتنظيمية ذات العلاقة.	
الضوابط		
٢-٧-م-١	بالإضافة للضوابط الفرعية ضمن الضابط ٢-٨-٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني الخاصة بالتشفير لدى مقدمي الخدمات، بحد أدنى ما يلي:	
	٢-٧-م-١-١	الالتزام باستخدام طرق وخوارزميات ومفاتيح وأجهزة تشفير محدثة وآمنة، وفقًا للمستوى المتقدم (Advanced) ضمن المعايير الوطنية للتشفير (NCS-١:٢٠٢٠).
		أدوات الأمن السيبراني ذات العلاقة: • نموذج معيار التشفير. • نموذج معيار إدارة مفاتيح التشفير. • نموذج سياسة التشفير. **إرشادات تطبيق الضوابط:** • العمل على بناء خدمات تخزين سحابية مشفرة متوافقة مع المعايير الوطنية للتشفير (NCS-١:٢٠٢٠).
		المخرجات المتوقعة: • إثبات يوضح آليات تشفير البيانات متوافقة مع (NCS-١:٢٠٢٠).
	٢-٧-م-١-٢	القدرة على إصدار شهادات رقمية وإدارتها بطرق آمنة، أو استخدام شهادات رقمية صادرة من جهات موثوقة (Trusted Certification Authority).
		أدوات الأمن السيبراني ذات العلاقة: • نموذج معيار التشفير. • نموذج معيار إدارة مفاتيح التشفير. • نموذج سياسة التشفير.

		إرشادات تطبيق الضوابط: • العمل على بناء مصدر اعتماد الشهادات (Certification Authority) وقدرتها على الإصدار وذلك باعتبار أفضل الممارسات في هذا المجال (مثل: بيئة مخصصة ومعزولة، ومراقبة صارمة للوصول، ووجود وحدات أمان للأجهزة (Hardware Security Modules in place). • التأكد من مراجعة الشهادات المستخدمة لضمان صدورها من قبل سلطة أو مصدر اعتماد موثوق. **المخرجات المتوقعة:** • تثبيت وتفعيل مصدر/سلطة اعتماد موثوق. • شهادات موثقة ومعتمدة.
٢-٨	إدارة النسخ الاحتياطية (Backup and Recovery Management)	
الهدف	ضمان حماية بيانات ومعلومات مقدمي الخدمات والمشتركين والإعدادات التقنية للأنظمة والتطبيقات الخاصة بهم من الأضرار الناجمة عن المخاطر السيبرانية، وذلك وفقًا للسياسات والإجراءات التنظيمية لدى مقدمي الخدمات، والمتطلبات التشريعية والتنظيمية ذات العلاقة.	
الضوابط		
٢-٨-م-١	بالإضافة للضوابط الفرعية ضمن الضابط ٢-٩-٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني الخاصة بإدارة النسخ الاحتياطية لدى مقدمي الخدمات، بحد أدنى ما يلي:	
	٢-٨-م-١-١	تأمين الوصول، والتخزين، والنقل لمحتوى النسخ الاحتياطية لبيانات المشترك ووسائطها، وحمايتها من الإتلاف، أو التعديل، أو الاطلاع غير المصرح به. **أدوات الأمن السيبراني ذات العلاقة:** • نموذج سياسة النسخ الاحتياطية. • نموذج معيار النسخ الاحتياطية. • نموذج سياسة أمن وسائط التخزين. **إرشادات تطبيق الضوابط:** • العمل على تحديد المخاطر المتعلقة بالوصول، والتخزين، والنقل لمحتوى النسخ الاحتياطية لبيانات المشترك ووسائطها، بما في ذلك المخاطر المتعلقة بالإتلاف، التعديل، أو الاطلاع غير المصرح به (على سبيل المثال: التلف العرضي، السرقة، فقد الوسائط).

		• العمل على تحديد الإجراءات الأمنية لتأمين الوصول، والتخزين، والنقل لمحتوى النسخ الاحتياطية لبيانات المشترك (على سبيل المثال: التحكم في الوصول، التشفير). • العمل على تطبيق الإجراءات المحددة. • التأكد من مراجعة الإجراءات الأمنية المطبقة بشكل دوري للتأكد من قابلية تطبيقها.
		المخرجات المتوقعة: • قائمة بالمخاطر المحددة. • إثبات يوضح الإجراءات الأمنية المحددة والمطبقة. • تقارير المراجعة الدورية.
	٢-٨-م-١-٢	تأمين الوصول، والتخزين، والنقل لمحتوى النسخ الاحتياطية للأنظمة التقنية السحابية (CTS)، ووسائطها، وحمايتها من الإتلاف، أو التعديل، أو الاطلاع غير المصرح به.
		أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة النسخ الاحتياطية. • نموذج معيار النسخ الاحتياطية. • نموذج سياسة أمن وسائط التخزين. **إرشادات تطبيق الضوابط:** • العمل على تحديد المخاطر المتعلقة بالوصول، والتخزين، والنقل لمحتوى النسخ الاحتياطية للأنظمة التقنية السحابية (CTS) ووسائطها، بما في ذلك المخاطر المتعلقة بالإتلاف، التعديل، أو الاطلاع غير المصرح به (على سبيل المثال: التلف العرضي، السرقة، فقد الوسائط). • العمل على تحديد الإجراءات الأمنية لتأمين الوصول، والتخزين، والنقل لمحتوى النسخ الاحتياطية للأنظمة التقنية السحابية (CTS) (على سبيل المثال: التحكم في الوصول، التشفير). • العمل على تطبيق الإجراءات المحددة. • التأكد من مراجعة الإجراءات الأمنية المطبقة بشكل دوري للتأكد من قابلية تطبيقها.
		المخرجات المتوقعة: • قائمة بالمخاطر المحددة.

		• إثبات يوضح الإجراءات الأمنية المحددة والمطبقة. • تقارير المراجعة الدورية.
٢-٩	إدارة الثغرات (Vulnerabilities Management)	
الهدف	ضمان اكتشاف الثغرات التقنية في الوقت المناسب، ومعالجتها بشكل فعال؛ وذلك لمنع احتمالية استغلال هذه الثغرات من قبل الهجمات السيبرانية أو تقليلها، وكذلك التقليل من الآثار المترتبة على الأعمال الخاصة بمقدمي الخدمات والمشتركين.	
الضوابط		
٢-٩-م-١	بالإضافة للضوابط الفرعية ضمن الضابط ٢-١٠-٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني الخاصة بإدارة الثغرات لدى مقدمي الخدمات، بحد أدنى ما يلي:	
	٢-٩-م-١-١	تقييم ومعالجة الثغرات لمكونات الأنظمة التقنية السحابية (CTS) الخارجية مرة واحدة شهرياً على الأقل، وكل ثلاثة أشهر على الأقل لمكونات الأنظمة التقنية السحابية (CTS) الداخلية.
		أدوات الأمن السيبراني ذات العلاقة: • نموذج إجراء تقييم الثغرات الأمنية ويشمل ذلك نموذج سجل لإدارة الثغرات المكتشفة. • نموذج سجل الثغرات. • نموذج سياسة إدارة الثغرات. • نموذج معيار إدارة الثغرات. **إرشادات تطبيق الضوابط:** • العمل على تحديد وتطبيق سياسة إدارة تهديدات وثغرات الأمن السيبراني والتي تتضمن المقصد، الهدف، والحوكمة لكيفية معالجة مقدم الخدمة للتهديدات والثغرات ضمن النطاق المحدد في نموذج المسؤوليات الأمنية المشتركة كحد أدنى. يجب أن تحدد السياسة: ○ التأكد من المدة الزمنية لتقييم الثغرات الخاصة بمكونات الأنظمة التقنية السحابية (CTS) الخارجية - مرة واحدة شهرياً. ○ التأكد من المدة الزمنية لتقييم الثغرات الخاصة بمكونات الأنظمة التقنية السحابية (CTS) الداخلية - كل ثلاثة أشهر. ○ العمل على معالجة التهديدات والثغرات لمكونات الأنظمة التقنية السحابية (CTS) الخارجية والداخلية بناءً على تصنيفها والمخاطر السيبرانية المترتبة عليها. ○ العمل على تحديد طرق اكتشاف الثغرات الأمنية المستخدمة.	

		○ العمل على تحديد المكونات التي يجب تضمينها في النطاق مع مراعاة المتطلبات القانونية، التشريعية، والتعاقدية المعمول بها. ○ العمل على تصنيف مستوى شدة الثغرات بناءً على متطلبات الجهة والمدة الزمنية، وكيفية إبلاغ الأشخاص المعنيين عن الثغرات التي يجب الإبلاغ عنها ومراجعتها، لا سيما الثغرات الحرجة. ○ التأكد من كيفية تتبع الإجراءات التصحيحية لإغلاق الثغرات في الوقت المناسب بطريقة فعالة.
		المخرجات المتوقعة: • سياسة إدارة التهديدات والثغرات. • عينة من التقييمات. • عينة من خطة الإجراءات التصحيحية.
	٢-٩-م-١-٢	إشعار المشترك بالثغرات المكتشفة التي قد تؤثر عليه، وكيفية معالجتها.
		أدوات الأمن السيبراني ذات العلاقة: • نموذج إجراء تقييم الثغرات الأمنية ويشمل ذلك نموذج سجل لإدارة الثغرات المكتشفة. • نموذج سجل الثغرات. • نموذج سياسة إدارة الثغرات. • نموذج معيار إدارة الثغرات. **إرشادات تطبيق الضوابط:** • التأكد من تبليغ المشترك بالثغرات المكتشفة التي قد تؤثر عليه وتضمين معلومات كافية لتحليل المخاطر ذات الصلة وكيفية معالجتها.
		المخرجات المتوقعة: • الوثائق والتقارير المرسلة للمشتركين بخصوص الثغرات الأمنية التي قد تؤثر عليهم والتوعية بكيفية معالجتها.
٢-١٠	**اختبار الاختراق (Penetration Testing)**	
الهدف	تقييم واختبار مدى فعالية قدرات تعزيز الأمن السيبراني لدى مقدمي الخدمات، وذلك من خلال عمل محاكاة لتقنيات وأساليب الهجوم السيبراني الفعلية. ولاكتشاف نقاط الضعف الأمنية غير المعروفة والتي قد تؤدي إلى الاختراق السيبراني لمقدمي الخدمات. وذلك وفقاً للمتطلبات التشريعية والتنظيمية ذات العلاقة.	

الضوابط		
٢-١٠-م-١	بالإضافة للضوابط الفرعية ضمن الضابط ٢-١١-٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني الخاصة باختبار الاختراق لدى مقدمي الخدمات، بحد أدنى ما يلي:	
	٢-١٠-م-١-١	يجب أن يشمل نطاق عمل اختبار الاختراق الأنظمة التقنية السحابية (CTS)، وأن يتم عمل اختبار الاختراق كل ستة أشهر؛ على الأقل.
		أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة اختبار الاختراق. • نموذج معيار اختبار الاختراق. **إرشادات تطبيق الضوابط:** • العمل على تحديد مكونات الأنظمة التقنية السحابية (CTS). • العمل على اختبار الاختراق على جميع مكونات الأنظمة التقنية السحابية (CTS) دورياً (كل ستة أشهر). • التأكد من اكتمال نطاق اختبار الاختراق على الأنظمة التقنية السحابية (CTS).
		المخرجات المتوقعة: • تقارير اختبارات الاختراق على جميع مكونات الأنظمة التقنية السحابية (CTS).
٢-١١	**إدارة سجلات الأحداث ومراقبة الأمن السيبراني (Cybersecurity Event Logs and Monitoring Management)**	
الهدف	ضمان تجميع وتحليل ومراقبة سجلات أحداث الأمن السيبراني في الوقت المناسب من أجل الاكتشاف الاستباقي للهجمات السيبرانية وإدارة مخاطرها بفعالية لمنع أو تقليل الآثار المترتبة على أعمال مقدمي الخدمات والمشتركين.	
الضوابط		
٢-١١-م-١	بالإضافة للضوابط الفرعية ضمن الضابط ٢-١٢-٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني لإدارة سجلات الأحداث ومراقبة الأمن السيبراني لدى مقدمي الخدمات، بحد أدنى ما يلي:	
	٢-١١-م-١-١	تفعيل وحماية سجلات الأحداث (Event Logs) والتدقيق (Audit Trial) للأنظمة التقنية السحابية (CTS).
		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 وتطبيق سياسة إدارة سجلات الأحداث والتي تتضمن المقصد، الهدف، والحوكمة لكيفية تفعيل مقدم الخدمة لسجلات أحداث الأمن السيبراني ومراقبتها ضمن النطاق المحدد في نموذج المسؤوليات الأمنية المشتركة كحد أدنى. يجب أن تحدد السياسة: ○ العمل على طرق حماية السجلات التي يتم انشاؤها من التلاعب أو من تقنيات التهرب من التسجيل. ○ العمل على طرق حماية السجلات أثناء النقل الى مستودع السجلات للحفاظ على سريتها وسلامتها (على سبيل المثال: التشفير). المخرجات المتوقعة: • سياسة ادارة سجلات الأحداث. • إثبات يؤكد وجود نظام مركزي ومحمي لجمع سجلات الأحداث.
	٢-١١-م-١-٢	تفعيل سجلات الأحداث الخاصة بمحاولات عمليات الدخول (Login) وجمعها. **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 إعداد آليات التحقق لتسجيل محاولات الدخول (على سبيل المثال: البيانات، الوقت، طريقة التحقق، اسم النظام/التطبيق، هوية المستخدم). • العمل على جمع وحفظ هذه المعلومات بطريقة آمنة. **المخرجات المتوقعة:** • إثبات يوضح آليات التحقق من محاولات الدخول. • إثبات يوضح محاولات الدخول المسجلة والمخزنة.
	٢-١١-م-١-٣	تفعيل وحماية سجلات الأحداث لجميع الأنشطة والعمليات التي يقوم بها مقدم الخدمة على أنظمة المشتركين، بهدف دعم عمليات التحليل الرقمي الجنائي (Digital Forensics).

		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 متطلبات تسجيل أنشطة مقدم الخدمة (CSP) والمشتركين (CST) بشكل كافي لدعم التحليل الجنائي (على سبيل المثال: سلسلة عهدة الأدلة). • العمل على تفعيل خاصية التسجيل لالتقاط الأحداث/الأنشطة وحماية السجلات (على سبيل المثال: التأكد من سرية وسلامة وتوافر السجلات عن طريق التشفير، دوال اختزال رموز توثيق الرسائل (HMAC)، التخزين المكرر (Redundant Storage). **المخرجات المتوقعة:** • إثبات يوضح أحداث/أنشطة مقدمي الخدمة (CSP) والمشتركين (CST).
	٢-١١-م-١-٤	حماية سجلات الأحداث (Event Logs) الخاصة بالأمن السيبراني، من الوصول غير المصرح به، أو العبث، أو التغيير، أو الحذف غير المشروع، وذلك وفقًا للمتطلبات التشريعية، أو التنظيمية.
		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 المتطلبات القانونية والتشريعية المتعلقة بسجلات التدقيق. • العمل على تحديد وتطبيق سياسة إدارة سجل الأمن السيبراني والتحكم في الوصول التي تتضمن المقصد، الهدف، والحوكمة لكيفية تمكين مقدم الخدمة (CSP) لتسجيل ومراقبة أحداث الأمن السيبراني لنطاقها بموجب نموذج المسؤولية الأمنية المشتركة. كحد أدنى، يجب أن تحدد السياسات ما يلي: ○ التأكد من طرق حماية السجلات حيث يتم إنشاؤها لمنع التلاعب بالسجل أو التهرب من تقنيات التسجيل. ○ التأكد من طرق حماية السجلات اثناء النقل إلى مستودع السجلات للحفاظ على سريتها وسلامتها (على سبيل المثال: التشفير). ○ التأكد من طرق إتلاف السجل بشكل أمن. ○ العمل على تقييد الوصول إلى السجلات.

		○ العمل على إعطاء صلاحية القراءة فقط لاستعراض سجلات الأحداث.
		المخرجات المتوقعة: ● إثبات يؤكد حماية سجلات أحداث الأمن السيبراني. ● إثبات يوضح القيود المطبقة لحماية السجلات. ● إثبات يوضح آليات إتلاف السجل بشكل آمن. ● قائمة المتطلبات القانونية والتشريعية لسجلات التدقيق.
	٢-١١-م-١-٥	المراقبة الأمنية المستمرة لأحداث الأمن السيبراني (Cybersecurity Events) باستخدام تقنيات (SIEM) بحيث تشمل جميع الأحداث المتعلقة بالأنظمة التقنية السحابية (CTS).
		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 متطلبات مراقبة أحداث الأمن السيبراني (على سبيل المثال: تسجيل عمليات التحقق من هوية المستخدم، رفع الامتيازات، تشغيل البرامج). ● العمل على تحديد نطاق مراقبة أحداث الأمن السيبراني لتشمل جميع الاحداث المتعلقة بالأنظمة التقنية السحابية (Cloud Technology Stack). ● العمل على تحديد ونشر نظام SIEM لمراقبة سجلات أحداث الأمن السيبراني. ● العمل على مراقبة سجلات أحداث الأمن السيبراني بشكل مستمر (يومياً على الأقل).
		المخرجات المتوقعة: ● إثبات يؤكد مراقبة سجلات الأمن السيبراني في SIEM. ● قائمة بمتطلبات مراقبة أحداث الأمن السيبراني. ● عينة من تقارير / تنبيهات المراقبة.
	٢-١١-م-١-٦	المراجعة الدورية لسجلات الأحداث (Event Logs) والتدقيق (Audit Trail) بحيث تشمل الأحداث والسجلات المتعلقة بالأنظمة التقنية السحابية (CTS)، التي تم تنفيذها من قبل مقدم الخدمة.

		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 نطاق مراجعة سجلات أحداث مقدمي الخدمة بحيث تشمل الأحداث والسجلات المتعلقة بالأنظمة التقنية السحابية (CTS). • العمل على تحديد معايير المراجعة. • العمل على اختيار وتعيين مراجعين مهارات ومستقلين لسجلات أحداث الأمن السيبراني / مسارات التدقيق. • العمل على اختيار وتعيين مراجعين مستقلين وذو كفاءة عالية لمراجعة سجلات أحداث الأمن السيبراني / مسارات التدقيق. • التأكد من مراجعة سجلات أحداث الأمن السيبراني/ مسارات التدقيق دورياً. **المخرجات المتوقعة:** • تقارير مراجعة سجلات أحداث الأمن السيبراني من قبل مراجعين مستقلين ذو كفاءة عالية. • عينة من التقارير والتنبيهات وحالات الاستخدام (Use Case).
	٢-١١-م-١-٧	استخدام وسائل آلية لمراقبة سجلات الأحداث الخاصة بعمليات الدخول عن بعد (Remote Access). **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 تسجيل عمليات الدخول عن بعد والأحداث ذات الصلة. • العمل على تحديد علامات ومؤشرات وأنماط عمليات الدخول عن بعد الضارة. • التأكد من مراقبة واكتشاف ومنع عمليات الدخول عن بعد تلقائياً. **المخرجات المتوقعة:** • إثبات يوضح عمليات الدخول عن بعد المراقبة تلقائياً.

	٢-١١-م-١-٨	التعامل الآمن مع بيانات المستخدمين المتواجدة في سجلات الأحداث (Event Logs) والتدقيق (Audit Trails) وسجلات أحداث الأمن السيبراني (Cybersecurity Events Logs).
		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 الكشف عن بيانات سجلات الأحداث / مسارات التدقيق المتعلقة بالمستخدم. • التأكد من إخفاء هوية تلك البيانات باستخدام (Tokens).
		المخرجات المتوقعة: • إثبات يوضح معلومات الهوية الشخصية تكون مجهولة في السجلات.
٢-١٢	إدارة حوادث وتهديدات الأمن السيبراني (Cybersecurity Incident and Threat Management)	
الهدف	ضمان تحديد واكتشاف حوادث الأمن السيبراني في الوقت المناسب وإدارتها بشكل فعّال والتعامل مع تهديدات الأمن السيبراني استباقيًا من أجل منع أو تقليل الآثار المترتبة على أعمال مقدمي الخدمات.	
الضوابط		
٢-١٢-م-١	بالإضافة للضوابط الفرعية ضمن الضابط ٢-١٣-٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني لإدارة حوادث وتهديدات الأمن السيبراني لدى مقدمي الخدمات، بحد أدنى ما يلي:	
	٢-١٢-م-١-١	الاشتراك مع المجموعات والجهات المتخصصة والموثوقة للحصول على آخر التهديدات والمستجدات في مجال الأمن السيبراني.
		أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة إدارة حوادث وتهديدات الأمن السيبراني. • نموذج معيار إدارة حوادث وتهديدات الأمن السيبراني. • الدليل الإرشادي للاستجابة لحوادث الأمن السيبراني. • نماذج الخطط التفصيلية للاستجابة لحوادث الأمن السيبراني. **إرشادات تطبيق الضوابط:**

		• العمل على تحديد جهات خارجية مختصة وموثوقة للحصول على المعلومات الاستباقية (مثل: OSINT). • العمل على متابعة النشرات الصادرة من هيئة الأمن السيبراني والجهات المختصة والموثوقة. • العمل على تحليل موجزات وخدمات المعلومات الاستباقية للمخاطر ذات العلاقة بمقدمي الخدمة. • العمل على تحديد افضل الممارسات في إدارة التهديدات مع مستشاري الأمن السيبراني الخارجيين.
		المخرجات المتوقعة: • قائمة بالجهات الخارجية الموثوقة والمختصة بتقديم المعلومات الاستباقية. • إثبات يوضح معلومات استباقية عن حوادث الأمن السيبراني. • إثبات يوضح قاعدة معرفية لأفضل الممارسات في مجال الأمن السيبراني.
	٢-١٢-م-١-٢	تدريب العاملين (موظفين ومتعاقدين) على الاستجابة لحوادث الأمن السيبراني بما يتماشى مع الأدوار والمسؤوليات.
		أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة إدارة حوادث وتهديدات الأمن السيبراني. • نموذج معيار إدارة حوادث وتهديدات الأمن السيبراني. • الدليل الإرشادي للاستجابة لحوادث الأمن السيبراني. • نماذج الخطط التفصيلية للاستجابة لحوادث الأمن السيبراني. **إرشادات تطبيق الضوابط:** • العمل على إنشاء برنامج تدريبي للأمن السيبراني للموظفين والمتعاقدين. • العمل على تدريب الموظفين على الإبلاغ عن حوادث الأمن السيبراني والتعامل معها بناءً على أدوارهم ومسؤولياتهم (على سبيل المثال: ما هو حادث الأمن السيبراني وكيفية الإبلاغ عنه). • التأكد من ملائمة البرنامج التدريبي مع الأدوار والمسؤوليات المختلفة.
		المخرجات المتوقعة: • وثائق توضح برنامج تدريبي للأمن السيبراني يلائم أدوار ومسؤوليات مختلف الفئات للإبلاغ عن حوادث الأمن السيبراني والتعامل معها. • عينة من شهادة/ حضور التدريب.

	٢-١٢-م-١-٣	اختبار قدرات الاستجابة لحوادث الأمن السيبراني دورياً. **أدوات الأمن السيبراني ذات العلاقة:** • نموذج سياسة إدارة حوادث وتهديدات الأمن السيبراني. • نموذج معيار إدارة حوادث وتهديدات الأمن السيبراني. • الدليل الإرشادي للاستجابة لحوادث الأمن السيبراني. • نماذج الخطط التفصيلية للاستجابة لحوادث الأمن السيبراني. **إرشادات تطبيق الضوابط:** • العمل على جدولة المراجعة الدورية لخطط الاستجابة للحوادث. • العمل على تحديد منهجية الاختبار واستخدام طريقة الاختبار المناسبة (على سبيل المثال: تدريب محاكاة الجاهزية، الإرشادات التفصيلية، محاكاة الحوادث). • التأكد من تضمين الدروس المستفادة في منهجية الاختبار لتكون مرحلة إلزامية. **المخرجات المتوقعة:** • إثبات خطة الاستجابة للحوادث / جدول اختبار الإجراء. • وثيقة توضح منهجية اختبار قدرات الاستجابة لحوادث الأمن السيبراني. • سجلات الدروس المستفادة.
	٢-١٢-م-١-٤	تحليل وتحديد الأسباب الجذرية (Root Cause Analysis) لحوادث الأمن السيبراني، ووضع الخطط الكفيلة بمعالجتها. **أدوات الأمن السيبراني ذات العلاقة:** • نموذج سياسة إدارة حوادث وتهديدات الأمن السيبراني. • نموذج معيار إدارة حوادث وتهديدات الأمن السيبراني. • الدليل الإرشادي للاستجابة لحوادث الأمن السيبراني. • نماذج الخطط التفصيلية للاستجابة لحوادث الأمن السيبراني. **إرشادات تطبيق الضوابط:** • العمل على تحسين خطط الاستجابة للحوادث لكي تكون مرحلة تحليل الأسباب الجذرية (Root Cause Analysis) إلزامية في الاستجابة للحوادث. • التأكد من جمع وتحليل وتحديد أولويات ومعالجة استنتاجات تحليلات الأسباب الجذرية (Root Cause Analyses).

		المخرجات المتوقعة: • وثيقة توضح خطة الاستجابة للحوادث التي تتضمن مرحلة تحليل الأسباب الجذرية. • إثبات يؤكد تحديد الأولويات لاستنتاجات تحليل السبب الجذري (Root Cause Analysis) ومعالجتها. • إثبات يؤكد التحسين المستمر لخطة الاستجابة للحوادث بناءً على استنتاجات تحليل السبب الجذري (Root Cause Analysis). • عينة من تحليل الأسباب الجذرية (Root Cause Analysis).
	٢-١٢-م-١-٥	تقديم الدعم إلى المشتركين في حالات القضايا القانونية، والتحليل الرقمي الجنائي، والحفاظ على الأدلة الرقمية التي تقع تحت إدارة ومسؤولية مقدم الخدمة حسب المتطلبات التشريعية والتنظيمية ذات العلاقة.
		أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة إدارة حوادث وتهديدات الأمن السيبراني. • نموذج معيار إدارة حوادث وتهديدات الأمن السيبراني. • الدليل الإرشادي للاستجابة لحوادث الأمن السيبراني. • نماذج الخطط التفصيلية للاستجابة لحوادث الأمن السيبراني. **إرشادات تطبيق الضوابط:** • العمل على تحليل المتطلبات القانونية والتشريعية للمشتركين (CSTs). • العمل على بناء القدرات القانونية والتحليلية الجنائية لدعم المشتركين (CSTs) في التزاماتهم القانونية ذات العلاقة بالخدمات السحابية. • العمل على إنشاء اجراء لتتبع حركة الادلة للتأكد من سلامتها اثناء النقل والتخزين.
		المخرجات المتوقعة: • إثبات يؤكد فهم ومعرفة المتطلبات القانونية والتشريعية للمشتركين. • إنشاء/ بناء القدرات القانونية والتحليل الجنائي. • إثبات يؤكد مراقبة عملية نقل الأدلة والتأكد من سلامتها.
	٢-١٢-م-١-٦	تبليغ المشترك بشكل فوري عن حوادث الأمن السيبراني التي قد تؤثر عليه، في حال اكتشاف الحادثة.

		أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة إدارة حوادث وتهديدات الأمن السيبراني. • نموذج معيار إدارة حوادث وتهديدات الأمن السيبراني. • الدليل الإرشادي للاستجابة لحوادث الأمن السيبراني. • نماذج الخطط التفصيلية للاستجابة لحوادث الأمن السيبراني. **إرشادات تطبيق الضوابط:** • العمل على تحليل الحوادث المحددة لمعرفة تأثيرها على المشتركين (CSTs) (مثل: كيفية استخدام المشتركين للخدمة المتأثرة). • التأكد من الإبلاغ فوراً عن هذه الحوادث للمشتركين (CST) مع معلومات كافية. يجب على مقدم الخدمة تحليل المخاطر المترتبة ومتابعة الاستجابة للحوادث.
		المخرجات المتوقعة: • إثبات يؤكد تحليل تأثير جميع الحوادث المحددة على المشتركين (CSTs). • إثبات يؤكد الإبلاغ عن الحوادث التي تؤثر على المشتركين (CSTs) على الفور مع معلومات كافية. • عينة من حوادث تم إبلاغ المشترك (CST) عنها.
	٢-١٢-م-١-٧	دعم المشتركين للتعامل مع حوادث الأمن السيبراني حسب الاتفاقية ما بين مقدم الخدمة والمشترك.
		أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة إدارة حوادث وتهديدات الأمن السيبراني. • نموذج معيار إدارة حوادث وتهديدات الأمن السيبراني. • الدليل الإرشادي للاستجابة لحوادث الأمن السيبراني. • نماذج الخطط التفصيلية للاستجابة لحوادث الأمن السيبراني. **إرشادات تطبيق الضوابط:** • العمل على مواءمة إجراءات التعامل مع الحوادث بين مقدم الخدمة (CSP) والمشتركين (CST) قبل تقديم الخدمات (على سبيل المثال: تكامل أنظمة الاستجابة للحوادث).

		• العمل على إبلاغ المشتركين (CSTs) عن الحوادث (التي تؤثر بهم) فوراً مع المعلومات الكافية لتحليل المخاطر ذات الصلة ولمواءمة الاستجابة للحوادث عند المشتركين.
		المخرجات المتوقعة: • وثيقة العقد بين مقدم الخدمة والمشتركين والذي يتضمن اجراءات التعامل مع الحوادث المتفق عليها. • إثبات يوضح عملية الإبلاغ عن الحوادث التي تؤثر على المشتركين التي تم إنشائها.
	٢-١٢-م-١-٨	قياس ومراقبة مؤشرات الأداء الخاصة بإدارة حوادث الأمن السيبراني، ومراقبة مدى الالتزام بمتطلبات العقود والتشريعات.
		أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة إدارة حوادث وتهديدات الأمن السيبراني. • نموذج معيار إدارة حوادث وتهديدات الأمن السيبراني. • الدليل الإرشادي للاستجابة لحوادث الأمن السيبراني. • نماذج الخطط التفصيلية للاستجابة لحوادث الأمن السيبراني. • نموذج تقرير مؤشرات الأداء الرئيسية. **إرشادات تطبيق الضوابط:** • العمل على تحديد المتطلبات التعاقدية والتشريعية لإدارة حوادث الأمن السيبراني. • العمل على إنشاء مقاييس حوادث الأمن السيبراني (الامتثال والفعالية) في شكل (KPI) و(KCI) (على سبيل المثال: متوسط وقت الاكتشاف، متوسط وقت الاستجابة، متوسط وقت الاحتواء). • التأكد من أن يتم اختبار المقاييس. • اعتماد المقاييس من قبل الشخص المسؤول. • العمل على إنشاء لوحات المعلومات (dashboards) وتقارير الالتزام للإبلاغ عن المقاييس. • التأكد من مراجعة لوحات المعلومات (dashboards) وتقارير الالتزام دورياً.
		المخرجات المتوقعة: • سجل المتطلبات التعاقدية والتشريعية.

		• إثبات يوضح مقاييس حوادث الأمن السيبراني (KPI, KCI) التي تم اختبارها واعتمادها. • إثبات يوضح لوحة المعلومات (dashboards) وتقارير الالتزام الخاصة بالمقاييس. • وثيقة نماذج سجلات لوحات المعلومات (dashboards) ومراجعة تقارير الالتزام. • عينة من لوحة المعلومات (dashboards) وتقرير الالتزام.
٢-١٣	الأمن المادي (Physical Security)	
الهدف	ضمان حماية الأصول المعلوماتية والتقنية الخاصة بمقدمي الخدمات من الوصول المادي غير المصرح به والفقدان والسرقة والتخريب.	
الضوابط		
٢-١٣-م-١	بالإضافة للضوابط الفرعية ضمن الضابط ٢-١٤-٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني الخاصة بالأمن المادي لدى مقدمي الخدمات، بحد أدنى ما يلي:	
	٢-١٣-م-١-١	المراقبة المستمرة لعمليات الدخول والخروج للمباني والمواقع لدى مقدم الخدمة.
		أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني المتعلق بالأمن المادي. • نموذج معيار المادي. **إرشادات تطبيق الضوابط:** • العمل على تحديد جميع نقاط الوصول / بوابات المواقع والمباني. • العمل على تعريف نقاط الهجوم ضد نقاط الوصول (نظرًا للاستخدام الغير المصرح به، وإعادة استخدام رموز الوصول المسروقة، والتلاعب بأنظمة منع الوصول). • العمل على تعريف متطلبات مراقبة الوصول إلى مواقع ومباني مزودي خدمات الحوسبة السحابية. • العمل على تعريف عملية مراقبة الوصول وكشف انتهاكات الوصول بطريقة فعالة. • العمل على تنفيذ أنظمة تقنية لمراقبة الوصول بطريقة فعالة. • العمل على ضم المحللين المدربين عند الحاجة إلى الحكم المهني في عملية المراقبة.

		• الاحتفاظ بسجلات المراقبة - سجلات الوصول ومن ومتى تمت مراجعة هذه السجلات لمدة لا تقل عن ستة (٦) أشهر. • العمل على تسجيل تواريخ وأوقات دخول ومغادرة الزائرين ومراقبة جميع الزائرين ما لم يتم الموافقة على وصولهم مسبقًا. • التأكد من مراقبة نقاط الدخول والخروج إلى مناطق الخدمة والتسليم ونقاط أخرى يمكن للأشخاص غير المصرح لهم الدخول إلى المبنى. • التأكد من مراقبة الوصول عن طريق مراجعة سجلات الوصول ومحاولات الوصول وتسجيلات الوصول. **المخرجات المتوقعة:** • إثبات يؤكد جرد أبواب ونقاط الوصول للمواقع والمباني. • إثبات يؤكد توثيق نقاط الهجوم المعرفة، ومتطلبات مراقبة الوصول وعملية مراقبة الوصول (الإجراء أو التعليمات). • وثيقة سجلات وتسجيلات الوصول. • وثائق مراجعة سجلات وتسجيلات الوصول.
	٢-١٣-م-١-٢	منع الوصول غير المصرح به للأجهزة التي تتعامل مباشرة مع الأنظمة التقنية السحابية (CTS). **أدوات الأمن السيبراني ذات العلاقة:** • نموذج سياسة الأمن السيبراني المتعلق بالأمن المادي. • نموذج معيار الأمن المادي. **إرشادات تطبيق الضوابط:** • العمل على بناء حاجز أمني معزول لمناطق تخزين البيانات ومعالجتها، بما في ذلك الأبواب وآليات المصادقة الفيزيائية ونقاط التحكم في الوصول ومعدات المراقبة. • العمل على وضع أجهزة تكنولوجيا السحابة في منطقة آمنة داخل الحاجز في غرفة الخادم المخصصة بالوصول المحدود للأشخاص المصرح لهم فقط. • التأكد من تأمين الأجهزة في تكنولوجيا السحابة باستخدام صناديق حماية لمنع الضرر أو إدخال أجهزة خارجية مثل (محركات أقراص USB ومحركات أقراص SSDالمحمولة وما إلى ذلك). **المخرجات المتوقعة:** • إثبات يؤكد وجود محيط مغلق بشكل فيزيائي للخوادم وتخزين البيانات مع نقاط تحكم في الوصول.

		• إثبات يوضح الأجهزة مقفلة في رفوف آمنة تمنع الضرر وإدخال الأجهزة الخارجية المحمولة.
	٢-١٣-م-١-٣	التخلص الآمن من أجهزة البنية التحتية (Infrastructure Hardware)، وبالأخص معدات التخزين (Storage Equipment) باتباع أفضل الممارسات والتشريعات ذات العلاقة.
		أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني المتعلق بالأمن المادي. • نموذج معيار الأمن المادي. **إرشادات تطبيق الضوابط:** • العمل على تحديد اللوائح القانونية وأفضل الممارسات للتخلص من الأجهزة الأساسية. • العمل على تعريف الأدوار والمسؤوليات في عملية التخلص. • العمل على اختيار أساليب تدمير وتطهير الأجهزة (Storage Cleansing and Destruction)، (مثل: المسح الكريبتوغرافي، إزالة المغناطيسية، تدمير المواد الفيزيائية للوسائط: الطحن، الحرق، الذوبان، إلخ أو التقطيع الصناعي) المناسبة لنوع الأجهزة مع ضمان عدم إمكانية استرداد البيانات المخزنة على هذه الأجهزة. • العمل على تسجيل عملية التخلص من الأجهزة.
		المخرجات المتوقعة: • وثائق تؤكد جمع اللوائح القانونية وأفضل الممارسات للتخلص من الأجهزة الأساسية. • إثبات يؤكد الموافقة رسميًا على سياسة التخلص من الأجهزة الأساسية في بنية السحابة. • إثبات يؤكد إنشاء نظام لتسجيل وتتبع عملية التخلص من الأجهزة الأساسية.
٢-١٤	حماية تطبيقات الويب (Web Application Security)	
الهدف	ضمان حماية تطبيقات الويب الخارجية لدى مقدمي الخدمات ضد المخاطر السيبرانية.	
الضوابط		

٢-١٤-م-١	بالإضافة للضوابط الفرعية ضمن الضابط ٢-١٥-٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني الخاصة بحماية تطبيقات الويب لدى مقدمي الخدمات، بحد أدنى ما يلي:	
	٢-١٤-م-١-١	حماية المعلومات المستخدمة في إجراء المعاملات عن طريق تطبيقات الويب من المخاطر المحتملة، مثل: انقطاع الاتصال (Incomplete Transmission)، التوجيه الخاطئ (Mis-routing)، التعديل غير المصرح به، الاطلاع غير المصرح به.
		أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة حماية تطبيقات الويب. • نموذج معيار حماية تطبيقات الويب. **إرشادات تطبيق الضوابط:** • العمل على تحديد المخاطر المحتملة المتعلقة بالمعلومات المشاركة في معاملات خدمات التطبيقات. • العمل على تحديد التدابير الأمنية التي يمكن تطبيقها لحماية المعلومات المشاركة في معاملات خدمات التطبيقات ضد المخاطر المحددة. • العمل على تنفيذ التدابير الأمنية المحددة. • التأكد من مراجعة وتحديث المخاطر المحددة والتدابير المتبعة بشكل دوري (أو إضافة جديدة إذا كانت ذات صلة) لضمان تطبيقها. • العمل على تكوين جدران الحماية لتطبيقات الويب لفحص حركة المرور، وتطبيق القواعد، وإجراء المراقبة السلوكية. • التأكد من حظر الوصول من المصادر المعروفة بالخبث أو السمعة السيئة. • التأكد من تطبيق بروتوكول أمان طبقة النقل (TLS) أو طبقة حماية أخرى لتشفير نقل البيانات والتكامل. • التأكد من مراجعة دورية تعرض التطبيق للإنترنت لاكتشاف التعرض غير المقصود للبيانات. • التأكد من رفض كلمات المرور الافتراضية أو الشائعة للتطبيقات. • التأكد من مراقبة جداول التوجيه للتغييرات الضارة / غير المقصودة أو عمليات إعادة توجيه الخدمة. • العمل على إنشاء مراقبة مستمرة للمعاملات أقرب إلى الوقت الحقيقي.
		المخرجات المتوقعة: • إثبات يوضح تكوين جدران حماية تطبيقات الويب بشكل مناسب. • إنشاء التفتيش على حركة المرور ومراقبة السلوك. • إثبات يؤكد حجب الوصول من مصادر خبيثة و / وسمعة سيئة معروفة. • إثبات يؤكد تطبيق طبقة حماية تكامل وتشفير نقل البيانات (TLS).

		• إثبات يؤكد التعرض المنتظم للتطبيق لمراجعة الإنترنت ومجموعة الكشف عن التعرض غير المقصود للبيانات. • إثبات يوضح رفض كلمات المرور الافتراضية أو الشائعة للتطبيقات. • إثبات يوضح تحديد التغييرات الخبيثة / غير المقصودة أو عمليات إعادة توجيه الخدمة في جداول التوجيه التي تم تنفيذها. • وثائق أو تقارير تؤكد المراقبة المستمرة للمعاملات المنشأة.
٢-١٥	إدارة المفاتيح (Key Management)	
الهدف	ضمان الإدارة الآمنة لمفاتيح التشفير، لحماية السرية والسلامة والتوافر للأصول المعلوماتية والتقنية، لدى مقدمي الخدمات والمشتركين.	
الضوابط		
٢-١٥-م-١	يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني، الخاصة بعملية إدارة المفاتيح لدى مقدمي الخدمات.	
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة التشفير. • نموذج معيار إدارة مفاتيح التشفير. **إرشادات تطبيق الضوابط:** • العمل على تحديد متطلبات الأمن السيبراني لجوانب إدارة المفاتيح (مثل: تبادل المفاتيح، التخزين، الاستخدام، الملكية)، استخدام الخوارزميات والدوال المذكورة في معايير التشفير الوطنية (المستوى المتقدم). • العمل على تعريف معيار إدارة المفاتيح لتلبية متطلبات الأمن السيبراني. • التأكد من الموافقة الرسمية على المعيار. • التأكد من مراجعة المعيار بشكل دوري (على سبيل المثال: سنوياً على الأقل).	
	المخرجات المتوقعة: • وثيقة توضح معيار إدارة المفاتيح الذي يتمتع بالموافقة الرسمية ويتم مراجعته بشكل دوري. • تقارير المراجعة الدورية.	
٢-١٥-م-٢	يجب تطبيق متطلبات الأمن السيبراني، الخاصة بعملية إدارة المفاتيح لدى مقدمي الخدمات.	
	إرشادات تطبيق الضوابط: • العمل على تطبيق معيار إدارة المفاتيح المحددة (مثل: تحسين خدمة إدارة المفاتيح، تقييد الوصول والمراقبة). • العمل على التحكم في تنفيذ المعيار بشكل فعّال.	

		• التأكد من الإبلاغ عن انتهاكات المعيار. • التأكد من توثيق وإدارة التوقعات.
		المخرجات المتوقعة: • إثبات يؤكد تنفيذ ومتابعة متطلبات الأمن السيبراني لعملية إدارة المفاتيح وفقاً للسياسة المحددة والوثائق المرتبطة
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).
		أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة التشفير. **إرشادات تطبيق الضوابط:** • العمل على تحديد المسؤوليات المترتبة على مالكي المفاتيح التشفيرية خلال دورة حياة المفتاح بأكملها (مثلاً: إنشاء مفتاح، التصريح باستخدام المفتاح، التخلص من المفتاح). • العمل على تعيين ملكية المفاتيح التشفيرية لموظفي مزود الخدمة السحابية. • التأكد من مراجعة المفاتيح التشفيرية بشكل دوري للتأكد من عدم وجود المفاتيح اليتامى (يجب أن يكون لكل مفتاح مالك نشط معين). • العمل على تعيين مالكين للمفاتيح التشفيرية الجديدة كخطوة إلزامية عند إنشاء المفاتيح.
		المخرجات المتوقعة: • إثبات يوضح تحديد المفاتيح التشفيرية وأصحابها.
	٢-١٥-م-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 سياسة التشفير. **إرشادات تطبيق الضوابط:** • العمل على وضع واختبار خطط استعادة المفاتيح التشفيرية لفقدان أو تلف المفاتيح التشفيرية (مثلاً: طباعة المفاتيح التشفيرية، ووضعها في أظرف مع وضع

		علامات، وتخزينها في خزائن في أماكن خارجية آمنة وموثوقة مثل صناديق الإيداع أو حاويات آمنة في البنوك).
		المخرجات المتوقعة: • وثيقة توضح خطة استرجاع المفاتيح التشفيرية.
	٢-١٥-م-٣-٣	تفعيل سجلات الأحداث المتعلقة بمفاتيح التشفير، ومراقبتها.
		أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة التشفير. **إرشادات تطبيق الضوابط:** • العمل على أنشطة إدارة مفتاح السجل (على سبيل المثال: تاريخ الإنشاء، تاريخ التجديد، تاريخ انتهاء الصلاحية، تاريخ إيقاف التشغيل، تفاصيل المفتاح والشهادة، متى تم الوصول إلى المفتاح من قبل المستخدمين ولأي غرض، أي تفاصيل إضافية تتطلبها المتطلبات القانونية أو التنظيمية). • العمل على بناء قدرة مراقبة من فئة SIEM لهذه السجلات.
		المخرجات المتوقعة: • وثيقة توضح مقارنة قائمة الخدمات السحابية النشطة بقائمة الخدمات السحابية المراقبة. • عينة من تقارير / تنبيهات / حالات استخدام نظام إدارة معلومات الأمان والأحداث (SIEM).
٢-١٥-م-٤		يجب مراجعة متطلبات الأمن السيبراني، الخاصة بإدارة المفاتيح لدى مقدمي الخدمات، ومراجعة تطبيقها دورياً.
		أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة مراجعة وتدقيق الأمن السيبراني. • نموذج يشرح دورة حياة عملية إدارة الإجراءات والسياسات ومعايير الأمن السيبراني، بما في ذلك البناء والتطوير والاعتمادات والمراجعات الدورية. **إرشادات تطبيق الضوابط:** • التأكد من مراجعة متطلبات الأمن السيبراني لإدارة المفاتيح بشكل دوري، على الأقل مرة في السنة. • العمل على الاحتفاظ بسجلات المراجعات الدورية (مثل: من قام بالمراجعة ومتى تمت المراجعة وسجل التغييرات).

	المخرجات المتوقعة: • إثبات يؤكد وجود متطلبات الأمن السيبراني لإدارة المفاتيح بشكل دوري. • سجلات المراجعات الدورية.
٢-١٦	**أمن تطوير الأنظمة (System Development Security)**
الهدف	ضمان تطوير الأنظمة لدى مقدم الخدمة، وتكاملها، ونشرها بطريقة آمنة.
الضوابط	
٢-١٦-م-١	يجب تحديد متطلبات الأمن السيبراني لتطوير الأنظمة لدى مقدمي الخدمات، وتوثيقها واعتمادها.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة دورة حياة تطوير البرمجيات الآمنة. **إرشادات تطبيق الضوابط:** • العمل على تحديد متطلبات الأمن السيبراني لتطوير النظام باستخدام الاستبيانات وورش العمل مع أصحاب المصلحة ذوي الصلة. • العمل على توثيق هذه المتطلبات (معيار الأمن السيبراني لتطوير النظام).
	المخرجات المتوقعة: • إثبات يؤكد الموافقة الرسمية والمراجعة الدورية لمتطلبات الأمن السيبراني لتطوير النظام.
٢-١٦-م-٢	يجب تطبيق متطلبات الأمن السيبراني لتطوير الأنظمة لدى مقدمي الخدمات.
	إرشادات تطبيق الضوابط: • العمل على فرض معيار الأمن السيبراني لتطوير النظام. • العمل على قياس الامتثال لهذا المعيار. • العمل على إدارة الاستثناءات لهذا المعيار. • العمل على تصعيد المخالفات المتعلقة بهذا المعيار.
	المخرجات المتوقعة: • إثبات يؤكد فرض متطلبات الأمن السيبراني للمعيار الآمن لتطوير النظام. • وثيقة أداة قياس الامتثال لتطبيق المعيار. • وثائق إجراءات تصعيد المخالفات.
٢-١٦-م-٣	يجب أن تغطي متطلبات الأمن السيبراني لتطوير الأنظمة لدى مقدمي الخدمات بحد أدنى الضوابط التالية خلال دورة حياة التطوير:

	٢-١٦-م-٣-١	أخذ متطلبات الأمن السيبراني (للأنظمة التقنية السحابية (CTS)، والأنظمة ذات العلاقة) بالاعتبار عند تصميم وتطوير خدمات الحوسبة السحابية.
		أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة دورة حياة تطوير البرمجيات الآمنة. **إرشادات تطبيق الضوابط:** • العمل على تحديد متطلبات الأمن السيبراني للتكنولوجيا السحابية والأنظمة ذات الصلة لخدمات الحوسبة السحابية. • العمل على تطبيق المتطلبات المحددة خلال عملية التصميم والتنفيذ لخدمات الحوسبة السحابية. • التأكد من مراجعة الامتثال للمتطلبات بشكل دوري ومراقبة ما إذا كانت هناك متطلبات جديدة قابلة للتطبيق.
		المخرجات المتوقعة: • وثيقة تطبيق متطلبات الأمن السيبراني (للأنظمة التقنية السحابية (CTS)، والأنظمة ذات العلاقة) في مرحلة التصميم والتنفيذ. • عينة من مراجعة الامتثال.
	٢-١٦-م-٣-٢	حماية بيئات التطوير (Development Environments) والاختبار (Testing Environments) وما تحويه من بيانات، ومنصات التكامل (Integration Platforms).
		أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة دورة حياة تطوير البرمجيات الآمنة. **إرشادات تطبيق الضوابط:** • العمل على تحديد المخاطر المتعلقة ببيئات التطوير وبيئات الاختبار ومنصات التكامل. • العمل على وضع وتنفيذ تدابير الحماية لتوفير بيئة آمنة للتطوير والاختبار، بالإضافة إلى منصات التكامل الآمنة، مع مراعاة المخاطر المحددة. • العمل على ضمان تضمين حماية البيانات المستخدمة في بيئة الاختبار في تدابير الحماية المنفذة.
		المخرجات المتوقعة: • قائمة بالمخاطر المحددة.

		• إثبات يؤكد تحديد التدابير الوقائية وضمان حماية البيانات المستخدمة في بيئة الاختبار.
٢-١٦-م-٤	يجب مراجعة متطلبات الأمن السيبراني لتطوير الأنظمة لدى مقدمي الخدمات، ومراجعة تطبيقها، دورياً.	
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة مراجعة وتدقيق الأمن السيبراني. • نموذج إجراء تطوير وثائق الأمن السيبراني. **إرشادات تطبيق الضوابط:** • التأكد من مراجعة المتطلبات بشكل دوري وفقًا للإطار الزمني المحدد، على الأقل مرة في السنة. • العمل على تحديد الأدوار والمسؤوليات في عملية المراجعة. • العمل على تحديث المتطلبات إذا كان ذلك مطلوباً. • الاحتفاظ بسجلات المراجعات الدورية (مثل: من قام بالمراجعة ومتى تمت المراجعة وسجل التغييرات).	
	المخرجات المتوقعة: • إثبات يؤكد وجود متطلبات الأمن السيبراني لتطوير النظام. • عينة من المراجعات الدورية.	
٢-١٧	أمن وسائط التخزين (Storage Media Security)	
الهدف	ضمان التعامل الآمن مع المعلومات والبيانات عبر الوسائط المادية، لدى مقدم الخدمة.	
الضوابط		
٢-١٧-م-١	يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني لاستخدام وسائط المعلومات والبيانات المادية لدى مقدمي الخدمات.	
	إرشادات تطبيق الضوابط: • العمل على تحديد متطلبات الأمن السيبراني لاستخدام المعلومات والبيانات المادية (مثل: التصنيف، التشفير، التخزين الآمن، التخلص الآمن) - باستخدام الاستبيانات وإجراء ورش العمل مع أصحاب المصلحة ذوي الصلة. • العمل على تحديد معيار استخدام المعلومات ووسائط البيانات لوثائق هذه المتطلبات. • التأكد من الموافقة الرسمية على المعيار. • التأكد من مراجعة المعيار بشكل دوري (مثل: سنوياً).	

		المخرجات المتوقعة: • إثبات لمعيار استخدام وسائط المعلومات والبيانات المادية الموافق عليه من قبل أصحاب المصلحة.
٢-١٧-م-٢		يجب تطبيق متطلبات الأمن السيبراني لاستخدام وسائط المعلومات والبيانات المادية لدى مقدمي الخدمات.
		إرشادات تطبيق الضوابط: • العمل على فرض معيار الأمن السيبراني لاستخدام وسائط المعلومات والبيانات (مثل: التحكم في الوصول، التشفير).
		المخرجات المتوقعة: • وثيقة تصنيف وسائط المعلومات والبيانات، وتخزينها بشكل آمن، والتخلص منها بطريقة آمنة.
٢-١٧-م-٣		متطلبات الأمن السيبراني لاستخدام وسائط المعلومات والبيانات المادية لدى مقدمي الخدمات يجب أن تغطي بحد أدنى ما يلي:
	٢-١٧-م-٣-١	يجب التأكد من عدم احتواء الوسائط على أية بيانات أو معلومات، قبل إعادة استخدام الوسائط أو التخلص منها.
		إرشادات تطبيق الضوابط: • العمل على تحديد متطلبات تطهير وسائط التخزين (Storage Cleansing) لضمان محوها بطريقة آمنة (مثل: العملية لا يمكن عكسها). • العمل على تحديد أساليب تطهير وسائط التخزين(Storage Cleansing) (مثل: مسح وسائط التخزين ببيانات إدخال عشوائية عدة مرات، تدمير أو محو مفاتيح التشفير، إزالة المجال المغناطيسي). • العمل على اختيار أدوات التطهير التي تنفذ الأساليب المحددة. • العمل على فرض تطهير الوسائط عن طريق جعلها خطوة إلزامية في عملية إعادة استخدام أو التخلص من الوسائط (مثل: إنشاء تدفق عمل مناسب).
		المخرجات المتوقعة: • وثيقة استخدام أدوات وإجراءات تطهير الوسائط بشكل إلزامي في حال إعادة استخدام أو التخلص من الوسائط.
	٢-١٧-م-٣-٢	يجب استخدام وسائل آمنة عند التخلص من الوسائط.

		إرشادات تطبيق الضوابط: • العمل على تحديد متطلبات التخلص الآمن من الوسائط. • تحديد الأساليب التي تلبي هذه المتطلبات. • العمل على تطبيق الأساليب المقبولة للتخلص الآمن من البيانات في وسائط التخزين. • التأكد من عدم إمكانية استرداد البيانات باستخدام أي وسيلة. **المخرجات المتوقعة:** • إثبات يؤكد تحديد وتطبيق المتطلبات والأساليب المقبولة للتخلص من الوسائط.
	٢-١٧-م-٣-٣	الحفاظ على سرية وسلامة البيانات على أجهزة وسائط التخزين الخارجية. **إرشادات تطبيق الضوابط:** • العمل على تحديد المخاطر المتعلقة بسرية وسلامة البيانات على الوسائط القابلة للإزالة (مثل: سرقة الوسائط). • العمل على تحديد الضوابط والمتطلبات المعمول بها لسرية البيانات وسلامتها على الوسائط القابلة للإزالة (على سبيل المثال: التشفير والأمن المادي). • العمل على تطبيق التدابير الأمنية المناسبة لضمان سرية وسلامة البيانات على الوسائط القابلة للإزالة. • التأكد من مراجعة وتحديث الضوابط والمتطلبات بشكل دوري للتأكد من قابليتها للتطبيق. **المخرجات المتوقعة:** • قائمة بالمخاطر المحددة. • إثبات يؤكد تحديد ضوابط ومتطلبات للبيانات على الوسائط القابلة للإزالة. • تقارير المراجعة الدورية.
	٢-١٧-م-٣-٤	وضع ترميز أو علامة (Labelling) مقروءة على الوسائط توضح تصنيفها ومدى حساسية المعلومات والبيانات التي تحتويها. **إرشادات تطبيق الضوابط:** • العمل على إنشاء قواعد واضحة لتسمية الوسائط بما في ذلك تصنيفها وحساسية المعلومات (مثل: السرية الشديدة، سرية، محدودة). • التأكد من أن التصنيف ومستويات الحساسية المستخدمة محددة بوضوح وتم الاتفاق عليها.

		• التأكد من تسمية كل الوسائط المستخدمة وفقًا للقواعد التي تم إنشائها. • التأكد من تسمية كل الوسائط الجديدة التي سيتم استخدامها وفقًا للقواعد التي تم إنشائها.
		المخرجات المتوقعة: • إثبات يؤكد تصنيف كل وسائط وفقاً للقواعد التي تم إنشائها. • إثبات يؤكد وجود قواعد للترميز للوسائط المصنفة.
	٢-١٧-م-٣-٥	الحفظ الآمن لأجهزة وسائط التخزين الخارجية.
		إرشادات تطبيق الضوابط: • العمل على تحديد المخاطر المتعلقة بتخزين الوسائط القابلة للإزالة (مثل: سرقة الوسائط). • العمل على تحديد الضوابط القابلة للتطبيق (بما في ذلك الضوابط المادية) ومتطلبات التخزين الآمن للوسائط القابلة للإزالة، مع مراعاة المخاطر المحددة. • العمل على تطبيق هذه الضوابط (مثل: التحكم في الوصول والتدفئة والتهوية وتكييف الهواء).
		المخرجات المتوقعة: • قائمة بالمخاطر المحددة لتخزين الوسائط القابلة للإزالة. • إثبات يؤكد وجود ضوابط ومتطلبات التخزين الآمن للوسائط القابلة للإزالة.
	٢-١٧-م-٣-٦	التقييد الحازم لاستخدام وسائط التخزين الخارجية على الأنظمة التقنية السحابية (CTS).
		إرشادات تطبيق الضوابط: • العمل على تحديد المخاطر المتعلقة باستخدام وسائط قابلة للنقل داخل مجموعة التقنية السحابية (مثل: سرقة الوسائط). • العمل على تحديد واعتماد قيود وتحكمات مناسبة للوسائط القابلة للنقل داخل مجموعة التقنية السحابية، مع مراعاة المخاطر المحددة. • العمل على تنفيذ القيود والضوابط (مثل التشفير، الملكية، علامات RFID).
		المخرجات المتوقعة: • قائمة بالمخاطر المحددة لاستخدام وسائط التخزين الخارجية على الأنظمة التقنية السحابية.

		• إثبات يوضح القيود والضوابط المعتمدة لاستخدام وسائط التخزين الخارجية على الأنظمة التقنية السحابية.
٢-١٧-م-٤	يجب مراجعة متطلبات الأمن السيبراني لاستخدام وسائط المعلومات والبيانات المادية لدى مقدمي الخدمات، ومراجعة تطبيقها، دوريًا.	
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة مراجعة وتدقيق الأمن السيبراني. • نموذج إجراء تطوير وثائق الأمن السيبراني. **إرشادات تطبيق الضوابط:** • التأكد من مراجعة المتطلبات بشكل دوري وفقًا للإطار الزمني المحدد، على الأقل مرة واحدة في السنة. • العمل على تحديد الأدوار والمسؤوليات في عملية المراجعة. • العمل على تحديث المتطلبات، إن كان ذلك ينطبق. • التأكد من الحفاظ على سجلات المراجعات الدورية (مثل من قام بالمراجعة ومتى تمت المراجعة وسجل التغييرات).	
	المخرجات المتوقعة: • إثبات يؤكد الالتزام بمتطلبات الأمن السيبراني ووسائط البيانات في الاستخدام. • سجلات المراجعة الدورية.	

٣ صمود الأمن السيبراني (Cybersecurity Resilience)

٣-١	جوانب صمود الأمن السيبراني في إدارة استمرارية الأعمال (Cybersecurity Resilience Aspects of Business Continuity Management "BCM")
الهدف	ضمان توافر متطلبات صمود الأمن السيبراني في إدارة استمرارية أعمال مقدمي الخدمات والمشتركين، وضمان معالجة وتقليل الآثار المترتبة على الاضطرابات في الخدمات الإلكترونية الحرجة لمقدمي الخدمات والمشتركين وأنظمة وأجهزة معالجة معلوماتها جراء الكوارث الناتجة عن التهديدات السيبرانية.
الضوابط	
٣-١-م-١	بالإضافة للضوابط الفرعية ضمن الضابط ٣-١-٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني لجوانب صمود الأمن السيبراني في إدارة استمرارية الأعمال لدى مقدمي الخدمات، بحد أدنى ما يلي:
٣-١-م-١-١	تطوير وتنفيذ إجراءات التعافي من الكوارث واستمرارية الأعمال بصورة آمنة.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني ضمن استمرارية الأعمال. **إرشادات تطبيق الضوابط:** • العمل على تحديد متطلبات إجراءات استعادة الكوارث واستمرارية العمل، مع مراعاة المخاطر المحددة المتعلقة بالحوسبة السحابية. • العمل على تحديد واعتماد وتنفيذ إجراءات وخطط التعافي من الكوارث واستمرارية العمل بما في ذلك التدابير الأمنية، مع مراعاة المتطلبات المحددة. • العمل على التواصل بشكل واضح وتوفير الوثائق للأشخاص المخولين ذلك. • العمل على اختبار الإجراءات بشكل دوري وعند التغييرات الكبيرة لضمان تطبيقها.
	المخرجات المتوقعة: • وثيقة توضح إجراءات وخطة للتعافي من كوارث الحوسبة السحابية. • وثيقة توضح إجراءات وخطة استمرارية الأعمال للحوسبة السحابية.
٣-١-م-١-٢	تطوير وتنفيذ إجراءات لضمان صمود واستمرارية أنظمة الأمن السيبراني المخصصة لحماية الأنظمة التقنية السحابية (CTS).

		أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني ضمن استمرارية الأعمال. **إرشادات تطبيق الضوابط:** • العمل على إنشاء إجراءات لضمان الصمود والاستمرارية التي تتعلق بأمان الحوسبة السحابية. • التأكد من مراجعة الإجراءات بشكل دوري. • العمل على جعل آليات الصمود والاستمرارية مبدأ معمارياً للأمن السيبراني. • العمل على إنشاء دليل لتقنيات وأساليب ضمان الصمود والاستمرارية.
		المخرجات المتوقعة: • وثيقة توضح إجراءات مطورة لضمان صمود واستمرارية أنظمة الأمن السيبراني المخصصة لحماية الأنظمة التقنية السحابية (CTS). • وثائق وتقارير المراجعة الدورية. • إثبات يوضح تقنيات وأساليب ضمان الصمود والاستمرارية.

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

٤-١	الأمن السيبراني المتعلق بالأطراف الخارجية (Third Party Cybersecurity)	
الهدف	ضمان حماية أصول مقدمي الخدمات والمشتركين من مخاطر الأمن السيبراني المتعلقة بالأطراف الخارجية) بما في ذلك خدمات الإسناد "Outsourcing" والخدمات المُدارة"Managed Services") وفقًا للسياسات والإجراءات التنظيمية لديهم والمتطلبات التنظيمية والتشريعية ذات العلاقة.	
الضوابط		
٤-١-م-١	بالإضافة إلى تطبيق الضابطين ٤-١-٢ و٤-١-٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني المتعلق بالأطراف الخارجية لدى مقدمي الخدمات، بحد أدنى ما يلي:	
	٤-١-م-١-١	ضمان تنفيذ مقدم الخدمة لطلبات الهيئة الوطنية للأمن السيبراني الخاصة بإزالة البرمجيات أو الخدمات المقدمة من أطراف خارجية التي قد تعتبر تهديدًا على الأمن السيبراني للجهات الوطنية، من السوق (Marketplace) المقدم للمشتركين.
		أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني المتعلّق بالأطراف الخارجية. **إرشادات تطبيق الضوابط:** • العمل على الحفاظ على دليل لمزودي الخدمات الخارجيين وبرامجهم المتاحة لشركات التقنية السحابية. • العمل على إنشاء عملية فعالة لإزالة برامج محددة من السوق استنادًا إلى طلبات الهيئة الوطنية للأمن السيبراني. • العمل على إدخال بيانات قانونية مناسبة تتيح لمزودي خدمات التقنية السحابية إزالة أي برنامج يُعتبر تهديدًا للأمن السيبراني من السوق. **المخرجات المتوقعة:** • مراجعة دليل مزودي البرامج الخارجية وبرمجياتهم. • وثيقة توضح إجراءات إزالة برامج محددة من السوق بناءً على طلبات المشرعين.
	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.

		أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني المتعّلق بالأطراف الخارجية. **إرشادات تطبيق الضوابط:** • العمل على إدخال التزامات قانونية على الموردين ومقدمي الخدمات من الأطراف الخارجية لتوفير وثائق أمان لتجهيزاتهم أو منتجاتهم أو خدماتهم. • العمل على تعريف جوانب الأمان التي يجب توثيقها (مثل: الهندسة الأمنية، وضوابط الأمان المعتمدة، وتقنيات الأمان المستخدمة). • العمل على استلام ومراجعة الوثائق المقدمة بشكل دوري. **المخرجات المتوقعة:** • وثائق الأمان للمعدات أو الخدمات من الموردين ومقدمي الخدمات من الأطراف الخارجية. • وثائق وتقارير المراجعة الدورية.
	٤-١-م-١-٣	الزام الأطراف الخارجية بالمتطلبات التنظيمية، والتشريعية ذات الصلة بنطاق عملهم. **أدوات الأمن السيبراني ذات العلاقة:** • نموذج سياسة الأمن السيبراني المتعّلق بالأطراف الخارجية. **إرشادات تطبيق الضوابط:** • العمل على تحديد وتوثيق القوانين والمتطلبات التنظيمية ذات الصلة بمقدمي الخدمات من الأطراف الخارجية بشكل دوري (مثل: سنويًا). • التأكد من مراجعة مقدمي الخدمات من الأطراف الخارجية أو طلب مراجعات مستقلة للتحقق من امتثالهم. **المخرجات المتوقعة:** • إثبات يؤكد تحديد القوانين والمتطلبات التنظيمية ذات الصلة لكل مقدم خدمة من الأطراف الخارجية. • وثائق وتقارير المراجعة الدورية لمقدمي الخدمة من الأطراف الخارجية للامتثال للقوانين والمتطلبات التنظيمية.

	٤-١-م-١-٤	يجب على الطرف الخارجي إدارة مخاطر الأمن السيبراني الخاصة به.
		أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني المتعّلق بالأطراف الخارجية. **إرشادات تطبيق الضوابط:** • العمل على تضمين المخاطر المتعلقة بمقدمي الخدمات من الأطراف الخارجية (مثل: مخاطر سلسلة التوريد) في عمليات إدارة المخاطر والحوكمة الأمنية.
		المخرجات المتوقعة: • إثبات يؤكد دمج المخاطر المتعلقة بالأطراف الخارجية في عمليات إدارة المخاطر. • عينة من سجل المخاطر يتضمن المخاطر المتعلقة بالأطراف الخارجية المحددة.


الهيئة الوطنية
للأمن السيبراني
National Cybersecurity Authority