الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

الدليل الإرشادي لتطبيق الضوابط الأساسية للأمن السيبراني

Guide to Essential Cybersecurity Controls Implementation **(GECC – 1 : 2023)**

إشارة المشاركة: أبيض
تصنيف الوثيقة: عام

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

بسم الله الرحمن الرحيم

بروتوكول الإشارة الضوئية (TLP):

تم إنشاء نظام بروتوكول الإشارة الضوئية لمشاركة أكبر قدر من المعلومات الحساسة ويستخدم على نطاق واسع في العالم وهناك أربعة ألوان (إشارات ضوئية):

أحمر – شخصي وسري للمستلم فقط

المستلم لا يحق له مشاركة المصنف بالإشارة الحمراء مع أي فرد سواء من داخل او خارج المنشأة خارج النطاق المحدد للإستلام.

برتقالي – مشاركة محدودة

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

أخضر – مشاركة في نفس المجتمع

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

أبيض – غير محدود

قائمة المحتويات

مقدمة ٧
الهدف ٧
نطاق العمل وقابلية التطبيق ٧
الهيكلية ٩
إرشادات تطبيق الضوابط الأساسية للأمن السيبراني ١٠

قائمة الأشكال

شكل ١: المكونات الأساسية والفرعية للضوابط الأساسية للأمن السيبراني ٨
شكل ٢: هيكلية الدليل الإرشادي للضوابط الأساسية للأمن السيبراني ٩

مقدمة

طورت الهيئة الوطنية للأمن السيبراني (ويشار لها في هذه الوثيقة بـ "الهيئة") الدليل الإرشادي لتطبيق ضوابط الأمن السيبراني المنصوص عليها في الضوابط الأساسية للأمن السيبراني (ECC - 1: 2018) (ويشار لها في هذه الوثيقة بـ "الضوابط")، وذلك للمساهمة في تمكين الجهات الوطنية من تطبيق متطلبات الالتزام بالضوابط الأساسية للأمن السيبراني. 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 الضوابط الأساسية للأمن السيبراني 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 كما هو مذكور في الضوابط الأساسية للأمن السيبراني (ECC-1:2018) وهو: الجهات الحكومية في المملكة العربية السعودية (وتشمل الـوزارات والهيئات والمؤسسات وغيرها) والجهات والشركات التابعة لها، وجهات القطاع الخاص التي تمتلك بنى تحتية وطنية حساسة (Critical National Infrastructure "CNIs") أو تقوم بتشغيلها أو استضافتها، (ويشار لها جميعاً في هذا الوثيقة بـ "الجهة").

مكونات وهيكلية الضوابط الأساسية للأمن السيبراني

يوضح الشكل رقم (١) أدناه المكونات الأساسية والفرعية للضوابط الأساسية للأمن السيبراني

١	حوكمة الأمن السيبراني Cybersecurity Governance	١-١	استراتيجية الأمن السيبراني Cybersecurity Strategy	١-٢	إدارة الأمن السيبراني Cybersecurity Management
		١-٣	سياسات وإجراءات الأمن السيبراني Cybersecurity Policies and Procedures	١-٤	أدوار ومسؤوليات الأمن السيبراني Cybersecurity Roles and Responsibilities
		١-٥	إدارة مخاطر الأمن السيبراني Cybersecurity Risk Management	١-٦	الأمن السيبراني ضمن إدارة المشاريع المعلوماتية والتقنية Cybersecurity in Information Technology Projects
		١-٧	الالتزام بتشريعات وتنظيمات ومعايير الأمن السيبراني Cybersecurity Regulatory Compliance	١-٨	المراجعة والتدقيق الدوري للأمن السيبراني Periodical Cybersecurity Review and Audit
		١-٩	الأمن السيبراني المتعلق بالموارد البشرية Cybersecurity in Human Resources	١-١٠	برنامج التوعية والتدريب بالأمن السيبراني Cybersecurity Awareness and Training Program
٢	تعزيز الأمن السيبراني Cybersecurity Defense	٢-١	إدارة الأصول Asset Management	٢-٢	إدارة هويات الدخول والصلاحيات Identity and Access Management
		٢-٣	حماية الأنظمة وأجهزة معالجة المعلومات Information System and Processing Facilities Protection	٢-٤	حماية البريد الإلكتروني Email Protection
		٢-٥	إدارة أمن الشبكات Networks Security Management	٢-٦	أمن الأجهزة المحمولة Mobile Devices Security
		٢-٧	حماية البيانات والمعلومات Data and Information Protection	٢-٨	التشفير Cryptography
		٢-٩	إدارة النسخ الاحتياطية Backup and Recovery Management	٢-١٠	إدارة الثغرات Vulnerability Management
		٢-١١	اختبار الاختراق Penetration Testing	٢-١٢	إدارة سجلات الأحداث ومراقبة الأمن السيبراني Cybersecurity Event Logs and Monitoring Management
		٢-١٣	إدارة حوادث وتهديدات الأمن السيبراني Cybersecurity Incident and Threat management	٢-١٤	الأمن المادي Physical Security
		٢-١٥	حماية تطبيقات الويب Web Application 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 والحوسبة السحابية Third-Party and Cloud Computing Cybersecurity	٤-١	الأمن السيبراني المتعلق بالأطراف الخارجية Third-Party Cybersecurity	٤-٢	الأمن السيبراني المتعلق بالحوسبة السحابية والاستضافة Cloud Computing and Hosting Cybersecurity
٥	الأمن السيبراني لأنظمة التحكم الصناعي ICS Cybersecurity	٥-١	حماية أجهزة وأنظمة التحكم الصناعي Industrial Control Systems (ICS) Protection		

شكل ١: المكونات الأساسية والفرعية للضوابط الأساسية للأمن السيبراني

هيكلية الدليل الإرشادي

يوضح الشكل رقم (٢) أدناه هيكلية الدليل الإرشادي للضوابط الأساسية للأمن السيبراني

1 الرقم المرجعي للمكون الأساسي	اسم المكون الأساسي
الرقم المرجعي للمكون الفرعي	اسم المكون الفرعي
الهدف	
الضوابط	
الرقم المرجعي للضابط	بنود الضابط
أدوات الأمن السيبراني ذات العلاقة: **إرشادات تطبيق الضوابط:**	
المخرجات المتوقعة:	

شكل ٢: هيكلية الدليل الإرشادي للضوابط الأساسية للأمن السيبراني

إرشادات تطبيق الضوابط الأساسية للأمن السيبراني

١ حوكمة الأمن السيبراني (Cybersecurity Governance)

١-١	استراتيجية الأمن السيبراني
الهدف	ضمان إسهام خطط العمل للأمن السيبراني والأهداف والمبادرات والمشاريع داخل الجهة في تحقيق المتطلبات التشريعية والتنظيمية ذات العلاقة.
الضوابط	
١-١-١	يجب تحديد وتوثيق واعتماد استراتيجية الأمن السيبراني للجهة ودعمها من قبل رئيس الجهة أو من ينيبه (ويشار له في هذه الضوابط باسم «صاحب الصلاحية»)، وأن تتماشى الأهداف الاستراتيجية للأمن السيبراني للجهة مع المتطلبات التشريعية والتنظيمية ذات العلاقة.
	أدوات الأمن السيبراني ذات العلاقة: ● جميع نماذج استراتيجية الأمن السيبراني وخارطة الطريق. **إرشادات تطبيق الضوابط:** ● عقد ورشة عمل مع أصحاب المصلحة والمعنيين في الجهة لمواءمة أهداف استراتيجية الأمن السيبراني مع الأهداف الاستراتيجية للجهة. ● العمل على تطوير وتوثيق استراتيجية الأمن السيبراني للجهة، بحيث تتواءم الأهداف الاستراتيجية للأمن السيبراني للجهة مع المتطلبات التشريعية والتنظيمية ذات العلاقة وعلى سبيل المثال لا الحصر: (ضوابط الأمن السيبراني للحوسبة السحابية «CCC»، وضوابط الأمن السيبراني للأنظمة الحساسة «CSCC»)، وغالبا ما تحتوي استراتيجية الأمن السيبراني على ما يلي: ○ الرؤية ○ الرسالة ○ الأهداف الاستراتيجية ○ خطة لتنفيذ الاستراتيجية ○ المشاريع ○ المبادرات

	• من أجل أن تكون استراتيجية الأمن السيبراني في الجهة فعّالة، يجب أن يتم اعتماد وموافقة صاحب الصلاحية بناءً على دليل الصلاحيات المعتمد في الجهة.
	المخرجات المتوقعة: • وثيقة استراتيجية الأمن السيبراني المعتمدة في الجهة (نسخة إلكترونية أو نسخة ورقية رسمية). • المبادرات والمشاريع الواردة في استراتيجية الأمن السيبراني لدى الجهة.
١-١-٢	يجب العمل على تنفيذ خطة عمل لتطبيق استراتيجية الأمن السيبراني من قبل الجهة.
	أدوات الأمن السيبراني ذات العلاقة: • جميع نماذج استراتيجية الأمن السيبراني وخارطة الطريق. • نموذج تقرير وقياس أداء الأمن السيبراني. **إرشادات تطبيق الضوابط:** • العمل على تطوير خطة عمل لتطبيق استراتيجية الأمن السيبراني من قبل الجهة والتي تشمل تنفيذ مبادرات ومشاريع الاستراتيجية، من أجل: ○ تحديد أولويات الأمن السيبراني. ○ تقديم التوصيات المتعلّقة بأعمال الأمن السيبراني في الجهة بشكل يتوافق مع طبيعة عملها. ○ متابعة تنفيذ مشاريع ومبادرات استراتيجية الأمن السيبراني، والقيام بالخطوات التصحيحة إن تطلب الأمر. ○ ضمان تنفيذ المبادرات والمشاريع حسب المتطلبات. ○ تقديم رؤية واضحة وموحّدة ونشرها بين جميع أصحاب المصلحة الداخليين والخارجيين. ○ الحصول على موافقة الهيئة الوطنية للأمن السيبراني فيما يخص أي من مبادرات الأمن السيبراني التي تتخطى نطاق الجهة.
	المخرجات المتوقعة: • خطة عمل تنفيذ الاستراتيجية. • قائمة المشاريع والمبادرات للأمن السيبراني وحالة إنجازها.
١-١-٣	يجب مراجعة استراتيجية الأمن السيبراني على فترات زمنية مخطط لها (أو في حال حدوث تغييرات في المتطلبات التشريعية والتنظيمية ذات العلاقة).
	إرشادات تطبيق الضوابط:

	• العمل على مراجعة وتحديث استراتيجية الأمن السيبراني بشكل دوري حسب خطة موثقة ومعتمدة للمراجعة وذلك بناءً على: ○ فترات محددة حسب أفضل الممارسات (يتم تحديدها من قبل الجهة، وتوثيقها مع الاعتماد اللازم في وثيقة الاستراتيجية). ○ في حال حدوث تغييرات في المتطلبات التشريعية والتنظيمية ذات العلاقة (مثال: حدوث تغييرات في متطلبات الأمن السيبراني التي تنطبق على الجهة). ○ في حال حدوث تغييرات جوهرية في الجهة. • العمل على توثيق إجراءات المراجعة والتغييرات التي تمت على استراتيجية الأمن السيبراني، بحيث يتم اعتماد هذه التغييرات من قبل صاحب الصلاحية.
	المخرجات المتوقعة: • وثيقة معتمدة تحدد جدول المراجعة لإستراتيجية الأمن السيبراني. • استراتيجية محدثة للأمن السيبراني بعد توثيق التغييرات على متطلبات الأمن السيبراني ومعتمده من قبل صاحب الصلاحية. • تقارير حالة المشاريع. • موافقة رسمية من قبل صاحب الصلاحية على الاستراتيجية المحدثة (مثال: عن طريق البريد الإلكتروني الرسمي للجهة، أو التوقيع الورقي أو الإلكتروني).

٢-١	إدارة الأمن السيبراني
الهدف	ضمان التزام ودعم صاحب الصلاحية للجهة فيما يتعلق بإدارة وتطبيق برامج الأمن السيبراني في تلك الجهة وفقاً للمتطلبات التشريعية والتنظيمية ذات العلاقة.
الضوابط	
١-٢-١	يجب إنشاء إدارة معنية بالأمن السيبراني في الجهة مستقلة عن إدارة تقنية المعلومات والاتصالات (ICT/ IT) (وفقاً للأمر السامي الكريم رقم ٣٧١٤٠ وتاريخ ١٤ / ٨ / ١٤٣٨ هـ). ويفضل ارتباطها مباشرة برئيس الجهة أو من ينيبه، مع الأخذ بالاعتبار عدم تعارض المصالح.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج الهيكل التنظيمي لإدارة الأمن السيبراني. • نموذج أدوار ومسؤوليات الأمن السيبراني. • نموذج السياسة العامة للأمن السيبراني.

	إرشادات تطبيق الضوابط: ● العمل على إنشاء إدارة معنية بالأمن السيبراني في الجهة، وذلك لتمكينها من تنفيذ مهام الأمن السيبراني الموكلة إليها بالشكل المطلوب، مع الأخذ بالاعتبار النقاط التالية: ○ التأكد من أن ارتباط الإدارة المعنية بالأمن السيبراني مختلف عن ارتباط الإدارة المعنية بتقنية المعلومات أو الإدارة المعنية بالتحول الرقمي وذلك تنفيذاً للأمر السامي الكريم رقم ٣٧١٤٠ بتاريخ ١٤٣٨/٨/١٤هـ. ○ التأكد من أن الإدارة المعنية بالأمن السيبراني مرتبطة برئيس الجهة أو نائب/مساعد رئيس الجهة للقطاعات المعنية بالتشريع وعلى سبيل المثال لا الحصر: مساعد أو نائب الرئيس لقطاعات الأعمال أو للقطاعات المعنية بالتشريع، أو وكلاء ورؤساء قطاعات الأعمال في الجهة. ○ من أجل تجنب تعارض المصالح، التأكد من أن: ○ الإدارة المعنية بالأمن السيبراني مسؤولة عن جميع أنشطة المراقبة الخاصة بالأمن السيبراني (من ضمنها مراقبة الالتزام ومراقبة التشغيل والعمليات الخ.) ○ الإدارة المعنية بالأمن السيبراني مسؤولة عن جميع أنشطة حوكمة الأمن السيبراني (من ضمنها تحديد متطلبات الأمن السيبراني، وإدارة مخاطر الأمن السيبراني الخ.)
	المخرجات المتوقعة: ● الهيكل التنظيمي الخاص بالجهة (نسخة إلكترونية أو نسخة ورقية رسمية)، بحيث يغطي الهيكل التنظيمي للإدارة المعنية بالأمن السيبراني. ● قرار إنشاء إدارة الأمن السيبراني ومهامها (نسخة إلكترونية أو نسخة ورقية رسمية). ● تقارير نتائج الالتزام بسياسات الأمن السيبراني.
٢-٢-١	يجب أن يشغل رئاسة الإدارة المعنية بالأمن السيبراني والوظائف الإشرافية والحساسة بها مواطنون متفرغون وذو كفاءة عالية في مجال الأمن السيبراني.
	إرشادات تطبيق الضوابط: ● العمل على تعيين مواطنين متفرغين وذوي كفاءة عالية وذلك لشغل الأدوار الوظيفية التالية : ○ رئيس الإدارة المعنية بالأمن السيبراني وهو من يقوم بقيادة أعمال الأمن السيبراني داخل الجهة، ووضع الرؤية والتوجه بشأن الأمن السيبراني، والاستراتيجيات والموارد والأنشطة ذات العلاقة وتقديم المرئيات لقيادة الجهة حيال أساليب الإدارة الفعالة لمخاطر الأمن السيبراني للجهة. ○ الوظائف الإشرافية داخل الإدارة المعنية بالأمن السيبراني (مثال: مدراء الإدارات والأقسام الفرعية داخل الإدارة المعنية بالأمن السيبراني حسب الهيكل التنظيمي أو/و نموذج الحوكمة والتشغيل للإدارة المعنية بالأمن السيبراني المعتمد من قبل صاحب الصلاحية في الجهة)، وفي حال وجود شاغر لإحدى الوظائف الإشرافية، يتم تكليف أحد الموظفين للقيام بتسيير عمل الإدارة أو القسم حتى يتم شغل الوظيفة الإشرافية حسب خطة زمنية محددة. ○ الأدوار الوظيفية الحساسة ضمن الإدارة المعنية بالأمن السيبراني في الجهة التي تتضمن مسؤوليات تتطلب السرية والموثوقية والتي يؤدي عدم تأديتها على الوجه المطلوب إلى تأثيرات سلبية كبيرة على الأمن السيبراني للجهة وأعمالها وأنظمتها، ويؤخذ بالاعتبار كذلك المتطلبات التشريعية

	والتنظيمية الوطنية المتعلقة بتوطين وظائف الأمن السيبراني في الجهة من موظفين ومتعاقدين بشكل مباشر أو غير مباشر (ويشمل ذلك -على سبيل المثال لا الحصر- الأوامر الملكية والأوامر السامية وقرارات مجلس الوزراء المتعلقة بالأمن السيبراني، والتعاميم والقرارات التنظيمية الصادرة عن الهيئة الوطنية للأمن السيبراني). يمكن الاستفادة من الإطار السعودي لكوادر الأمن السيبراني (سيوف) كمرجع فيما يتعلق بالوظائف ذات العلاقة بالأمن السيبراني. • العمل على تحديد المؤهل العلمي وسنوات الخبرة اللازمة لإشغال رئاسة الإدارة المعنية بالأمن السيبراني والأدوار الوظيفية الإشرافية والحساسة -على سبيل المثال لا الحصر : ○ أن يتم تطوير وصف وظيفي لوظيفة رئيس الإدارة المعنية بالأمن السيبراني بحيث يتم تضمين الحد الأدنى من عدد سنوات الخبرة المطلوبة، ومجالها، وتضمين المؤهل العلمي المناسب والتدريب والشهادات الاحترافية المناسبة في مجال الأمن السيبراني والمجالات التقنية اعتماداً على الإطار السعودي لكوادر الأمن السيبراني (سيوف).
	المخرجات المتوقعة: • قائمة تفصيلية بجميع العاملين (من موظفين ومتعاقدين بشكل مباشر أو غير مباشر) المتعلقة أعمالهم بالأمن السيبراني في الجهة، على أن توضح الأسماء والجنسيات ونوع التعاقد والمسميات الوظيفية والأدوار الوظيفية وسنوات الخبرة والمؤهلات التعليمية والمهنية. • الوصف الوظيفي لوظيفة رئيس الإدارة المعنية بالأمن السيبراني والوظائف الإشرافية والحساسة ذات العلاقة بالأمن السيبراني، اعتماداً على الإطار السعودي لكوادر الأمن السيبراني (سيوف).
٣-٢-١	يجب إنشاء لجنة إشرافية للأمن السيبراني بتوجيه من صاحب الصلاحية للجهة لضمان التزام ودعم ومتابعة تطبيق برامج وتشريعات الأمن السيبراني، ويتم تحديد وتوثيق واعتماد أعضاء اللجنة ومسؤولياتها وإطار حوكمة أعمالها على أن يكون رئيس الإدارة المعنية بالأمن السيبراني أحد أعضائها. ويفضل ارتباطها مباشرة برئيس الجهة أو من ينيبه، مع الأخذ بالاعتبار عدم تعارض المصالح.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج الوثيقة المنظمة للجنة الاشرافية للأمن السيبراني. **إرشادات تطبيق الضوابط:** • العمل على إنشاء اللجنة الإشرافية للأمن السيبراني باعتبارها لجنة مختصة في توجيه شؤون وعمليات وبرامج ومبادرات الأمن السيبراني في الجهة وقيادتها، حيث يكون ارتباط اللجنة مباشرة برئيس الجهة أو من ينيبه، مع الأخذ بالاعتبار عدم تعارض المصالح. • العمل على تحديد أعضاء اللجنة الإشرافية حيث تشمل اللجنة الإشرافية للأمن السيبراني على أعضاء مسؤولين مؤثرين أو تتأثر أعمالهم بالأمن السيبراني لدى الجهة وعلى سبيل المثال لا الحصر: رئيس الجهة أو من ينيبه، رئيس الإدارة المعنية بالأمن السيبراني، رئيس الإدارة المعنية بتقنية المعلومات، رئيس الإدارة المعنية بالالتزام، رئيس الإدارة المعنية بالموارد البشرية، وتحديد المهام والمسؤوليات الخاصة باللجنة الإشرافية وإطار حوكمة أعمالها، وتوثيقها بشكل رسمي في وثيقة ميثاق العمل الخاصة باللجنة (Committee Charter)، على أن يتم اعتماد ميثاق عمل اللجنة من قبل صاحب الصلاحية (رئيس الجهة أو من ينيبه). • العمل على تضمين رئيس الإدارة المعنية بالأمن السيبراني كأحد أعضاء اللجنة الدائمين.

	• العمل على عقد اجتماعات دورية (وذلك استناداً على الفترة الزمنية المحددة في وثيقة ميثاق عمل اللجنة)، بحيث تغطي الاجتماعات الدورية ضمان متابعة تطبيق برامج وتشريعات الأمن السيبراني في الجهة، وإدارة مخاطر الأمن السيبراني ورفع محاضر الاجتماع لرئيس الجهة. • العمل على إجراء مراجعة لتطبيق كافة سياسات وإجراءات الأمن السيبراني الخاصة بالجهة. • العمل على تحديث المبادرات والأهداف الخاصة باستراتيجية الأمن السيبراني. • العمل على التأكد من موائمة استراتيجية الأمن السيبراني مع استراتيجية الجهة بشكل دوري.
	المخرجات المتوقعة: • وثيقة لميثاق العمل الخاصة باللجنة الإشرافية في الجهة وتوضح الوثيقة تاريخ إنشاء اللجنة ومرجعيتها واعتمادها من قبل صاحب الصلاحية في الجهة. • قائمة موثقة ومعتمدة موضح بها أسماء أعضاء اللجنة الإشرافية للأمن السيبراني في الجهة. • لائحة أعمال اللجنة الإشرافية للأمن السيبراني في الجهة. • محاضر اجتماعات تم عقدها للجنة الإشرافية للأمن السيبراني في الجهة.

١-٣	سياسات وإجراءات الأمن السيبراني
الهدف	ضمان توثيق ونشر متطلبات الأمن السيبراني والتزام الجهة بها، وذلك وفقاً لمتطلبات الأعمال التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية ذات العلاقة.
الضوابط	
١-٣-١	يجب على الإدارة المعنية بالأمن السيبراني في الجهة تحديد سياسات وإجراءات الأمن السيبراني وما تشمله من ضوابط ومتطلبات الأمن السيبراني، وتوثيقها واعتمادها من قبل صاحب الصلاحية في الجهة، كما يجب نشرها إلى ذوي العلاقة من العاملين في الجهة والأطراف المعنية بها.
	أدوات الأمن السيبراني ذات العلاقة: • جميع نماذج السياسات والإجراءات والمعايير المدرجة ضمن أدوات الأمن السيبراني. **إرشادات تطبيق الضوابط:** • العمل على تحديد متطلبات الأمن السيبراني، وتوثيقها في سياسات وإجراءات ومعايير الأمن السيبراني، بحيث يتم اعتمادها من قبل صاحب الصلاحية في الجهة بناء على دليل الصلاحيات المعتمد لدى الجهة. • التأكّد من نشر السياسات والإجراءات للعاملين في الجهة والأطراف المعنية بها الداخليين والخارجيين، من خلال قنوات الاتصال المعتمدة وذلك حسب النطاق المحدد في السياسة (مثال: نشر السياسات والإجراءات عن طريق البوابة الداخلية للجهة، أو نشر السياسات والإجراءات عن طريق البريد الإلكتروني).
	المخرجات المتوقعة: • جميع سياسات وإجراءات ومعايير الأمن السيبراني الموثقة والمعتمدة من قبل صاحب الصلاحية في الجهة أو من ينيبه. • نشر سياسات وإجراءات ومعايير الأمن السيبراني للعاملين والأطراف المعنية.

١-٣-٢	يجب على الإدارة المعنية بالأمن السيبراني ضمان تطبيق سياسات وإجراءات الأمن السيبراني في الجهة وما تشمله من ضوابط ومتطلبات.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج تعهد وإقرار الموظف باتباع سياسات الأمن السيبراني. • نموذج تعهد وإقرار الموظف بالمحافظة على سرية المعلومات. **إرشادات تطبيق الضوابط:** • العمل على وضع خطة عمل لتطبيق سياسات وإجراءات ومعايير الأمن السيبراني وتشمل جميع أصحاب المصلحة الداخليين والخارجيين وهم كل من تنطبق عليهم سياسات وإجراءات ومعايير الجهة، ومتابعتها ومراقبتها بشكل دوري لضمان التطبيق الكامل لجميع المتطلبات وبشكل فعّال. • تأكد الإدارة المعنية بالأمن السيبراني من تنفيذ ضوابط الأمن السيبراني والالتزام بالسياسات والإجراءات والمعايير الموثقة والمعتمدة في الجهة. • العمل على ضمان تطبيق سياسات وإجراءات ومعايير الأمن السيبراني وما تشمله من ضوابط ومتطلبات بشكل يدوي أو بشكل الكتروني (مؤتمت).
	المخرجات المتوقعة: • وثيقة خطة عمل لتطبيق سياسات وإجراءات الأمن السيبراني في الجهة. • تقرير يوضح مراجعة تطبيق سياسات وإجراءات الأمن السيبراني.
١-٣-٣	يجب أن تكون سياسات وإجراءات الأمن السيبراني مدعومة بمعايير تقنية أمنية (على سبيل المثال: المعايير التقنية الأمنية لجدار الحماية وقواعد البيانات، وأنظمة التشغيل، إلخ).
	أدوات الأمن السيبراني ذات العلاقة: • جميع نماذج المعايير المدرجة ضمن أدوات الأمن السيبراني **إرشادات تطبيق الضوابط:** • العمل على تحديد وتوثيق واعتماد المعايير التقنية بحيث تغطي الأصول المعلوماتية والتقنية في الجهة. (على سبيل المثال: المعايير التقنية الأمنية لجدار الحماية، أجهزة الشبكة، وقواعد البيانات، أنظمة التشغيل للخوادم، أنظمة التشغيل للأجهزة الشخصية، معيار التطوير الآمن، معيار التشفير، إلخ..). • العمل على نشر المعايير التقنية للإدارات ذات العلاقة في الجهة (مثال: الإدارة المعنية بتقنية المعلومات) والتأكد من تطبيقها بشكل دوري على الأصول المعلوماتية والتقنية.
	المخرجات المتوقعة: • وثائق معايير الأمن السيبراني التقنية المعتمدة في الجهة.
١-٣-٤	يجب مراجعة سياسات وإجراءات ومعايير الأمن السيبراني وتحديثها على فترات زمنية مخطط لها (أو في حالة حدوث تغييرات في المتطلبات التشريعية والتنظيمية والمعايير ذات العلاقة)، كما يجب توثيق التغييرات واعتمادها.
	إرشادات تطبيق الضوابط:

	• العمل على مراجعة سياسات وإجراءات ومعايير الأمن السيبراني في الجهة بشكل دوري حسب خطة موثقة ومعتمدة للمراجعة وبناءً على فترة زمنية محددة في وثيقة السياسات (على سبيل المثال، يتم إجراء المراجعة الدورية سنوياً). • العمل على مراجعة وتحديث سياسات وإجراءات ومعايير الأمن السيبراني في الجهة في حال حدوث تغييرات في المتطلبات التشريعية والتنظيمية ذات العلاقة (على سبيل المثال، عند صدور نظام تشريعي جديد في الأمن السيبراني ينطبق على الجهة). • العمل على توثيق المراجعة والتغييرات التي تتم على سياسات وإجراءات ومعايير الأمن السيبراني في الجهة واعتمادها من قبل رئيس الجهة أو من ينيبه.
	المخرجات المتوقعة: • وثيقة معتمدة تحدد جدول المراجعة. • وثيقة معتمدة توضح مراجعة سياسات وإجراءات ومعايير الأمن السيبراني في الجهة بشكل دوري بناءً على الفترة الزمنية المحددة للمراجعة. • وثائق السياسات والإجراءات والمعايير بما يوضح أنه تم مراجعتها وتحديثها وتم توثيق التغييرات واعتمادها من قبل صاحب الصلاحية. • الموافقة الرسمية والاعتماد من قبل صاحب الصلاحية على السياسات والإجراءات والمعايير المحدثة.

٤-١	أدوار ومسؤوليات الأمن السيبراني
الهدف	ضمان تحديد أدوار ومسؤوليات واضحة لجميع الأطراف المشاركة في تطبيق ضوابط الأمن السيبراني في الجهة.
الضوابط	
١-٤-١	يجب على صاحب الصلاحية تحديد وتوثيق واعتماد الهيكل التنظيمي للحوكمة والأدوار والمسؤوليات الخاصة بالأمن السيبراني للجهة، وتكليف الأشخاص المعنيين بها، كما يجب تقديم الدعم اللازم لإنفاذ ذلك، مع الأخذ بالاعتبار عدم تعارض المصالح.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج أدوار ومسؤوليات الأمن السيبراني. **إرشادات تطبيق الضوابط:** • العمل على تحديد وتوثيق الأدوار والمسؤوليات المتعلقة بالأمن السيبراني والتأكد من أن جميع الأطراف المشاركة في تطبيق ضوابط الأمن السيبراني في الجهة على دراية بمسؤولياتهم في تطبيق برامج ومتطلبات الأمن السيبراني. • العمل على أن يكون الهيكل التنظيمي والأدوار والمسؤوليات في الجهة مدعوم من قبل الإدارة التنفيذية. وذلك من خلال اعتماد وموافقة صاحب الصلاحية. • العمل على تضمين الأدوار والمسؤوليات التالية (على سبيل المثال لا الحصر):

	○ الأدوار والمسؤوليات ذات العلاقة باللجنة الإشرافية للأمن السيبراني. ○ الأدوار والمسؤوليات ذات العلاقة برئيس الإدارة المعنية بالأمن السيبراني. ○ الأدوار والمسؤوليات ذات العلاقة بالإدارة المعنية بالأمن السيبراني (على سبيل المثال، تطوير وتحديث سياسات ومعايير الأمن السيبراني، إجراء تقييم مخاطر الأمن السيبراني، إجراء التحقق من الالتزام بالسياسات وتشريعات الأمن السيبراني، مراقبة أحداث الأمن السيبراني، مسح الثغرات، إدارة الصلاحيات، إعداد وتطبيق برنامج التوعية بالأمن السيبراني، إلخ..) ○ الأدوار والمسؤوليات ذات العلاقة بالأمن السيبراني للإدارات الأخرى في الجهة (كالإدارة المعنية بتقنية المعلومات، الإدارة المعنية بشؤون الموظفين، الإدارة المعنية بالأمن المادي، إلخ..) ○ الأدوار والمسؤوليات ذات العلاقة بالأمن السيبراني لكافة العاملين. • العمل على إسناد الأدوار المسؤوليات للعاملين في الجهة، مع الأخذ بالاعتبار عدم تعارض المصالح.
	المخرجات المتوقعة: • وثيقة الهيكل التنظيمي لإدارة الأمن السيبراني. • وثيقة أدوار ومسؤوليات الأمن السيبراني المعتمدة بالجهة (نسخة إلكترونية أو نسخة ورقية رسمية). • وثيقة توضح إسناد أدوار ومسؤوليات الأمن السيبراني للعاملين في الجهة.
١-٤-٢	يجب مراجعة أدوار ومسؤوليات الأمن السيبراني في الجهة وتحديثها على فترات زمنية مخطط لها (أو في حالة حدوث تغييرات في المتطلبات التشريعية والتنظيمية ذات العلاقة).
	إرشادات تطبيق الضوابط: • العمل على مراجعة وتحديث أدوار ومسؤوليات الأمن السيبراني للجهة بشكل دوري حسب خطة موثقة ومعتمدة للمراجعة بناءً على فترة زمنية محددة (على سبيل المثال، يتم إجراء المراجعة الدورية بشكل سنوي). • العمل على مراجعة وتحديث أدوار ومسؤوليات الأمن السيبراني للجهة عند حدوث تغييرات في المتطلبات التشريعية والتنظيمية ذات العلاقة (على سبيل المثال، عند صدور تنظيم تشريعي جديد في الأمن السيبراني ينطبق على الجهة). • العمل على توثيق المراجعة والتغييرات التي تمت على متطلبات الأمن السيبراني الخاصة بأدوار ومسؤوليات الأمن السيبراني للجهة واعتمادها من قبل صاحب الصلاحية.
	المخرجات المتوقعة: • وثيقة معتمدة تحدد جدول المراجعة لأدوار ومسؤوليات الامن السيبراني. • وثيقة الأدوار والمسؤوليات بما يوضح أن تكون محدثة وتم توثيق التغييرات على متطلبات الأمن السيبراني الخاصة بالأدوار والمسؤوليات واعتمادها من قبل صاحب الصلاحية.

١-٥	إدارة مخاطر الأمن السيبراني

الهدف	ضمان إدارة مخاطر الأمن السيبراني على نحو ممنهج يهدف إلى حماية الأصول المعلوماتية والتقنية للجهة، وذلك وفقاً للسياسات والإجراءات التنظيمية للجهة والمتطلبات التشريعية والتنظيمية ذات العلاقة.
الضوابط	
١-٥-١	يجب على الإدارة المعنية بالأمن السيبراني في الجهة تحديد وتوثيق واعتماد منهجية وإجراءات إدارة مخاطر الأمن السيبراني في الجهة. وذلك وفقاً لاعتبارات السرية وتوافر وسلامة الأصول المعلوماتية والتقنية.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة إدارة مخاطر الأمن السيبراني • نموذج إجراءات إدارة مخاطر الأمن السيبراني **إرشادات تطبيق الضوابط:** • العمل على تحديد وتوثيق متطلبات إدارة مخاطر الأمن السيبراني المبنية على التشريعات ذات العلاقة وأفضل الممارسات والمعايير لإدارة مخاطر الأمن السيبراني في الجهة، وذلك وفقاً لاعتبارات سرية الأصول المعلوماتية والتقنية وتوافرها وسلامتها. لتغطي: ○ المنهجية والإجراءات لإدارة مخاطر الأمن السيبراني في الجهة، بحيث تحتوي على: - تحديد الأصول ومعرفة أهميتها. - تحديد المخاطر التي تمس أعمال أو أصول أو العاملين في الجهة. - تقييم المخاطر، بحيث يتم تحديد احتمالية الحدوث ومستوى تأثير المخاطر التي تم تحديدها. - استجابة المخاطر، بحيث يتم تحديد أساليب التعامل مع المخاطر السيبرانية. - متابعة المخاطر، بحيث يتم تحديث سجل المخاطر بعد كل عملية تقييم للمخاطر وخطة الإستجابة لها. • العمل على أن تكون منهجية وإجراءات إدارة مخاطر الأمن السيبراني في الجهة مدعومة من قبل الإدارة التنفيذية، وذلك من خلال اعتماد وموافقة صاحب الصلاحية.
	المخرجات المتوقعة: • منهجية إدارة مخاطر الأمن السيبراني المعتمدة (نسخة إلكترونية أو نسخة ورقية رسمية). • إجراءات إدارة مخاطر الأمن السيبراني المعتمدة.
٢-٥-١	يجب على الإدارة المعنية بالأمن السيبراني تطبيق منهجية وإجراءات إدارة مخاطر الأمن السيبراني في الجهة.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سجل إدارة مخاطر الأمن السيبراني. إرشادات تطبيق الضوابط: • العمل على تطبيق كافة متطلبات منهجية وإجراءات إدارة مخاطر الأمن السيبراني المعتمدة في الجهة. • العمل على إنشاء سجل مخاطر الأمن السيبراني لتوثيق المخاطر ومتابعتها.

	• العمل على وضع خطط لمعالجة مخاطر الأمن السيبراني للجهة.
	المخرجات المتوقعة: • سجل مخاطر الأمن السيبراني للجهة (Risk Register). • خطط معالجة مخاطر الأمن السيبراني للجهة (Risk Treatment Plan). • تقرير يوضح تقييم مخاطر الأمن السيبراني، ومتابعتها.
١-٥-٣	يجب تنفيذ إجراءات تقييم مخاطر الأمن السيبراني بحد أدنى في الحالات التالية:
١-٣-٥-١	في مرحلة مبكرة من المشاريع التقنية.
	إرشادات تطبيق الضوابط: • العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية. • العمل على تضمين متطلبات الأمن السيبراني ضمن المرحلة الأولى من دورة حياة المشاريع المعلوماتية والتقنية (Technical Project Lifecycle) في الجهة. • العمل على تنفيذ إجراءات تقييم مخاطر الأمن السيبراني في مرحلة مبكرة من المشاريع التقنية لتجنب الأحداث أو الظروف التي من الممكن أن تنتهك سريّة الأصول المعلوماتية والتقنية وسلامتها وتوافرها، ويشمل ذلك على وجه الخصوص تحديد الأصول المعلوماتية والتقنية في المشاريع التقنية، والتهديدات التي من المحتمل أن تتعرّض لها والثغرات ذات الصلة. • العمل على معالجة جميع مخاطر الأمن السيبراني المحددة حسب منهجية إدارة مخاطر الأمن السيبراني المعتمدة.
	المخرجات المتوقعة: • تقرير يوضح تحديد وتقييم ومعالجة مخاطر الأمن السيبراني خلال دورة حياة المشاريع المعلوماتية والتقنية في الجهة.
٢-٣-٥-١	قبل إجراء تغيير جوهري في البنية التقنية.
	إرشادات تطبيق الضوابط: • العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية. • العمل على تضمين متطلبات الأمن السيبراني ضمن دورة إدارة التغيرات التقنية في الجهة (IT Change Management). • العمل على تنفيذ إجراءات تقييم مخاطر الأمن السيبراني قبل إجراء تغيير جوهري في البنية التقنية لتجنب الأحداث أو الظروف التي من الممكن أن تنتهك سريّة الأصول المعلوماتية والتقنية وسلامتها وتوافرها، ويشمل ذلك على وجه الخصوص تحديد الأصول المعلوماتية والتقنية ضمن طلبات التغيرات في البيئة التقنية أو التي سيؤثر عليها التغيير، والتهديدات التي من المحتمل أن تتعرّض لها والثغرات ذات الصلة. ومن تلك

التغييرات، على سبيل المثال لا الحصر: تحديث أساسي وحساس لأحد أو عدة أنظمة في الشبكة، كالأنظمة الخاصة بقواعد البيانات، أو تغيير جذري في تخطيط الشبكة. • العمل على معالجة جميع مخاطر الأمن السيبراني المحددة حسب منهجية إدارة مخاطر الأمن السيبراني المعتمدة.	
المخرجات المتوقعة: • تقرير يوضح تحديد وتقييم ومعالجة مخاطر الأمن السيبراني المتعلقة بالتغييرات الجوهرية التي تمّت على بيئة الإنتاج للأصول المعلوماتية والتقنية الخاصة بالجهة (Production Environment).	
١-٥-٣-٣	عند التخطيط للحصول على خدمات طرف خارجي.
إرشادات تطبيق الضوابط: • العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية. • العمل على تضمين متطلبات الأمن السيبراني ضمن إجراءات إدارة الأطراف الخارجية وإدارة العقود والمشتريات في الجهة (Third Party Management). • العمل على تنفيذ إجراءات تقييم مخاطر الأمن السيبراني عند التخطيط للحصول على خدمات طرف خارجي لتجنب الأحداث أو الظروف التي من الممكن أن تنتهك سريّة الأصول المعلوماتية والتقنية وسلامتها وتوافرها، ويشمل ذلك على وجه الخصوص التهديدات المنكشفة من الأطراف الخارجية و التي من المحتمل أن تتعرّض لها الجهة والثغرات ذات الصلة ، وتطبيق أهمية الأطراف الخارجية بناءً على نتائج تقييم مخاطر الامن السيبراني. • العمل على معالجة جميع مخاطر الأمن السيبراني المحددة حسب منهجية إدارة مخاطر الأمن السيبراني المعتمدة.	
المخرجات المتوقعة: • تقرير يوضح تحديد وتقييم ومعالجة مخاطر الأمن السيبراني للأطراف الخارجية والتي تقدم خدمات إسناد لتقنية المعلومات أو الخدمات المدارة.	
١-٥-٣-٤	عند التخطيط وقبل إطلاق منتجات وخدمات تقنية جديدة.
إرشادات تطبيق الضوابط: • العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية. • العمل على تضمين متطلبات الأمن السيبراني ضمن إجراءات إطلاق منتجات وخدمات تقنية جديدة في الجهة (Release Management).	

	• العمل على تنفيذ إجراءات تقييم مخاطر الأمن السيبراني عند التخطيط وقبل إطلاق منتجات وخدمات تقنية جديدة لتجنب الأحداث أو الظروف التي من الممكن أن تنتهك سريّة الأصول المعلوماتية والتقنية وسلامتها وتوافرها، ويشمل ذلك على وجه الخصوص تحديد الأصول المعلوماتية والتقنية، والتهديدات التي من المحتمل أن تتعرّض لها والثغرات ذات الصلة. • العمل على معالجة جميع مخاطر الأمن السيبراني المحددة حسب منهجية إدارة مخاطر الأمن السيبراني المعتمدة.
	المخرجات المتوقعة: • تقرير يوضح تحديد وتقييم ومعالجة مخاطر الأمن السيبراني عند التخطيط وقبل إطلاق منتجات وخدمات تقنية جديدة على بيئة الإنتاج.
١-٥-٤	يجب مراجعة منهجية وإجراءات إدارة مخاطر الأمن السيبراني وتحديثها على فترات زمنية مخطط لها (أو في حالة حدوث تغييرات في المتطلبات التشريعية والتنظيمية والمعايير ذات العلاقة)، كما يجب توثيق التغييرات واعتمادها.
	إرشادات تطبيق الضوابط: • العمل على مراجعة وتحديث منهجية وإجراءات إدارة مخاطر الأمن السيبراني، ومتطلبات الأمن السيبراني الخاصة بإدارة المخاطر للجهة بشكل دوري حسب خطة موثقة ومعتمدة للمراجعة بناءً على فترة زمنية محددة (على سبيل المثال، يتم اجراء المراجعة الدورية بشكل سنوي). • العمل على مراجعة وتحديث منهجية وإجراءات إدارة مخاطر الأمن السيبراني، ومتطلبات الأمن السيبراني الخاصة بإدارة المخاطر للجهة عند حدوث تغييرات في المتطلبات التشريعية والتنظيمية ذات العلاقة (على سبيل المثال، عند صدور تنظيم تشريعي جديد في الأمن السيبراني ينطبق على الجهة). • العمل على توثيق المراجعة والتغييرات التي تمت على متطلبات الأمن السيبراني الخاصة بمنهجية وإجراءات إدارة مخاطر الأمن السيبراني في الجهة واعتمادها من قبل صاحب الصلاحية.
	المخرجات المتوقعة: • وثيقة معتمدة تحدد جدول المراجعة لمنهجية وإجراءات إدارة مخاطر الأمن السيبراني. • منهجية وإجراءات مخاطر الأمن السيبراني بما يوضح أنه تم مراجعتها وتحديثها وتم توثيق التغييرات واعتمادها من قبل صاحب الصلاحية.

٦-١	الأمن السيبراني ضمن إدارة المشاريع المعلوماتية والتقنية
الهدف	التأكد من أن متطلبات الأمن السيبراني مضمنة في منهجية وإجراءات إدارة مشاريع الجهة لحماية السرية وسلامة الأصول المعلوماتية والتقنية للجهة ودقتها وتوافرها، وذلك وفقاً للسياسات والإجراءات التنظيمية للجهة والمتطلبات التشريعية والتنظيمية ذات العلاقة.
الضوابط	

١-٦-١	يجب تضمين متطلبات الأمن السيبراني في منهجية وإجراءات إدارة المشاريع وفي إدارة التغيير على الأصول المعلوماتية والتقنية في الجهة لضمان تحديد مخاطر الأمن السيبراني ومعالجتها كجزء من دورة حياة المشروع التقني، وأن تكون متطلبات الأمن السيبراني جزء أساسي من متطلبات المشاريع التقنية.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الدورة التطويرية للبرمجيات الآمنة • نموذج إجراءات الدورة التطويرية للبرمجيات الآمنة **إرشادات تطبيق الضوابط:** • العمل على تضمين متطلبات الأمن السيبراني في منهجية وإجراءات إدارة المشاريع وفي إدارة التغيير على الأصول المعلوماتية والتقنية في الجهة لضمان تحديد مخاطر الأمن السيبراني ومن هذه المتطلبات وعلى سبيل المثال لا الحصر: ○ فحص واكتشاف الثغرات قبل نشر الخدمات أو الأنظمة على الإنترنت أو عند القيام بأي تغيير على الأنظمة ضمن إدارة المشاريع المعلوماتية والتقنية. ○ معالجة الثغرات المكتشفة قبل إطلاق وتدشين المشاريع والتغييرات. ○ إجراء مراجعة الإعدادات والتحصين (Secure Configuration and Hardening) وحزم التحديثات ومعالجة الملاحظات المكتشفة قبل إطلاق وتدشين المشاريع والتغييرات. ○ متطلبات الارتباط مع أنظمة المراقبة السيبرانية. • العمل على ان تكون متطلبات الأمن السيبراني في منهجية وإجراءات إدارة المشاريع مدعومة من قبل الإدارة التنفيذية، وذلك من خلال اعتماد وموافقة رئيس الجهة أو من ينيبه.
	المخرجات المتوقعة: • وثيقة منهجية إدارة المشاريع في الجهة. • وثيقة منهجية أو إجراءات إدارة التغيير على الأصول المعلوماتية والتقنية للجهة.
١-٦-٢	يجب أن تغطي متطلبات الأمن السيبراني لإدارة المشاريع والتغييرات على الأصول المعلوماتية والتقنية للجهة بحد أدنى ما يلي:
١-٦-٢-١	تقييم الثغرات ومعالجتها.
	إرشادات تطبيق الضوابط: • العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية. • العمل على تحديد الأنظمة والخدمات والمكونات التقنية التي يجب إجراء فحص الثغرات عليها ضمن نطاق المشاريع التقنية وطلبات التغييرات. • تطوير واعتماد إجراءات خاصة بتنفيذ فحص واكتشاف الثغرات ومعالجتها وفقاً للمتطلبات التشريعية والتنظيمية ذات العلاقة. • العمل على إجراء فحص الثغرات (Vulnerabilities Assessment)، وذلك قبل إطلاق المشاريع التقنية لبيئة الإنتاج، والعمل على تقييمها في الوقت المناسب ومعالجتها بشكل فعال.

	• العمل على إجراء فحص الثغرات (Vulnerabilities Assessment)، وذلك قبل تطبيق التغييرات على بيئة الإنتاج، والعمل على تقييمها في الوقت المناسب ومعالجتها بشكل فعال.
	المخرجات المتوقعة: • وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية). • تقرير يوضح تقييم ومعالجة ثغرات الأمن السيبراني ضمن دورة حياة إدارة المشاريع والتغييرات على الأصول المعلوماتية والتقنية.
١-٦-٢-٢	إجراء مراجعة الإعدادات والتحصين (Secure Configuration and Hardening) وحزم التحديثات قبل إطلاق وتدشين المشاريع والتغييرات.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج قائمة التحقق لمتطلبات الأمن السيبراني لإدارة المشاريع والتغييرات على الأصول المعلوماتية والتقنية • نموذج قائمة التحقق لمتطلبات الأمن السيبراني لتطوير التطبيقات **إرشادات تطبيق الضوابط:** • العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية. • العمل على تحديد الأنظمة والخدمات والمكونات التقنية التي يجب إجراء مراجعة الإعدادات والتحصين عليها ضمن نطاق المشاريع التقنية وطلبات التغييرات. • التأكد من توفير معايير تقنية أمنية (Technical Security Standards) للأنظمة والخدمات والمكونات التقنية التي يجب إجراء مراجعة الإعدادات والتحصين عليها. • تطوير واعتماد إجراءات خاصة بتنفيذ مراجعة الإعدادات والتحصين للمشاريع والتغيرات التقنية وفقاً للمتطلبات التشريعية والتنظيمية ذات العلاقة. • العمل على إجراء مراجعة الإعدادات والتحصين (Secure Configuration and Hardening) وحزم التحديثات قبل إطلاق وتدشين المشاريع التقنية على بيئة الإنتاج. • العمل على إجراء مراجعة الإعدادات والتحصين (Secure Configuration and Hardening) وحزم التحديثات وذلك قبل تطبيق التغييرات على بيئة الإنتاج.
	المخرجات المتوقعة: • وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية). • معايير تقنية أمنية للأنظمة والخدمات والمكونات التقنية التي يجب إجراء مراجعة الإعدادات والتحصين عليها. • تقرير يوضح تقييم ومراجعة الإعدادات والتحصين وحزم التحديثات والإصلاحات ضمن دورة حياة إدارة المشاريع والتغييرات على الأصول المعلوماتية والتقنية للجهة قبل إطلاق وتدشين المشاريع وقبل التغييرات.

١-٦-٣	يجب أن تغطي متطلبات الأمن السيبراني لمشاريع تطوير التطبيقات والبرمجيات الخاصة للجهة بحد أدنى ما يلي:	
	١-٦-٣-١	استخدام معايير التطوير الآمن للتطبيقات (Secure Coding Standards).
	أدوات الأمن السيبراني ذات العلاقة: • نموذج معيار التطوير الآمن للتطبيقات **إرشادات تطبيق الضوابط:** • العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية. • العمل على تحديد وتوثيق واعتماد متطلبات الأمن السيبراني التقنية للتطوير الآمن للبرمجيات والتطبيقات (Secure Coding Standards)، شاملة ذكر جميع المراحل المطلوبة في التطوير، وذلك استناداً على المتطلبات التشريعية والتنظيمية ذات العلاقة، وأفضل الممارسات والمعايير المتعلقة بتطوير البرمجيات والتطبيقات وحمايتها من التهديدات الداخلية والخارجية في الجهة لتقليل المخاطر السيبرانية و التركيز على الأهداف الأساسية للحماية وهي: سرية المعلومات، وسلامتها، وتوافرها. • العمل على نشر معايير التطوير الآمن للتطبيقات للإدارات ذات العلاقة في الجهة (مثال: الإدارة المعنية بتقنية المعلومات) والتأكد من تطبيقها بشكل دوري.	
	المخرجات المتوقعة: • وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية). • معايير التطوير الآمن للتطبيقات (Secure Coding Standards) المعتمدة بالجهة. • وثائق تؤكد تطبيق معايير التطوير الآمن للتطبيقات على الأصول المعلوماتية والتقنية.	
	١-٦-٣-٢	استخدام مصادر مرخصة وموثوقة لأدوات تطوير التطبيقات والمكتبات الخاصة بها (Libraries).
	إرشادات تطبيق الضوابط: • العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية. • العمل على استخدام المصادر الحديثة والموثوق بها والمرخصة فقط لأدوات تطوير البرمجيات والمكتبات.	
	المخرجات المتوقعة: • وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية). • قائمة محدثة للبرامج المستخدمة لأدوات تطوير التطبيقات والمكتبات الخاصة بها وما يثبت أنها مرخصة وموثقة.	
	١-٦-٣-٣	إجراء اختبار للتحقق من مدى استيفاء التطبيقات للمتطلبات الأمنية السيبرانية للجهة.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج قائمة التحقق لمتطلبات الأمن السيبراني لتطوير التطبيقات **إرشادات تطبيق الضوابط:**	

	• العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية. • العمل على إجراء اختبار للتحقق من مدى استيفاء التطبيقات للمتطلبات الأمنية السيبرانية للجهة كإجراء اختبار الاختراق وذلك لضمان تطبيق ضوابط الأمن السيبراني على تطوير التطبيقات الآمن وكشف نقاط الضعف والثغرات والمشكلات في البرمجيات. • تحديد متطلبات إدارة الصلاحيات للمستخدمين ومراجعة معمارية الأمن السيبراني.
	المخرجات المتوقعة: • وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية). • قائمة مشاريع تطوير التطبيقات وقائمة الاختبارات الأمنية التي يتم عملها للتحقق من شمولية الاختبارات ومدى استيفاء التطبيقات للمتطلبات الأمنية السيبرانية للجهة وتقارير تنفيذها.
١-٦-٣-٤	أمن التكامل (Integration) بين التطبيقات.
	إرشادات تطبيق الضوابط: • العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية. • العمل على ضمان أمن التكامل بين التطبيقات عن طريق وعلى سبيل المثال لا الحصر إجراء الاختبارات الأمنية لتقنيات التكامل المختلفة ومنها: ○ إجراء اختبار تكامل النظام (SIT). ○ إجراء اختبار واجهة برمجة التطبيقات (API).
	المخرجات المتوقعة: • وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية). • تقرير يوضح اختبار وتقييم التكامل الآمن بين التطبيقات للمتطلبات الأمنية السيبرانية للجهة وتقارير تنفيذها.
١-٦-٣-٥	إجراء مراجعة الإعدادات والتحصين (Secure Configuration and Hardening) وحزم التحديثات قبل إطلاق وتدشين التطبيقات.
	إرشادات تطبيق الضوابط: • العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية. • العمل على إجراء مراجعة الإعدادات والتحصين (Secure Configuration and Hardening) وحزم التحديثات قبل إطلاق وتدشين التطبيقات والتأكد من تطبيقها في الحالات التالية: ○ مراجعة الإعدادات والتحصين للأصول المعلوماتية والتقنية والتطبيقات دورياً والتأكد من تطبيقها وفقاً للمعايير التقنية الأمنية المعتمدة.

	○ مراجعة الإعدادات والتحصين قبل إطلاق وتدشين المشاريع والتغييرات المتعلقة بالأصول المعلوماتية والتقنية. ○ مراجعة الإعدادات والتحصين قبل إطلاق وتدشين التطبيقات. ● اعتماد صورة (Image) لإعدادات وتحصين الأصول المعلوماتية والتقنية الخاصة بالجهة وفقاً للمعايير التقنية الأمنية، وحفظها في مكان آمن. ● توفير التقنيات اللازمة لإدارة الإعدادات والتحصين مركزياً، والتأكد من إمكانية تطبيق أو تحديث الإعدادات والتحصين تلقائياً لكافة الأصول المعلوماتية والتقنية في مواعيد زمنية محددة ومخطط لها.
	المخرجات المتوقعة: ● وثائق توضح تحديد وتوثيق متطلبات هذا الضابط في وثيقة متطلبات الأمن السيبراني المعتمدة من قبل صاحب الصلاحية. ● تقارير أو إثبات يوضح إجراء مراجعة الإعدادات والتحصين وحزم التحديثات قبل إطلاق وتدشين التطبيقات. ● تقارير أو إثبات يوضح إجراء مراجعة الإعدادات والتحصين وحزم التحديثات بشكل دوري.
١-٦-٤	يجب مراجعة متطلبات الأمن السيبراني في إدارة المشاريع في الجهة دورياً.
	إرشادات تطبيق الضوابط: ● العمل على مراجعة متطلبات الأمن السيبراني في إدارة المشاريع بشكل دوري حسب خطة موثقة ومعتمدة للمراجعة بناءً على فترة زمنية محددة (على سبيل المثال، يتم إجراء المراجعة الدورية بشكل سنوي). ● العمل على توثيق المراجعة والتغييرات التي تمت على متطلبات الأمن السيبراني في إدارة المشاريع في الجهة واعتمادها من قبل رئيس الجهة أو من ينيبه.
	المخرجات المتوقعة: ● وثيقة معتمدة تحدد جدول المراجعة لوثيقة متطلبات الأمن السيبراني في إدارة المشاريع. ● إثبات يؤكد القيام بالمراجعة الدورية لمتطلبات الأمن السيبراني في إدارة المشاريع والتغييرات على الأصول المعلوماتية والتقنية للجهة.

١-٧	الالتزام بتشريعات وتنظيمات ومعايير الأمن السيبراني
الهدف	ضمان التأكد من أن برنامج الأمن السيبراني لدى الجهة يتوافق مع المتطلبات التشريعية والتنظيمية ذات العلاقة.
الضوابط	
١-٧-١	يجب على الجهة الالتزام بالمتطلبات التشريعية والتنظيمية الوطنية المتعلقة بالأمن السيبراني.
	أدوات الأمن السيبراني ذات العلاقة: ● نموذج سياسة الالتزام بتشريعات وتنظيمات الأمن السيبراني **إرشادات تطبيق الضوابط:**

	• العمل مع أصحاب العلاقة في الجهة (مثل: الإدارة المعنية بالشؤون القانونية، أو الإدارة المعنية بالحوكمة والالتزام المؤسسي) على تحديد قائمة المتطلبات التشريعية والتنظيمية السيبرانية ذات الصلة بأعمال الجهة الصادرة عن الهيئة الوطنية للأمن السيبراني، وتوثيقها وتحديثها دورياً. (ويشمل ذلك -على سبيل المثال لا الحصر- الأوامر الملكية والأوامر السامية وقرارات مجلس الوزراء المتعلقة بالأمن السيبراني، والتعاميم والقرارات التنظيمية الصادرة عن الهيئة الوطنية للأمن السيبراني) • الالتزام بجميع المتطلبات التشريعية والتنظيمية الوطنية المتعلقة بالأمن السيبراني المشار إليها في الفقرة السابقة. • توفير الأدوات اللازمة للتحقق من مدى الالتزام بالمتطلبات التشريعية والتنظيمية الوطنية المتعلقة بالأمن السيبراني. • إعداد تقارير دورية توضح مدى التزام الجهة بجميع المتطلبات التشريعية والتنظيمية الوطنية المتعلقة بالأمن السيبراني، على أن يتم تقديمها للهيئة الوطنية للأمن السيبراني عند الطلب.
	المخرجات المتوقعة: • وثيقة تحدد وتوثق متطلبات هذا الضابط (مثل سياسة أو/وإجراء أو/و خطاب معتمد من قبل صاحب الصلاحية). • قائمة محدثة توضح حصر قائمة المتطلبات التشريعية والتنظيمية السيبرانية ذات الصلة بأعمال الجهة الصادرة عن الهيئة الوطنية للأمن السيبراني والتي تنطبق على الجهة. • تقرير يوضح مدى التزام الجهة بالتشريعات والتنظيمات الوطنية المتعلقة بالأمن السيبراني والتي تنطبق على الجهة.
٢-٧-١	في حال وجود اتفاقيات أو التزامات دولية معتمدة محلياً تتضمن متطلبات خاصة بالأمن السيبراني، فيجب على الجهة الالتزام بتلك المتطلبات.
	إرشادات تطبيق الضوابط: • العمل مع أصحاب العلاقة في الجهة على تحديد قائمة الاتفاقيات أو الالتزامات الدولية، المتعلقة بالأمن السيبراني، والمتطلبات ذات العلاقة، وتوثيقها واعتمادها من قبل صاحب الصلاحية وتحديثها دورياً، مع أخذ الموافقة من قبل الهيئة الوطنية للأمن السيبراني عليها مسبقاً. • العمل على الالتزام بجميع الاتفاقيات أو الالتزامات الدولية، المتعلقة بالأمن السيبراني المعتمدة من الهيئة الوطنية للأمن السيبراني داخل الجهة. • العمل على توفير التقنيات اللازمة؛ للتحقق من الالتزام بمتطلبات الجهات التشريعية والتنظيمية، المتعلقة بالأمن السيبراني.
	المخرجات المتوقعة: • وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية). • قائمة محدثة للاتفاقيات والالتزامات الدولية والمعتمدة محليا والتي تنطبق على الجهة ذات العلاقة بالأمن السيبراني.

	• تقرير يوضح مدى الالتزام بالاتفاقيات أو الالتزامات الدولية، المتعلقة بالأمن السيبراني التي تنطبق على الجهة.

١-٨	المراجعة والتدقيق الدوري للأمن السيبراني
الهدف	ضمان التأكد من أن ضوابط الأمن السيبراني لدى الجهة مطبقة وتعمل وفقاً للسياسات والإجراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية الوطنية ذات العلاقة، والمتطلبات الدولية المقرة تنظيميا على الجهة.
الضوابط	
١-٨-١	يجب على الإدارة المعنية بالأمن السيبراني في الجهة مراجعة تطبيق ضوابط الأمن السيبراني دورياً.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج إجراءات التدقيق للأمن السيبراني • نموذج سجل خطة التدقيق للأمن السيبراني **إرشادات تطبيق الضوابط:** • العمل على مراجعة تطبيق كافة متطلبات الأمن السيبراني في الجهة من قبل الإدارة المعنية بالأمن السيبراني، وذلك بشكل دوري حسب خطة موثقة ومعتمدة للمراجعة وبناءً على فترة زمنية محددة في وثيقة السياسات (على سبيل المثال يكون إجراء المراجعة بشكل ربع سنوي)، لضمان التأكد من أن ضوابط الأمن السيبراني لدى الجهة مطبقة بشكل فعّال وتعمل وفقاً للسياسات والإجراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية الوطنية ذات العلاقة، والمتطلبات الدولية المقرة تنظيميا على الجهة.
	المخرجات المتوقعة: • وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية). • الخطة المعتمدة لمراجعة تطبيق ضوابط الأمن السيبراني. • وثائق تؤكد تطبيق معايير الأمن السيبراني (Cybersecurity Standards) على الأصول المعلوماتية والتقنية والمادية. • تقارير المراجعة الدورية لتطبيق ضوابط الأمن السيبراني في الجهة.
٢-٨-١	يجب مراجعة وتدقيق تطبيق ضوابط الأمن السيبراني في الجهة، من قبل أطراف مستقلة عن الإدارة المعنية بالأمن السيبراني (مثل الإدارة المعنية بالمراجعة في الجهة) على أن تتم المراجعة والتدقيق بشكل مستقل يراعى فيه مبدأ عدم تعارض المصالح، وذلك وفقاً للمعايير العامة المقبولة للمراجعة والتدقيق والمتطلبات التشريعية والتنظيمية ذات العلاقة.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج إجراءات التدقيق للأمن السيبراني • نموذج سجل خطة التدقيق للأمن السيبراني

	إرشادات تطبيق الضوابط: • العمل على مراجعة وتدقيق تطبيق ضوابط الأمن السيبراني في الجهة، من قبل أطراف مستقلة عن الإدارة المعنية بالأمن السيبراني مثل الإدارة المعنية بالمراجعة في الجهة (Internal Audit)، او من قبل أطراف خارجية يتم التعاون معها بشكل مستقل عن الإدارة المعنية للأمن السيبراني بما يحقق مبدأ عدم تعارض المصالح عند مراجعة تطبيق كافة متطلبات الأمن السيبراني في الجهة. • العمل على إجراء المراجعة بشكل دوري حسب خطة موثقة ومعتمدة للمراجعة وبناءً على فترة زمنية محددة في وثيقة السياسات (على سبيل المثال يكون إجراء المراجعة بشكل سنوي)، وذلك لضمان التأكد من أن ضوابط الأمن السيبراني لدى الجهة مطبقة بشكل فعّال وتعمل وفقاً للسياسات والإجراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية الوطنية المقرة من قبل الهيئة الوطنية للأمن السيبراني، والمتطلبات الدولية المقرَة تنظيمياً على الجهة. **المخرجات المتوقعة:** • وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية). • الخطة المعتمدة لمراجعة وتدقيق تطبيق ضوابط الأمن السيبراني. • تقارير التدقيق (من قبل الإدارة المعنية بالمراجعة الداخلية أو من قبل مراجع خارجي مستقل) التي تمت على جميع متطلبات الأمن السيبراني في الجهة
١-٨-٣	يجب توثيق نتائج مراجعة وتدقيق الأمن السيبراني، وعرضها على اللجنة الإشرافية للأمن السيبراني وصاحب الصلاحية. كما يجب أن تشتمل النتائج على نطاق المراجعة والتدقيق، والملاحظات المكتشفة، والتوصيات والإجراءات التصحيحية، وخطة معالجة الملاحظات. **أدوات الأمن السيبراني ذات العلاقة:** • نموذج سجل تقرير التدقيق للأمن السيبراني **إرشادات تطبيق الضوابط:** • العمل على تحديد وتوثيق نتائج مراجعة وتدقيق الأمن السيبراني بحيث يشمل تقرير المراجعة على: ○ نطاق المراجعة والتدقيق. ○ الملاحظات المكتشفة ○ التوصيات والإجراءات التصحيحية ○ خطة معالجة الملاحظات • العمل على مشاركة ومناقشة نتائج مراجعة وتدقيق الأمن السيبراني الدورية مع اللجنة الإشرافية للأمن السيبراني وصاحب الصلاحية **المخرجات المتوقعة:** • وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية).

	• تقارير التدقيق (من قبل الإدارة المعنية بالمراجعة الداخلية أو الإدارة المعنية بالالتزام في الجهة أو من قبل مراجع خارجي مستقل) التي تمت على جميع متطلبات الأمن السيبراني في الجهة • إثبات يؤكد عرض نتائج مراجعة وتدقيق الامن السيبراني على اللجنة الإشرافية للأمن السيبراني وصاحب الصلاحية في الجهة.

٩-١	الأمن السيبراني المتعلق بالموارد البشرية
الهدف	ضمان التأكد من أن مخاطر ومتطلبات الأمن السيبراني المتعلقة بالعاملين (موظفين ومتعاقدين) في الجهة تعالج بفعالية قبل وأثناء وعند انتهاء/إنهاء عملهم، وذلك وفقاً للسياسات والإجراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية ذات العلقة.
الضوابط	
١-٩-١	يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني المتعلقة بالعاملين قبل توظيفهم وأثناء عملهم وعند انتهاء/إنهاء عملهم في الجهة.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للموارد البشرية. **إرشادات تطبيق الضوابط:** • العمل على تحديد متطلبات الأمن السيبراني المتعلقة بالعاملين وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية. المتطلبات تشمل على سبيل المثال لا الحصر: ○ تضمين مسؤوليات الأمن السيبراني وبنود المحافظة على سرية المعلومات (Non-Disclosure Agreement) في عقود العاملين في الجهة (لتشمل خلال وبعد انتهاء/إنهاء العلاقة الوظيفية مع الجهة). ○ إجراء مسح أمني للعاملين في وظائف الأمن السيبراني، والوظائف التقنية ذات الصلاحيات الهامة والحساسة، والوظائف ذات العلاقة بالأنظمة الحساسة • التأكد من شمولية متطلبات الأمن السيبراني المتعلقة بالعاملين خلال دورة حياة عمل الموظف (Lifecycle) في الجهة، ويشمل ذلك لمتطلبات التالية: ○ متطلبات الأمن السيبراني قبل التوظيف. ○ متطلبات الأمن السيبراني اثناء فترة العمل. ○ متطلبات الأمن السيبراني عند الانتهاء من العمل أو إنهائها. • العمل على أن تكون السياسة في الجهة مدعومة من قبل الإدارة التنفيذية. وذلك من خلال اعتماد وموافقة رئيس الجهة أو من ينيبه.
	المخرجات المتوقعة: • سياسة الأمن السيبراني للموارد البشرية المعتمدة من قبل صاحب الصلاحية.
٢-٩-١	يجب تطبيق متطلبات الأمن السيبراني المتعلقة بالعاملين في الجهة.

		إرشادات تطبيق الضوابط: • العمل على تطبيق كافة متطلبات الأمن السيبراني المتعلقة بالعاملين والتي تم تحديدها وتوثيقها واعتمادها في وثيقة سياسة الأمن السيبراني للموارد البشرية. • العمل على وضع خطة عمل لتطبيق كافة متطلبات الأمن السيبراني المتعلقة بالعاملين في الجهة. • تضمين متطلبات الأمن السيبراني المتعلقة بالعاملين في إجراءات الموارد البشرية في الجهة لضمان الالتزام بمتطلبات الأمن السيبراني لجميع أصحاب المصلحة الداخليين والخارجيين.
		المخرجات المتوقعة: • وثائق تؤكد تطبيق متطلبات الأمن السيبراني الخاصة المتعلقة بالعاملين والتي تم توثيقها في وثيقة سياسة الأمن السيبراني للموارد البشرية. • نماذج عقود العاملين في إدارة الأمن السيبراني (نسخة موقعة). • طلبات المسح الأمني للعاملين في وظائف الأمن السيبراني والوظائف التقنية ذات الصلاحيات الهامة والحساسة.
١-٩-٣	يجب أن تغطي متطلبات الأمن السيبراني قبل بدء علاقة العاملين المهنية بالجهة بحد أدنى ما يلي:	
	١-٣-٩-١	تضمين مسؤوليات الأمن السيبراني وبنود المحافظة على سرية المعلومات (Non-Disclosure Clauses) في عقود العاملين في الجهة (لتشمل خلال وبعد انتهاء/إنهاء العلاقة الوظيفية مع الجهة).
		أدوات الأمن السيبراني ذات العلاقة: • نماذج التعهد والمحافظة على السرية. **إرشادات تطبيق الضوابط:** • العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية. • العمل مع الإدارات ذات العلاقة لتضمين مسؤوليات الأمن السيبراني وبنود المحافظة على سرية المعلومات (Non-Disclosure Clauses) في عقود العاملين في الجهة (لتشمل خلال وبعد انتهاء/إنهاء العلاقة الوظيفية مع الجهة). • تضمين هذه المتطلبات في إجراءات الموارد البشرية في الجهة لضمان الالتزام بمتطلبات الأمن السيبراني لجميع أصحاب المصلحة الداخليين والخارجيين.
		المخرجات المتوقعة: • وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية). • نماذج عقود العاملين في الجهة (نسخة موقعة). • نماذج عقود العاملين في إدارة الأمن السيبراني (نسخة موقعة).

	١-٩-٣-٢	إجراء المسح الأمني (Screening or Vetting) للعاملين في وظائف الأمن السيبراني والوظائف التقنية ذات الصلاحيات الهامة والحساسة.
	إرشادات تطبيق الضوابط: • العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية. • العمل مع الإدارات ذات العلاقة لضمان إجراء المسح الأمني (Screening or Vetting) لجميع العاملين في وظائف الأمن السيبراني. • العمل مع الإدارات ذات العلاقة لضمان إجراء المسح الأمني لجميع العاملين في الوظائف التقنية ذات الصلاحيات الهامة والحساسة، ومنها (العاملون في إدارة قواعد البيانات، العاملون في إدارة جدار الحماية، العاملون في إدارة الأنظمة). • تضمين هذه المتطلبات في إجراءات الموارد البشرية في الجهة لضمان الالتزام بمتطلبات الأمن السيبراني لجميع أصحاب المصلحة الداخليين والخارجيين	
	المخرجات المتوقعة: • وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية). • إثبات يؤكد عمل إجراء المسح الأمني للعاملين في وظائف الأمن السيبراني والوظائف التقنية ذات الصلاحيات الهامة والحساسة على سبيل المثال لا الحصر: ○ وثيقة رسمية من الجهات ذات العلاقة توضح إجراء المسح الأمني	
١-٩-٤	يجب أن تغطي متطلبات الأمن السيبراني خلال علاقة العاملين المهنية بالجهة بحد أدنى ما يلي:	
	١-٩-٤-١	التوعية بالأمن السيبراني (عند بداية المهنة الوظيفية وخلالها).
	إرشادات تطبيق الضوابط: • العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية. • العمل مع الإدارات ذات العلاقة على تقديم التوعية بالأمن السيبراني عند بداية المهنة الوظيفية وخلالها وذلك من خلال قنوات الاتصال المعتمدة في الجهة. • تضمين هذه المتطلبات في إجراءات الموارد البشرية في الجهة لضمان الالتزام بمتطلبات الأمن السيبراني لجميع أصحاب المصلحة الداخليين والخارجيين • العمل على أن تكون السياسة في الجهة مدعومة من قبل الإدارة التنفيذية. وذلك من خلال اعتماد وموافقة صاحب الصلاحية.	
	المخرجات المتوقعة: • وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية).	

	• وثائق تؤكد على تقديم محتوى توعوي للعاملين في الجهة مختص بالأمن السيبراني قبل مباشرة العمل في الجهة وتزويدهم بصلاحيات الدخول من خلال رسائل البريد الالكتروني أو عقد ورش عمل أو أيا كانت الوسيلة وعلى سبيل المثال لا الحصر: ○ استعراض رسائل التوعية بالأمن السيبراني التي تم مشاركتها مع الموظفين من خلال رسائل البريد الالكتروني ○ استعراض المحتوى الذي تم عرضه في ورشة العمل ○ استعراض خطة التوعية بالأمن السيبراني
١-٩-٤-٢	تطبيق متطلبات الأمن السيبراني والالتزام بها وفقاً لسياسات وإجراءات وعمليات الأمن السيبراني للجهة.
	إرشادات تطبيق الضوابط: • العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية. • العمل على ضمان اطلاع وإقرار جميع العاملين في الجهة على سياسات وإجراءات الأمن السيبراني، وذلك لتوعية العاملين في الجهة أهمية دورهم في تطبيق متطلبات الأمن السيبراني. • تضمين متطلبات الأمن السيبراني المتعلقة بالعاملين في إجراءات الموارد البشرية في الجهة لضمان الالتزام بمتطلبات الأمن السيبراني لجميع أصحاب المصلحة الداخليين والخارجيين.
	المخرجات المتوقعة: • وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية) • نموذج إقرار بسياسات الأمن السيبراني من قبل أحد العاملين في الجهة (نسخة موقعة).
١-٩-٥	يجب مراجعة وإلغاء الصلاحيات للعاملين مباشرة بعد انتهاء/إنهاء الخدمة المهنية لهم بالجهة.
	إرشادات تطبيق الضوابط: • العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية. • العمل على مراجعة وإلغاء الصلاحيات للعاملين مباشرة بعد انتهاء/إنهاء الخدمة المهنية لهم بالجهة في الجهة وقد تشمل الآتي: ○ تحديد إجراءات انتهاء الخدمة المهنية أو إنهائها بشكل يغطي متطلبات الأمن السيبراني. ○ التأكد من إعادة جميع الأصول الخاصة بالجهة وإلغاء صلاحيات الدخول للعاملين عند انتهاء علاقتهم بالجهة مباشرة.
	المخرجات المتوقعة: • نموذج إخلاء طرف مع توفير عيّنة موقعة ومعتمدة لتطبيق الإجراءات.

١-٩-٦	يجب مراجعة متطلبات الأمن السيبراني المتعلقة بالعاملين في الجهة دورياً.
	إرشادات تطبيق الضوابط: • مراجعة وتحديث سياسة ومتطلبات الأمن السيبراني الخاصة بالعاملين في الجهة بشكل دوري حسب خطة موثقة ومعتمدة للمراجعة بناءً على فترة زمنية محددة (بشكل سنوي على سبيل المثال)، أو في حالة حدوث تغييرات في المتطلبات التشريعية والتنظيمية ذات العلاقة. كما يجب توثيق المراجعة والتغييرات التي تمت على متطلبات الأمن السيبراني الخاصة بالعاملين في الجهة واعتمادها من قبل رئيس الجهة أو من ينيبه.
	المخرجات المتوقعة: • وثيقة معتمدة تحدد جدول المراجعة للسياسة. • وثيقة السياسة بما يوضح أن تكون محدثة وتم توثيق التغييرات على متطلبات الأمن السيبراني الخاصة بالعاملين في الجهة واعتمادها من قبل رئيس الجهة أو من ينيبه. • موافقة رسمية من قبل رئيس الجهة أو من ينيبه على السياسة المحدثة (مثال: عن طريق البريد الإلكتروني الرسمي للجهة، أو التوقيع الورقي أو الإلكتروني).

١-١٠	برنامج التوعية والتدريب بالأمن السيبراني
الهدف	ضمان التأكد من أن العاملين بالجهة لديهم التوعية الأمنية اللازمة وعلى دراية بمسؤولياتهم في مجال الأمن السيبراني. والتأكد من تزويد العاملين بالجهة بالمهارات والمؤهلات والدورات التدريبية المطلوبة في مجال الأمن السيبراني لحماية الأصول المعلوماتية والتقنية للجهة والقيام بمسؤولياتهم تجاه الأمن السيبراني.
الضوابط	
١-١٠-١	يجب تطوير واعتماد برنامج للتوعية بالأمن السيبراني في الجهة من خلال قنوات متعددة دورياً، وذلك لتعزيز الوعي بالأمن السيبراني وتهديداته ومخاطره، وبناء ثقافة إيجابية للأمن السيبراني.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج برنامج التوعية • نموذج محتوى التوعية لجميع الموظفين • نموذج محتوى التوعية للوظائف الإشرافية والتنفيذية • نموذج محتوى التوعية للموظفين المشغلين للأصول المعلوماتية والتقنية **إرشادات تطبيق الضوابط:** • العمل على تطوير واعتماد برنامج وخطة للتوعية بالأمن السيبراني في الجهة من خلال قنوات متعددة دورياً، على سبيل المثال لا الحصر: ○ رسائل توعوية عن طريق البريد الإلكتروني ○ عقد ورش عمل للتوعية بالأمن السيبراني. ○ توزيع منشورات توعوية. ○ عرض توعوي من خلال اللوحات الجدارية.

	○ اطلاق منصة تدريب وتوعية بالأمن السيبراني. ● قد يتضمن البرنامج خطة للتنسيق مع الإدارة المعنية بالموارد البشرية والإدارة المعنية بالإعلام والتواصل الداخلي والإدارة المعنية بالأمن السيبراني وذلك لتعزيز الوعي بالأمن السيبراني وتهديداته ومخاطره، وبناء ثقافة إيجابية للأمن السيبراني. ● العمل على أن يكون البرنامج في الجهة مدعوم من قبل الإدارة التنفيذية. وذلك من خلال اعتماد وموافقة صاحب الصلاحية.
	المخرجات المتوقعة: ● وثيقة برنامج التوعية المعتمدة في الجهة.
١-١٠-٢	يجب تطبيق البرنامج المعتمد للتوعية بالأمن السيبراني في الجهة.
	إرشادات تطبيق الضوابط: ● العمل على تطبيق البرنامج المعتمد للتوعية والتدريب بالأمن السيبراني بالتنسيق مع الإدارة المعنية بالتوعية والتدريب بالأمن السيبراني وقد تشمل الآتي: ○ تنفيذ البرنامج المعتمد للتوعية بالأمن السيبراني في الجهة وعلى سبيل المثال لا الحصر إرسال رسائل توعوية من خلال البريد الإلكتروني أو عقد ورش عمل للتوعية بالأمن السيبراني. ○ إجراء تقييم للوعي الأمني لجميع العاملين وتحديد نقاط الضعف المتعلقة بالأمن السيبراني والعمل على معالجتها.
	المخرجات المتوقعة: ● خطة العمل لتطبيق برنامج التوعية بالأمن السيبراني المعتمدة في الجهة. ● برامج توعوية يتم مشاركتها مع الموظفين. ● قوائم المستفيدون من البرامج التوعوية.
١-١٠-٣	يجب أن يغطي برنامج التوعية بالأمن السيبراني كيفية حماية الجهة من أهم المخاطر والتهديدات السيبرانية وما يستجد منها، بما في ذلك:
	١-١٠-٣-١ التعامل الآمن مع خدمات البريد الإلكتروني خصوصاً مع رسائل التصيد الإلكتروني.
	إرشادات تطبيق الضوابط: ● العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية. ● العمل على تقديم برامج توعوية في الأمن السيبراني بحيث تغطي التعامل الآمن مع خدمات البريد الالكتروني خصوصا مع رسائل التصيد الالكتروني والهندسة الاجتماعية.
	المخرجات المتوقعة: ● وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية) ● خطة العمل لتطبيق برنامج التوعية بالأمن السيبراني المعتمدة في الجهة.

• إثبات على تقديم محتوى توعوي للتعامل الآمن مع خدمات البريد الالكتروني خصوصا مع رسائل التصيد الالكتروني.	
١-١٠-٣-٢	التعامل الآمن مع الأجهزة المحمولة ووسائط التخزين.
إرشادات تطبيق الضوابط: • العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية. • العمل على تقديم برامج توعوية في الأمن السيبراني بحيث تغطي التعامل الآمن مع الأجهزة المحمولة ووسائط التخزين.	
المخرجات المتوقعة: • وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية) • خطة العمل لتطبيق برنامج التوعية بالأمن السيبراني المعتمدة في الجهة. • إثبات على تقديم محتوى توعوي للتعامل الآمن مع الأجهزة المحمولة ووسائط التخزين.	
١-١٠-٣-٣	التعامل الآمن مع خدمات تصفح الإنترنت.
إرشادات تطبيق الضوابط: • العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية. • العمل على تقديم برامج توعوية في الأمن السيبراني بحيث تغطي التعامل الآمن مع خدمات تصفح الإنترنت، وخصوصًا التعامل مع المواقع المشبوهة مثل: مواقع التصيد الوهمية والمواقع والروابط المشبوهة.	
المخرجات المتوقعة: • وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية) • خطة العمل لتطبيق برنامج التوعية بالأمن السيبراني المعتمدة في الجهة. • إثبات على تقديم محتوى توعوي للتعامل الآمن مع خدمات تصفح الانترنت.	
١-١٠-٣-٤	التعامل الآمن مع وسائل التواصل الاجتماعي.
إرشادات تطبيق الضوابط: • العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية. • العمل على تقديم برامج توعوية في الأمن السيبراني بحيث تغطي التعامل الآمن مع وسائل التواصل الاجتماعي.	
المخرجات المتوقعة:	

		• وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية) • خطة العمل لتطبيق برنامج التوعية بالأمن السيبراني المعتمدة في الجهة. • إثبات على تقديم محتوى توعوي للتعامل الآمن مع وسائل التواصل الاجتماعي.
١-١٠-٤	يجب توفير المهارات المتخصصة والتدريب اللازم للعاملين في المجالات الوظيفية ذات العلاقة المباشرة بالأمن السيبراني في الجهة، وتصنيفها بما يتماشى مع مسؤولياتهم الوظيفية فيما يتعلق بالأمن السيبراني، بما في ذلك:	
	١-١٠-٤-١	موظفو الإدارة المعنية بالأمن السيبراني.
	إرشادات تطبيق الضوابط: • العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية. • العمل على تطوير وتنفيذ خطة معتمدة للتدريب في مجال الأمن السيبراني لموظفو الإدارة المعنية بالأمن السيبراني بالتنسيق مع الإدارة المعنية بالتدريب في الجهة وقد تشمل الآتي: ○ تنفيذ الخطة التدريبية للأمن السيبراني في الجهة بالتنسيق مع الإدارة المعنية بالتدريب وتطوير الموظفين. ○ المساعدة في تحديد المسارات المهنية للأمن السيبراني لإتاحة الفرصة للنمو المهني والترقيات في المجالات المهنية المتعلقة بالأمن السيبراني. ○ تقديم الدعم في المطالبة بالتمويل الكافي للموارد التدريبية المتعلقة بالأمن السيبراني، بما في ذلك الدورات الداخلية والدورات المتعلقة بالقطاع، والمدربين والمواد ذات الصلة.	
	المخرجات المتوقعة: • وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية) • خطط وبرامج التدريب المعتمدة لموظفي إدارة الأمن السيبراني في الجهة. • شهادات تدريبية في مجال الأمن السيبراني.	
	٢-١٠-٤-١	الموظفون العاملون في تطوير البرامج والتطبيقات والموظفون المشغلون للأصول المعلوماتية والتقنية للجهة.
	إرشادات تطبيق الضوابط: • العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية. • العمل على تطوير وتنفيذ خطة معتمدة للتدريب في مجال التطوير الآمن للبرامج والتطبيقات والإدارة الآمنة للأصول المعلوماتية والتقنية للجهة للموظفين المعنيين بالتنسيق مع الإدارة المعنية بالتدريب في الجهة وقد تشمل الآتي: ○ تنفيذ الخطة التدريبية لتطوير البرامج والتطبيقات والموظفون المشغلون للأصول المعلوماتية والتقنية للجهة بالتنسيق مع الإدارة المعنية بالتدريب وتطوير الموظفين.	

		○ المساعدة في تحديد المسارات المهنية لمطوري البرامج والتطبيقات والموظفون المشغلون للأصول المعلوماتية والتقنية للجهة لإتاحة الفرصة للنمو المهني والترقيات في المجالات المهنية المتعلقة بتطوير البرمجيات. ● تقديم الدعم في المطالبة بالتمويل الكافي للموارد التدريبية المتعلقة بتطوير البرامج والتطبيقات والموظفون المشغلون للأصول المعلوماتية والتقنية للجهة، بما في ذلك الدورات الداخلية والدورات المتعلقة بالقطاع، والمدربين والمواد ذات الصلة.
		المخرجات المتوقعة: ● وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية) ● برامج التدريب المعتمدة للموظفين العاملين في تطوير البرامج والتطبيقات والموظفين المشغلين للأصول المعلوماتية والتقنية للجهة. ● شهادات تدريبية في مجال تطوير البرامج والتطبيقات.
	١-١٠-٤-٣	الوظائف الإشرافية والتنفيذية.
		إرشادات تطبيق الضوابط: ● العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية. ● العمل على تطوير وتنفيذ خطة معتمدة للتدريب في مجالات الأمن السيبراني للوظائف الإشرافية والتنفيذية بالتنسيق مع الإدارة المعنية بالتدريب في الجهة وقد تشمل الآتي: ○ توعية عن أهمية الأمن السيبراني وتطوير ثقافة الأمن السيبراني وأبرز المخاطر والتهديدات مثل رسائل التصيّد الإلكتروني للوظائف الإشرافية والتنفيذية (Whale phishing) ○ تنفيذ الخطة التدريبية للوظائف الإشرافية والتنفيذية في الجهة بالتنسيق مع الإدارة المعنية بالتدريب وتطوير الموظفين. ○ المساعدة في تحديد المسارات المهنية للوظائف الإشرافية والتنفيذية لإتاحة الفرصة للنمو المهني والترقيات في المجالات المهنية المتعلقة بالأمن السيبراني. ○ تقديم الدعم في المطالبة بالتمويل الكافي للموارد التدريبية المتعلقة بالوظائف الإشرافية والتنفيذية، بما في ذلك الدورات الداخلية والدورات المتعلقة بالقطاع، والمدربين والمواد ذات الصلة.
		المخرجات المتوقعة: ● وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية) ● برامج التدريب الأمنية والمخصصة للوظائف الإشرافية والتنفيذية في الجهة. ● شهادات تدريبية في مجال الوظائف الإشرافية والتنفيذية.
١-١٠-٥		يجب مراجعة تطبيق برنامج التوعية بالأمن السيبراني في الجهة دورياً.
		إرشادات تطبيق الضوابط:

	• العمل على مراجعة تطبيق متطلبات الأمن السيبراني لبرامج التوعية والتدريب بالأمن السيبراني من خلال إجراء تقييم دوري (وذلك حسب خطة موثقة ومعتمدة للمراجعة، وبناء على فترة زمنية محددة "على سبيل المثال، بشكل ربع سنوي") لتنفيذ الخطط التوعوية والتدريبية من قبل الإدارة المعنية بالأمن السيبراني وبالتعاون مع الإدارات ذات العلاقة (كالإدارة المعنية بالتوعية والتدريب). • مراجعة التطبيق قد تتم من خلال القنوات التقليدية (مثل البريد الإلكتروني) أو قد يكون مؤتمت باستخدام نظام لإدارة الالتزام. الجهة قد تضع خطة مراجعة توضح فيها جدول مراجعة تطبيق متطلبات الأمن السيبراني لتطبيق برامج التوعية والتدريب بالأمن السيبراني.
	المخرجات المتوقعة: • نتائج مراجعة تطبيق برنامج التوعية بالأمن السيبراني في الجهة. • وثيقة تحدد دورة مراجعة تطبيق التوعية والتدريب في مجال الأمن السيبراني (جدول تقييم الالتزام). • وثيقة تقرير تقييم الالتزام توضح تقييم تطبيق متطلبات الأمن السيبراني لتطبيق برامج التوعية والتدريب بالأمن السيبراني.

٢ تعزيز الأمن السيبراني (Cybersecurity Defense)

٢-١	إدارة الأصول (Asset Management)
الهدف	للتأكد من أن الجهة لديها قائمة جرد دقيقة وحديثة للأصول تشمل التفاصيل ذات العلاقة لجميع الأصول المعلوماتية والتقنية المتاحة للجهة، من أجل دعم العمليات التشغيلية للجهة ومتطلبات الأمن السيبراني، لتحقيق سرية وسلامة الأصول المعلوماتية والتقنية للجهة ودقتها وتوافرها.
الضوابط	
٢-١-١	يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني لإدارة الأصول المعلوماتية والتقنية للجهة.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة إدارة الأصول **إرشادات تطبيق الضوابط:** • العمل على تطوير وتوثيق متطلبات الأمن السيبراني لإدارة الأصول المعلوماتية والتقنية للجهة، وقد تشمل الآتي: ○ تحديد متطلبات أنواع الأصول المعلوماتية والتقنية ووصفها.

	○ تحديد متطلبات مستويات تصنيف الأصول المعلوماتية والتقنية من حيث البيانات المتضمنة والمعالجة، و أهمية الأصل التقني من منظور الأمن السيبراني. ○ تحديد متطلبات المراحل المحددة لدورة حياة الأصل المعلوماتية والتقنية (على سبيل المثال لا الحصر: الحفظ، المعالجة، التخزين، الإتلاف..إلخ). ○ تحديد متطلبات الأدوار والمسؤوليات فيما يتعلق بملكية وإدارة الأصول المعلوماتية والتقنية ● العمل على أن تكون المتطلبات في الجهة مدعومة من قبل الإدارة التنفيذية. وذلك من خلال اعتماد وموافقة صاحب الصلاحية.
	المخرجات المتوقعة: ● وثيقة (مثل سياسة أومعيار) توضح متطلبات الأمن السيبراني لإدارة الأصول المعلوماتية المعتمدة من قبل الجهة (مثال: نسخة إلكترونية أو نسخة ورقية رسمية). ● موافقة رسمية من قبل رئيس الجهة أو من ينيبه على المتطلبات (مثال: عن طريق البريد الإلكتروني الرسمي للجهة، أو التوقيع الورقي أو الإلكتروني).
٢-١-٢	يجب تطبيق متطلبات الأمن السيبراني لإدارة الأصول المعلوماتية والتقنية للجهة.
	إرشادات تطبيق الضوابط: ● العمل على تطبيق كافة متطلبات الأمن السيبراني لإدارة الأصول المعلوماتية والتقنية للجهة وقد تشمل الآتي: ○ تنفيذ متطلبات الأمن السيبراني المعتمدة لإدارة الأصول المعلوماتية والتقنية في الجهة وعلى سبيل المثال لا الحصر تصنيف جميع الأصول المعلوماتية والتقنية للجهة وتوثيقها واعتمادها في وثيقة معتمدة ورسمية (مثال: سجل موثّق لإدارة الأصول المعلوماتية والتقنية للجهة) ، كذلك ترميز جميع الأصول المعلوماتية والتقنية للجهة بناءً على التصنيف المعتمد للأصول المعلوماتية والتقنية للجهة. ○ إنشاء إجراءات محددة للتعامل مع الأصول بناءً على تصنيفها ووفقاً للمتطلبات التشريعية والتنظيمية ذات العلاقة.
	المخرجات المتوقعة: ● وثائق تؤكد تطبيق متطلبات الأمن السيبراني لإدارة الأصول المعلوماتية والتقنية والتي تم توثيقها في وثيقة السياسات. ● خطة عمل لتطبيق متطلبات الأمن السيبراني لإدارة الأصول المعلوماتية والتقنية. ● تقديم سجل موثّق ومحدث بأحدث المعلومات عن جميع الأصول المعلوماتية والتقنية (كجدول Excel أو معروض من خلال وسائل آلية باستخدام حلول مثل CMDB). ● الإجراءات المحددة والمعتمدة للتعامل مع الأصول بناءً على تصنيفها ووفقاً للمتطلبات التشريعية والتنظيمية ذات العلاقة.
٣-١-٢	يجب تحديد وتوثيق واعتماد ونشر سياسة الاستخدام المقبول للأصول المعلوماتية والتقنية للجهة.

	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الاستخدام المقبول للأصول **إرشادات تطبيق الضوابط:** • العمل على تطوير سياسة الاستخدام المقبول للأصول المعلوماتية والتقنية للجهة وقد تشمل الآتي: ○ مجموعة من القواعد التنظيمية المحددة بشأن الوصول إلى الأصول واستخدامها ○ مجموعة من الأمثلة الواضحة للاستخدام غير المقبول ○ العواقب المترتبة في حال تم انتهاك القواعد المحددة ضمن الاستخدام المقبول للأصول ○ الطريقة المتبعة لمراقبة الالتزام بالقواعد المحددة ضمن الاستخدام المقبول للأصول المعلوماتية والتقنية للجهة. • نشر سياسة الاستخدام المقبول للأصول المعلوماتية والتقنية للجهة لجميع العاملين والأطراف المعنية في الجهة على سبيل المثال لا الحصر عبر البريد الإلكتروني الرسمي للجهة أو من خلال الموقع الإلكتروني للجهة. • العمل على أن تكون السياسة في الجهة مدعومة من قبل الإدارة التنفيذية. وذلك من خلال اعتماد وموافقة رئيس الجهة أو من ينيبه. **المخرجات المتوقعة:** • وثيقة السياسة المعتمدة التي تغطي متطلبات الاستخدام المقبول للأصول المعلوماتية والتقنية للجهة (مثال: نسخة إلكترونية أو نسخة ورقية رسمية). • نشر سياسة الاستخدام المقبول للأصول المعلوماتية والتقنية للجهة لجميع العاملين والأطراف المعنية في الجهة على سبيل المثال لا الحصر نموذج ايميل رسمي للجهة يوضح نشر السياسة لجميع العاملين والأطراف المعنية في الجهة، أو من خلال دليل حي ومباشر بما يفيد نشر السياسة على الموقع الإلكتروني للجهة وما يثبت اطلاع جميع العاملين والأطراف المعنية في الجهة. • موافقة رسمية من قبل رئيس الجهة أو من ينيبه على السياسة (مثال: عن طريق البريد الإلكتروني الرسمي للجهة، أو التوقيع الورقي أو الإلكتروني).
٢-١-٤	يجب تطبيق سياسة الاستخدام المقبول للأصول المعلوماتية والتقنية للجهة. **إرشادات تطبيق الضوابط:** • العمل على تطبيق متطلبات سياسة الاستخدام المقبول للأصول المعلوماتية والتقنية للجهة وقد تشمل الآتي: ○ تنفيذ متطلبات الاستخدام المقبول للأصول المعلوماتية والتقنية من قبل الجهة على سبيل المثال لا الحصر: يتم الطلب من كل موظف الاطلاع والإقرار على سياسة الاستخدام المقبول للأصول المعلوماتية والتقنية. ○ نشر هذه المتطلبات من خلال قنوات الاتصال المعتمدة في الجهة وذلك لتوعية أصحاب المصلحة الداخليين والخارجيين في الجهة لتطبيق هذه المتطلبات. ○ تحديد الآليات والتقنيات المناسبة لرصد مخالفات عدم تطبيق متطلبات سياسة الاستخدام المقبول والتحذير بوجود إجراءات تأديبية في حال رصد مخالفات.

	المخرجات المتوقعة: • خطة عمل لتطبيق متطلبات الاستخدام المقبول للأصول المعلوماتية والتقنية للجهة لإدارة الأصول المعلوماتية والتقنية. • إثبات ما يظهر حول نشر هذه المتطلبات من خلال قنوات الاتصال المعتمدة في الجهة. • نموذج مكتمل ومعتمد يوضح إقرار جميع موظفي الجهة بسياسة الاستخدام المقبول (مثال: نسخة مادية ممسوحة ضوئيًا أو من خلال منصة رقمية أو نسخة ورقية رسمية).
٢-١-٥	يجب تصنيف الأصول المعلوماتية والتقنية للجهة وترميزها (Labelling) والتعامل معها وفقاً للمتطلبات التشريعية والتنظيمية ذات العلاقة.
	إرشادات تطبيق الضوابط: • العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني لإدارة الأصول المعلوماتية والتقنية للجهة، واعتمادها من قبل صاحب الصلاحية. • العمل مع الإدارات المعنية لتحديد جميع الأصول المعلوماتية والتقنية والتي تشمل (على سبيل المثال لا الحصر): ○ البنية التحتية (مثل الخوادم) ○ التطبيقات والخدمات ○ الشبكات (مثل الموجه) ○ أجهزة المستخدمين ○ الأجهزة الطرفية (مثل الطابعات) ○ الأنظمة التشغيلية (ان وجد) • توثيق جميع الأصول المعلوماتية والتقنية في سجل موحّد مع تحديد خصائصها مثل (اسم الأصل والوصف والمالك وحساسيته). • العمل مع ملّاك الأصول لتحديد وتوثيق واعتماد تصنيف الأصول في السجل وفقاً للمتطلبات التشريعية والتنظيمية ذات العلاقة. • العمل مع الإدارات المعنية للتأكد من ترميز الأصول بناءً على تصنيفها على سبيل المثال لا الحصر وضع ملصقات على الأصول أو ترميزها آلياً عن طريق الأنظمة الحديثة. • العمل مع الإدارات المعنية للتأكد من التعامل مع الأصول وفقًا لمستوى التصنيف المحدد والمعتمد وبناءً على الإجراءات المعتمدة للتعامل مع كل أصل.
	المخرجات المتوقعة: • وثيقة سياسة الأمن السيبراني التي تغطي متطلبات إدارة الأصول المعلوماتية والتقنية للجهة (مثال: نسخة إلكترونية أو نسخة ورقية رسمية). • موافقة رسمية من قبل رئيس الجهة أو من ينيبه على السياسة (مثال: عن طريق البريد الإلكتروني الرسمي للجهة، أو التوقيع الورقي أو الإلكتروني).

	• وثيقة توضح طريقة ونظام تصنيف الأصول وترميزها والمتطلبات المتعلقة بذلك. • وثيقة خطة عمل لتطبيق متطلبات تصنيف الأصول المعلوماتية والتقنية للجهة وترميزها (Labelling) والتعامل معها وفقاً للمتطلبات التشريعية والتنظيمية ذات العلاقة. • سجل محدث ويشمل جميع الأصول المعلوماتية والتقنية بما يوضح مستوى التصنيف لكل أصل (مثال: جدول Excel أو من خلال وسائل آلية باستخدام حلول تقنية مثل CMDB). • دليل يوضح أن أصول الجهة مصنفة وفقًا لمستوى التصنيف المحدد والمعتمد. • دليل يوضح أن أصول الجهة تم ترميزها وفقًا لمستوى التصنيف المحدد والمعتمد على سبيل المثال لا الحصر عن طريق الملصقات الترميزية التي تثبت ترميز جميع الأصول في الجهة. • دليل على تطبيق الضوابط على أصول الجهة بما يتوافق مع مستوى تصنيفها على سبيل المثال لا الحصر الإجراءات المتبعة عند التعامل مع كل أصل بناءً على تصنيفه.
٢-١-٦	يجب مراجعة متطلبات الأمن السيبراني لإدارة الأصول المعلوماتية والتقنية للجهة دورياً. **إرشادات تطبيق الضوابط:** • مراجعة وتحديث متطلبات الأمن السيبراني الخاصة بإدارة الأصول المعلوماتية والتقنية للجهة بشكل دوري حسب خطة موثقة ومعتمدة للمراجعة بناءً على فترة زمنية محددة أو في حالة حدوث تغييرات في المتطلبات التشريعية والتنظيمية ذات العلاقة. • توثيق المراجعة والتغييرات التي تتم على متطلبات الأمن السيبراني الخاصة بإدارة الأصول المعلوماتية والتقنية للجهة واعتمادها من قبل رئيس الجهة أو من ينيبه. **المخرجات المتوقعة:** • نتائج مراجعة تطبيق متطلبات الأمن السيبراني لإدارة الأصول المعلوماتية والتقنية للجهة. • وثيقة تحدد دورة مراجعة تطبيق متطلبات الأمن السيبراني لإدارة الأصول المعلوماتية والتقنية للجهة (جدول تقييم الالتزام). • سجل التحديثات والتغييرات التي تمت على متطلبات الأمن السيبراني الخاصة بإدارة الأصول المعلوماتية والتقنية. • وثيقة تقرير تقييم الالتزام توضح نتائج تقييم تطبيق متطلبات الأمن السيبراني لإدارة الأصول المعلوماتية والتقنية للجهة. • 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. • 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).

٢-٢	إدارة هويات الدخول والصلاحيات (Identity and Access Management)
الهدف	ضمان حماية الأمن السيبراني للوصول المنطقي (Logical Access) إلى الأصول المعلوماتية والتقنية للجهة من أجل منع الوصول غير المصرح به وتقييد الوصول إلى ما هو مطلوب لإنجاز الأعمال المتعلقة بالجهة.
الضوابط	
٢-٢-١	يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني لإدارة هويات الدخول والصلاحيات في الجهة.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة إدارة هويات الدخول والصلاحيات **إرشادات تطبيق الضوابط:** • العمل على تطوير وتوثيق سياسة الأمن السيبراني لإدارة هويات الدخول والصلاحيات في الجهة وقد تحتوي على سبيل المثال لا الحصر: ○ منح حق الوصول، بما يشمل: - حق الوصول لحسابات المستخدمين. - حق الوصول للحسابات الهامة والحسّاسة. - حق الوصول عن بعد إلى شبكات وأنظمة الجهة. - تحديد صلاحيات كل نوع من المستخدمين واعتمادها. ○ إلغاء وتغيير حق الوصول ○ مراجعة هويات الوصول والصلاحيات ○ إدارة كلمات المرور • 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 هويات الدخول والصلاحيات، (مثال: نسخة إلكترونية أو نسخة ورقية رسمية). • موافقة رسمية من قبل رئيس الجهة أو من ينيبه على السياسة (مثال: عن طريق البريد الإلكتروني الرسمي للجهة، أو التوقيع الورقي أو الإلكتروني).
٢-٢-٢	يجب تطبيق متطلبات الأمن السيبراني لإدارة هويات الدخول والصلاحيات في الجهة.
	إرشادات تطبيق الضوابط:

	• العمل على تطبيق كافة متطلبات الأمن السيبراني عند تطبيق إجراءات إدارة هويات الدخول والصلاحيات المعتمدة في الجهة، كما يوصى أن تغطي إدارة هويات الدخول والصلاحيات بحد أدنى ما يلي وعلى سبيل المثال لا الحصر: ○ التحقق من هوية المستخدم (User Authentication) بناءً على إدارة تسجيل المستخدم ○ إدارة كلمة المرور بناءً على سياسة كلمة المرور لدى الجهة. ○ إدارة تصاريح وصلاحيات المستخدمين (Authorization) بناءً على مبدأ الحاجة إلى المعرفة والاستخدام ○ إدارة تصاريح وصلاحيات المستخدمين (Authorization) بناءً على مبدأ الحد الأدنى من الصلاحيات والامتيازات ومبدأ فصل المهام (Segregation of Duties). ○ إدارة تصاريح الدخول عن بُعد إلى شبكات الجهة ○ إدارة إلغاء وتحديث صلاحية الوصول
	المخرجات المتوقعة: • خطة عمل لتطبيق متطلبات الأمن السيبراني لإدارة هويات الدخول والصلاحيات في الجهة. • إثبات يوضح تطبيق ضوابط التحقّق والصلاحيات على جميع الأصول التقنية والمعلوماتية في الجهة على سبيل المثال لا الحصر: ضبط جميع إعدادات الأنظمة المعلوماتية التقنية بما يتوافق مع ضوابط ومتطلبات الأمن السيبراني لإدارة هويات الدخول والصلاحيات.
٢-٢-٣	يجب أن تغطي متطلبات الأمن السيبراني المتعلقة بإدارة هويات الدخول والصلاحيات في الجهة بحد أدنى ما يلي:
١-٣-٢-٢	التحقق من هوية المستخدم (User Authentication) بناءً على إدارة تسجيل المستخدم، وإدارة كلمة المرور.
	إرشادات تطبيق الضوابط: • العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني لإدارة هويات الدخول والصلاحيات، واعتمادها من قبل صاحب الصلاحية. • ضمان تعريف جميع الموظفين بمعرّف فريد، قد يكون رقم وظيفي، أو اسم الموظف، أو آليات التسمية الأخرى لضمان أن تكون أسماء المستخدمين فريدة. • العمل على إعداد معايير كلمة المرور أخذًا بالاعتبار أفضل الممارسات، على سبيل المثال لا الحصر: ○ مدة صلاحية كلمة المرور (Expiration Period) ○ تعقيد كلمة المرور (complexity) ○ تأمين كلمة المرور (lockout) ○ تفعيل كلمة المرور (activation) ○ سجل كلمة المرور (history) ○ الية إنشاء كلمة المرور وتزويدها للمستخدم بطريقة آمنة وموثوقة من خلال إجراءات محددة ومعتمدة.

المخرجات المتوقعة:

- وثيقة سياسة الأمن السيبراني لإدارة هويات الدخول والصلاحيات، (مثال: نسخة إلكترونية أو نسخة ورقية رسمية).
- وثيقة سياسة إدارة كلمة المرور في الجهة (مثال: نسخة إلكترونية أو نسخة ورقية رسمية).
- موافقة رسمية من قبل رئيس الجهة أو مالك النظام أو من ينيبه على هذه السياسات (مثال: عن طريق البريد الإلكتروني الرسمي للجهة، أو التوقيع الورقي أو الإلكتروني).
- إثبات يوضح تطبيق ضوابط التحقّق والصلاحيات على جميع الأصول التقنية والمعلوماتية في الجهة على سبيل المثال لا الحصر: ضبط جميع إعدادات الأنظمة المعلوماتية التقنية بما يتوافق مع ضوابط ومتطلبات الأمن السيبراني لإدارة هويات الدخول والصلاحيات.

٢-٢-٣-٢	التحقق من الهوية متعدد العناصر (Multi-Factor Authentication) لعمليات الدخول عن بعد.

إرشادات تطبيق الضوابط:

- العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني لإدارة هويات الدخول والصلاحيات، واعتمادها من قبل صاحب الصلاحية.
- العمل على تطوير إجراءات لعمليات الدخول عن بعد والتي تحتوي على التحقق من الهوية متعدد العناصر (Multi-Factor Authentication).
- ضمان توفير التقنيات المناسبة والمتقدمة للتحقق من الهوية متعدد العناصر وربطها مع تقنيات الدخول عن بعد (مثل VPN).
- العمل على استخدام اثنين من عناصر التحقق التالية لتطبيق التحقق متعدد العناصر:
  - شيء تعرفه (Something you know)، على سبيل المثال لا الحصر: استخدام كلمة المرور.
  - شيء تملكه (Something you have)،على سبيل المثال لا الحصر: استخدام كلمة المرور الصالحة لمرة واحدة (One time password) من خلال الرسائل النصية أو التطبيقات.
  - شيء تمثله (Something you are)، على سبيل المثال لا الحصر: استخدام المعرفات الحيوية في التحقق مثل بصمة الإصبع أو الوجة.

المخرجات المتوقعة:

- وثيقة سياسة الأمن السيبراني لإدارة هويات الدخول والصلاحيات، (مثال: نسخة إلكترونية أو نسخة ورقية رسمية).
- موافقة رسمية من قبل رئيس الجهة أو من ينيبه على هذه السياسة (مثال: عن طريق البريد الإلكتروني الرسمي للجهة، أو التوقيع الورقي أو الإلكتروني).
- دليل يوضح تطبيق متطلبات التحقق من الهوية متعدد العناصر لعمليات الدخول عن بعد على سبيل المثال لا الحصر: لقطة شاشة توضح ضبط إعدادات الأنظمة حتى يتم ضمان التأكد من طلب التحقق من الهوية متعدد العناصر لعمليات الدخول عن بعد.

٢-٢-٣-٣	إدارة تصاريح وصلاحيات المستخدمين (Authorization) بناءً على مبادئ التحكم بالدخول والصلاحيات (مبدأ الحاجة إلى المعرفة والاستخدام "Need-to-know and Need-to-use"، ومبدأ الحد الأدنى من الصلاحيات والامتيازات "Least Privilege"، ومبدأ فصل المهام "Segregation of Duties").

إرشادات تطبيق الضوابط:

- العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني لإدارة هويات الدخول والصلاحيات، واعتمادها من قبل صاحب الصلاحية.
- العمل على تحديد صلاحيات أساسية لجميع موظفي الجهة، مثل صلاحية استخدام البريد الإلكتروني والبوابة الداخلية ونظام الموارد البشرية.
- تحديد مجموعات بحيث أن كل مجموعة لديها صلاحيات محددة بناءً على الأدوار الوظيفية، ووضع وتوثيق وتوضيح صلاحيات ومسؤوليات كل موظف بما يتوافق مع مرتبته الوظيفية وخبراته العملية.
- إدارة تصاريح وصلاحيات المستخدمين على جميع الأصول التقنية والمعلوماتية في الجهة من خلال نظام مركزي آلي للتحكّم في الوصول، مثل برنامج الدليل النشط (Active Directory).
- العمل على تطوير وإعتماد إجراءات محددة لمنح الصلاحيات للعاملين في الجهة، حيث توجد متطلبات لطلب الصلاحية ومنها:
  - معلومات مقدم الطلب (الهوية)
  - تفاصيل الصلاحية المعنية (شرح للصلاحية والأصول المعنية)
  - وصف متطلبات الأعمال للصلاحية
  - المدة الزمنية المطلوبة للصلاحية
  - الموافقات اللازمة (مثل موافقة المدير المباشر)

المخرجات المتوقعة:

- وثيقة سياسة الأمن السيبراني لإدارة هويات الدخول والصلاحيات، (مثال: نسخة إلكترونية أو نسخة ورقية رسمية).
- إثبات يوضح تطبيق متطلبات إدارة تصاريح وصلاحيات المستخدمين، على سبيل المثال لا الحصر: لقطة شاشة توضح ضبط إعدادات الأنظمة حتى يتم ضمان التأكد من تطبيق إدارة تصاريح وصلاحيات المستخدمين (Authorization) بناءً على مبادئ التحكم بالدخول والصلاحيات (مبدأ الحاجة إلى المعرفة والاستخدام "Need-to-know and Need-to-use"، ومبدأ الحد الأدنى من الصلاحيات والامتيازات "Least Privilege"، ومبدأ فصل المهام "Segregation of Duties".

٢-٢-٣-٤	إدارة الصلاحيات الهامة والحساسة (Privileged Access Management).

إرشادات تطبيق الضوابط:

- العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني لإدارة هويات الدخول والصلاحيات، واعتمادها من قبل صاحب الصلاحية.

- العمل على تحديد الصلاحيات الهامة والحساسة على مستوى البنية التحتية والشبكات والتطبيقات في الجهة
- العمل على تحديد العاملين الذين لديهم هذه الصلاحيات الهامة والحساسة.
- العمل على تطوير إجراءات إدارة الصلاحيات الهامة والحساسة معتمدة في الجهة، مع لأخذ بعين الاعتبار التالي:
  - منع استخدام الحسابات ذات الصلاحيات الهامة والحسّاسة في الأعمال اليومية العادية على أن يتم استخدام حساب مستخدم عادي لهذا الغرض.
  - منع استخدام الحسابات ذات الصلاحيات الهامة والحسّاسة للوصول الى الانترنت.
  - منع استخدام الحسابات ذات الصلاحيات الهامة والحسّاسة للوصول للبريد الالكتروني.
  - تقييد استخدام الحسابات ذات الصلاحيات الهامة والحسّاسة لعمليات الدخول عن بعد.
  - تعطيل/حذف الحسابات الحساسة الافتراضية (default accounts)ز
  - التأكد من وجود نظام حماية أجهزة المستخدمين مثبت ومحدث على الجهاز الذي سوف يتم استخدامه للدخول للحسابات ذات الصلاحيات الهامة والحسّاسة.
  - بناء نسخ آمنه من أنظمة التشغيل المستخدمة في الجهة و إعدادها بشكل آمن ز
  - تثبيت برامج الحماية وتعطيل الخدمات الغير متستخدمة. ليتم استخدام هذه النسخ في تهيئة الأجهزة المكتبية والخوادم.
- العمل على تحديد والتقنيات والآليات الحديثة والمتقدمة لإدارة الصلاحيات الهامة والحساسة.
- منح الصلاحيات الهامة والحساسة بناءً على المهام الوظيفية بعد أخذ الموافقات اللازمة، مع الأخذ بالاعتبار مبدأ فصل المهام.
- المراقبة المستمرة لسجلات أحداث الأمن السيبراني للحسابات ذات الصلاحيات الهامة والحساسة.

المخرجات المتوقعة:

- وثيقة سياسة إدارة الحسابات الهامة والحساسة في الجهة (مثال: نسخة إلكترونية أو نسخة ورقية رسمية).
- موافقة رسمية من قبل رئيس الجهة أو من ينيبه على السياسة (مثال: عن طريق البريد الإلكتروني الرسمي للجهة، أو التوقيع الورقي أو الإلكتروني).
- إثبات يوضح تطبيق متطلبات إدارة الصلاحيات الهامة والحساسة على سبيل المثال لا الحصر: لقطة شاشة توضح ضبط إعدادات الأنظمة حتى يتم ضمان التأكد من تطبيق منح مدراء الأنظمة بالصلاحيات الهامة والحساسة المحددة والمعتمدة.

٢-٢-٣-٥	المراجعة الدورية لهويات الدخول والصلاحيات.

إرشادات تطبيق الضوابط:

- العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني لإدارة هويات الدخول والصلاحيات، واعتمادها من قبل صاحب الصلاحية.
- العمل على تحديد الصلاحيات الهامة والحساسة على مستوى البنية التحتية والشبكات والتطبيقات في الجهة
- العمل على تحديد العاملين الذين لديهم هذه الصلاحيات الهامة والحساسة

	• العمل على تطوير خطة للمراجعة الدورية لهويات الدخول والصلاحيات على التالي: ○ على مستوى جميع التطبيقات في الجهة ○ على مستوى الشبكات ○ على مستوى البنية التحتية والخوادم ○ على مستوى أجهزة المستخدمين • العمل على مراجعة الصلاحيات بالتعاون مع الإدارة المعنية بتقنية المعلومات ومدراء التطبيقات لإبطال حق الوصول في الحالات التالية (على سبيل المثال على الحصر): ○ الصلاحية لم يتم استخدامها لفترة زمنية طويلة (مثل لأكثر من ٣ أشهر) ○ وجود الصلاحية يسبب تعارض في المصالح ○ لم يتم تأكيد حاجة العامل للصلاحية من قبل مديره ○ انتهاء الفترة الزمنية المحددة لمنح الصلاحية
	المخرجات المتوقعة: • وثيقة سياسة إدارة الحسابات الهامة والحساسة في الجهة (مثال: نسخة إلكترونية أو نسخة ورقية رسمية). • موافقة رسمية من قبل رئيس الجهة أو من ينيبه على السياسة (مثال: عن طريق البريد الإلكتروني الرسمي للجهة، أو التوقيع الورقي أو الإلكتروني). • إثبات يوضح تطبيق متطلبات المراجعة الدورية لهويات الدخول والصلاحيات على سبيل المثال لا الحصر: وثيقة رسمية ومعتمدة توضح القيام بالمراجعة المراجعة الدورية لهويات الدخول والصلاحيات.
٤-٢-٢	يجب مراجعة تطبيق متطلبات الأمن السيبراني لإدارة هويات الدخول والصلاحيات في الجهة دورياً.
	إرشادات تطبيق الضوابط: • العمل على مراجعة تطبيق متطلبات الأمن السيبراني لإدارة هويات الدخول والصلاحيات في الجهة من خلال إجراء تقييم دوري (وذلك حسب خطة موثقة ومعتمدة للمراجعة، وبناء على فترة زمنية محددة "على سبيل المثال لا الحصر، بشكل ربع سنوي") لتنفيذ متطلبات إدارة هويات الدخول والصلاحيات من قبل الإدارة المعنية بالأمن السيبراني وبالتعاون مع الإدارات ذات العلاقة (كالإدارة المعنية بتقنية المعلومات). • مراجعة وتحديث متطلبات الأمن السيبراني الخاصة بإدارة هويات الدخول والصلاحيات في الجهة بشكل دوري حسب خطة موثقة ومعتمدة للمراجعة بناءً على فترة زمنية محددة أو في حالة حدوث تغييرات في المتطلبات التشريعية والتنظيمية ذات العلاقة. • توثيق المراجعة والتغييرات التي تتم على متطلبات الأمن السيبراني الخاصة بإدارة هويات الدخول والصلاحيات في الجهة واعتمادها من قبل رئيس الجهة أو من ينيبه.
	المخرجات المتوقعة: • نتائج مراجعة تطبيق متطلبات إدارة هويات الدخول والصلاحيات في الجهة.

	• وثيقة تحدد دورة مراجعة تطبيق متطلبات الأمن السيبراني لإدارة هويات الدخول والصلاحيات في الجهة (جدول تقييم الالتزام). • وثيقة تقرير تقييم الالتزام توضح نتائج تقييم تطبيق متطلبات الأمن السيبراني لتطبيق متطلبات إدارة هويات الدخول والصلاحيات في الجهة. • 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. • 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).

٢-٣	حماية الأنظمة وأجهزة معالجة المعلومات (Information System and Processing Facilities Protection)
الهدف	ضمان حماية الأنظمة وأجهزة معالجة المعلومات بما في ذلك أجهزة المستخدمين والبنى التحتية للجهة من المخاطر السيبرانية.
الضوابط	
٢-٣-١	يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني لحماية الأنظمة وأجهزة معالجة المعلومات للجهة.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة أمن قواعد البيانات **إرشادات تطبيق الضوابط:** • العمل على تطوير وتوثيق سياسة الأمن السيبراني لحماية الأنظمة وأجهزة معالجة المعلومات في الجهة، وقد تشمل الآتي: ○ تقنيات وآليات الحماية الحديثة والمتقدمة وتوفيرها والتأكد من موثوقيتها. ○ إعدادات تقنيات وآليات الحماية من البرمجيات الضارة. ○ نطاق الأجهزة المراد حمايتها، على أن تشمل جميع أجهزة المستخدمين وأنظمة الجهة الحساسة وغيرها. ○ بناء نسخ آمنه من أنظمة التشغيل المستخدمة في الجهة وإعدادها بشكل آمن وتثبيت برامج الحماية وتعطيل الخدمات الغير متستخدمة فيها، ليتم استخدام هذه النسخ في تهيئة الأجهزة المكتبية والخوادم. ○ التأكد من خلوا أجهزة المستخدمين وأنظمة الجهة من البرمجيات الضارة بشكل دوري.

	○ التقييد الحازم لاستخدام أجهزة وسائط التخزين الخارجية والأمن المتعلق بها. ○ إدارة حزم التحديثات والإصلاحات للأنظمة والتطبيقات والأجهزة. ○ تحديد مصادر مزامنة التوقيت (Clock Synchronization) المركزي في الجهة، بحيث تكون من مصدر دقيق وموثوق. ● العمل على أن تكون السياسة في الجهة مدعومة من قبل الإدارة التنفيذية. وذلك من خلال اعتماد وموافقة رئيس الجهة أو من ينيبه.
	المخرجات المتوقعة: ● وثيقة سياسة الأمن السيبراني التي تغطي متطلبات حماية الأنظمة وأجهزة معالجة المعلومات في الجهة (مثال: نسخة إلكترونية أو نسخة ورقية رسمية). ● موافقة رسمية من قبل رئيس الجهة أو من ينيبه على السياسة (مثال: عن طريق البريد الإلكتروني الرسمي للجهة، أو التوقيع الورقي أو الإلكتروني). ● نموذج سياسة الإعدادات والتحصين ● نموذج سياسة أمن الخوادم ● نموذج سياسة الحماية من البرمجيات الضارة ● نموذج سياسة وسائط التخزين ● نموذج سياسة إدارة حزم التحديثات والإصلاحات
٢-٣-٢	يجب تطبيق متطلبات الأمن السيبراني لحماية الأنظمة وأجهزة معالجة المعلومات للجهة.
	إرشادات تطبيق الضوابط: ● العمل على تطبيق كافة متطلبات الأمن السيبراني لحماية الأنظمة وأجهزة معالجة المعلومات، وقد تشمل الآتي: ○ توفير تقنيات وآليات الحماية الحديثة والمتقدمة والتأكد من موثوقيتها. ○ التأكد من نطاق الأجهزة المراد حمايتها ومراجعتها دورياً. ○ التقييد الحازم لاستخدام أجهزة وسائط التخزين الخارجية والأمن المتعلق بها. ○ تطبيق حزم التحديثات والإصلاحات على جميع نطاق الأجهزة والأنظمة والتطبيقات الخاصة بالجهة. ○ العمل على مزامنة التوقيت (Clock Synchronization) مركزياً ومن مصدر دقيق وموثوق.
	المخرجات المتوقعة: ● وثائق تؤكد تطبيق متطلبات الأمن السيبراني لحماية الأنظمة وأجهزة معالجة المعلومات في الجهة والتي تم توثيقها في وثيقة السياسات. ● قائمة محدثة أنظمة الحماية من الفيروسات لدى الجهة ونطاق تنزيلها. ● تقييد استخدام أجهزة وسائط التخزين الخارجية وإجراءات الموافقة على استخدامها. ● إثبات يوضح شمول نطاق حزم التحديثات والإصلاحات جميع الأجهزة والأنظمة والتطبيقات.

	• إثبات استخدام الجهة لخادم مركزي ومصدر موثوق لمزامنة التوقيت.
٢-٣-٣	يجب أن تغطي متطلبات الأمن السيبراني لحماية الأنظمة وأجهزة معالجة المعلومات للجهة بحد أدنى ما يلي:
٢-٣-٣-١	الحماية من الفيروسات والبرامج والأنشطة المشبوهة والبرمجيات الضارة (Malware) على أجهزة المستخدمين والخوادم باستخدام تقنيات وآليات الحماية الحديثة والمتقدمة، وإدارتها بشكل آمن.
	إرشادات تطبيق الضوابط: • العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية. • العمل على توفير تقنيات وآليات الحماية من الفيروسات والبرامج والأنشطة المشبوهة والبرمجيات الضارة (Malware) والعمل على الآتي: ○ التأكد المستمر من أن التقنيات المستخدمة حديثة ومتقدمة وتحتوي على الحماية من الهجمات المتقدمة والمستمرة (APT). ○ تحديد نطاق الأصول التي سيتم تنزيل نظام الحماية عليها وتحديد وتحديث حالتها. ○ تنزيل نظام الحماية على جميع نطاق أجهزة المستخدمين وأنظمة الجهة والخوادم. ○ مراجعة نظام الحماية بشكل دوري للتأكد من شمولية نطاق نظام الحماية لجميع أجهزة المستخدمين وأنظمة الجهة والخوادم من خلال وحدة التحكم الخاصة بنظام الحماية. ○ وضع وتنفيذ خطة عمل تصحيحية (عند الحاجة) لتثبيت نظام الحماية على جميع الأجهزة مع اتخاذ إجراءات تجاه الأجهزة والأنظمة التي تتكرر عندها ملاحظة عدم تثبيت نظام الحماية الحديث والمتقدم. ○ متابعة نظام الحماية دورياً للتأكد من التحديثات المستحدثة وإطلاق هذه التحديثات على كل أجهزة المستخدمين وأنظمة الجهة والخوادم.
	المخرجات المتوقعة: • وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية). • قائمة أنظمة الحماية من الفيروسات ودليل احتواءها على الحماية من الهجمات المتقدمة المستمرة (على سبيل المثال لا الحصر: لقطة شاشة أو دليل مباشر من صفحة متابعة الهجمات المتقدمة والمستمرة في نظام الحماية). • تقارير أو إثبات يوضح تنزيل تقنيات الحماية في جميع أجهزة الموظفين وأنظمة الجهة والخوادم. • تقارير أو إثبات يوضح متابعة نطاق تنزيل هذه التقنيات وتحديثها دورياً.
٢-٣-٣-٢	التقييد الحازم لاستخدام أجهزة وسائط التخزين الخارجية والأمن المتعلق بها.
	إرشادات تطبيق الضوابط:

- العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية.
- العمل على تقييد استخدام أجهزة وسائط التخزين الخارجية، من خلال:
  - إنشاء مجموعات في نظام إدارة الصلاحيات على حسب الصلاحية بحيث يكون استخدام وسائط التخزين الخارجية غير مفعل على جميع أجهزة الموظفين وأنظمة الجهة والخوادم تلقائياً.
  - تحديد إجراءات موثقة لتقديم الموافقة على استخدام وسائط التخزين الخارجية (على سبيل المثال لا الحصر: طلب الموافقات عن طريق البريد الالكتروني، أو ورقياً، أو عن طريق نظام داخلي)، بحيث تحتوي على:
    - سبب طلب الموافقة على الاستخدام.
    - تاريخ بدء ونهاية الاستخدام.
    - آلية التعامل مع البيانات المخزنة في وسائط التخزين بحيث يتم فحصه قبل الاستخدام ومسح البيانات بعد الانتهاء.

المخرجات المتوقعة:

- وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية).
- تقرير أو إثبات يوضح تقييد استخدام أجهزة وسائط التخزين الخارجية (على سبيل المثال لا الحصر: لقطة شاشة أو دليل مباشر من نظام إدارة الصلاحيات توضح التقييد الحازم والمنع من استخدام أجهزة وسائط التخزين الخارجية على أجهزة المستخدمين والخوادم).
- إجراءات الموافقة على استخدام أجهزة وسائط التخزين لجزء من الأجهزة الموافق عليها.

٢-٣-٣-٣	إدارة حزم التحديثات والإصلاحات للأنظمة والتطبيقات والأجهزة (Patch Management).

إرشادات تطبيق الضوابط:

- العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية.
- العمل على تحديد إجراءات ادارة حزم التحديثات والاصلاحات للأنظمة والأجهزة والتطبيقات بحيث تحتوي على:
  - تحديد نطاق الأنظمة التي يتم تطبيق حزم التحديثات والإصلاحات فيها لتشمل:
    - أجهزة المستخدمين
    - نظم التشغيل
    - أجهزة الشبكة
    - قواعد البيانات
    - التطبيقات

	○ تحديد المدة الزمنية اللازمة لتطبيق حزم التحديثات والاصلاحات على حسب نوعية نظام التشغيل ومدى حساسية النظام والتحديثات والإصلاحات المطبقة عليها وأهمية التحديثات. ○ تضمين إجراءات حزم التحديثات والإصلاحات في منهجية إدارة التغيير أو تضمين إدارة التغيير في سياسة إدارة حزم التحديثات والإصلاحات. ○ تضمين موافقة إدارة التغيير من ضمن الموافقات في نموذج إجراء حزم التحديثات والاصلاحات على جميع نطاق الأنظمة والأجهزة والتطبيقات، على سبيل المثال لا الحصر: طلب الموافقات عن طريق البريد الالكتروني، أو ورقياً، أو عن طريق نظام داخلي. ○ تطبيق حزم التحديثات والإصلاحات على النطاق المحدد بعد الحصول على الموافقة اللازمة. ○ مراجعة تطبيق حزم التحديثات والإصلاحات باستمرار للتأكد من أن جميع التحديثات اللازمة تم تطبيقها على جميع نطاق الأجهزة والأنظمة والتطبيقات. ○ متابعة التحديثات والإصلاحات المطلوبة دورياً للتأكد من المستجدات من خلال، على سبيل المثال لا الحصر: نظام الحماية، نظام إدارة التحديثات والإصلاحات، تنبيهات الثغرات المرسلة عن طريق البريد الإلكتروني.
	المخرجات المتوقعة: • وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية). • إثبات يوضح تضمين ادارة التغيير في إجراءات حزم التحديثات والاصلاحات (على سبيل المثال لا الحصر: تضمين إجراءات حزم التحديثات والاصلاحات في منهجية ادارة التغيير، أو إلزام ادارة التغيير من خلال تضمينها في سياسة متطلبات ادارة حزم التحديثات والاصلاحات). • إجراءات الموافقة يوضح إلزام موافقة ادارة التغيير على حزم التحديثات. • تقارير أو إثبات يوضح شمول نطاق حزم التحديثات والإصلاحات جميع الأجهزة والأنظمة والتطبيقات. • تقارير أو إثبات أن حزم التحديثات والإصلاحات تتم حسب المدة المحددة في الإجراءات (على سبيل المثال لا الحصر: لقطة شاشة أو دليل مباشر يعرض التاريخ والنطاق لعدة عينات من إجراءات حزم التحديثات الموافق عليها عن طريق البريد الالكتروني أو النظام الداخلي أو ورقياً وتم التحديث بالانتهاء منها مسبقا بحيث تشمل جميع اجهزة وأنظمة وتطبيقات الجهة بشكل دوري).
٢-٣-٣-٤	مزامنة التوقيت (Clock Synchronization) مركزياً ومن مصدر دقيق وموثوق ، ومن هذه المصادر ما توفره الهيئة السعودية للمواصفات والمقاييس والجودة.
	إرشادات تطبيق الضوابط: • العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية. • العمل على مزامنة التوقيت (Clock Synchronization) من خلال خادم مركزي للجهة لبروتوكول وقت الشبكة (NTP). • ضبط توقيت الخادم المركزي ليتزامن مع، على سبيل المثال لا الحصر، أحد المصادر الموثوقة التالية:

	○ الهيئة السعودية للمواصفات والمقاييس والجودة (time.saso.gov.sa). ○ مدينة الملك عبدالعزيز للعلوم والتقنية (time.isu.net.sa).
	المخرجات المتوقعة: • وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية). • إثبات استخدام الجهة لخادم مركزي لمزامنة التوقيت (على سبيل المثال لا الحصر: لقطة شاشة أو دليل مباشر لوجود هذا الخادم في الشبكة مع وجود جميع التفاصيل الخاصة بالخادم) • إثبات استخدام مصدر دقيق وموثوق (على سبيل المثال لا الحصر: لقطة شاشة أو دليل مباشر لإعدادات هذا الخادم تثبت استخدام مصدر الهيئة السعودية للمواصفات والمقاييس والجودة أو غيره).
٢-٣-٤	يجب مراجعة متطلبات الأمن السيبراني لحماية الأنظمة وأجهزة معالجة المعلومات للجهة دورياً.
	إرشادات تطبيق الضوابط: • العمل على مراجعة متطلبات الأمن السيبراني لحماية الأنظمة وأجهزة معالجة المعلومات للجهة بشكل دوري حسب خطة موثقة ومعتمدة للمراجعة بناءً على فترة زمنية محددة (على سبيل المثال لا الحصر، يتم اجراء المراجعة الدورية بشكل سنوي). • العمل على توثيق المراجعة والتغييرات التي تمت على متطلبات الأمن السيبراني لحماية الأنظمة وأجهزة معالجة المعلومات للجهة واعتمادها من قبل رئيس الجهة أو من ينيبه.
	المخرجات المتوقعة: • وثيقة معتمدة تحدد جدول المراجعة لوثيقة المتطلبات. • إثبات يؤكد القيام بالمراجعة الدورية لمتطلبات الأمن لحماية الأنظمة وأجهزة معالجة المعلومات في الجهة. • موافقة رسمية من قبل رئيس الجهة أو من ينيبه على وثيقة المتطلبات المحدثة (مثال: عن طريق البريد الإلكتروني الرسمي للجهة، أو التوقيع الورقي أو الإلكتروني).

٢-٤	**حماية البريد الإلكتروني (Email Protection)**
الهدف	ضمان حماية البريد الإلكتروني للجهة من المخاطر السيبرانية.
الضوابط	
٢-٤-١	يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني لحماية البريد الإلكتروني للجهة.

	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة أمن البريد الإلكتروني **إرشادات تطبيق الضوابط:** • العمل على تطوير وتوثيق سياسة الأمن السيبراني لحماية البريد الإلكتروني في الجهة وقد تشمل الآتي: ○ متطلبات تقنيات وآليات الحماية الحديثة والمتقدمة وتوفيرها والتأكد من موثوقيتها. ○ متطلبات إعدادات تقنيات وآليات حماية البريد الإلكتروني للجهة. ○ متطلبات الأدوار والمسؤوليات للبريد الإلكتروني للحسابات العامة والمشتركة. ○ متطلبات حجم مرفقات البريد الإلكتروني الصادر والوارد، وسعة صندوق البريد لكل مستخدم. ○ متطلبات التصميم الآمن للبنية التحتية للبريد الإلكتروني. • العمل على أن تكون السياسة في الجهة مدعومة من قبل الإدارة التنفيذية. وذلك من خلال اعتماد وموافقة رئيس الجهة أو من ينيبه. **المخرجات المتوقعة:** • وثيقة سياسة ومعيار حماية البريد الإلكتروني المعتمدة من قبل الجهة (مثال: نسخة إلكترونية أو نسخة ورقية رسمية). • موافقة رسمية من قبل رئيس الجهة أو من ينيبه على السياسة (مثال: عن طريق البريد الإلكتروني الرسمي للجهة، أو التوقيع الورقي أو الإلكتروني).
٢-٤-٢	يجب تطبيق متطلبات الأمن السيبراني لحماية البريد الإلكتروني للجهة. **إرشادات تطبيق الضوابط:** • العمل على تطبيق كافة متطلبات الأمن السيبراني لحماية البريد الإلكتروني للجهة وقد تشمل الآتي: ○ تنفيذ متطلبات الأمن السيبراني المعتمدة لحماية البريد الإلكتروني للجهة وعلى سبيل المثال لا الحصر استخدام الجهة التقنيات المناسبة والمتقدمة لتحليل وتصفية رسائل البريد الالكتروني. ○ استخدام التقنيات المتقدمة لحماية البريد الالكتروني للجهة من رسائل التصيّد الإلكتروني والرسائل الاقتحامية على سبيل المثال لا الحصر وجود اشتراك رسمي و فعّال لدى مقدمي خدمة حماية البريد الإلكتروني. ○ يكون الدخول للبريد الإلكتروني عن طريق وسيط على سبيل المثال لا الحصر (Loadbalancer) **المخرجات المتوقعة:** • خطة عمل لتطبيق متطلبات الأمن السيبراني لحماية البريد الإلكتروني في الجهة. • تطبيق ضوابط حماية البريد الإلكتروني للجهة، على سبيل المثال لا الحصر:

		o استخدام الجهة تقنيات حديثة لحماية البريد الإلكتروني وتحليل وتصفية رسائل البريد الإلكتروني وحظر الرسائل المشبوهة، مثل الرسائل الاقتحامية (Spam Emails) ورسائل التصيّد الإلكتروني (Phishing Emails). o ضبط إعدادات برنامج مكافحة الفيروسات على خوادم البريد الإلكتروني لفحص جميع رسائل البريد الإلكتروني الواردة والصادرة. o توثيق مجال البريد الإلكتروني لـلجهة عن طريق استخدام الوسائل اللازمة؛ مثل طريقة إطار سياسة المرسل (Sender Policy Framework)، كما يجب التأكد من موثوقية مجالات رسائل البريد الواردة عن طريق التقنيات الحديثة مثل (Incoming message DMARC verification).
٢-٤-٣	يجب أن تغطي متطلبات الأمن السيبراني لحماية البريد الإلكتروني للجهة بحد أدنى ما يلي:	
	٢-٤-٣-١	تحليل وتصفية (Filtering) رسائل البريد الإلكتروني (وخصوصاً رسائل التصيّد الإلكتروني « Phishing Emails» والرسائل الاقتحامية «Spam Emails») باستخدام تقنيات وآليات الحماية الحديثة والمتقدمة للبريد الإلكتروني.
		إرشادات تطبيق الضوابط: • العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني لحماية البريد الإلكتروني للجهة، واعتمادها من قبل صاحب الصلاحية. • تحديد التقنيات المتقدمة وتوفيرها لاستخدام خواص تحليل وتصفية رسائل البريد الإلكتروني للجهة. • العمل على تفعيل خواص التحليل والتصفية في نظام حماية البريد الالكتروني من خلال لوحة التحكم. • مراجعة قائمة رسائل البريد الالكتروني المشبوهة كرسائل التصيد أو رسائل اقتحامية وغيرها بشكل دوري من خلال النظام من قبل الفريق المتخصص لمتابعة حماية البريد الالكتروني. • التأكد من اضافة مؤشرات الاختراق المستجدة الخاصة بالبريد الالكتروني في نظام الحماية بشكل مستمر.
		المخرجات المتوقعة: • وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية). • لقطة شاشة أو دليل مباشر تظهر وجود ما يثبت الاشتراك والاستخدام لتقنيات حديثة ومتقدمة لتحليل وتصفية رسائل البريد الإلكتروني في الجهة. • لقطة شاشة أو دليل مباشر من ضبط إعدادات البريد الإلكتروني بما يثبت وجود خاصية تحليل وتصفية رسائل البريد الإلكتروني وبما يشمل رسائل التصيّد الإلكتروني «Phishing Emails» والرسائل الاقتحامية « Spam Emails».
	٢-٤-٣-٢	التحقق من الهوية متعدد العناصر (Multi-Factor Authentication) للدخول عن بعد والدخول عن طريق صفحة موقع البريد الإلكتروني (Webmail).

إرشادات تطبيق الضوابط:

- العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني لحماية البريد الإلكتروني للجهة، واعتمادها من قبل صاحب الصلاحية.
- العمل على تفعيل خاصية التحقق من الهوية متعدد العناصر للدخول عن بعد والدخول عن طريق صفحة موقع البريد الإلكتروني للجهة من خلال، على سبيل المثال لا الحصر، أحد الطرق التالية:
  - استخدام الرسائل النصية المرتبطة بالرقم الخاص بمستخدم البريد الالكتروني.
  - التطبيقات المتقدمة والموثوقة للحصول على رمز التحقق من الهوية متعدد العناصر.
  - استخدام تطبيقات إدارة الأجهزة المحمولة للسماح بأجهزة المستخدمين (كعنصر آخر للدخول) على البريد الالكتروني للبروتوكلات التي لا تدعم (مثل بروتوكولات: EWS, outlook anywhere) الرسائل النصية او التطبيقات التي توفر رمز التحقق.

المخرجات المتوقعة:

- وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية).
- لقطة شاشة أو دليل مباشر من ضبط إعدادات البريد الإلكتروني بما يثبت تفعيل التحقق من الهوية متعدد العناصر للدخول عن طريق صفحة موقع البريد الإلكتروني للجهة.
- لقطة شاشة أو دليل مباشر يثبت استخدام التقنيات المتقدمة والموثوقة للتحقق من الهوية متعدد العناصر للدخول.

٢-٤-٣-٣	النسخ الاحتياطي والأرشفة للبريد الإلكتروني.

إرشادات تطبيق الضوابط:

- العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني لحماية البريد الإلكتروني للجهة، واعتمادها من قبل صاحب الصلاحية.
- تحديد التقنيات المتوافقة مع الأنظمة التقنية والبنية التحتية التقنية للجهة لعمل النسخ الاحتياطي والأرشفة للبريد الإلكتروني للجهة.
- تحديد مدة الاحتفاظ بالنسخ الاحتياطية والأرشفة للبريد الإلكتروني للجهة.
- العمل على القيام بالنسخ الاحتياطي على مستوى خوادم البريد الإلكتروني للجهة.
- العمل على تفعيل خاصية أرشفة جميع صناديق البريد الإلكتروني للجهة.

المخرجات المتوقعة:

- وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية).
- لقطة شاشة أو دليل مباشر يظهر وجود ما يثبت الاشتراك والاستخدام لتقنيات حديثة ومتقدمة لإجراء النسخ الاحتياطي والأرشفة للبريد الإلكتروني وبالسعة والمدة المعتمدة.
- تقارير النسخ الاحتياطي الخاصة بخوادم البريد الالكتروني للجهة.

• لقطة شاشة أو دليل مباشر يوضح تفعيل خاصية أرشفة صناديق البريد الالكتروني.	
٢-٤-٣-٤	الحماية من التهديدات المتقدمة المستمرة (APT Protection)، التي تستخدم عادة الفيروسات والبرمجيات الضارة غير المعروفة مسبقاً (Zero-Day Malware)، وإدارتها بشكل آمن.
إرشادات تطبيق الضوابط: • العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني لحماية البريد الإلكتروني للجهة، واعتمادها من قبل صاحب الصلاحية. • تحديد التقنيات المتقدمة وتوفيرها في الجهة والتي توفر حماية البريد الالكتروني من التهديدات المتقدمة المستمرة والبرمجيات الضارة غير المعروفة مسبقاً. • العمل على تفعيل خواص الحماية من التهديدات المتقدمة المستمرة والبرمجيات الضارة غير المعروفة مسبقاً في نظام حماية البريد الالكتروني. • مراجعة قائمة رسائل البريد الالكتروني المشبوهة التي تم تصفيتها من قبل النظام لاحتوائها على التهديدات المتقدمة المستمرة والبرمجيات الضارة غير المعروفة مسبقاً. • اتخاذ الإجراءات اللازمة لحماية جهاز مستقبل رسالة البريد الالكتروني المشبوهة في حال لم يتم حظرها من قبل نظام الحماية، والعمل على حظر العوامل ومؤشرات الاختراق التي تشير لتلك الشبهة.	
المخرجات المتوقعة: • وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية). • لقطة شاشة أو دليل مباشر تظهر وجود ما يثبت الاشتراك والاستخدام لتقنيات حديثة ومتقدمة لإجراء الحماية من التهديدات المتقدمة المستمرة للبريد الإلكتروني للجهة. • لقطة شاشة أو دليل مباشر توضح إعدادات البريد الإلكتروني للجهة وإظهار ما يثبت تفعيل خاصية الحماية من التهديدات المتقدمة المستمرة.	
٢-٤-٣-٥	توثيق مجال البريد الإلكتروني للجهة بالطرق التقنية، مثل طريقة إطار سياسة المرسل (Sender Policy Framework)
إرشادات تطبيق الضوابط: • العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني لحماية البريد الإلكتروني للجهة، واعتمادها من قبل صاحب الصلاحية. • إنشاء سجل إطار سياسة المرسل (SPF Record) يحتوي على الخوادم المصرح لها بإرسال البريد الالكتروني لحماية الجهة من خطر الانتحال (Spoofing).	

	○ إنشاء سجل البريد المعرف بمفاتيح النطاق (DKIM Record) والذي يقوم باستخدام التوقيع الرقمي في جميع رسائل البريد الالكتروني الصادرة من نطاق الجهة وذلك لضمان سلامة رسائل البريد الالكتروني (Integrity). ● إنشاء سجل سياسة مصادقة الرسائل والإبلاغ عنها (DMARC) والذي يستفيد من تقنيات مصادقة البريد الإلكتروني الحالية SPF و DKIM لحماية نطاقات البريد الالكتروني من هجمات الانتحال. ● العمل على التأكد من ربط نطاق البريد الالكتروني مع خدمة توثيق البريد الخاصة بمنصة حصين. **المخرجات المتوقعة:** ● وثائق توضح تحديد وتوثيق متطلبات هذا الضابط بسياسات أو إجراءات معتمدة من قبل صاحب الصلاحية. ● لقطة شاشة تظهر إعداد سجل سياسة المرسل (SPF Record) والذي يوضح الخوادم المصرح لها بإرسال البريد الالكتروني من نطاق الجهة.
٢-٤-٤	يجب مراجعة تطبيق متطلبات الأمن السيبراني الخاصة بحماية البريد الإلكتروني للجهة دورياً. **إرشادات تطبيق الضوابط:** ● العمل على مراجعة تطبيق متطلبات الأمن السيبراني لحماية البريد الإلكتروني للجهة من خلال إجراء تقييم دوري (وذلك حسب خطة موثقة ومعتمدة للمراجعة، وبناء على فترة زمنية محددة "على سبيل المثال، بشكل ربع سنوي") لتنفيذ إجراءات حماية البريد الإلكتروني للجهة من قبل الإدارة المعنية بالأمن السيبراني وبالتعاون مع الإدارات ذات العلاقة (كالإدارة المعنية بتقنية المعلومات). ● مراجعة التطبيق قد تتم من خلال القنوات التقليدية (مثل البريد الإلكتروني) أو قد يكون مؤتمت باستخدام نظام لإدارة الالتزام. الجهة قد تضع خطة مراجعة توضح فيها جدول مراجعة تطبيق متطلبات الأمن السيبراني لحماية البريد الإلكتروني للجهة. ● مراجعة وتحديث متطلبات الأمن السيبراني الخاصة بحماية البريد الإلكتروني للجهة بشكل دوري حسب خطة موثقة ومعتمدة للمراجعة بناءً على فترة زمنية محددة أو في حالة حدوث تغييرات في المتطلبات التشريعية والتنظيمية ذات العلاقة. ● توثيق المراجعة والتغييرات التي تتم على متطلبات الأمن السيبراني الخاصة بحماية البريد الإلكتروني للجهة واعتمادها من قبل رئيس الجهة أو من ينيبه. **المخرجات المتوقعة:** ● نتائج مراجعة تطبيق متطلبات الأمن السيبراني لحماية البريد الإلكتروني للجهة. ● وثيقة تحدد دورة مراجعة تطبيق متطلبات الأمن السيبراني لحماية البريد الإلكتروني للجهة (جدول تقييم الالتزام). ● وثيقة تقرير تقييم الالتزام توضح تقييم تطبيق متطلبات الأمن السيبراني لحماية البريد الإلكتروني للجهة ● 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. • 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).

٢-٥	إدارة أمن الشبكات (Networks Security Management)
الهدف	ضمان حماية شبكات الجهة من المخاطر السيبرانية.
الضوابط	
٢-٥-١	يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني لإدارة أمن شبكات الجهة.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة أمن الشبكات **إرشادات تطبيق الضوابط:** • العمل على تطوير وتوثيق سياسة الأمن السيبراني لإدارة أمن شبكات الجهة وقد تشمل الآتي: ○ متطلبات الوصول إلى الشبكة ○ متطلبات وصول الأطراف الخارجية إلى الشبكة ○ متطلبات حماية الشبكات ○ متطلبات الأمن المادي والبيئي لضمان حفظ أجهزة الشبكات في بيئة آمنة وملائمة • تحديد وتوثيق واعتماد معايير تقنية أمنية لجميع أجهزة الشبكة المستخدمة داخل الجهة • العمل على أن تكون السياسة في الجهة مدعومة من قبل الإدارة التنفيذية. وذلك من خلال اعتماد وموافقة رئيس الجهة أو من ينيبه.
	المخرجات المتوقعة: • وثيقة سياسة إدارة أمن شبكات المعتمدة من قبل الجهة (مثال: نسخة إلكترونية أو نسخة ورقية رسمية). • وثيقة سياسة الأمن السيبراني والذي يغطي متطلبات المعايير التقنية الأمنية لإدارة أمن شبكات الجهة (مثال: نسخة إلكترونية أو نسخة ورقية رسمية). • موافقة رسمية من قبل رئيس الجهة أو من ينيبه على السياسة والمعيار التقني (مثال: عن طريق البريد الإلكتروني الرسمي للجهة، أو التوقيع الورقي أو الإلكتروني).
٢-٥-٢	يجب تطبيق متطلبات الأمن السيبراني لإدارة أمن شبكات الجهة.

	إرشادات تطبيق الضوابط: • العمل على تطبيق كافة متطلبات الأمن السيبراني لإدارة أمن شبكات الجهة وقد تشمل الآتي: ○ ضمان العزل والتقسيم المادي أو المنطقي لأجزاء الشبكات للجهة ○ استخدام جدار الحماية (Firewall) لحماية شبكات الجهة ○ تطبيق مبدأ الدفاع الأمني متعدد المراحل (Defense-in-Depth) لتوفير حماية متقدمة وأكثر فعاليّة لأجهزة شبكات الجهة ○ عزل شبكة بيئة الإنتاج عن شبكات بيئات التطوير والاختبار في الجهة ○ ضمان أمن التصفح والاتصال بالإنترنت في الجهة بما يشمل ضبط إعدادات أجهزة الشبكة والتقييد الحازم للوصول للمواقع المشبوهة ○ حماية قناة تصفح الإنترنت من التهديدات المتقدمة المستمرة ○ ضمان أمن الشبكات اللاسلكية وحمايتها في الجهة ○ ضمان أمن قيود وإدارة منافذ وبروتوكولات وخدمات الشبكة في الجهة ○ استخدام أنظمة الحماية المتقدمة لاكتشاف ومنع الاختراقات في شبكات الجهة ○ ضمان أمن نظام أسماء النطاقات للجهة • إنشاء إجراءات محددة لضمان التنفيذ والتطبيق المستمر لمتطلبات الأمن السيبراني المعتمدة لإدارة أمن شبكات الجهة ووفقاً للمتطلبات التشريعية والتنظيمية ذات العلاقة.
	المخرجات المتوقعة: • خطة عمل لتطبيق متطلبات الأمن السيبراني لإدارة الأصول المعلوماتية والتقنية. • عينة توضح تطبيق ضوابط إدارة أمن شبكات الجهة، على سبيل المثال لا الحصر: ○ عينة توضح استخدام الجهة تقنيات حديثة لإدارة أمن شبكات الجهة اللازمة ووضع القيود وإدارة منافذ وبروتوكولات وخدمات الشبكة ○ عينة توضح ضبط إعدادات الشبكات بما يمنع ربط الأنظمة الحساسة بالشبكة اللاسلكية للجهة ○ عينة توضح تطبيق العزل المنطقي بين شبكة بيئة الإنتاج وشبكة بيئة الاختبار والشبكات الأخرى • عينة من الإجراءات المحددة والمعتمدة للتعامل مع أجهزة الشبكات والأنظمة الحساسة للجهة
٢-٥-٣	يجب أن تغطي متطلبات الأمن السيبراني لإدارة أمن شبكات الجهة بحد أدنى ما يلي:
٢-٥-٣-١	العزل والتقسيم المادي أو المنطقي لأجزاء الشبكات بشكل آمن، واللازم للسيطرة على مخاطر الأمن السيبراني ذات العلاقة، باستخدام جدار الحماية (Firewall) ومبدأ الدفاع الأمني متعدد المراحل (Defense-in-Depth)
	إرشادات تطبيق الضوابط: • العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني لإدارة أمن شبكات الجهة، واعتمادها من قبل صاحب الصلاحية.

- العمل على تحديد مناطق للشبكة بناءً على مستوى الثقة (trust level)، فعلى سبيل المثال، مستوى الثقة في المنطقة التي تتم من خلالها الاتصال بالإنترنت "متدني"، ومستوى الثقة في المنطقة المعزولة عن الإنترنت التي تستضيف قواعد البيانات "عالي"
- العمل على تحديد الإجراءات اللازمة لضمان العزل والتقسيم المادي أو المنطقي لأجزاء الشبكة في الجهة (على سبيل المثال لا الحصر إجراءات استخدام الشبكة الداخلية الافتراضية لعزل أجزاء الشبكة)
- تفعيل التقنيات المناسبة والمتقدمة للعزل والتقسيم المادي أو المنطقي لأجزاء الشبكات بشكل آمن وعلى سبيل المثال لا الحصر:
  - العزل باستخدام جدار الحماية (Firewall)
  - العزل للأنظمة التي يتم الوصول لها من خارج الجهة في منطقة محايدة (DMZ)
  - العزل لأجزاء الشبكة عن طريق الشبكة الداخلية الافتراضية (VLAN)
  - تطبيق مبدأ الدفاع الأمني متعدد المراحل (Defense-in-Depth)، والذي يشمل تطبيق ضوابط تقنية وضوابط إدارية للحماية.

المخرجات المتوقعة:

- وثيقة سياسة الأمن السيبراني التي تغطي متطلبات إدارة أمن الشبكات للجهة (مثال: نسخة إلكترونية أو نسخة ورقية رسمية).
- موافقة رسمية من قبل رئيس الجهة أو من ينيبه على السياسة (مثال: عن طريق البريد الإلكتروني الرسمي للجهة، أو التوقيع الورقي أو الإلكتروني).
- عينة توضح تطبيق المتطلبات المتعلقة بالعزل والتقسيم المادي أو المنطقي لأجزاء الشبكات بشكل آمن، على سبيل المثال لا الحصر:
  - دليل يوضح تطبيق متطلبات العزل والتقسيم المادي أو المنطقي لأجزاء الشبكات بشكل آمن والدفاع الأمني متعدد المراحل (مثال: لقطة شاشة تظهر وجود ما يثبت الاشتراك والاستخدام لتقنيات حديثة ومتقدمة لتطبيق العزل والتقسيم المادي أو المنطقي لأجزاء الشبكات بشكل آمن)
  - عينة توضح تطبيق متطلبات التقنيات المناسبة والمتقدمة للعزل والتقسيم المادي أو المنطقي لأجزاء الشبكات بشكل آمن والدفاع الأمني متعدد المراحل (مثال: لقطة شاشة توضح ما يثبت إجراء العزل والتقسيم المادي أو المنطقي لأجزاء الشبكات بشكل آمن وكذلك العرض والاطلاع على تخطيط ورسم البنية التحتية للشبكات(Network Diagram)

٢-٥-٣-٢	عزل شبكة بيئة الإنتاج عن شبكات بيئات التطوير والاختبار.

إرشادات تطبيق الضوابط:

- العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني لإدارة أمن شبكات الجهة، واعتمادها من قبل صاحب الصلاحية.
- القيام بالتقسيم المنطقي لنطاقات الشبكة بحيث توضح عناوين شبكات بيئة الإنتاج وشبكات بيئة التطوير والاختبار (مثال: باستخدام تقنيات VLANs).

- إعداد الشبكة لضمان عزل شبكات بيئة الإنتاج عن شبكات بيئة التطوير والاختبار عن طريق استخدام أنظمة جدار الحماية،
- توثيق التقسيمات المنطقية وتخطيط الشبكات (Network Diagram) لتوضيح عزل شبكات بيئة الإنتاج عن شبكات التطوير والاختبار.

المخرجات المتوقعة:

- وثيقة سياسة الأمن السيبراني التي تغطي جميع متطلبات إدارة أمن شبكات الجهة (مثال: نسخة إلكترونية أو نسخة ورقية رسمية).
- موافقة رسمية من قبل رئيس الجهة أو من ينيبه على هذه المتطلبات (مثال: عن طريق البريد الإلكتروني الرسمي للجهة، أو التوقيع الورقي أو الإلكتروني).
- قائمة عناوين الخوادم في بيئة الإنتاج وبيئة التطوير والاختبار.
- وثيقة محدثة توضح تخطيط الشبكات (Network Diagram) توضح التقسيمات المنطقية وتوضح العزل بين شبكة بيئة الإنتاج عن شبكات بيئات التطوير والاختبار.

٢-٥-٣-٣	أمن التصفح والاتصال بالإنترنت، ويشمل ذلك التقييد الحازم للمواقع الإلكترونية المشبوهة، ومواقع مشاركة وتخزين الملفات، ومواقع الدخول عن بعد.

إرشادات تطبيق الضوابط:

- العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني لإدارة أمن شبكات الجهة، واعتمادها من قبل صاحب الصلاحية.
- العمل على تحديد الإجراءات اللازمة لضمان أمن التصفح والاتصال بالإنترنت في الجهة، على سبيل المثال لا الحصر:
  - إجراءات التقييد الحازم للمواقع الالكترونية المشبوهة ومواقع مشاركة وتخزين الملفات، ومواقع الدخول عن بعد
  - ضبط إعدادات أنظمة جدار الحماية (Firewall) بحيث يكون الاتصال عن طريق استخدام موزع اتصالات الانترنت (Proxy) لتحليل وتصفية البيانات المنتقلة من وإلى الجهة.

المخرجات المتوقعة:

- وثيقة سياسة الأمن السيبراني التي تغطي جميع متطلبات إدارة أمن شبكات الجهة (مثال: نسخة إلكترونية أو نسخة ورقية رسمية).
- موافقة رسمية من قبل رئيس الجهة أو من ينيبه على هذه المتطلبات (مثال: عن طريق البريد الإلكتروني الرسمي للجهة، أو التوقيع الورقي أو الإلكتروني).
- عينة توضح تطبيق المتطلبات المتعلقة بأمن التصفح والاتصال بالإنترنت، على سبيل المثال لا الحصر:
  - عينة توضح تطبيق متطلبات أمن التصفح والاتصال بالإنترنت (مثال: لقطة شاشة تظهر وجود ما يثبت الاستخدام لتقنيات حديثة ومتقدمة لتطبيق أمن التصفح والاتصال بالإنترنت)

	○ عينة توضح تطبيق متطلبات التقنيات المناسبة والمتقدمة لأمن التصفح والاتصال بالإنترنت (مثال: لقطة شاشة توضح ما يثبت إجراء وضبط إعدادات الشبكة وأنظمة جدار الحماية للجهة لضمان أمن التصفح والاتصال بالإنترنت وما يثبت التقييد الحازم للمواقع الإلكترونية المشبوهة، ومواقع مشاركة وتخزين الملفات، ومواقع الدخول عن بعد)
٢-٥-٣-٤	أمن الشبكات اللاسلكية وحمايتها باستخدام وسائل آمنة للتحقق من الهوية والتشفير، وعدم ربط الشبكات اللاسلكية بشبكة الجهة الداخلية إلا بناءً على دراسة متكاملة للمخاطر المترتبة على ذلك والتعامل معها بما يضمن حماية الأصول التقنية للجهة.

أدوات الأمن السيبراني ذات العلاقة:

- نموذج معيار أمن الشبكات اللاسلكية.

إرشادات تطبيق الضوابط:

- العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني لإدارة أمن شبكات الجهة، واعتمادها من قبل صاحب الصلاحية.
- تطبيق متطلبات أمن الشبكات اللاسلكية في الجهة وقد تشمل الآتي:
  - التقنيات المناسبة والمتقدمة لأمن الشبكات اللاسلكية وحمايتها.
  - التحقق من اسم المستخدم وربط الاتصال بالشبكة اللاسلكية باسم المستخدم وذلك قبل منح المستخدم صلاحية الدخول على الشبكة اللاسلكية
  - فصل الشبكة الداخلية (LAN) عن الشبكة اللاسلكية وذلك بعزل الشبكتين عن بعضهما، كذلك عزل شبكة الزوار اللاسلكية عن الشبكة اللاسلكية للجهة.
- العمل على تشفير الاتصال اللاسلكي وذلك بضبط الإعدادات المتعلقة بأجهزة الشبكة اللاسلكية بما يدعم أعلى معايير التشفير وما يتوافق مع المتطلبات التشريعية والتنظيمية ذات العلاقة
- العمل على إجراء دراسة متكاملة للمخاطر المترتبة على ربط الشبكات اللاسلكية بشبكة الجهة الداخلية في حال كان هناك الحاجة لربطها، والتعامل معها بما يضمن حماية الأصول التقنية للجهة ويجب أن يكون هناك ما يثبت تحليل ودراسة المخاطر على سبيل المثال لا الحصر عمل تقرير متكامل ويشمل تحديد المخاطر وتصنيفها والملاحظات وخطة المعالجة (مثال: من خلال برنامج أتمتة متقدم أو سجل للمخاطر Excel sheet)

المخرجات المتوقعة:

- وثيقة معيار أمن الشبكات اللاسلكية (Wireless Security) المعتمدة من قبل الجهة (مثال: نسخة إلكترونية أو نسخة ورقية رسمية).
- عينة توضح تطبيق المتطلبات المتعلقة بأمن الشبكات اللاسلكية وحمايتها، على سبيل المثال لا الحصر:
  - عينة توضح تطبيق متطلبات أمن الشبكات اللاسلكية وحمايتها (مثال: لقطة شاشة تظهر وجود ما يثبت الاشتراك والاستخدام لتقنيات حديثة ومتقدمة لتطبيق أمن الشبكات اللاسلكية وحمايتها على سبيل المثال لا الحصر تشفير الاتصال عن طريق الشبكة اللاسلكية، كذلك إظهار ضبط الإعدادات لأجهزة الشبكة

وأنظمة جدار الحماية بما يتوافق مع التحقق من اسم المستخدم قبل منحه صلاحية الاتصال بالشبكة اللاسلكية للجهة)

- عينة توضح إجراء دراسة متكاملة للمخاطر المترتبة على ربط الشبكات اللاسلكية بشبكة الجهة الداخلية، في حال كان هناك حاجة لربطها، والتعامل معها بما يضمن حماية الأصول التقنية للجهة ويجب أن يكون هناك ما يثبت تحليل ودراسة المخاطر على سبيل المثال لا الحصر عمل تقرير متكامل ويشمل المخاطر وتصنيفها والملاحظات وخطة المعالجة من خلال برنامج أتمتة متقدم أو برنامج الاكسل Excel Sheet
- عينة توضح فصل الشبكة الداخلية (LAN) عن الشبكة اللاسلكية وذلك بعزل الشبكتين عن بعضهما، كذلك عزل شبكة الزوار اللاسلكية عن الشبكة اللاسلكية للجهة.

٢-٥-٣-٥	قيود وإدارة منافذ وبروتوكولات وخدمات الشبكة.

إرشادات تطبيق الضوابط:

- العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني لإدارة أمن شبكات الجهة، واعتمادها من قبل صاحب الصلاحية.
- تطبيق متطلبات قيود وإدارة منافذ وبروتوكولات وخدمات الشبكة في الجهة وقد تشمل الآتي:
  - التقنيات المناسبة والمتقدمة لقيود وإدارة منافذ وبروتوكولات وخدمات الشبكة.
  - إجراءات إدارة منافذ وبروتوكلات وخدمات الشبكة وصلاحيات الوصول.
- العمل على تقييد المنافذ والبروتوكولات الغير المستخدمة في الجهة على سبيل المثال لا الحصر:
  - التقييد عن طريق أنظمة جدار الحماية.
  - إغلاق المنافذ الغير المستخدمة بشكل فعلي.
- العمل على المراجعة الدورية لإعدادات أنظمة الحماية وتحديثها بشكل مستمر على سبيل المثال لا الحصر:
  - المراجعة الدورية بشكل سنوي على الأقل.
  - وضع جميع الضوابط التقنية والمعايير التي يتم مراجعتها والتأكد منها حول إعدادات أنظمة الحماية ضمن برنامج أتمتة متقدم أو من خلال برنامج الاكسل Excel Sheet ومتابعتها وتحديثها إن تطلب الأمر وذلك بعد الحصول على الموافقة المسبقة من قبل صاحب الصلاحية.
  - العمل على إنشاء إجراءات الموافقة لتحديث قواعد وإعدادات أنظمة الحماية (Firewall Rules) بما يضمن عدم إجراء أي تحديث أو تغيير عليها إلا بعد الحصول على الموافقة من صاحب الصلاحية.

المخرجات المتوقعة:

- وثيقة سياسة الأمن السيبراني التي تغطي جميع متطلبات إدارة أمن شبكات الجهة (مثال: نسخة إلكترونية أو نسخة ورقية رسمية).
- موافقة رسمية من قبل رئيس الجهة أو من ينيبه على هذه المتطلبات (مثال: عن طريق البريد الإلكتروني الرسمي للجهة، أو التوقيع الورقي أو الإلكتروني).
- عينة توضح تطبيق المتطلبات المتعلقة بقيود وإدارة منافذ وبروتوكولات وخدمات الشبكة، على سبيل المثال لا الحصر:

	o عينة توضح تطبيق متطلبات قيود وإدارة منافذ وبروتوكولات وخدمات الشبكة (مثال: لقطة شاشة تظهر وجود ما يثبت الاشتراك والاستخدام لتقنيات حديثة ومتقدمة لتطبيق قيود وإدارة منافذ وبروتوكولات وخدمات الشبكة عن طريق نظام جدار الحماية) o عينة توضح المراجعة الدورية لإعدادات أنظمة الحماية وتحديثها بشكل مستمر على سبيل المثال لا الحصر المراجعة الدورية بشكل سنوي على الأقل ووضع جميع الضوابط التقنية والمعايير التي يتم مراجعتها والتأكد منها حول إعدادات أنظمة الحماية ضمن برنامج أتمتة متقدم أو من خلال برنامج الاكسل Excel Sheet، وكذلك دعم المراجعة بالحصول على الموافقة المسبقة للمراجعة والتحديث للإعدادات إن تطلب الأمر ذلك o عينة تظهر وجود نموذج إجراءات الموافقة لتحديث قواعد وإعدادات أنظمة الحماية (Firewall Rules) بما يضمن عدم إجراء أي تحديث أو تغيير عليها إلا بعد الحصول على الموافقة من صاحب الصلاحية، كذلك عينة توضح ما سبق وأن تم تحديثه على قواعد وإعدادات أنظمة الحماية (Firewall Rules)
٢-٥-٣-٦	أنظمة الحماية المتقدمة لاكتشاف ومنع الاختراقات (Intrusion Prevention Systems)
	إرشادات تطبيق الضوابط: ● العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني لإدارة أمن شبكات الجهة، واعتمادها من قبل صاحب الصلاحية. ● تطبيق متطلبات أنظمة الحماية المتقدمة لاكتشاف ومنع الاختراقات في الجهة وقد تشمل الآتي: ○ أنظمة الحماية المتقدمة لاكتشاف ومنع الاختراقات ○ التقنيات المناسبة والمتقدمة لأنظمة الحماية المتقدمة لاكتشاف ومنع الاختراقات ● العمل على حماية الجهة وذلك باستخدام أنظمة الحماية المتقدمة (IPS/IDS) بحيث تغطي جميع أجهزة البنية التحتية للجهة وبما يشمل: ○ الشبكة الداخلية ○ والمنطقة المحايدة للجهة (DMZ)، ○ والشبكة اللاسلكية للجهة ● العمل على المراجعة الدورية لإعدادات أنظمة الحماية المتقدمة (IPS/IDS) ووضع جميع الضوابط التقنية والمعايير التي يتم مراجعتها والتأكد منها حول إعدادات أنظمة الحماية المتقدمة (IPS/IDS) ضمن برنامج أتمتة متقدم أو من خلال برنامج الاكسل Excel Sheet ومتابعتها وتحديثها إن تطلب الأمر وذلك بعد الحصول على الموافقة المسبقة من قبل صاحب الصلاحية
	المخرجات المتوقعة: ● وثيقة سياسة الأمن السيبراني التي تغطي جميع متطلبات إدارة أمن شبكات الجهة (مثال: نسخة إلكترونية أو نسخة ورقية رسمية). ● موافقة رسمية من قبل رئيس الجهة أو من ينيبه على هذه المتطلبات (مثال: عن طريق البريد الإلكتروني الرسمي للجهة، أو التوقيع الورقي أو الإلكتروني).

		• عينة توضح تطبيق المتطلبات المتعلقة بأنظمة الحماية المتقدمة لاكتشاف ومنع الاختراقات، على سبيل المثال لا الحصر: o عينة توضح تطبيق متطلبات أنظمة الحماية المتقدمة لاكتشاف ومنع الاختراقات (مثال: لقطة شاشة تظهر وجود ما يثبت الاشتراك والاستخدام لتقنيات حديثة ومتقدمة لتطبيق أنظمة الحماية المتقدمة لاكتشاف ومنع الاختراقات، كذلك الاطلاع على البنية التحتية التقنية وإظهار ما يثبت استخدام أنظمة الحماية المتقدمة (IPS/IDS) وشمولية جميع أصول الجهة المعلوماتية والتقنية ضمن أنظمة الحماية المتقدمة) o تقرير المراجعة الدورية لإعدادات أنظمة الحماية المتقدمة (IPS/IDS) ووضع جميع الضوابط التقنية والمعايير التي يتم مراجعتها والتأكد منها حول إعدادات أنظمة الحماية المتقدمة (IPS/IDS) ضمن برنامج أتمتة متقدم أو من خلال برنامج الاكسل Excel Sheet، وكذلك دعم المراجعة بالحصول على الموافقة المسبقة للمراجعة والتحديث للإعدادات إن تطلب الأمر ذلك
	٢-٥-٣-٧	أمن نظام أسماء النطاقات (DNS).
		إرشادات تطبيق الضوابط: • العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني لإدارة أمن شبكات الجهة، واعتمادها من قبل صاحب الصلاحية. • استخدام أنظمة أو خدمات أمن نظام أسماء النطاقات (DNS Security أو DNS Firewall) والتي تهدف إلى حماية أنظمة الجهة من هجمات حقن نظام أسماء النطاقات (DNS Poisoning) واستخدام خدمات أسماء النطاقات موثقة. • عدم استخدام خدمات أسماء النطاقات العامة مثل (Google DNS) أو أسماء النطاقات الخاصة بمزودي الخدمات.
		المخرجات المتوقعة: • وثيقة سياسة الأمن السيبراني التي تغطي جميع متطلبات إدارة أمن شبكات الجهة (مثال: نسخة إلكترونية أو نسخة ورقية رسمية). • موافقة رسمية من قبل رئيس الجهة أو من ينيبه على هذه المتطلبات (مثال: عن طريق البريد الإلكتروني الرسمي للجهة، أو التوقيع الورقي أو الإلكتروني). • لقطة شاشة تظهر إعدادات أسماء النطاقات في الجهة (DNS) والتي تشير إلى استخدام عنوان موثق لخدمات أسماء النطاقات. • لقطة شاشة توضح إعدادات نظام أمن أسماء النطاقات في الجهة (DNS Security) والتي تشير إلى حماية نطاق عناوين الجهة (IP range)
	٢-٥-٣-٨	حماية قناة تصفح الإنترنت من التهديدات المتقدمة المستمرة (APT Protection) التي تستخدم عادة الفيروسات والبرمجيات الضارة غير المعروفة مسبقاً (Zero-Day Malware) وإدارتها بشكل آمن.

	إرشادات تطبيق الضوابط: • العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني لإدارة أمن شبكات الجهة، واعتمادها من قبل صاحب الصلاحية. • تطبيق متطلبات حماية قناة تصفح الإنترنت من التهديدات المتقدمة المستمرة في الجهة وقد تشمل الآتي: ○ حماية قناة تصفح الإنترنت من التهديدات المتقدمة المستمرة. ○ التقنيات المناسبة والمتقدمة لحماية قناة تصفح الإنترنت من التهديدات المتقدمة المستمرة، والتأكد من فعالية تلك التقنيات. • حماية قناة تصفح الإنترنت من التهديدات المتقدمة المستمرة (APT) وذلك باستخدام الأنظمة والتقنيات المتقدمة للحماية من خطر الفيروسات والبرمجيات الضارة غير المعروفة مسبقاً (Zero-Day Malware) على سبيل المثال لا الحصر الاشتراك مع أحد مقدمي خدمات حماية قناة تصفح الإنترنت من التهديدات المتقدمة المستمرة (APT Protection) وإدارتها بشكل آمن
	المخرجات المتوقعة: • وثيقة سياسة الأمن السيبراني التي تغطي جميع متطلبات إدارة أمن شبكات الجهة (مثال: نسخة إلكترونية أو نسخة ورقية رسمية). • موافقة رسمية من قبل رئيس الجهة أو من ينيبه على هذه المتطلبات (مثال: عن طريق البريد الإلكتروني الرسمي للجهة، أو التوقيع الورقي أو الإلكتروني). • عينة توضح تطبيق المتطلبات المتعلقة بحماية قناة تصفح الإنترنت من التهديدات المتقدمة المستمرة، على سبيل المثال لا الحصر: ○ عينة توضح تطبيق متطلبات حماية قناة تصفح الإنترنت من التهديدات المتقدمة المستمرة (مثال: لقطة شاشة تظهر وجود ما يثبت الاشتراك والاستخدام لتقنيات حديثة ومتقدمة لتطبيق حماية قناة تصفح الإنترنت من التهديدات المتقدمة المستمرة وما يثبت بوجود خاصية (APT Protection) التي تستخدم عادة الفيروسات والبرمجيات الضارة غير المعروفة مسبقاً (Zero-Day Malware))
٤-٥-٢	يجب مراجعة تطبيق متطلبات الأمن السيبراني لإدارة أمن شبكات الجهة دورياً.
	إرشادات تطبيق الضوابط: • العمل على مراجعة تطبيق متطلبات الأمن السيبراني لإدارة أمن شبكات الجهة من خلال إجراء تقييم دوري (وذلك حسب خطة موثقة ومعتمدة للمراجعة، وبناء على فترة زمنية محددة "على سبيل المثال، بشكل ربع سنوي") لتنفيذ إجراءات إدارة أمن شبكات الجهة من قبل الإدارة المعنية بالأمن السيبراني وبالتعاون مع الإدارات ذات العلاقة (كالإدارة المعنية بتقنية المعلومات). • مراجعة التطبيق قد تتم من خلال القنوات التقليدية (مثل البريد الإلكتروني) أو قد يكون مؤتمت باستخدام نظام لإدارة الالتزام. الجهة قد تضع خطة مراجعة توضح فيها جدول مراجعة تطبيق متطلبات الأمن السيبراني لإدارة أمن شبكات الجهة.

	• مراجعة وتحديث متطلبات الأمن السيبراني الخاصة بإدارة أمن شبكات الجهة بشكل دوري حسب خطة موثقة ومعتمدة للمراجعة بناءً على فترة زمنية محددة أو في حالة حدوث تغييرات في المتطلبات التشريعية والتنظيمية ذات العلاقة. • توثيق المراجعة والتغييرات التي تتم على متطلبات الأمن السيبراني الخاصة بإدارة أمن شبكات الجهة واعتمادها من قبل رئيس الجهة أو من ينيبه.
	المخرجات المتوقعة: • نتائج مراجعة تطبيق متطلبات الأمن السيبراني لإدارة أمن شبكات الجهة. • وثيقة معتمدة تحدد دورة مراجعة تطبيق متطلبات الأمن السيبراني لإدارة أمن شبكات الجهة (جدول تقييم الالتزام). • وثيقة تقرير تقييم الالتزام توضح تقييم تطبيق متطلبات الأمن السيبراني لإدارة أمن شبكات الجهة. • 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. • 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).

٦-٢	أمن الأجهزة المحمولة (Mobile Devices Security)
الهدف	ضمان حماية أجهزة الجهة المحمولة (بما في ذلك أجهزة الحاسب المحمول والهواتف الذكية والأجهزة الذكية اللوحية) من المخاطر السيبرانية. وضمان التعامل بشكل آمن مع المعلومات الحساسة والمعلومات الخاصة بأعمال الجهة وحمايتها أثناء النقل والتخزين عند استخدام الأجهزة الشخصية للعاملين في الجهة (مبدأ «BYOD»).
الضوابط	
١-٦-٢	يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني الخاصة بأمن الأجهزة المحمولة والأجهزة الشخصية للعاملين (BYOD) عند ارتباطها بشبكة الجهة.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة أمن أجهزة المستخدمين والأجهزة المحمولة والأجهزة الشخصية **إرشادات تطبيق الضوابط:** • العمل على تطوير وتوثيق سياسة الأمن السيبراني لأمن الأجهزة المحمولة والأجهزة الشخصية للعاملين (BYOD) وقد تشمل الآتي: ○ متطلبات الأمن السيبراني لأمن الأجهزة المحمولة

	○ متطلبات الأمن السيبراني لأمن الأجهزة الشخصية (BYOD) ● العمل على أن تكون السياسة في الجهة مدعومة من قبل الإدارة التنفيذية. وذلك من خلال اعتماد وموافقة رئيس الجهة أو من ينيبه.
	المخرجات المتوقعة: ● وثيقة سياسة ومعيار أمن الأجهزة المحمولة والأجهزة الشخصية للعاملين (BYOD) المعتمدة في الجهة (مثال: نسخة إلكترونية أو نسخة ورقية رسمية). ● موافقة رسمية من قبل رئيس الجهة أو من ينيبه على السياسة والمعيار التقني (مثال: عن طريق البريد الإلكتروني الرسمي للجهة، أو التوقيع الورقي أو الإلكتروني).
٢-٦-٢	يجب تطبيق متطلبات الأمن السيبراني الخاصة بأمن الأجهزة المحمولة وأجهزة (BYOD) للجهة.
	إرشادات تطبيق الضوابط: ● العمل على تطبيق كافة متطلبات الأمن السيبراني الخاصة بأمن الأجهزة المحمولة وأجهزة (BYOD) للجهة وقد تشمل الآتي: ○ ضمان عزل وفصل وتشفير البيانات والمعلومات الخاصة بالجهة المخزنة على الأجهزة المحمولة وأجهزة (BYOD) عن بقية المعلومات والبيانات على الجهاز. ○ ضمان الاستخدام المحدد والمقيد بناءً على ما تتطلبه مصلحة أعمال الجهة. ○ ضمان عدم منح العاملين صلاحيات هامة وحساسة (Privileged Access) على أجهزة المستخدمين والأجهزة المحمولة، ويجب منح الصلاحيات وفقاً لمبدأ الحد الأدنى من الصلاحيات والامتيازات. ○ ضمان تشفير وسائط التخزين الخاصة بأجهزة المستخدمين والأجهزة المحمولة الهامة والحساسة والتي لها صلاحيات متقدمة. ○ ضمان حذف البيانات والمعلومات الخاصة بالجهة المخزنة على الأجهزة المحمولة وأجهزة (BYOD) عند فقدان الأجهزة أو بعد انتهاء/إنهاء العلاقة الوظيفية مع الجهة. ○ ضمان تفعيل إمكانية المسح عن بعد (Remote Wipe) على جميع الأجهزة المحمولة التي تخزن او تعالج معلومات الجهة المصنفة. ○ العمل على تنفيذ سياسات النطاق المناسبة (Group Policy) في الجهة وتطبيقها على جميع أجهزة المستخدمين والأجهزة المحمولة لضمان الالتزام بالضوابط التنظيمية والأمنية ○ العمل على تقديم التوعية الأمنية للمستخدمين. ○ العمل على إدارة أجهزة المستخدمين والأجهزة المحمولة مركزياً على سبيل المثال لا الحصر من خلال خادم الدليل النشط (Active Directory) أو عن طريق نظام إداري مركزي ○ العمل على تطبيق ضوابط الإعدادات والتحصين (Configuration and Hardening) لأجهزة المستخدمين والأجهزة المحمولة وفقاً لمعايير الأمن السيبراني. ○ العمل على إنشاء إجراءات محددة لضمان تنفيذ وتطبيق متطلبات الأمن السيبراني المعتمدة لإدارة الأجهزة المحمولة وأجهزة (BYOD) ووفقاً للمتطلبات التشريعية والتنظيمية ذات العلاقة.

	المخرجات المتوقعة: • خطة عمل لتطبيق متطلبات الأمن السيبراني لإدارة أمن الأجهزة المحمولة والأجهزة الشخصية للعاملين (BYOD). • عينة توضح تطبيق ضوابط أمن الأجهزة المحمولة والأجهزة الشخصية للعاملين (BYOD) في الجهة، على سبيل المثال لا الحصر: o عينة توضح استخدام الجهة تقنيات متقدمة لأمن الأجهزة المحمولة والأجهزة الشخصية للعاملين (BYOD) في الجهة (مثال: وجود التقنيات المتقدمة واللازمة لفصل وتشفير البيانات والمعلومات الخاصة بالجهة المخزنة على الأجهزة المحمولة وأجهزة (BYOD)). o عينة توضح إدارة أجهزة المستخدمين والأجهزة المحمولة مركزياً على سبيل المثال لا الحصر لقطة شاشة من خادم الدليل النشط (Active Directory)، كذلك الاطلاع على ضبط الإعدادات o الإجراءات المحددة والمعتمدة للتعامل الأجهزة المحمولة والأجهزة الشخصية للعاملين (BYOD) في الجهة.
٢-٦-٣	يجب أن تغطي متطلبات الأمن السيبراني الخاصة بأمن الأجهزة المحمولة وأجهزة (BYOD) للجهة بحد أدنى ما يلي:
٢-٦-٣-١	فصل وتشفير البيانات والمعلومات (الخاصة بالجهة) المخزنة على الأجهزة المحمولة وأجهزة (BYOD)
	إرشادات تطبيق الضوابط: • العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني لإدارة أمن الأجهزة المحمولة والأجهزة الشخصية للعاملين (BYOD)، واعتمادها من قبل صاحب الصلاحية. • العمل على تطبيق متطلبات فصل وتشفير البيانات والمعلومات الخاصة بالجهة والمخزنة على الأجهزة المحمولة وأجهزة (BYOD) في الجهة وقد تشمل الآتي: o فصل وتشفير البيانات والمعلومات. o التقنيات المناسبة والمتقدمة لفصل وتشفير البيانات والمعلومات. • العمل على استخدام التقنيات اللازمة (مثل Mobile Device Management) لتشفير البيانات والمعلومات الخاصة بالجهة المخزنة على الأجهزة المحمولة وأجهزة (BYOD).
	المخرجات المتوقعة: • وثيقة سياسة الأمن السيبراني التي تغطي جميع متطلبات أمن الأجهزة المحمولة والأجهزة الشخصية للعاملين (BYOD) في الجهة (مثال: نسخة إلكترونية أو نسخة ورقية رسمية).ن • موافقة رسمية من قبل رئيس الجهة أو من ينيبه على هذه المتطلبات (مثال: عن طريق البريد الإلكتروني الرسمي للجهة، أو التوقيع الورقي أو الإلكتروني). • عينة توضح تطبيق المتطلبات المتعلقة بأمن الأجهزة المحمولة والأجهزة الشخصية للعاملين (BYOD) في الجهة، على سبيل المثال لا الحصر:

	○ عينة توضح تطبيق متطلبات التقنيات المناسبة والمتقدمة لأمن الأجهزة المحمولة والأجهزة الشخصية للعاملين (BYOD) (مثال: لقطة شاشة توضح استخدام أنظمة متقدمة لتوفير وضمان تشفير البيانات على الأجهزة المحمولة والأجهزة الشخصية للعاملين (BYOD) في الجهة). ○ الإجراءات المحددة والمعتمدة لتشفير البيانات والمعلومات الخاصة بالجهة المخزنة على الأجهزة المحمولة وأجهزة (BYOD).
٢-٦-٣-٢	الاستخدام المحدد والمقيد بناءً على ما تتطلبه مصلحة أعمال الجهة.
	إرشادات تطبيق الضوابط: ● العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني لإدارة أمن الأجهزة المحمولة والأجهزة الشخصية للعاملين (BYOD)، واعتمادها من قبل صاحب الصلاحية. ● العمل على تطبيق متطلبات الاستخدام المحدد والمقيد بناءً على ما تتطلبه مصلحة أعمال الجهة وقد تشمل الآتي: ○ الاستخدام المحدد والمقيد بناءً على ما تتطلبه مصلحة أعمال الجهة. ○ التقنيات المناسبة والمتقدمة لـ لاستخدام المحدد والمقيد بناءً على ما تتطلبه مصلحة أعمال الجهة. ● العمل على تطوير الإجراءات اللازمة لتقييد استخدام الأجهزة المحمولة وربطها بشبكتها بناءً على ما تتطلبه مصلحة العمل. ● العمل على تقييم إعدادات الأجهزة المحمولة والضوابط الأمنية على سبيل المثال لا الحصر تطبيق حزم التحديثات والاصلاحات وتحديثات مكافح الفيروسات (Patches, AV) قبل ربطها على النطاق أو الشبكة الجهة.
	المخرجات المتوقعة: ● وثيقة سياسة الأمن السيبراني التي تغطي جميع متطلبات أمن الأجهزة المحمولة والأجهزة الشخصية للعاملين (BYOD) في الجهة (مثال: نسخة إلكترونية أو نسخة ورقية رسمية). ● موافقة رسمية من قبل رئيس الجهة أو من ينيبه على هذه المتطلبات (مثال: عن طريق البريد الإلكتروني الرسمي للجهة، أو التوقيع الورقي أو الإلكتروني). ● عينة توضح تطبيق المتطلبات المتعلقة بالاستخدام المحدد والمقيد بناءً على ما تتطلبه مصلحة أعمال الجهة، على سبيل المثال لا الحصر: ○ عينة توضح تطبيق متطلبات الاستخدام المحدد والمقيد بناءً على ما تتطلبه مصلحة أعمال الجهة (مثال: لقطة شاشة تظهر وجود ما يثبت عمل الإجراءات اللازمة لتقييد استخدام الأجهزة المحمولة وربطها بشبكتها بناءً على ما تتطلبه مصلحة العمل). ○ الإجراءات المحددة والمعتمدة لتقييد استخدام الأجهزة المحمولة (مثال: نموذج من الإجراءات، كذلك عينة من تقرير يوضح ما يثبت ضمان تقييم إعدادات الجهاز المحمول والضوابط الأمنية ومنها تطبيق حزم التحديثات وتحديثات مكافح الفيروسات قبل ربطه على الشبكة) .

٢-٦-٣-٣	حذف البيانات والمعلومات (الخاصة بالجهة) المخزنة على الأجهزة المحمولة وأجهزة (BYOD) عند فقدان الأجهزة أو بعد انتهاء/إنهاء العلاقة الوظيفية مع الجهة.

إرشادات تطبيق الضوابط:

- العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني لإدارة أمن الأجهزة المحمولة والأجهزة الشخصية للعاملين (BYOD)، واعتمادها من قبل صاحب الصلاحية.
- العمل على تطبيق متطلبات حذف البيانات والمعلومات الخاصة بالجهة والمخزنة على الأجهزة المحمولة وأجهزة (BYOD) وذلك عند فقدان الأجهزة أو بعد انتهاء/إنهاء العلاقة الوظيفية مع الجهة.
- العمل على استخدام التقنيات اللازمة (مثل Mobile Device Management) لضمان حذف البيانات والمعلومات الخاصة الحساسة بالجهة وذلك عند فقدان الأجهزة، وبعد انتهاء/انهاء العلاقة الوظيفية مع الجهة.

المخرجات المتوقعة:

- وثيقة سياسة الأمن السيبراني التي تغطي جميع متطلبات أمن الأجهزة المحمولة والأجهزة الشخصية للعاملين (BYOD) في الجهة (مثال: نسخة إلكترونية أو نسخة ورقية رسمية).
- موافقة رسمية من قبل رئيس الجهة أو من ينيبه على هذه المتطلبات (مثال: عن طريق البريد الإلكتروني الرسمي للجهة، أو التوقيع الورقي أو الإلكتروني).
- عينة توضح تطبيق المتطلبات المتعلقة بحذف البيانات والمعلومات الخاصة بالجهة المخزنة على الأجهزة المحمولة وأجهزة (BYOD)، على سبيل المثال لا الحصر:
  - عينة توضح تطبيق متطلبات حذف البيانات والمعلومات الخاصة بالجهة المخزنة على الأجهزة المحمولة وأجهزة (BYOD) (مثال: لقطة شاشة تظهر وجود ما يثبت عمل اللازم لحذف البيانات والمعلومات (الخاصة بالجهة) المخزنة على الأجهزة المحمولة والأجهزة الشخصية وذلك عند فقدانها على سبيل المثال الاشتراك مع أحد مقدمي خدمة حذف البيانات والإدارة المتكاملة الآمنة للأجهزة المحمولة وأجهزة (BYOD)).
  - عينة من نموذج الإجراءات المتبعة توضح ما يثبت ضمان حذف البيانات والمعلومات الخاصة بالجهة المخزنة على الأجهزة المحمولة والأجهزة الشخصية وذلك عند فقدانها أو بعد انتهاء/انهاء العلاقة الوظيفية مع الجهة.

٢-٦-٣-٤	التوعية الأمنية للمستخدمين.

إرشادات تطبيق الضوابط:

- العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني لإدارة أمن الأجهزة المحمولة والأجهزة الشخصية للعاملين (BYOD)، واعتمادها من قبل صاحب الصلاحية.
- العمل على تطبيق متطلبات التوعية الأمنية للمستخدمين وقد تشمل الآتي:
  - تقديم التوعية الأمنية للمستخدمين.

	○ التقنيات المناسبة والمتقدمة لتقديم التوعية الأمنية للمستخدمين. ● العمل على تنفيذ متطلبات هذا الضابط وذلك بتقديم التوعية الأمنية للمستخدمين حول الأجهزة المحمولة وأجهزة (BYOD) وبشكل دوري.
	المخرجات المتوقعة: ● وثيقة سياسة الأمن السيبراني التي تغطي جميع متطلبات أمن الأجهزة المحمولة والأجهزة الشخصية للعاملين (BYOD) في الجهة (مثال: نسخة إلكترونية أو نسخة ورقية رسمية). ● موافقة رسمية من قبل رئيس الجهة أو من ينيبه على هذه المتطلبات (مثال: عن طريق البريد الإلكتروني الرسمي للجهة، أو التوقيع الورقي أو الإلكتروني). ● عينة توضح تطبيق المتطلبات المتعلقة بالتوعية الأمنية للمستخدمين، على سبيل المثال لا الحصر: ○ عينة توضح تطبيق متطلبات التوعية الأمنية للمستخدمين (مثال: عرض تقديمي يوضح تقديم توعية أمنية للعاملين في الجهة بخصوص الاستخدام الأمثل والآمن للأجهزة المحمولة وأجهزة (BYOD) أو لقطة شاشة على شاشة الأجهزة المحمولة كظهور شاشة التوقف معها رسالة توعوية)
٢-٦-٤	يجب مراجعة تطبيق متطلبات الأمن السيبراني الخاصة لأمن الأجهزة المحمولة وأجهزة (BYOD) للجهة دورياً.
	إرشادات تطبيق الضوابط: ● العمل على مراجعة تطبيق متطلبات الأمن السيبراني لأمن الأجهزة المحمولة وأجهزة (BYOD) للجهة من خلال إجراء تقييم دوري (وذلك حسب خطة موثقة ومعتمدة للمراجعة، وبناء على فترة زمنية محددة "على سبيل المثال، بشكل ربع سنوي") لتنفيذ إجراءات أمن الأجهزة المحمولة وأجهزة (BYOD) للجهة من قبل الإدارة المعنية بالأمن السيبراني وبالتعاون مع الإدارات ذات العلاقة (كالإدارة المعنية بتقنية المعلومات). ● مراجعة التطبيق قد تتم من خلال القنوات التقليدية (مثل البريد الإلكتروني) أو قد يكون مؤتمت باستخدام نظام لإدارة الالتزام. الجهة قد تضع خطة مراجعة توضح فيها جدول مراجعة تطبيق متطلبات الأمن السيبراني لأمن الأجهزة المحمولة وأجهزة (BYOD). ● مراجعة وتحديث متطلبات الأمن السيبراني الخاصة بأمن الأجهزة المحمولة وأجهزة (BYOD) في الجهة بشكل دوري حسب خطة موثقة ومعتمدة للمراجعة بناءً على فترة زمنية محددة أو في حالة حدوث تغييرات في المتطلبات التشريعية والتنظيمية ذات العلاقة. ● توثيق المراجعة والتغييرات التي تتم على متطلبات الأمن السيبراني الخاصة بأمن الأجهزة المحمولة وأجهزة (BYOD) للجهة واعتمادها من قبل رئيس الجهة أو من ينيبه.
	المخرجات المتوقعة: ● نتائج مراجعة تطبيق متطلبات الأمن السيبراني لأمن الأجهزة المحمولة وأجهزة (BYOD) في الجهة. ● وثيقة تحدد دورة مراجعة تطبيق متطلبات الأمن السيبراني لأمن الأجهزة المحمولة وأجهزة (BYOD) (جدول تقييم الالتزام).

	• وثيقة تقرير تقييم الالتزام توضح تقييم تطبيق متطلبات الأمن السيبراني لأمن الأجهزة المحمولة وأجهزة (BYOD). • 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. • 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).

٢-٧	حماية البيانات والمعلومات (Data and Information Protection)
الهدف	ضمان حماية السرية وسلامة بيانات ومعلومات الجهة ودقتها وتوافرها، وذلك وفقاً للسياسات والإجراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية ذات العلاقة.
الضوابط	
١-٧-٢	يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني لحماية بيانات ومعلومات الجهة، والتعامل معها وفقاً للمتطلبات التشريعية والتنظيمية ذات العلاقة.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة أمن البيانات **إرشادات تطبيق الضوابط:** • العمل على تضمين وتوثيق متطلبات الأمن السيبراني لحماية البيانات والمعلومات في الجهة بما يتوافق مع السياسات الصادرة من مكتب إدارة البيانات الوطنية ومن هذه المتطلبات وعلى سبيل المثال لا الحصر: ○ متطلبات حماية بيانات ومعلومات الجهة. ○ متطلبات ملكية البيانات والمعلومات. ○ متطلبات تصنيف البيانات والمعلومات وآلية ترميزها. ○ متطلبات حماية خصوصية البيانات والمعلومات. • العمل ان تكون السياسة مدعومة من قبل الإدارة التنفيذية. وذلك من خلال اعتماد وموافقة رئيس الجهة أو من ينيبه.
	المخرجات المتوقعة: • وثيقة سياسة الأمن السيبراني التي تغطي متطلبات حماية بيانات ومعلومات الجهة (مثال: نسخة إلكترونية أو نسخة ورقية رسمية).

	• موافقة رسمية من قبل رئيس الجهة أو من ينيبه على السياسة (مثال: عن طريق البريد الإلكتروني الرسمي للجهة، أو التوقيع الورقي أو الإلكتروني).
٢-٧-٢	يجب تطبيق متطلبات الأمن السيبراني لحماية بيانات ومعلومات الجهة.
	إرشادات تطبيق الضوابط: • العمل على تطبيق كافة متطلبات الأمن السيبراني عند تطبيق إجراءات حماية البيانات والمعلومات في الجهة، كما يجب أن تغطي إجراءات حماية البيانات والمعلومات بحد أدنى ما يلي وعلى سبيل المثال لا الحصر: ○ تحديد ملكية البيانات والمعلومات. ○ تصنيف البيانات والمعلومات. ○ ترميز البيانات والمعلومات بما يتوافق مع آلية تصنيف البيانات والمعلومات المعتمدة في الجهة. • العمل على وضع خطة عمل لتطبيق كافة متطلبات الأمن السيبراني المتعلقة بحماية البيانات والمعلومات. • العمل على تطبيق ضوابط حماية البيانات لضمان حمايتها وفقًا لمستوى تصنيفها وأثرها. • أيضاً قد تضع الجهة خطة عمل لتطبيق متطلبات الأمن السيبراني الخاصة بحماية بيانات ومعلومات الجهة، لضمان التزام الجهة بتطبيق كافة متطلبات الأمن السيبراني، وتشمل جميع أصحاب المصلحة الداخليين والخارجيين، ومتابعتها ومراقبتها بشكل دوري لضمان التطبيق.
	المخرجات المتوقعة: • وثائق تؤكد تطبيق متطلبات الأمن السيبراني المتعلقة بحماية البيانات والمعلومات والتي تم توثيقها في وثيقة السياسات. • وثيقة خطة عمل لتطبيق متطلبات الأمن السيبراني لحماية بيانات ومعلومات الجهة. • دليل يوضح تطبيق ضوابط حماية بيانات ومعلومات الجهة، على سبيل المثال لا الحصر: o توفير مصفوفة حوكمة البيانات والمعلومات التي توضح ملكية البيانات والمعلومات. o وجود إجراءات للتعامل مع البيانات وفق تصنيفها وأثرها. o عينة من استخدام الجهة للتقنيات الحديثة لحماية بيانات ومعلومات الجهة (مثال: وجود التقنيات المتقدمة واللازمة لحماية بيانات ومعلومات الجهة وتشفيرها وحفظها من التعديل والتسريب).
٣-٧-٢	يجب أن تغطي متطلبات الأمن السيبراني لحماية البيانات والمعلومات بحد أدنى ما يلي:
١-٣-٧-٢	ملكية البيانات والمعلومات.
	إرشادات تطبيق الضوابط: • العمل على تحديد متطلبات ملكية البيانات والمعلومات بما يتوافق مع السياسات الصادرة من مكتب إدارة البيانات الوطنية وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية.

- العمل مع الإدارات ذات العلاقة لتحديد ملاك البيانات والمعلومات وتوثيق ملكيتها في السجلات المعنية (سجلات الأصول المعلوماتية).
- العمل على تطبيق متطلبات الأمن السيبراني لملكية البيانات والمعلومات في الجهة لضمان الالتزام بمتطلبات الأمن السيبراني لجميع أصحاب المصلحة الداخليين والخارجيين ومن هذه المتطلبات وعلى سبيل المثال لا الحصر ما يلي:
  - تعريف وتحديد البيانات التي تملكها الجهة.
  - تحديد ملاك البيانات في الجهة.
  - إسهام ملاك البيانات والمعلومات في عملية التصنيف والترميز بما يتوافق مع آلية تصنيف وترميز البيانات المعتمد في الجهة.
  - إجراء تقييم الأثر للبيانات ومناقشة ذلك مع ملاك البيانات لتحديد الأضرار المحتملة.

المخرجات المتوقعة:

- وثائق (كسياسات أو معايير معتمدة من قبل صاحب الصلاحية) توضح تحديد وتوثيق متطلبات هذا الضابط (مثال: نسخة إلكترونية أو نسخة ورقية رسمية).
- وثيقة خطة عمل لتطبيق متطلبات الأمن السيبراني المتعلقة بملكية البيانات والمعلومات.
- دليل يوضح تطبيق المتطلبات المتعلقة بملكية البيانات والمعلومات، على سبيل المثال لا الحصر:
  - وثيقة رسمية معتمدة من رئيس الجهة أو من ينيبه توضّح ملاك الأنظمة والبيانات والمعلومات في الجهة.
  - سجل قائمة البيانات التي تملكها الجهة موضح فيه ملاك هذه البيانات.

٢-٣-٧-٢	تصنيف البيانات والمعلومات وآلية ترميزها (Classification and Labeling Mechanisms).

إرشادات تطبيق الضوابط:

- العمل على تحديد متطلبات تصنيف وترميز البيانات والمعلومات بما يتوافق مع السياسات الصادرة من مكتب إدارة البيانات الوطنية وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية.
- تشكيل فريق عمل بين الادارة المعنية بالامن السيبراني ومكتب ادارة البيانات في الجهة.
- تطوير إجراءات تصنيف البيانات والمعلومات وآلية ترميزها.
- العمل على تطوير منهجية لتصنيف البيانات والمعلومات وآلية ترميزها مع الأخذ بعين الاعتبار المبادئ الرئيسية لتصنيف البيانات الصادرة عن مكتب إدارة البيانات الوطنية:
  - مبدأ الأصل في البيانات الإتاحة.
  - مبدأ الضرورة والتناسب.
  - مبدأ التصنيف في الوقت المناسب.
  - مبدأ المستوى الأعلى من الحماية.
  - مبدأ فصل المهام.
  - مبدأ الحاجة إلى المعرفة.

	○ مبدأ الحد الأدنى من الامتيازات. • تحديد الاليات والتقنيات المناسبة لأتمتة ترميز البيانات حسب تصنيفها ومن هذه التقنيات على سبيل المثال لا الحصر العلامات المائية.
	المخرجات المتوقعة: • وثائق توضح تحديد وتوثيق متطلبات هذا الضابط كسياسات أو معايير معتمدة من قبل صاحب الصلاحية (مثال: نسخة إلكترونية أو نسخة ورقية رسمية). • وثيقة حوكمة البيانات المعتمدة من قبل صاحب الصلاحية في الجهة. • دليل يوضح تطبيق متطلبات تصنيف البيانات والمعلومات وآلية ترميزها على سبيل المثال لا الحصر: ○ عينة من بيانات تم تصنيفها وترميزها وفقًا لآلية التصنيف والترميز الموثقة والمعتمدة في الجهة متضمنا أنشطة تصنيف البيانات وأثرها.
٢-٧-٣-٣	خصوصية البيانات والمعلومات.
	إرشادات تطبيق الضوابط: • العمل على تحديد متطلبات خصوصية البيانات والمعلومات وتوثيقها في وثيقة متطلبات الأمن السيبراني، على أن تكون متوافقة مع المتطلبات التشريعية والتنظيمية ذات العلاقة، واعتمادها من قبل صاحب الصلاحية، وقد تشمل الآتي: ○ تضمين مسؤوليات الأمن السيبراني وبنود في حماية خصوصية البيانات والمعلومات. ○ تطوير إجراءات خصوصية البيانات في الجهة لضمان الالتزام بمتطلبات الأمن السيبراني لجميع أصحاب المصلحة الداخليين والخارجيين. • العمل على تطبيق متطلبات الأمن السيبراني لخصوصية البيانات والمعلومات في الجهة لضمان الالتزام بمتطلبات الأمن السيبراني لجميع أصحاب المصلحة الداخليين والخارجيين.
	المخرجات المتوقعة: • وثائق توضح تحديد وتوثيق متطلبات هذا الضابط كسياسات أو معايير معتمدة من قبل صاحب الصلاحية (مثال: نسخة إلكترونية أو نسخة ورقية رسمية). • إجراءات موثقة ومعتمدة من قبل رئيس الجهة أو من ينيبه لكيفية التعامل مع البيانات والمعلومات وخصوصيتها.
٢-٧-٤	يجب مراجعة تطبيق متطلبات الأمن السيبراني لحماية بيانات ومعلومات الجهة دورياً.
	إرشادات تطبيق الضوابط: • العمل على مراجعة تطبيق متطلبات الأمن السيبراني لحماية بيانات ومعلومات الجهة من خلال إجراء تقييم دوري (وذلك حسب خطة موثقة ومعتمدة للمراجعة، وبناء على فترة زمنية محددة "على سبيل المثال لا

	الحصر، بشكل ربع سنوي") لتنفيذ متطلبات حماية البيانات والمعلومات من قبل الإدارة المعنية بالأمن السيبراني وبالتعاون مع الإدارات ذات العلاقة. • مراجعة التطبيق قد تتم من خلال القنوات التقليدية (مثل البريد الإلكتروني) أو قد يكون مؤتمت باستخدام نظام لإدارة الالتزام. الجهة قد تضع خطة مراجعة توضح فيها جدول مراجعة تطبيق متطلبات الأمن السيبراني لحماية بيانات ومعلومات الجهة. • مراجعة وتحديث متطلبات الأمن السيبراني الخاصة بحماية البيانات والمعلومات في الجهة بشكل دوري حسب خطة موثقة ومعتمدة للمراجعة بناءً على فترة زمنية محددة أو في حالة حدوث تغييرات في المتطلبات التشريعية والتنظيمية ذات العلاقة. • توثيق المراجعة والتغييرات التي تتم على متطلبات الأمن السيبراني الخاصة بحماية البيانات والمعلومات في الجهة واعتمادها من قبل رئيس الجهة أو من ينيبه.
	المخرجات المتوقعة: • نتائج مراجعة تطبيق متطلبات حماية البيانات والمعلومات في الجهة. • وثيقة تحدد دورة مراجعة تطبيق متطلبات الأمن السيبراني لحماية بيانات ومعلومات الجهة (جدول تقييم الالتزام). • وثيقة تقرير تقييم الالتزام توضح تقييم تطبيق متطلبات الأمن السيبراني لتطبيق متطلبات حماية البيانات والمعلومات في الجهة. • وثيقة معتمدة تحدد جدول المراجعة للسياسة. • وثيقة السياسة بما يوضح أن تكون محدثة وتم توثيق التغييرات على متطلبات الأمن السيبراني الخاصة بحماية بيانات ومعلومات الجهة واعتمادها من قبل رئيس الجهة أو من ينيبه. • 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).

٢-٨	التشفير (Cryptography)
الهدف	ضمان الاستخدام السليم والفعال للتشفير لحماية الأصول المعلوماتية الإلكترونية للجهة، وذلك وفقاً للسياسات والإجراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية ذات العلاقة.
الضوابط	
١-٨-٢	يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني للتشفير في الجهة.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة التشفير

	إرشادات تطبيق الضوابط: • العمل على تطوير وتوثيق سياسة الأمن السيبراني لإجراءات التشفير في الجهة، وقد تحتوي على سبيل المثال لا الحصر: ○ معايير حلول التشفير المعتمدة والقيود المطبقة عليها (تقنياً وتنظيمياً) ○ الإدارة الآمنة لمفاتيح التشفير خلال عمليات دورة حياتها ○ تشفير البيانات أثناء النقل والتخزين بناء على تصنيفها وحسب المتطلبات التشريعية والتنظيمية ذات العلاقة • العمل على ان تكون السياسة في الجهة مدعومة من قبل الإدارة التنفيذية. وذلك من خلال اعتماد وموافقة رئيس الجهة أو من ينيبه. **المخرجات المتوقعة:** • وثيقة سياسة الأمن السيبراني التي تغطي متطلبات إجراءات التشفير في الجهة (مثال: نسخة إلكترونية أو نسخة ورقية رسمية). • موافقة رسمية من قبل رئيس الجهة أو من ينيبه على السياسة (مثال: عن طريق البريد الإلكتروني الرسمي للجهة، أو التوقيع الورقي أو الإلكتروني).
٢-٨-٢	يجب تطبيق متطلبات الأمن السيبراني للتشفير في الجهة. **إرشادات تطبيق الضوابط:** • العمل على تطبيق كافة متطلبات الأمن السيبراني عند تطبيق إجراءات التشفير المعتمدة في الجهة، كما يوصى أن تغطي إجراءات التشفير بحد أدنى ما يلي وعلى سبيل المثال لا الحصر: ○ معايير حلول التشفير المعتمدة والقيود المطبقة عليها (تقنياً وتنظيمياً) ○ الإدارة الآمنة لمفاتيح التشفير خلال عمليات دورة حياتها ○ تشفير البيانات أثناء النقل والتخزين بناء على تصنيفها وحسب المتطلبات التشريعية والتنظيمية ذات العلاقة ○ تحديد خوارزميات التشفير المعتمدة في الجهة بناءً على المعايير الوطنية للتشفير ○ ضمان تطبيق التشفير على الأصول التقنية والمعلوماتية ○ استخدام شهادات TLS المعتمدة لخوادم الويب والتطبيقات العامة التي تم إصدارها من قبل جهة خارجية موثوق بها. **المخرجات المتوقعة:** • وثيقة خطة عمل لتطبيق متطلبات الأمن السيبراني لإجراءات التشفير في الجهة. • إثبات يوضح استخدام الجهة تقنيات حديثة للتشفير في الجهة (مثال: وجود التقنيات المتقدمة للتشفير في الجهة، إجراءات ومعايير أمنية تدعم تطبيق التشفير في الجهة).

٢-٨-٣	يجب أن تغطي متطلبات الأمن السيبراني للتشفير بحد أدنى ما يلي:	
	٢-٨-٣-١	معايير حلول التشفير المعتمدة والقيود المطبقة عليها (تقنياً وتنظيمياً).

أدوات الأمن السيبراني ذات العلاقة:

- نموذج معيار التشفير.

إرشادات تطبيق الضوابط:

- العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني للتشفير، واعتمادها من قبل صاحب الصلاحية.
- العمل على تحديد معايير حلول التشفير المعتمدة واستخدام المعايير الوطنية للتشفير الصادرة من الهيئة، على سبيل المثال لا الحصر:
  - أساسيات التشفير المتماثلة وغير المتماثلة المقبولة
  - إجراءات البنية التحتية للمفاتيح العامة
  - إجراءات إدارة دورة المفاتيح
- العمل على تحديد معايير حلول التشفير المعتمدة والقيود المطبقة عليها تقنياً والتأكد من موائمتها مع المعايير الوطنية للتشفير، على سبيل المثال لا الحصر:
  - تصاميم التشفير المتماثلة وغير المتماثلة المقبولة
  - بروتوكولات التطبيقات الشائعة المقبولة ذات العلاقة بالتشفير
  - تقنيات وأدوات البنية التحتية للمفاتيح العامة
  - تقنيات وأدوات إدارة دورة المفاتيح

المخرجات المتوقعة:

- وثيقة من معايير التشفير التقنية المعتمدة في الجهة (مثال: نسخة إلكترونية أو نسخة ورقية رسمية).
- موافقة رسمية من قبل رئيس الجهة أو من ينيبه على هذه المعايير (مثال: عن طريق البريد الإلكتروني الرسمي للجهة، أو التوقيع الورقي أو الإلكتروني).
- إثبات يوضح تطبيق متطلبات معايير حلول التشفير التقنية المعتمدة والقيود المطبقة عليها (مثال: لقطة شاشة توضح ما يثبت ضمان استخدام التقنيات الحديثة والمتقدمة لتطبيق معايير حلول التشفير التقنية المعتمدة والقيود المطبقة على جميع الأنظمة في الجهة).
- وثيقة من معايير التشفير التنظيمية المعتمدة في الجهة (مثال: نسخة إلكترونية أو نسخة ورقية رسمية).
- موافقة رسمية من قبل رئيس الجهة أو من ينيبه على هذه المعايير (مثال: عن طريق البريد الإلكتروني الرسمي للجهة، أو التوقيع الورقي أو الإلكتروني).
- إثبات يوضح تطبيق متطلبات معايير حلول التشفير التنظيمية المعتمدة والقيود المطبقة عليها (مثال: لقطة شاشة توضح ما يثبت ضمان استخدام التقنيات الحديثة والمتقدمة لتطبيق معايير حلول التشفير التنظيمية المعتمدة والقيود المطبقة على جميع الأنظمة في الجهة)

٢-٨-٣-٢	الإدارة الآمنة لمفاتيح التشفير خلال عمليات دورة حياتها.

إرشادات تطبيق الضوابط:

- العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني لتشفير، واعتمادها من قبل صاحب الصلاحية.
- العمل على تحديد إجراءات للإدارة الآمنة لمفاتيح التشفير خلال عمليات دورة حياتها واعتمادها في الجهة
- تحديد وتطبيق التقنيات المناسبة والمتقدمة للإدارة الآمنة لمفاتيح التشفير خلال عمليات دورة حياتها، على سبيل المثال لا الحصر:
  - آلية حفظ مفاتيح التشفير
  - آلية نقل مفاتيح التشفير
  - لآلية إنشاء وتدمير المفاتيح
- مراجعة فعالية التقنيات المستخدمة للإدارة الآمنة لمفاتيح التشفير.

المخرجات المتوقعة:

- وثيقة سياسة الأمن السيبراني التي تغطي متطلبات إجراءات التشفير في الجهة (مثال: نسخة إلكترونية أو نسخة ورقية رسمية).
- وثيقة إجراءات الأمن السيبراني التي تغطي إدارة مفاتيح التشفير في الجهة (مثال: نسخة إلكترونية أو نسخة ورقية رسمية).
- وثيقة تحدد دورة مراجعة فعالية التقنيات المستخدمة للإدارة الآمنة لمفاتيح التشفير خلال عمليات دورة حياتها.
- موافقة رسمية من قبل رئيس الجهة أو من ينيبه على هذه الوثائق (مثال: عن طريق البريد الإلكتروني الرسمي للجهة، أو التوقيع الورقي أو الإلكتروني).
- إثبات يوضح تطبيق متطلبات الإدارة الآمنة لمفاتيح التشفير خلال عمليات دورة حياتها (مثال: لقطة شاشة توضح ما يثبت ضمان ضبط إعدادات مفاتيح التشفير وفقاً لأفضل المعايير المتبعة للإدارة الآمنة لمفاتيح التشفير خلال عمليات دورة حياتها).

٢-٨-٣-٣	تشفير البيانات أثناء النقل والتخزين بناء على تصنيفها وحسب المتطلبات التشريعية والتنظيمية ذات العلاقة.

إرشادات تطبيق الضوابط:

- العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني للتشفير، واعتمادها من قبل صاحب الصلاحية.
- تحديد التقنيات المناسبة والمتقدمة لتشفير البيانات أثناء النقل بناء على تصنيفها، على سبيل المثال لا الحصر:
  - استخدام بروتوكول طبقة النقل الآمنة (TLS (Transport Layer Security
- تطبيق التقنيات المناسبة والمتقدمة لتشفير البيانات أثناء النقل بناء على تصنيفها.

	• مراجعة فعالية التقنيات المستخدمة لتشفير البيانات أثناء النقل بناء على تصنيفها. • تحديد التقنيات المناسبة والمتقدمة لتشفير البيانات أثناء التخزين بناء على تصنيفها، على سبيل المثال لا الحصر: ○ استخدام تشفير البيانات الشفاف TDE (Transparent Data Encryption) • تطبيق التقنيات المناسبة والمتقدمة لتشفير البيانات أثناء التخزين بناء على تصنيفها. • مراجعة فعالية التقنيات المستخدمة لتشفير البيانات أثناء النقل بناء على تصنيفها.
	المخرجات المتوقعة: • وثيقة إجراءات تشفير البيانات أثناء النقل في الجهة (مثال: نسخة إلكترونية أو نسخة ورقية رسمية). • موافقة رسمية من قبل رئيس الجهة أو من ينيبه على هذه الإجراءات (مثال: عن طريق البريد الإلكتروني الرسمي للجهة، أو التوقيع الورقي أو الإلكتروني). • إثبات يوضح تطبيق متطلبات تشفير البيانات أثناء النقل بناء على تصنيفها (على سبيل المثال لا الحصر: لقطة شاشة توضح تطبيق تشفير البيانات أثناء النقل بناء على تصنيفها). • وثيقة إجراءات تشفير البيانات أثناء التخزين في الجهة (مثال: نسخة إلكترونية أو نسخة ورقية رسمية). • موافقة رسمية من قبل رئيس الجهة أو من ينيبه على هذه الإجراءات (مثال: عن طريق البريد الإلكتروني الرسمي للجهة، أو التوقيع الورقي أو الإلكتروني). • إثبات يوضح تطبيق متطلبات تشفير البيانات أثناء النقل بناء على تصنيفها (على سبيل المثال لا الحصر: لقطة شاشة توضح تطبيق تشفير البيانات أثناء النقل بناء على تصنيفها).
٢-٨-٤	يجب مراجعة تطبيق متطلبات الأمن السيبراني للتشفير في الجهة دورياً.
	إرشادات تطبيق الضوابط: • العمل على مراجعة تطبيق متطلبات الأمن السيبراني لإجراءات تشفير في الجهة من خلال إجراء تقييم دوري (وذلك حسب خطة موثقة ومعتمدة للمراجعة، وبناء على فترة زمنية محددة "على سبيل المثال لا الحصر، بشكل ربع سنوي") لتنفيذ متطلبات إجراءات التشفير من قبل الإدارة المعنية بالأمن السيبراني وبالتعاون مع الإدارات ذات العلاقة (كالإدارة المعنية بتقنية المعلومات). • مراجعة وتحديث متطلبات الأمن السيبراني الخاصة بإجراءات التشفير في الجهة بشكل دوري حسب خطة موثقة ومعتمدة للمراجعة بناءً على فترة زمنية محددة أو في حالة حدوث تغييرات في المتطلبات التشريعية والتنظيمية ذات العلاقة. • توثيق المراجعة والتغييرات التي تتم على متطلبات الأمن السيبراني الخاصة بإجراءات التشفير في الجهة واعتمادها من قبل رئيس الجهة أو من ينيبه.
	المخرجات المتوقعة: • نتائج مراجعة تطبيق متطلبات التشفير في الجهة. • وثيقة تحدد دورة مراجعة تطبيق متطلبات الأمن السيبراني للتشفير في الجهة (جدول تقييم الالتزام). • وثيقة تقرير تقييم الالتزام توضح تقييم تطبيق متطلبات الأمن السيبراني لتطبيق متطلبات التشفير في الجهة. • وثيقة معتمدة تحدد جدول المراجعة للسياسة.

	• وثيقة السياسة بما يوضح أن تكون محدثة وتم توثيق التغييرات على متطلبات الأمن السيبراني الخاصة بالتشفير الجهة واعتمادها من قبل رئيس الجهة أو من ينيبه. • 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).

٢-٩	إدارة النسخ الاحتياطية (Backup and Recovery Management)
الهدف	ضمان حماية بيانات ومعلومات الجهة والإعدادات التقنية للأنظمة والتطبيقات الخاصة بالجهة من الاضرار الناتجة عن المخاطر السيبرانية، وذلك وفقاً للسياسات والإجراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية ذات العلاقة.
الضوابط	
٢-٩-١	يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني لإدارة النسخ الاحتياطية للجهة.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة إدارة النسخ الاحتياطية **إرشادات تطبيق الضوابط:** • العمل على تطوير وتوثيق سياسة الأمن السيبراني لإدارة النسخ الاحتياطي في الجهة وقد تحتوي على سبيل المثال لا الحصر: ○ نطاق النسخ الاحتياطية وشموليتها للأصول المعلوماتية والتقنية الحساسة. ○ القدرة السريعة على استعادة البيانات والأنظمة بعد التعرض لحوادث الأمن السيبراني ○ الفحص الدوري لفعالية استعادة النسخ الاحتياطي ○ الفترة المحددة لعمل النسخ الاحتياطية ○ تحديد التقنيات المناسبة والمتقدمة لعمل النسخ الاحتياطي • العمل على ان تكون السياسة في الجهة مدعومة من قبل الإدارة التنفيذية. وذلك من خلال اعتماد وموافقة رئيس الجهة أو من ينيبه.
	المخرجات المتوقعة: • وثيقة سياسة الأمن السيبراني التي تغطي متطلبات إدارة النسخ الاحتياطية في الجهة (مثال: نسخة إلكترونية أو نسخة ورقية رسمية). • موافقة رسمية من قبل رئيس الجهة أو من ينيبه على السياسة (مثال: عن طريق البريد الإلكتروني الرسمي للجهة، أو التوقيع الورقي أو الإلكتروني).
٢-٩-٢	يجب تطبيق متطلبات الأمن السيبراني لإدارة النسخ الاحتياطية للجهة.

	إرشادات تطبيق الضوابط: • العمل على تطبيق كافة متطلبات الأمن السيبراني عند تطبيق إدارة النسخ الاحتياطية المعتمدة في الجهة، كما يوصى أن تغطي إدارة النسخ الاحتياطية بحد أدنى ما يلي وعلى سبيل المثال لا الحصر: ○ استخدام التقنيات المناسبة والمتقدمة لنسخ الاحتياطية ○ العمل على تحديد نطاق النسخ الاحتياطية وشموليتها للأصول المعلوماتية والتقنية الحساسة ○ العمل على القدرة السريعة على استعادة البيانات والأنظمة بعد التعرض لحوادث الأمن السيبراني ○ العمل على تطبيق الفحص الدوري لفعالية استعادة النسخ الاحتياطي ○ العمل على تحديد الفترة اللازمة لعمل النسخ الاحتياطية على سبيل المثال لا الحصر: عمل نسخ احتياطي للبيانات المتغيرة في اخر ٢٤ ساعة
	المخرجات المتوقعة: • وثيقة خطة عمل لتطبيق متطلبات الأمن السيبراني لإدارة النسخ الاحتياطية • إثبات على سبيل المثال لا الحصر (لقطة شاشة) من أداة النسخ الاحتياطية تُظهر أحدث النسخ الاحتياطية التي تم أخذها، وجدول ونطاق النسخ الاحتياطية.
٢-٩-٣	يجب أن تغطي متطلبات الأمن السيبراني لإدارة النسخ الاحتياطية بحد أدنى ما يلي:
٢-٩-٣-١	نطاق النسخ الاحتياطية وشموليتها للأصول المعلوماتية والتقنية الحساسة.
	إرشادات تطبيق الضوابط: • العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني لإدارة النسخ الاحتياطية، واعتمادها من قبل صاحب الصلاحية. • تحديد نطاق النسخ الاحتياطية لكافة الأصول المعلوماتية والتقنية الحساسة والمهمة في الجهة على سبيل المثال لا الحصر: ○ قواعد البيانات ○ التطبيقات ○ الخوادم ○ أجهزة الشبكة • تحديد التقنيات المخصصة لعمل النسخ الاحتياطي. • تحديد المدة اللازمة لعمل النسخ الاحتياطية لجميع الأصول المعلوماتية والتقنية حسب الحساسية والتصنيف. • تطبيق النسخ الاحتياطية لكافة الأصول المعلوماتية والتقنية الحساسة والمهمة في الجهة. • مراجعة النسخ الاحتياطية في الجهة دورياً، بحيث تشمل على جميع النطاق المذكور مسبقاً وأي أصول معلوماتية وتقنية استجدت لدى الجهة.

المخرجات المتوقعة:

- وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية).
- تقرير من عمليات النسخ الاحتياطية الدورية حسب المدة المحددة لجميع نطاق الأصول.

٢-٩-٣-٢	القدرة السريعة على استعادة البيانات والأنظمة بعد التعرض لحوادث الأمن السيبراني.

إرشادات تطبيق الضوابط:

- العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني لإدارة النسخ الاحتياطية، واعتمادها من قبل صاحب الصلاحية.
- تحديد الإجراءات المناسبة لاستعادة البيانات والأنظمة بعد التعرض لحوادث الأمن السيبراني، وذلك من خلال على سبيل المثال لا الحصر:
  - تحديد نطاق استعادة النسخ الاحتياطية والذي من الممكن أن يحتوي على جميع الأجهزة والأنظمة والخوادم وتصنيفها على حسب أهميتها وحساسيتها.
  - تحديد مدة الاستعادة على حسب تصنيف وأهمية النطاق المحدد.
  - استخدام التقنيات المخصصة لاستعادة البيانات والأنظمة.
  - العمل على حساب المدة اللازمة لاستعادة جميع النسخ الاحتياطية لجميع نطاق الأصول بحيث يضمن القدرة السريعة لاستعادة النسخ الاحتياطية في حال التعرض لحادثة امن سيبراني.

المخرجات المتوقعة:

- وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية).
- تقرير الإجراءات المحددة لاستعادة النسخ الاحتياطية.

٢-٩-٣-٣	إجراء فحص دوري لمدى فعالية استعادة النسخ الاحتياطية.

إرشادات تطبيق الضوابط:

- العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني لإدارة النسخ الاحتياطية، واعتمادها من قبل صاحب الصلاحية.
- العمل على تطوير خطة لإجراء فحص دوري لمدى فعالية استعادة النسخ الاحتياطية
- العمل على التأكد من فعالية إجراءات الاستعادة من خلال اجراء اختبار لاستعادة النسخ الاحتياطية بشكل دوري بحيث يضمن قدرة استعادة البيانات والأنظمة حسب المدة المحددة في الإجراءات وحسب المدة التي تم حسابها لاكتمال استعادة النسخ الاحتياطية.

	المخرجات المتوقعة: • وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية). • تقارير اختبارات فحص فعالية النسخ الاحتياطية بحيث يوضح الفرق بين المدة المتوقعة ومدة الاختبار لاستعادة جميع النسخ الاحتياطية.
٢-٩-٤	يجب مراجعة تطبيق متطلبات الأمن السيبراني لإدارة النسخ الاحتياطية للجهة.
	إرشادات تطبيق الضوابط: • العمل على مراجعة تطبيق متطلبات الأمن السيبراني لإدارة النسخ الاحتياطية من خلال إجراء تقييم دوري (وذلك حسب خطة موثقة ومعتمدة للمراجعة، وبناء على فترة زمنية محددة "على سبيل المثال لا الحصر، بشكل ربع سنوي") لتنفيذ متطلبات إدارة النسخ الاحتياطية من قبل الإدارة المعنية بالأمن السيبراني وبالتعاون مع الإدارات ذات العلاقة (كالإدارة المعنية بتقنية المعلومات). • مراجعة التطبيق قد تتم من خلال القنوات التقليدية (مثل البريد الإلكتروني) أو قد يكون مؤتمت باستخدام نظام لإدارة الالتزام. الجهة قد تضع خطة مراجعة توضح فيها جدول مراجعة تطبيق متطلبات الأمن السيبراني لإدارة النسخ الاحتياطية. • مراجعة وتحديث متطلبات الأمن السيبراني الخاصة بإدارة النسخ الاحتياطية في الجهة بشكل دوري حسب خطة موثقة ومعتمدة للمراجعة بناءً على فترة زمنية محددة أو في حالة حدوث تغييرات في المتطلبات التشريعية والتنظيمية ذات العلاقة. • توثيق المراجعة والتغييرات التي تتم على متطلبات الأمن السيبراني الخاصة بإدارة النسخ الاحتياطية في الجهة واعتمادها من قبل رئيس الجهة أو من ينيبه.
	المخرجات المتوقعة: • نتائج مراجعة تطبيق متطلبات إدارة النسخ الاحتياطية في الجهة. • وثيقة تحدد دورة مراجعة تطبيق متطلبات الأمن السيبراني لإدارة النسخ الاحتياطية في الجهة (جدول تقييم الالتزام). • وثيقة تقرير تقييم الالتزام توضح تقييم تطبيق متطلبات الأمن السيبراني لتطبيق متطلبات إدارة النسخ الاحتياطية في الجهة. • وثيقة معتمدة تحدد جدول المراجعة للسياسة. • وثيقة السياسة بما يوضح أن تكون محدثة وتم توثيق التغييرات على متطلبات الأمن السيبراني الخاصة إدارة النسخ الاحتياطية في الجهة واعتمادها من قبل رئيس الجهة أو من ينيبه. • 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).

٢-١٠	إدارة الثغرات (Vulnerabilities Management)
الهدف	ضمان اكتشاف الثغرات التقنية في الوقت المناسب ومعالجتها بشكل فعال، وذلك لمنع أو تقليل احتمالية استغلال هذه الثغرات من قبل الهجمات السيبرانية وتقليل الاثار المترتبة على أعمال الجهة.
الضوابط	
٢-١٠-١	يجب تحديد وتوثيق اعتماد متطلبات الأمن السيبراني لإدارة الثغرات التقنية للجهة.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة إدارة الثغرات **إرشادات تطبيق الضوابط:** • العمل على تطوير وتوثيق سياسة الأمن السيبراني لإدارة الثغرات في الجهة، وقد تشمل الآتي: ○ متطلبات فحص وتقييم الثغرات لجميع الأصول التقنية. ○ متطلبات الفحص الدوري لثغرات. ○ متطلبات تصنيف الثغرات على حسب خطورتها. ○ متطلبات معالجة الثغرات باستخدام أدوات وأساليب فعالة. • العمل على ان تكون السياسة في الجهة مدعومة من قبل الإدارة التنفيذية. وذلك من خلال اعتماد وموافقة رئيس الجهة أو من ينيبه
	المخرجات المتوقعة: • وثيقة سياسة الأمن السيبراني التي تغطي متطلبات إدارة الثغرات (مثال: نسخة إلكترونية أو نسخة ورقية رسمية). • موافقة رسمية من قبل رئيس الجهة أو من ينيبه على السياسة (مثال: عن طريق البريد الإلكتروني الرسمي للجهة، أو التوقيع الورقي أو الإلكتروني).
٢-١٠-٢	يجب تطبيق متطلبات الأمن السيبراني لإدارة الثغرات للجهة.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج إجراءات إدارة الثغرات • نموذج سجل إدارة الثغرات **إرشادات تطبيق الضوابط:** • العمل على تطبيق كافة متطلبات الأمن السيبراني عند تطبيق إجراءات إدارة الثغرات المعتمدة في الجهة، كما يجب أن تغطي إجراءات إدارة الثغرات بحد أدنى ما يلي وعلى سبيل المثال لا الحصر:

	○ إجراءات فحص واكتشاف الثغرات دورياً ○ آلية تصنيف الثغرات حسب خطورتها. ○ إجراءات معالجة الثغرات بناء على تصنيفها والمخاطر السيبرانية المترتبة عليها. ○ آلية واجراء التصعيد للثغرات التقنية. ○ طرق ربط إجراءات إدارة الثغرات مع إجراءات إدارة حزم التحديثات والإصلاحات الأمنية. **المخرجات المتوقعة:** • إجراءات إدارة الثغرات • إجراءات إدارة حزم التحديثات والإصلاحات الأمنية • تقارير فحص واكتشاف الثغرات (قبل وبعد المعالجة) يوضح فيه تصنيف الثغرات
٢-١٠-٣	يجب أن تغطي متطلبات الأمن السيبراني لإدارة الثغرات بحد أدنى ما يلي: ٢-١٠-٣-١ فحص واكتشاف الثغرات دورياً. **إرشادات تطبيق الضوابط:** • العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية. • العمل على تحديد تقنيات وأدوات لفحص واكتشاف الثغرات على الأصول المعلوماتية والتقنية في الجهة • تثبيت وربط تقنيات وأدوات فحص واكتشاف الثغرات مع الأصول المعلوماتية والتقنية في الجهة • العمل على تطوير خطة دورية وإجراءات لفحص واكتشاف الثغرات على الأصول المعلوماتية والتقنية في الجهة والتي تشمل: ○ التطبيقات ○ الأجهزة والخوادم ○ قواعد البيانات ○ شبكات الجهة **المخرجات المتوقعة:** • وثيقة سياسة الأمن السيبراني التي تغطي عملية فحص واكتشاف الثغرات بشكل دوري (بناء على الخطة والفترة الزمنية المحددة في وثيقة السياسات) على الأصول التالية: ○ التطبيقات ○ الأجهزة والخوادم ○ قواعد البيانات ○ شبكات الجهة

(مثال: نسخة إلكترونية أو نسخة ورقية رسمية).

- موافقة رسمية من قبل رئيس الجهة أو من ينيبه على هذه المتطلبات (مثال: عن طريق البريد الإلكتروني الرسمي للجهة، أو التوقيع الورقي أو الإلكتروني).
- إجراءات إدارة الثغرات وخطة دورية لفحص واكتشاف الثغرات
- تقارير دورية لفحص واكتشاف الثغرات

٢-١٠-٣-٢	تصنيف الثغرات حسب خطورتها.

إرشادات تطبيق الضوابط:

- العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية.
- العمل على إعداد ومراجعة تقارير فحص واكتشاف الثغرات على الأصول المعلوماتية والتقنية في الجهة والتي تشمل تصنيف الثغرات بناءً على التالي:
  - وصف الثغرات وإمكانية استغلالها وحجم التأثير المتوقع للجهة
  - تجزئة الشبكة
  - تصنيف الأصول المعنية للثغرات
  - تصنيف الثغرات حسب المورد ونظام تسجيل الثغرات المشترك (CVSS)

المخرجات المتوقعة:

- وثيقة سياسة الأمن السيبراني التي تغطي الية ومنهجية تصنيف الثغرات بناء على حساسيتها والأخطار السيبرانية المترتبة عليها وبناء على تجزئة الشبكة الخاصة بالجهة (مثال: نسخة إلكترونية أو نسخة ورقية رسمية).
- موافقة رسمية من قبل رئيس الجهة أو من ينيبه على هذه الوثيقة (مثال: عن طريق البريد الإلكتروني الرسمي للجهة، أو التوقيع الورقي أو الإلكتروني).
- إجراءات إدارة الثغرات التي توضح آلية التصنيف
- تقارير فحص واكتشاف الثغرات يوضح فيه تصنيف الثغرات

٢-١٠-٣-٣	معالجة الثغرات بناء على تصنيفها والمخاطر السيبرانية المترتبة عليها.

إرشادات تطبيق الضوابط:

- العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية.
- مشاركة تقارير فحص واكتشاف الثغرات على الأصول المعلوماتية والتقنية في الجهة مع الإدارات المعنية والتي تشمل على سبيل المثال لا الحصر:
  - الإدارة المعنية بإدارة التطبيقات

- الإدارة المعنية بأجهزة المستخدمين
- الإدارة المعنية بالبنية التحتية
- الإدارة المعنية بإدارة قواعد البيانات
- الإدارة المعنية بالشبكات

- التأكد من ان التقارير التي تم مشاركتها تحتوي على:
  - وصف للثغرات
  - اسم الأصول المعنية التي تم فحص واكتشاف الثغرات فيها
  - تصنيف للثغرات
- العمل مع الإدارات المعنية لتحديد مدة زمنية وخطة لمعالجة الثغرات، مع الأخذ بعين الاعتبار تصنيف الثغرات وتصنيف الأصول المعنية
- وضع آلية للتأكد من معالجة الثغرات بناءً على الخطة

المخرجات المتوقعة:

- وثيقة سياسة الأمن السيبراني التي تغطي خطط معالجة الثغرات المكتشفة بالجهة (مثال: نسخة إلكترونية أو نسخة ورقية رسمية).
- موافقة رسمية من قبل رئيس الجهة أو من ينيبه على هذه الوثيقة (مثال: عن طريق البريد الإلكتروني الرسمي للجهة، أو التوقيع الورقي أو الإلكتروني).
- إجراءات إدارة الثغرات
- إجراءات إدارة حزم التحديثات والإصلاحات الأمنية
- تقارير فحص واكتشاف الثغرات (قبل وبعد المعالجة)

٢-١٠-٣-٤	إدارة حزم التحديثات والإصلاحات الأمنية لمعالجة الثغرات.

إرشادات تطبيق الضوابط:

- العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية.
- العمل على ربط إجراءات إدارة الثغرات مع إجراءات إدارة حزم التحديثات والإصلاحات الأمنية وإجراءات التغيير.
- تحليل تقارير فحص واكتشاف الثغرات لتحديد الأصول المعلوماتية والتقنية في الجهة والتي يجب التثبيت عليها حزم التحديثات والإصلاحات الأمنية.
- العمل مع الإدارات المعنية لتحديد مدة زمنية وخطة لتثبيت حزم التحديثات والإصلاحات، مع الأخذ بعين الاعتبار تصنيف الحاجة للتحديث وتصنيف الأصول المعنية.

المخرجات المتوقعة:

	• وثيقة من سياسة وإجراءات الأمن السيبراني التي تغطي متطلبات إدارة حزم التحديثات والإصلاحات الأمنية لمعالجة الثغرات. (مثال: نسخة إلكترونية أو نسخة ورقية رسمية). • موافقة رسمية من قبل رئيس الجهة أو من ينيبه على هذه الوثيقة (مثال: عن طريق البريد الإلكتروني الرسمي للجهة، أو التوقيع الورقي أو الإلكتروني). • إجراءات إدارة الثغرات • إجراءات إدارة حزم التحديثات والإصلاحات الأمنية • تقارير فحص واكتشاف الثغرات (قبل وبعد المعالجة)
٢-١٠-٣-٥	التواصل والاشتراك مع مصادر موثوقة فيما يتعلق بالتنبيهات المتعلقة بالثغرات الجديدة والمحدثة.
	إرشادات تطبيق الضوابط: • العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية. • العمل على تحديد والتسجيل مع المصادر الموثوقة فيما يتعلق بالتنبيهات المتعلقة بالثغرات الجديدة والمحدثة، وهذا يشمل: ○ الجهات الوطنية (مثل الهيئة الوطنية للأمن السيبراني والمركز الوطني الإرشادي للأمن السيبراني) ○ الموردين ومصنعي الأصول المعلوماتية والتقنية (OEMs) ○ المجموعات المتخصصة في مجال الأمن السيبراني بشكل عام وفي القطاع التابع للجهة ○ شركات الأمن السيبراني من خلال أدواتهم وتقنياتهم
	المخرجات المتوقعة: • وثيقة سياسة الأمن السيبراني التي تغطي هذا الضابط (مثال: نسخة إلكترونية أو نسخة ورقية رسمية). • موافقة رسمية من قبل رئيس الجهة أو من ينيبه على هذه الوثيقة (مثال: عن طريق البريد الإلكتروني الرسمي للجهة، أو التوقيع الورقي أو الإلكتروني). • قائمة من قنوات التواصل التي تم الاشتراك معها للحصول على التنبيهات المتعلقة بالثغرات الجديدة.
٢-١٠-٤	يجب مراجعة تطبيق متطلبات الأمن السيبراني لإدارة الثغرات التقنية للجهة دورياً.
	إرشادات تطبيق الضوابط: • العمل على مراجعة تطبيق متطلبات الأمن السيبراني لإدارة الثغرات في الجهة من خلال إجراء تقييم دوري (وذلك حسب خطة موثقة ومعتمدة للمراجعة، وبناء على فترة زمنية محددة "على سبيل المثال، بشكل ربع سنوي") لتنفيذ إجراءات إدارة الثغرات من قبل الإدارة المعنية بالأمن السيبراني وبالتعاون مع الإدارات ذات العلاقة (كالإدارة المعنية بتقنية المعلومات).

	• مراجعة التطبيق قد تتم من خلال القنوات التقليدية (مثل البريد الإلكتروني) أو قد يكون مؤتمت باستخدام نظام لإدارة الالتزام. الجهة قد تضع خطة مراجعة توضح فيها جدول مراجعة تطبيق متطلبات الأمن السيبراني لإدارة الثغرات في الجهة. • مراجعة وتحديث متطلبات الأمن السيبراني الخاصة بإدارة الثغرات في الجهة بشكل دوري حسب خطة موثقة ومعتمدة للمراجعة بناءً على فترة زمنية محددة أو في حالة حدوث تغييرات في المتطلبات التشريعية والتنظيمية ذات العلاقة. • توثيق المراجعة والتغييرات التي تتم على متطلبات الأمن السيبراني الخاصة بإدارة الثغرات في الجهة واعتمادها من قبل رئيس الجهة أو من ينيبه.
	المخرجات المتوقعة: • نتائج مراجعة تطبيق متطلبات الأمن السيبراني لإدارة الثغرات في الجهة. • وثيقة تحدد دورة مراجعة تطبيق متطلبات الأمن السيبراني لإدارة الثغرات (جدول تقييم الالتزام). • وثيقة تقرير تقييم الالتزام توضح تقييم تطبيق متطلبات الأمن السيبراني لإدارة الثغرات • 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. • 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).

٢-١١	اختبار الاختراق (Penetration Testing)
الهدف	تقييم واختبار مدى فعالية قدرات تعزيز الأمن السيبراني في الجهة، وذلك من خلال عمل محاكاة لتقنيات وأساليب الهجوم السيبراني الفعلية. ولاكتشاف نقاط الضعف الأمنية غير المعروفة والتي قد تؤدي إلى الاختراق السيبراني للجهة. وذلك وفقاً للمتطلبات التشريعية والتنظيمية ذات العلاقة.
الضوابط	
٢-١١-١	يجب تحديد وتوثيق اعتماد متطلبات الأمن السيبراني لعمليات اختبار الاختراق للجهة.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة اختبار الاختراق **إرشادات تطبيق الضوابط:** • العمل على تطوير وتوثيق سياسة الأمن السيبراني لإدارة اختبار الاختراق في الجهة وقد تشمل الآتي: ○ تحديد نطاق اختبار الاختراق في الجهة.

	○ متطلبات القيام بعملية اختبار الاختراق بشكل دوري ○ متطلبات اختبار الاختراق باستخدام أدوات وأساليب فعالة. ○ متطلبات تحديد الفريق المسؤول عن القيام بعملية اختبار الاختراق. ● العمل على ان تكون السياسة في الجهة مدعومة من قبل الإدارة التنفيذية. وذلك من خلال اعتماد وموافقة رئيس الجهة أو من ينيبه
	المخرجات المتوقعة: ● وثيقة سياسة الأمن السيبراني التي تغطي متطلبات إدارة اختبار الاختراق (مثال: نسخة إلكترونية أو نسخة ورقية رسمية). ● موافقة رسمية من قبل رئيس الجهة أو من ينيبه على السياسة (مثال: عن طريق البريد الإلكتروني الرسمي للجهة، أو التوقيع الورقي أو الإلكتروني).
٢-١١-٢	يجب تنفيذ عمليات اختبار الاختراق في الجهة.
	إرشادات تطبيق الضوابط: ● العمل على تطبيق كافة متطلبات الأمن السيبراني عند تطبيق إجراءات اختبار الاختراق المعتمدة في الجهة، كما يجب أن تغطي إجراءات اختبار الاختراق بحد أدنى ما يلي وعلى سبيل المثال لا الحصر: ○ إجراءات اختبار الاختراق دورياً ○ إجراءات تحديد نطاق عمل اختبار الاختراق
	المخرجات المتوقعة: ● خطة عمل لاختبار الاختراق ● تقارير اختبار الاختراق
٣-١١-٢	يجب أن تغطي متطلبات الأمن السيبراني لاختبار الاختراق بحد أدنى ما يلي:
١-٣-١١-٢	نطاق عمل اختبار الاختراق ليشمل جميع الخدمات المقدمة خارجياً (عـن طريق الإنترنت) ومكوناتها التقنية، ومنها: البنية التحتية، المواقع الإلكترونية، تطبيقات الويب، تطبيقات الهواتف الذكية واللوحية، البريد الإلكتروني والدخول عن بعد.
	إرشادات تطبيق الضوابط: ● العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية. ● العمل تحديد وتوثيق جميع الخدمات المقدمة عن طريق الإنترنت لدى الجهة ● العمل على تحديد جميع المكونات التقنية التي تدعم هذه الخدمات الخارجية، ومنها:

- المواقع الإلكترونية وتطبيقات الويب
- تطبيقات الهواتف الذكية والأجهزة اللوحية
  - يشمل ذلك ما تم نشره على متجر أبل (Apple Store) ومتجر قوقل بلاي (Google Play Store) وغيرها من متاجر التطبيقات
  - يشمل ذلك تطبيقات الهواتف غير المنشورة بالمتاجر والتي تكون خاصة للجهة
- واجهة برمجة التطبيقات
- الخوادم المستخدمة لدى الخدمات الخارجية (مثل خوادم الويب)
- الخوادم المستخدمة لدى خدمات الدخول عن بعد
- الخوادم المستخدمة لدى خدمة البريد الإلكتروني
- أجهزة الشبكة المستخدمة لتقديم الخدمات الخارجية

- تطوير وتنفيذ خطة عمل لاختبار الاختراق شامل ما تم ذكره أعلاه

المخرجات المتوقعة:

- وثيقة سياسة الأمن السيبراني التي تغطي اختبار الاختراق للأصول التالية: جميع الخدمات المقدمة خارجياً (عن طريق الإنترنت) ومكوناتها التقنية ومنها البنية التحتية، المواقع الإلكترونية، تطبيقات الويب، تطبيقات الهواتف الذكية واللوحية، والبريد الإلكتروني والدخول عن بعد.
- موافقة رسمية من قبل رئيس الجهة أو من ينيبه على الوثيقة (مثال: عن طريق البريد الإلكتروني الرسمي للجهة، أو التوقيع الورقي أو الإلكتروني).
- خطة عمل لاختبار الاختراق
- تقارير اختبار الاختراق

٢-١١-٣-٢	عمل اختبار الاختراق دورياً.

إرشادات تطبيق الضوابط:

- العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية.
- تطوير إجراءات لاختبار الاختراق
- تطوير وتنفيذ خطة عمل لاختبار الاختراق يوضح فيه الجدول السنوي الذي يتم اتباعه لاختبارات الاختراق على الأصول المعلوماتية والتقنية المعنية

المخرجات المتوقعة:

- وثيقة سياسة الأمن السيبراني التي تغطي عمل اختبار الاختراق بشكل دوري.
- موافقة رسمية من قبل رئيس الجهة أو من ينيبه على الوثيقة (مثال: عن طريق البريد الإلكتروني الرسمي للجهة، أو التوقيع الورقي أو الإلكتروني).
- خطة عمل لاختبار الاختراق

	• تقارير اختبار الاختراق
٢-١١-٤	يجب مراجعة تطبيق متطلبات الأمن السيبراني لعمليات اختبار الاختراق في الجهة دورياً.
	إرشادات تطبيق الضوابط: • العمل على مراجعة تطبيق متطلبات الأمن السيبراني لاختبار الاختراق للجهة من خلال إجراء تقييم دوري (وذلك حسب خطة موثقة ومعتمدة للمراجعة، وبناء على فترة زمنية محددة "على سبيل المثال، بشكل ربع سنوي") لتنفيذ إجراءات اختبار الاختراق من قبل الإدارة المعنية بالأمن السيبراني وبالتعاون مع الإدارات ذات العلاقة (كالإدارة المعنية بتقنية المعلومات). • مراجعة التطبيق قد تتم من خلال القنوات التقليدية (مثل البريد الإلكتروني) أو قد يكون مؤتمت باستخدام نظام لإدارة الالتزام. الجهة قد تضع خطة مراجعة توضح فيها جدول مراجعة تطبيق متطلبات الأمن السيبراني لاختبار الاختراق للجهة. • مراجعة وتحديث متطلبات الأمن السيبراني الخاصة باختبار الاختراق في الجهة بشكل دوري حسب خطة موثقة ومعتمدة للمراجعة بناءً على فترة زمنية محددة أو في حالة حدوث تغييرات في المتطلبات التشريعية والتنظيمية ذات العلاقة. • توثيق المراجعة والتغييرات التي تتم على متطلبات الأمن السيبراني الخاصة باختبار الاختراق في الجهة واعتمادها من قبل رئيس الجهة أو من ينيبه.
	المخرجات المتوقعة: • نتائج مراجعة تطبيق متطلبات الأمن السيبراني لاختبار الاختراق للجهة. • وثيقة تحدد دورة مراجعة تطبيق متطلبات الأمن السيبراني لاختبار الاختراق (جدول تقييم الالتزام). • وثيقة تقرير تقييم الالتزام توضح تقييم تطبيق متطلبات الأمن السيبراني لاختبار الاختراق • 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. • 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).

٢-١٢	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 الاثار المترتبة على أعمال الجهة.
الضوابط	

٢-١٢-١	يجب تحديد وتوثيق اعتماد متطلبات الأمن السيبراني لإدارة سجلات الأحداث ومراقبة الأمن السيبراني للجهة.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة إدارة سجلات الأحداث ومراقبة الأمن السيبراني **إرشادات تطبيق الضوابط:** • العمل على تطوير وتوثيق سياسة الأمن السيبراني لإدارة سجلات الأحداث ومراقبة الأمن السيبراني في الجهة، وقد تحتوي، على سبيل المثال لا الحصر، على ما يلي: ○ نطاق الأصول المعلوماتية التي يجب تفعيل سجلات الأحداث عليها. ○ تفعيل سجلات الأحداث الخاصة بالأمن السيبراني على الأصول المعلوماتية الحساسة لدى الجهة. ○ تفعيل سجلات الأحداث الخاصة بالحسابات ذات الصلاحيات الهامة والحساسة على الأصول المعلوماتية وأحداث عمليات الدخول عن بعد لدى الجهة. ○ التقنيات اللازمة لجمع سجلات الأحداث الخاصة بالأمن السيبراني المفعلة. ○ المراقبة المستمرة لسجلات الأحداث الخاصة بالأمن السيبراني. ○ مدة الاحتفاظ بسجلات الأحداث الخاصة بالأمن السيبراني (على ألا تقل عن ١٢ شهر). • العمل على ان تكون السياسة في الجهة مدعومة من قبل الإدارة التنفيذية. وذلك من خلال اعتماد وموافقة رئيس الجهة أو من ينيبه.
	المخرجات المتوقعة: • وثيقة سياسة الأمن السيبراني التي تغطي متطلبات إدارة سجلات الأحداث ومراقبة الأمن السيبراني (مثال: نسخة إلكترونية أو نسخة ورقية رسمية). • موافقة رسمية من قبل رئيس الجهة أو من ينيبه على هذه الوثيقة (مثال: عن طريق البريد الإلكتروني الرسمي للجهة، أو التوقيع الورقي أو الإلكتروني).
٢-١٢-٢	يجب تطبيق متطلبات الأمن السيبراني لسجلات الأحداث ومراقبة الأمن السيبراني للجهة.
	إرشادات تطبيق الضوابط: • العمل على تطبيق متطلبات الأمن السيبراني لحماية الأنظمة وأجهزة معالجة المعلومات، وقد تشمل، على سبيل المثال لا الحصر، على الآتي: ○ تحديد نطاق الأصول المعلوماتية التي يجب تفعيل سجلات الأحداث عليها، ويمكن الاستعانة بسجل الأصول المعلوماتية والتقنية الخاصة بالجهة والأصول المذكورة في سجل المخاطر لتحديد النطاق. ○ تفعيل سجلات الأحداث الخاصة بالأمن السيبراني على الأصول المعلوماتية الحساسة لدى الجهة. ○ تفعيل سجلات الأحداث الخاصة بالحسابات ذات الصلاحيات الهامة والحساسة على الأصول المعلوماتية وأحداث عمليات الدخول عن بعد لدى الجهة. ○ تحديد التقنيات اللازمة لجمع سجلات الأحداث الخاصة بالأمن السيبراني المفعلة. ○ تحديد فريق للمراقبة المستمرة لسجلات الأحداث الخاصة بالأمن السيبراني.

	○ تحديد مدة الاحتفاظ بسجلات الأحداث الخاصة بالأمن السيبراني (على ألا تقل عن ١٢ شهر)، والقيام بتحديد هذا البند في العقود والاتفاقيات في حال كان مركز العمليات الأمنية عند مقدم خدمة، والتأكد من الالتزام به.
	المخرجات المتوقعة: ● زيارة لمركز العمليات الأمنية الخاص بالجهة (إن وجد)، بحيث يتم الاطلاع على نظام إدارة المعلومات والأحداث الأمنية بشكل مباشر. ● نسخة من العقد أو الاتفاقية في حال كان مركز العمليات الأمنية أو المراقبة من قبل مقدم خدمة. ● تقرير يوضح ربط جميع الأجهزة والأنظمة الخاصة بالجهة بنظام إدارة المعلومات والأحداث الأمنية. ● جدول تقسيم الورديات الخاص بالجهة بحيث تغطي نموذج المراقبة المتبع.
٢-١٢-٣	يجب أن تغطي متطلبات إدارة سجلات الأحداث ومراقبة الأمن السيبراني بحد أدنى ما يلي:
٢-١٢-٣-١	تفعيل سجلات الأحداث (Event logs) الخاصة بالأمن السيبراني على الأصول المعلوماتية الحساسة لدى الجهة.
	إرشادات تطبيق الضوابط: ● العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية. ● العمل على تفعيل سجلات الأحداث (Event logs) الخاصة بالأمن السيبراني على الأصول المعلوماتية الحساسة لدى الجهة، والتي، على سبيل المثال لا الحصر، قد تتكون من الآتي: ○ أجهزة الشبكة ○ التطبيقات ○ قواعد البيانات ○ الخوادم ○ أجهزة المستخدمين (من خلال نظام الحماية). ● العمل على تفعيل تلك السجلات من خلال إعدادات الأجهزة والأنظمة المذكورة مسبقاً والتي من الممكن التحكم بها من خلال لوحة التحكم الخاصة بها. ● العمل على تطوير عدد من القواعد (Rules) في نظام إدارة المعلومات والأحداث الأمنية بحيث تمكن الفريق الخاص بالمراقبة من متابعة السجلات المفعلة الخاصة بالأصول المعلوماتية الحساسة (بعد القيام بربطها).
	المخرجات المتوقعة: ● وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية). ● لقطة شاشة أو مثال مباشر من لوحة التحكم الخاصة بالأنظمة المذكورة تبين تفعيل سجلات الأحداث.

• لقطة شاشة أو مثال مباشر توضح مراقبة هذه السجلات من خلال نظام إدارة المعلومات والأحداث الأمنية (SIEM).	
٢-٣-١٢-٢	تفعيل سجلات الأحداث الخاصة بالحسابات ذات الصلاحيات الهامة والحساسة على الأصول المعلوماتية وأحداث عمليات الدخول عن بعد لدى الجهة.
إرشادات تطبيق الضوابط: • العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية. • العمل على تفعيل سجلات الأحداث الخاصة بالحسابات ذات الصلاحيات الهامة والحساسة (على سبيل المثال لا الحصر: الحسابات الخاصة بإدارة قواعد البيانات والأنظمة) على: ○ الأصول المعلوماتية، بحيث تكون جميع التغييرات التي تتم من خلالها مسجلة ومحفوظة. ○ أحداث عمليات الدخول عن بعد، حيث أن هذه العمليات يجب أن تكون للحالات الضرورية فقط وأي دخول يتم عن بعد يجب أن يكون مسجلاً لمتابعة التغييرات التي تتم خلالها. • تطوير عدد من القواعد (Rules) في نظام إدارة المعلومات والأحداث الأمنية بحيث تمكن الفريق الخاص للمراقبة من متابعة السجلات المفعلة الخاصة بالحسابات ذات الصلاحيات الهامة والحساسة (بعد القيام بربطها).	
المخرجات المتوقعة: • وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية). • لقطة شاشة أو مثال مباشر توضح تفعيل السجلات الخاصة ببعض الحسابات ذات الصلاحيات الهامة والحساسة في نظام إدارة الصلاحيات. • لقطة شاشة أو مثال مباشر توضح مراقبة هذه السجلات من خلال نظام إدارة المعلومات والأحداث الأمنية (SIEM). • لقطة شاشة أو مثال مباشر توضح تفعيل السجلات الخاصة ببعض الحسابات ذات الصلاحيات الهامة والحساسة في نظام الدخول عن بعد. • لقطة شاشة أو مثال مباشر توضح مراقبة هذه السجلات من خلال نظام إدارة المعلومات والأحداث الأمنية (SIEM).	
٣-٣-١٢-٢	تحديد التقنيات اللازمة (SIEM) لجمع سجلات الأحداث الخاصة بالأمن السيبراني.
إرشادات تطبيق الضوابط: • العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية. • العمل على توفير التقنيات اللازمة (SIEM) لجمع سجلات الأحداث الخاصة بالأمن السيبراني.	

- العمل على تحديد نطاق الأجهزة والأنظمة والتطبيقات التي يتم ربطها بنظام إدارة المعلومات والأحداث الأمنية (SIEM) بناء على حساسيتها، بحيث تحتوي على سبيل المثال لا الحصر:
  - أجهزة المستخدمين (من خلال نظام الحماية)
  - التطبيقات
  - قواعد البيانات
  - أجهزة الشبكة
  - الخوادم
- العمل على ربط جميع أجهزة وأنظمة الجهة الحساسة بما فيها ما ذكر مسبقاً بنظام إدارة المعلومات والأحداث الأمنية (SIEM).
- مراجعة ربط أجهزة وأنظمة الجهة دورياً، بحيث يضمن شمول جميع النطاق المذكور مسبقاً وأي أنظمة وأجهزة استجدت لدى الجهة.

المخرجات المتوقعة:

- وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية).
- زيارة لمركز العمليات الأمنية الخاص بالجهة (إن وجد)، بحيث يتم الاطلاع على نظام إدارة المعلومات والأحداث الأمنية بشكل مباشر.
- تقرير يوضح ربط جميع الأجهزة والأنظمة الخاصة بالجهة بنظام إدارة المعلومات والأحداث الأمنية (على سبيل المثال لا الحصر: قائمة في ملف Excel أو نسخة إلكترونية)، ويتضمن إضافة أي أجهزة أو أنظمة مستجدة في الجهة.
- عقد يوضح فيه ما سبق في حال كان مركز العمليات الأمنية من مقدم خدمة.

٢-١٢-٣-٤	المراقبة المستمرة لسجلات الأحداث الخاصة بالأمن السيبراني.

إرشادات تطبيق الضوابط:

- العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية.
- تحديد فريق للمراقبة المستمرة لسجلات الأحداث الخاصة بالأمن السيبراني أو نظام إدارة المعلومات والأحداث الأمنية (SIEM) واعتماد نموذج المراقبة ٧/٢٤، بحيث تكون المراقبة مستمرة في جميع أيام الأسبوع وخلال جميع ساعات اليوم.
- هذا الفريق من الممكن أن يتكون من موظفين الجهة أو من خلال التعاقد مع خدمة خارجية للمراقبة.
- في حال التعاقد مع خدمة خارجية للمراقبة، بحيث يكون موقع الوصول لنظام إدارة المعلومات والأحداث الأمنية الخاص بالجهة في المملكة، مع الأخذ بالاعتبار أن هذا النظام متواجد أيضا داخل المملكة.

المخرجات المتوقعة:

- وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية).

	• جدول تقسيم الورديات الخاص بالجهة بحيث تغطي نموذج المراقبة المتبع. • عقد يوضح فيه نموذج المراقبة المتبع في حال كان مركز العمليات الأمنية أو المراقبة من قبل مقدم خدمة.
٢-١٢-٣-٥	مدة الاحتفاظ بسجلات الأحداث الخاصة بالأمن السيبراني (على ألا تقل عن ١٢ شهر).
	إرشادات تطبيق الضوابط: • العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية. • العمل على تحديد مدة الاحتفاظ بسجلات الأحداث الخاصة بالأمن السيبراني ل ١٢ شهر على الأقل من خلال إعدادات إدارة نظام إدارة المعلومات والأحداث الأمنية. • العمل على الحصول على المساحة الكافية لحفظ هذه السجلات. • العمل على مراجعة السجلات المحفوظة دورياً للتأكد من أن السجلات، التي لم يمر عليها عام واحد على الأقل، لم يتم استبدالها بالأحدث، وزيادة حجم المساحة في حال حدوث ذلك.
	المخرجات المتوقعة: • وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية). • لقطة شاشة أو دليل مباشر من نظام إدارة المعلومات والأحداث الأمنية يوضح إعدادات حفظ السجلات لـ ١٢ شهر على الأقل. • عينة من السجلات المحفوظة المستخرجة من نظام إدارة المعلومات والأحداث الأمنية بحيث تكون تلك السجلات هي ما قد مر عليها ١٢ شهراً على الأقل.
٢-١٢-٤	يجب مراجعة تطبيق متطلبات إدارة سجلات الأحداث ومراقبة الأمن السيبراني في الجهة دورياً.
	إرشادات تطبيق الضوابط: • العمل على مراجعة تطبيق متطلبات الأمن السيبراني لإدارة الأحداث ومراقبة الأمن السيبراني من خلال إجراء تقييم دوري (وذلك حسب خطة موثقة ومعتمدة للمراجعة، وبناء على فترة زمنية محددة، على سبيل المثال لا الحصر: بشكل ربع سنوي) لتنفيذ متطلبات إدارة الأحداث ومراقبة الأمن السيبراني من قبل الإدارة المعنية بالأمن السيبراني وبالتعاون مع الإدارات ذات العلاقة (كمركز العمليات الأمنية، ان وجد). • العمل على مراجعة التطبيق قد تتم من خلال القنوات التقليدية (مثل البريد الإلكتروني) أو قد يكون مؤتمت باستخدام نظام لإدارة الالتزام. الجهة قد تضع خطة مراجعة توضح فيها جدول مراجعة تطبيق متطلبات الأمن السيبراني لإدارة الأحداث ومراقبة الأمن السيبراني. • العمل على مراجعة وتحديث متطلبات الأمن السيبراني الخاصة بإدارة الأحداث ومراقبة الأمن السيبراني في الجهة بشكل دوري حسب خطة موثقة ومعتمدة للمراجعة بناءً على فترة زمنية محددة أو في حالة حدوث تغييرات في المتطلبات التشريعية والتنظيمية ذات العلاقة.

	• العمل على توثيق المراجعة والتغييرات التي تتم على متطلبات الأمن السيبراني الخاصة بإدارة الأحداث ومراقبة الأمن السيبراني في الجهة واعتمادها من قبل رئيس الجهة أو من ينيبه.
	المخرجات المتوقعة: • نتائج مراجعة تطبيق متطلبات إدارة الأحداث ومراقبة الأمن السيبراني في الجهة. • وثيقة تحدد دورة مراجعة تطبيق متطلبات الأمن السيبراني لإدارة الأحداث ومراقبة الأمن السيبراني في الجهة (جدول تقييم الالتزام). • وثيقة تقرير تقييم الالتزام توضح تقييم تطبيق متطلبات الأمن السيبراني لتطبيق متطلبات إدارة الأحداث ومراقبة الأمن السيبراني في الجهة. • 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. • 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).

٢-١٣	إدارة حوادث وتهديدات الأمن السيبراني (Cybersecurity Incident and Threat Management)
الهدف	ضمان تحديد واكتشاف حوادث الأمن السيبراني في الوقت المناسب وإدارتها بشكل فعال والتعامل مع تهديدات الأمن السيبراني استباقياً من أجل منع أو تقليل الآثار المترتبة على أعمال الجهة. مع مراعاة ما ورد في الامر السامي الكريم رقم ٣٧١٤٠ تاريخ ١٤٣٨/٨/١٤هـ.
٢-١٣-١	يجب تحديد وتوثيق واعتماد متطلبات إدارة حوادث وتهديدات الأمن السيبراني في الجهة.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة إدارة حوادث وتهديدات الأمن السيبراني **إرشادات تطبيق الضوابط:** • العمل على تطوير وتوثيق سياسة الأمن السيبراني لإدارة حوادث وتهديدات الأمن السيبراني في الجهة، وقد تحتوي، على سبيل المثال لا الحصر، على ما يلي: ○ تحديد خطة للاستجابة لحوادث الأمن السيبراني. ○ تصنيف حوادث الأمن السيبراني على حسب مستوى الخطورة. ○ تحديد الأدوار والمسؤوليات الخاصة للاستجابة لحوادث الأمن السيبراني وطريقة التواصل مع جميع المعنيين. ○ آلية تبليغ الهيئة الوطنية للأمن السيبراني عند حدوث حادثة أمن سيبراني.

	○ مشاركة التنبيهات والمعلومات الاستباقية ومؤشرات الاختراق وتقارير حوادث الأمن السيبراني مع الهيئة الوطنية للأمن السيبراني. ○ الحصول على المعلومات الاستباقية والية التعامل معها. ○ المراجعة الدورية لخطة الاستجابة لحوادث الأمن السيبراني. ● العمل على ان تكون السياسة في الجهة مدعومة من قبل الإدارة التنفيذية. وذلك من خلال اعتماد وموافقة رئيس الجهة أو من ينيبه.
	المخرجات المتوقعة: ● وثيقة سياسة الأمن السيبراني التي تغطي متطلبات إدارة حوادث وتهديدات الأمن السيبراني (مثال: نسخة إلكترونية أو نسخة ورقية رسمية). ● موافقة رسمية من قبل رئيس الجهة أو من ينيبه على هذه الوثيقة (مثال: عن طريق البريد الإلكتروني الرسمي للجهة، أو التوقيع الورقي أو الإلكتروني).
٢-١٣-٢	يجب تطبيق متطلبات إدارة حوادث وتهديدات الأمن السيبراني في الجهة.
	إرشادات تطبيق الضوابط: ● العمل على تطبيق كافة متطلبات الأمن السيبراني لإدارة حوادث وتهديدات الأمن السيبراني، وقد تشمل، على سبيل المثال لا الحصر، على الآتي: ○ تحديد خطة للاستجابة لحوادث الأمن السيبراني. ○ تصنيف حوادث الأمن السيبراني على حسب مستوى الخطورة. ○ تحديد الأدوار والمسؤوليات الخاصة للاستجابة لحوادث الأمن السيبراني وطريقة التواصل مع جميع المعنيين. ○ تحديد آلية تبليغ الهيئة الوطنية للأمن السيبراني عند حدوث حادثة أمن سيبراني. ○ مشاركة التنبيهات والمعلومات الاستباقية ومؤشرات الاختراق وتقارير حوادث الأمن السيبراني مع الهيئة الوطنية للأمن السيبراني. ○ الحصول على المعلومات الاستباقية والية التعامل معها. ○ المراجعة الدورية لخطة الاستجابة لحوادث الأمن السيبراني.
	المخرجات المتوقعة: ● الخطة المعتمدة للاستجابة لحوادث الأمن السيبراني (نسخة إلكترونية). ● عينة من تقرير حادثة أمن سيبراني سابقة. ● آليه تصنيف حوادث الأمن السيبراني حسب مستوى الخطورة.
٢-١٣-٣	يجب أن تغطي متطلبات إدارة حوادث وتهديدات الأمن السيبراني بحد أدنى ما يلي:
٢-١٣-٣-١	وضع خطط الاستجابة للحوادث الأمنية وآليات التصعيد.

أدوات الأمن السيبراني ذات العلاقة:

- نموذج خطة إدارة الأحداث
- نموذج إجراءات إدارة الأحداث

إرشادات تطبيق الضوابط:

- العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية.
- العمل على بناء خطط الاستجابة لحوادث الأمن السيبراني، بحيث تحتوي على:
  - إيضاح لأنواع الحوادث وتصنيفها حسب مستوى خطورتها على عمل الجهة.
  - تحديد الأدوار والمسؤوليات الخاصة للاستجابة لحوادث الأمن السيبراني وطريقة التواصل مع جميع المعنيين.
  - تحديد طرق وقنوات التواصل المخصصة لحالات الطوارىء
  - تحديد خطط تفصيلية (Playbook) الاستجابة للحوادث، بحيث تحتوي على التالي:
    - تصنيف الحادثة حسب حدتها، ومستوى الاستجابة المطلوبة، والجهات التي يجب أن تشارك في أنشطة الاستجابة.
    - الابلاغ عن تهديدات وحوادث الأمن السيبراني لكل من الهيئة.
    - تحديد إجراءات سير العمل في الاستجابة لحوادث الأمن السيبراني وفق ماتصدره الهيئة الوطنية للأمن السيبراني.
- العمل على إنشاء تقرير لحادثة الأمن السيبراني عند الانتهاء من الاستجابة، بحيث يحتوي، على سبيل المثال لا الحصر، على التالي:
  - الأشخاص المشاركين في الاستجابة للحادثة ووسيلة التواصل.
  - المعلومات الأساسية للحادثة، على سبيل المثال لا الحصر: التاريخ والوقت، نطاق الحادثة، مستوى الخطورة.. الخ.
  - ملخص الحادثة.
  - خطوات الاحتواء والإزالة.
  - التوصيات الحالية والمستقبلية.
- العمل على مراجعة خطة الاستجابة بشكل دوري وتحديثها في حال لزم ذلك.

المخرجات المتوقعة:

- وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية).
- الخطة المعتمدة للاستجابة لحوادث الأمن السيبراني (نسخة إلكترونية).
- عينة من تقرير حادثة أمن سيبراني سابقة.

٢-١٣-٣-٢	تصنيف حوادث الأمن السيبراني.

إرشادات تطبيق الضوابط:

- العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية.
- العمل على تحديد آليه تصنيف حوادث الأمن السيبراني في الجهة والإشارة إليها في سياسة الاستجابة للحوادث والحرص على موائمتها مع آليه تصنيف المخاطر المعتمدة لدى الجهة.
- العمل على تصنيف الحوادث في حال حدوثها وتحديد مدة وآلية التعامل مع هذه الحوادث بناء على آلية التصنيف المتبعة.
- العمل على توثيق ذلك التصنيف في تقرير حادثة الأمن السيبراني.

المخرجات المتوقعة:

- وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية).
- وثيقة توضح آليه تصنيف حوادث الأمن السيبراني حسب الحساسية ومستوى الخطورة.
- عينة من تقرير حادثة أمن سيبراني يوضح فيها تصنيف الحادثة والبلاغ

٢-١٣-٣-٣	تبليغ الهيئة عند حدوث حادثة أمن سيبراني.

إرشادات تطبيق الضوابط:

- العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية.
- العمل على تحديد إجراءات موثقة لتبليغ الهيئة الوطنية للأمن السيبراني في حال حدوث حادثة أمن سيبراني، بحيث تحتوي على:
  - الأدوار والمسؤوليات الخاصة بالجهة للاستجابة لحوادث الأمن السيبراني وطريقة التواصل مع جميع المعنيين.
  - المعلومات الأساسية للحادثة، على سبيل المثال لا الحصر: التاريخ والوقت، نطاق الحادثة، مستوى الخطورة.. الخ.
  - ملخص الحادثة.
- العمل على تبليغ الهيئة عند حدوث حادثة أمن السيبراني من خلال القنوات المعتمدة لدى الهيئة والمتمثلة في: منصة حصين/البريد الإلكتروني الرسمي الخاص بالهيئة للتبليغ عن الحوادث"is@nca.gov.sa" ، ومتابعة المستجدات والتعليمات التي قد تصدرها الهيئة بشأن التبليغ عن الحوادث باستمرار.

المخرجات المتوقعة:

- وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية).
- نسخة من ملف الإجراءات المتبعة لتبليغ الهيئة عن حوادث الأمن السيبراني.
- عينة من تبليغ الهيئة عن حادثة أمن سيبراني سابقة، على سبيل المثال لا الحصر: لقطة شاشة أو دليل مباشر من البريد الالكتروني المرسل للهيئة.

٢-١٣-٣-٤	مشاركة التنبيهات والمعلومات الاستباقية ومؤشرات الاختراق وتقارير حوادث الأمن السيبراني مع الهيئة.

إرشادات تطبيق الضوابط:

- العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية.
- العمل على تحديد إجراءات موثقة لمشاركة الهيئة الوطنية للأمن السيبراني التالي:
  - التنبيهات والمعلومات الاستباقية ومؤشرات الاختراق التي قد ترفع مستوى الاشتباه لحصول حادثة أمن سيبراني.
  - تقارير حوادث الأمن السيبراني بعد الانتهاء من التعامل مع الحادثة.
- العمل على مشاركة التنبيهات والمعلومات الاستباقية ومؤشرات الاختراق وتقارير الحوادث مع الهيئة من خلال البريد الإلكتروني الرسمي للتسجيل في عضوية مشاركة المعلومات "is@nca.gov.sa"، ومتابعة المستجدات والتعليمات التي قد تصدرها الهيئة بشأن التبليغ عن التنبيهات والمعلومات الاستباقية ومؤشرات الاختراق باستمرار.

المخرجات المتوقعة:

- وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية).
- الإجراءات المتبعة لمشاركة التنبيهات والمعلومات الاستباقية ومؤشرات الاختراق مع الهيئة (على سبيل المثال لا الحصر: بريد الكتروني سابق تم ارسال تقرير المؤشرات مع الهيئة من خلاله).
- عينة من ارسال تقرير حادثة أمن سيبراني مع الهيئة (على سبيل المثال لا الحصر: بريد الكتروني سابق تم ارسال تقرير حادثة امن سيبراني مع الهيئة من خلاله).

٢-١٣-٣-٥	الحصول على المعلومات الاستباقية (Threat Intelligence) والتعامل معها.

إرشادات تطبيق الضوابط:

- العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية.
- العمل على الاشتراك مع المنصات المسؤولة عن ارسال المعلومات الاستباقية (Threat Intelligence) عن طريق البريد الإلكتروني أو المنصات التقنية الأخرى، ومن هذه المنصات:
  - المركز الوطني الإرشادي للأمن السيبراني (Saudi CERT).
  - منصة مشاركة المعلومات الخاصة بحصين.
  - النشرة البريدية الخاصة بهيئة الاتصالات وتقنية المعلومات.
  - النشرات المقدمة من قبل الشركات المختصة بالأمن السيبراني.
  - النشرات المقدمة من قبل مقدمي الخدمات الأمنية والتقنية التي تم التعاقد معها مسبقاً من قبل الجهة.
- العمل على التعامل مع التنبيهات المرسلة من قبل هذه المنصات من خلال:

	○ ارسالها للفريق المعني للتعامل معها (على سبيل المثال لا الحصر: إدارة تقنية المعلومات، مركز العمليات الأمنية، الإدارة الخاصة بالتحديثات والثغرات). ○ تحديد مدة للتعامل مع هذه التنبيهات حسب مستوى الخطورة. ○ المتابعة المستمرة للتأكد من انه تم التعامل مع التنبيهات المرسلة للفريق المعني بشكل أمن (على سبيل المثال لا الحصر: التأكد من تطبيق التحديث الخاص بالثغرات المرسلة). **المخرجات المتوقعة:** • وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية). • لقطة شاشة أو دليل مباشر توضح اشتراك الجهة مع أحد المنصات. • لقطة شاشة أو دليل حي لمثال من التنبيهات التي تم التعامل معها مسبقاً حسب الإجراءات اللازمة.
٢-١٣-٤	يجب مراجعة تطبيق إدارة حوادث وتهديدات الأمن السيبراني في الجهة دورياً. **إرشادات تطبيق الضوابط:** • العمل على مراجعة تطبيق متطلبات الأمن السيبراني لإدارة حوادث وتهديدات الأمن السيبراني في الجهة من خلال إجراء تقييم دوري (وذلك حسب خطة موثقة ومعتمدة للمراجعة، وبناء على فترة زمنية محددة "على سبيل المثال لا الحصر، بشكل ربع سنوي") لتنفيذ متطلبات إدارة حوادث وتهديدات الأمن السيبراني من قبل الإدارة المعنية بالأمن السيبراني وبالتعاون مع الإدارات ذات العلاقة (كالإدارة المعنية بإدارة الحوادث). • العمل على مراجعة التطبيق قد تتم من خلال القنوات التقليدية (مثل البريد الإلكتروني) أو قد يكون مؤتمت باستخدام نظام لإدارة الالتزام. الجهة قد تضع خطة مراجعة توضح فيها جدول مراجعة تطبيق متطلبات الأمن السيبراني لإدارة حوادث وتهديدات الأمن السيبراني في الجهة. • العمل على مراجعة وتحديث متطلبات الأمن السيبراني الخاصة بإدارة حوادث وتهديدات الأمن السيبراني في الجهة بشكل دوري حسب خطة موثقة ومعتمدة للمراجعة بناءً على فترة زمنية محددة أو في حالة حدوث تغييرات في المتطلبات التشريعية والتنظيمية ذات العلاقة. • العمل على توثيق المراجعة والتغييرات التي تتم على متطلبات الأمن السيبراني الخاصة بإدارة حوادث وتهديدات الأمن السيبراني في الجهة واعتمادها من قبل رئيس الجهة أو من ينيبه. **المخرجات المتوقعة:** • نتائج مراجعة تطبيق متطلبات إدارة حوادث وتهديدات الأمن السيبراني في الجهة. • وثيقة تحدد دورة مراجعة تطبيق متطلبات الأمن السيبراني لإدارة حوادث وتهديدات الأمن السيبراني في الجهة (جدول تقييم الالتزام). • وثيقة تقرير تقييم الالتزام توضح تقييم تطبيق متطلبات الأمن السيبراني لتطبيق متطلبات إدارة حوادث وتهديدات الأمن السيبراني في الجهة.

٢-١٤	الأمن المادي (Physical Security)
الهدف	ضمان حماية الأصول المعلوماتية والتقنية للجهة من الوصول المادي غير المصرح به والفقدان والسرقة والتخريب.
الضوابط	
٢-١٤-١	يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني لحماية الأصول المعلوماتية والتقنية للجهة من الوصول المادي غير المصرح به والفقدان والسرقة والتخريب.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني المتعلق بالأمن المادي **إرشادات تطبيق الضوابط:** • العمل على تضمين وتوثيق متطلبات الأمن السيبراني لحماية الأصول المعلوماتية والتقنية للجهة من الوصول المادي غير المصرح به والمخاطر السيبرانية ومن هذه المتطلبات وعلى سبيل المثال لا الحصر: ○ الدخول المصرح به للأماكن الحساسة في الجهة. ○ سجلات الدخول والمراقبة(CCTV). ○ حماية معلومات سجلات الدخول والمراقبة. ○ أمن إتلاف وإعادة استخدام الأصول المادية التي تحوي معلومات مصنفة. ○ أمن الأجهزة والمعدات داخل مباني الجهة وخارجها. • العمل على ان تكون متطلبات الأمن السيبراني لحماية الأصول المعلوماتية والتقنية للجهة من الوصول المادي غير المصرح به مدعومة من قبل الإدارة التنفيذية. وذلك من خلال اعتماد وموافقة رئيس الجهة أو من ينيبه.
	المخرجات المتوقعة: • وثيقة سياسة الأمن السيبراني التي تغطي متطلبات حماية الأصول المعلوماتية والتقنية للجهة من الوصول المادي غير المصرح به والمخاطر السيبرانية (نسخة إلكترونية أو نسخة ورقية رسمية). • موافقة رسمية من قبل رئيس الجهة أو من ينيبه على الوثيقة (مثال: عن طريق البريد الإلكتروني الرسمي للجهة، أو التوقيع الورقي أو الإلكتروني).
٢-١٤-٢	يجب تطبيق متطلبات الأمن السيبراني لحماية الأصول المعلوماتية والتقنية للجهة من الوصول المادي غير المصرح به والفقدان والسرقة والتخريب.
	إرشادات تطبيق الضوابط: • العمل على تطبيق كافة متطلبات الأمن السيبراني عند تطبيق إجراءات حماية الأصول المعلوماتية والتقنية من الوصول المادي غير المصرح به والفقدان والسرقة والتخريب في الجهة، كما يجب أن تغطي الإجراءات للجهة بحد أدنى ما يلي وعلى سبيل المثال لا الحصر:

		○ الدخول المصرح به للأماكن الحساسة في الجهة. ○ سجلات الدخول والمراقبة(CCTV). ○ حماية معلومات سجلات الدخول والمراقبة. ○ أمن إتلاف وإعادة استخدام الأصول المادية التي تحوي معلومات مصنفة. ○ أمن الأجهزة والمعدات داخل مباني الجهة وخارجها. • العمل على وضع خطة عمل لتطبيق كافة متطلبات الأمن السيبراني المتعلقة بحماية الأصول المعلوماتية والتقنية من الوصول المادي غير المصرح به والفقدان والسرقة والتخريب. • تضمين متطلبات الأمن السيبراني المتعلقة بحماية الأصول المعلوماتية والتقنية من الوصول المادي غير المصرح به والفقدان والسرقة والتخريب في إجراءات حمايتها لضمان الالتزام بمتطلبات الأمن السيبراني لجميع أصحاب المصلحة الداخليين والخارجيين.
		المخرجات المتوقعة: • وثائق تؤكد تطبيق متطلبات الأمن السيبراني المتعلقة بحماية الأصول المعلوماتية والتقنية من الوصول المادي غير المصرح به والفقدان والسرقة والتخريب والتي تم توثيقها في وثيقة السياسات. • وثيقة خطة عمل لتطبيق متطلبات الأمن السيبراني لحماية الأصول المعلوماتية والتقنية من الوصول المادي غير المصرح به والفقدان والسرقة والتخريب للجهة. • دليل يوضح تطبيق ضوابط حماية الأصول المعلوماتية والتقنية من الوصول المادي غير المصرح به والفقدان والسرقة والتخريب الجهة، على سبيل المثال لا الحصر: ○ نموذج طلب دخول مستخدم تم اعتماده والموافقة عليه. ○ جدولة زيارة إلى غرفة سجلات الدخول والمراقبة CCTV لتقييم عملية المراقبة والأجهزة المستخدمة. ○ جدولة زيارة إلى غرفة التخزين الآمنة التي تحتوي على السجلات المؤرشفة. ○ عينة من تطبيق إتلاف الوسائط الرقمية (مثال: بريد إلكتروني). ○ إجراءات أمن الأجهزة والمعدات داخل مباني الجهة وخارجها الموثقة والمعتمدة من قبل صاحب الصلاحية.
٢-١٤-٣	يجب أن تغطي متطلبات الأمن السيبراني لحماية الأصول المعلوماتية والتقنية للجهة من الوصول المادي غير المصرح به والفقدان والسرقة والتخريب للجهة بحد أدنى ما يلي:	
٢-١٤-٣-١	الدخول المصرح به للأماكن الحساسة في الجهة (مثل: مركز بيانات الجهة، مركز التعافي من الكوارث، أماكن معالجة المعلومات الحساسة، مركز المراقبة الأمنية، غرف اتصالات الشبكة، مناطق الإمداد الخاصة بالأجهزة والعتاد التقنية، وغيرها).	
		إرشادات تطبيق الضوابط: • العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية. • العمل على تحديد نطاق الأماكن الحساسة الخاصة بالجهة والتي تشمل (على سبيل المثال لا الحصر):

	○ مراكز البيانات. ○ مركز التعافي من الكوارث. ○ أماكن معالجة المعلومات الحساسة. ○ مركز المراقبة الأمنية. ○ غرف اتصالات الشبكة. ○ مناطق الإمداد الخاصة بالأجهزة والعتاد التقنية. ● العمل على تطوير نموذج طلب دخول إلى الأماكن الحساسة حيث يشمل (على سبيل المثال لا الحصر): ○ اسم الشخص المعني بالدخول. ○ سبب طلب دخول الشخص المعني. ○ فترة الدخول للشخص المعني. ● العمل على تطوير إجراءات موافقة لطلب الدخول من قبل أصحاب الصلاحية. ● العمل على تحديد آلية الدخول للأماكن الحساسة (مثال: الدخول بالبطاقة، الدخول ببصمة الإصبع، الدخول ببصمة الوجه، وغيرها). ● العمل على الحد من صلاحية إدارة نظام الوصول المادي إلى أشخاص بصلاحيات محددة يمكن تدقيقها ومراجعتها. ● العمل على إنشاء جدول دوري لمراجعة وتحديث صلاحيات الوصول المادي للمناطق الحساسة. ● العمل على مراجعة صلاحيات الدخول بناء على الجدول الدوري الذي تم إنشاؤه. ● العمل على إلغاء صلاحيات الدخول بعد انتهاء المدة الموثقة بنموذج الطلب المعتمد من قبل صاحب الصلاحية. ● العمل على عدم منح الأطراف الخارجية صلاحية وصول مادي لمرافق الجهة إلا بعد تحقيق اشتراطات أمنية، على أن يتم مراقبة وصولهم ومرافقتهم في الأماكن التي تتطلب ذلك.
	المخرجات المتوقعة: ● وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية) (مثال: نسخة إلكترونية أو نسخة ورقية رسمية). ● نموذج طلب دخول مستخدم تم اعتماده والموافقة عليه. ● جدولة زيارة إلى أحد الأماكن الحساسة (مركز البيانات على سبيل المثال لا الحصر) لتقييم عملية الدخول ● دليل يثبت إلغاء صلاحيات الدخول بعد انتهاء المدة الموثقة على نموذج الطلب المعتمد (مثال: عن طريق البريد الإلكتروني)
٢-١٤-٣-٢	سجلات الدخول والمراقبة (CCTV).
	إرشادات تطبيق الضوابط:

- العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية.
- العمل على تحديد نطاق سجلات الدخول والمراقبة والتي تشمل (على سبيل المثال لا الحصر):
  - جميع المباني الخاصة للجهة، والتي يشمل المبنى الرئيسي للجهة وجميع فروعها.
  - الأماكن الحساسة بناء على تقييم المخاطر، والتي يشمل مراكز البيانات وغرف الاتصالات.
- العمل على وجود سجلات المراقبة لجميع المباني الخاصة بالجهة من عدة جوانب وأهمها:
  - داخل المبنى.
  - خارج المبنى.
  - ممرات المبنى.
  - عند أبواب الدخول والمغادرة.

المخرجات المتوقعة:

- وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية) (مثال: نسخة إلكترونية أو نسخة ورقية رسمية).
- جدولة زيارة إلى غرفة سجلات الدخول والمراقبة CCTV لتقييم عملية المراقبة والأجهزة المستخدمة.
- جدولة زيارة إلى مباني الجهة التي تشمل كاميرات المراقبة لتقييم فعاليتها وأماكن تثبيتها ونطاق مراقبتها.

٢-١٤-٣-٣	حماية معلومات سجلات الدخول والمراقبة.

إرشادات تطبيق الضوابط:

- العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية.
- العمل على إعتماد مكان منفصل يشمل سجلات الدخول والمراقبة لضمان حمايتها.
- العمل على إتخاذ الإجراءات اللازمة لتجنب فقدان السجلات. (مثل: النسخ الإحتياطي).
- العمل على حماية السجلات ومصادر المعلومات ونظام الـ(DVR) من الوصول غير المصرّح به.
- العمل على توثيق وتحديد مدة للاحتفاظ بسجلات الدخول والمراقبة.
- العمل على تطوير خطة دورية لأرشفة سجلات الدخول والمراقبة.
- العمل على أرشفة سجلات الدخول والمراقبة حسب الخطة الدورية في غرفة تخزين آمنة تحتوي على أجهزة مراقبة CCTV.

المخرجات المتوقعة:

- وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية) (مثال: نسخة إلكترونية أو نسخة ورقية رسمية).

• جدولة زيارة إلى غرفة سجلات الدخول والمراقبة CCTV للتأكد من حماية سجلات الدخول والمراقبة بمكان منفصل ووصول آمن. • جدولة زيارة إلى غرفة التخزين الآمنة التي تحتوي على السجلات المؤرشفة.	
٢-١٤-٣-٤	أمن إتلاف وإعادة استخدام الأصول المادية التي تحتوي معلومات مصنفة (وتشمل: الوثائق الورقية ووسائط الحفظ والتخزين).
إرشادات تطبيق الضوابط: • العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية. • العمل على تحديد نطاق الأصول المادية التي تحتوي على معلومات مصنفة والتي تشمل (على سبيل المثال لا الحصر): ○ الوثائق الورقية. ○ وسائط الحفظ والتخزين. • العمل على تطوير منهجية وإجراءات لإتلاف الأصول المادية التي تحوي معلومات مصنفة. • العمل على توفير الأجهزة اللازمة لإتلاف الأصول المادية التي تحوي معلومات مصنفة والتي تشمل (على سبيل المثال لا الحصر): ○ آلة تقطيع الورق. ○ آلة إتلاف الأقراص الصلبة. • العمل على تطوير منهجية وإجراءات لإعادة استخدام الأصول المادية التي تحوي معلومات مصنفة، وتشمل طرق لمحو ومسح المعلومات مثل إزالة المغنطة (degaussing) والملء بالأصفار (zero filling) • العمل على توثيق واعتماد إجراءات لإعادة استخدام الأصول المادية على تحتوي على معلومات مصنفة.	
المخرجات المتوقعة: • وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية) (مثال: نسخة إلكترونية أو نسخة ورقية رسمية). • عينة من تطبيق إتلاف الوثائق الورقية (مثال: بريد إلكتروني موجه إلى أصحاب المصلحة يؤكد إتلاف العينة). • عينة من تطبيق إتلاف الوسائط الرقمية (مثال: بريد إلكتروني). • إجراءات إعادة استخدام الأصول المادية التي تحتوي على معلومات مصنفة الموثقة والمعتمدة من صاحب الصلاحية. • عينة من تطبيق إجراء إعادة استخدام الأصول المادية التي تحتوي على معلومات مصنفة (مثال: نسخة من الوثائق الورقية التي تم إتلافها ومشاركتها).	
٢-١٤-٣-٥	أمن الأجهزة والمعدات داخل مباني الجهة وخارجها.

	إرشادات تطبيق الضوابط: • العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية. • العمل على تحديد نطاق الأجهزة والمعدات داخل مباني الجهة وخارجها والتي تشمل (على سبيل المثال لا الحصر): ○ مراكز البيانات. ○ مركز التعافي من الكوارث. ○ أماكن معالجة المعلومات الحساسة. ○ مركز المراقبة الأمنية. ○ غرف اتصالات الشبكة. ○ مناطق الإمداد الخاصة بالأجهزة والعتاد التقنية. • العمل على تطوير إجراءات خاصة بأمن الأجهزة والمعدات داخل مباني الجهة وخارجها. • العمل على تطوير خطة موثقة ومعتمدة لصيانة الأجهزة والمعدات داخل مباني الجهة وخارجها. • الاستعانة بالحلول التقنية وبرامج حماية الأجهزة داخل المباني وخارجها. • العمل على صيانة المعدات والأجهزة داخل المباني وخارجها بشكل دوري. • العمل على تطوير واعتماد لائحة وإجراءات الأمن المادي والسلامة خاصة بالجهة بحيث تشمل تحديداً دقيقاً للواجبات والمهام لتكون بمثابة إطار عام لخدمة السلامة في سبيل حماية الأرواح والأصول والمعلومات.
	المخرجات المتوقعة: • وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية) (مثال: نسخة إلكترونية أو نسخة ورقية رسمية). • إجراءات أمن الأجهزة والمعدات داخل مباني الجهة وخارجها الموثقة والمعتمدة من قبل صاحب الصلاحية. • عينة من تطبيق أمن الأجهزة والمعدات داخل مباني الجهة وخارجها (مثال: جدول الصيانة المُوضح فيه تواريخ المراجعة)
٢-١٤-٤	يجب مراجعة تطبيق متطلبات الأمن السيبراني لحماية الأصول المعلوماتية والتقنية للجهة من الوصول المادي غير المصرح به والفقدان والسرقة والتخريب دورياً.
	إرشادات تطبيق الضوابط: • العمل على مراجعة تطبيق متطلبات الأمن السيبراني لحماية الأصول المعلوماتية والتقنية للجهة من الوصول المادي غير المصرح به والفقدان والسرقة والتخريب للجهة من خلال إجراء تقييم دوري (وذلك حسب خطة موثقة ومعتمدة للمراجعة، وبناء على فترة زمنية محددة "على سبيل المثال، بشكل ربع سنوي") لحماية الأصول المعلوماتية والتقنية للجهة من الوصول المادي غير المصرح به والفقدان والسرقة والتخريب من قبل الإدارة المعنية بالأمن السيبراني وبالتعاون مع الإدارات ذات العلاقة (كالإدارة المعنية بالأمن والسلامة).

	• مراجعة التطبيق قد تتم من خلال القنوات التقليدية (مثل البريد الإلكتروني) أو قد يكون مؤتمت باستخدام نظام لإدارة الالتزام. الجهة قد تضع خطة مراجعة توضح فيها جدول مراجعة تطبيق متطلبات الأمن السيبراني لحماية الأصول المعلوماتية والتقنية للجهة من الوصول المادي غير المصرح به والفقدان والسرقة والتخريب للجهة. • مراجعة وتحديث متطلبات الأمن السيبراني الخاصة بحماية الأصول المعلوماتية والتقنية للجهة من الوصول المادي غير المصرح به والفقدان والسرقة والتخريب للجهة بشكل دوري حسب خطة موثقة ومعتمدة للمراجعة بناءً على فترة زمنية محددة أو في حالة حدوث تغييرات في المتطلبات التشريعية والتنظيمية ذات العلاقة. • توثيق المراجعة والتغييرات التي تتم على متطلبات الأمن السيبراني لحماية الأصول المعلوماتية والتقنية للجهة من الوصول المادي غير المصرح به والفقدان والسرقة والتخريب في الجهة واعتمادها من قبل رئيس الجهة أو من ينيبه.
	المخرجات المتوقعة: • نتائج مراجعة تطبيق متطلبات الأمن السيبراني لحماية الأصول المعلوماتية والتقنية للجهة من الوصول المادي غير المصرح به والفقدان والسرقة والتخريب. • وثيقة تحدد دورة مراجعة تطبيق متطلبات الأمن السيبراني لحماية الأصول المعلوماتية والتقنية للجهة من الوصول المادي غير المصرح به والفقدان والسرقة والتخريب (جدول تقييم الالتزام). • وثيقة تقرير تقييم الالتزام توضح تقييم تطبيق متطلبات الأمن السيبراني لحماية الأصول المعلوماتية والتقنية للجهة من الوصول المادي غير المصرح به والفقدان والسرقة والتخريب. • 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. • 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).

٢-١٥	حماية تطبيقات الويب (Web Application Security)
الهدف	ضمان حماية تطبيقات الويب الخارجية للجهة من المخاطر السيبرانية.
الضوابط	
٢-١٥-١	يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني لحماية تطبيقات الويب الخارجية للجهة من المخاطر السيبرانية.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة حماية تطبيقات الويب

	إرشادات تطبيق الضوابط: • العمل على تضمين وتوثيق متطلبات الأمن السيبراني لحماية تطبيقات الويب الخارجية للجهة من المخاطر السيبرانية ومن هذه المتطلبات وعلى سبيل المثال لا الحصر: ○ استخدام جدار الحماية لتطبيقات الويب (Web Application Firewall). ○ استخدام مبدأ المعمارية متعددة المستويات (Multi-tier Architecture). ○ استخدام بروتوكولات آمنة مثل بروتوكول(HTTPS). ○ استخدام معايير تطوير وتحديث التطبيقات واختبارها ○ توضيح سياسة الاستخدام الآمن للمستخدمين. ○ التحقق من الهوية متعدد العناصر (Multi-Factor Authentication) لعمليات دخول المستخدمين. ○ الفحص بحثاً عن نقاط الضعف الخاصة بالتطبيق (Vulnerability Assessment). ○ النسخ الاحتياطي بانتظام في مواقع آمنة (Backup Log Files). ○ الفحص المنتظم للمنافذ المفتوحة والخدمات والعمليات والبروتوكولات غير المستخدمة (Regular screening of open ports, services, processes, and unused protocols). • العمل على ان تكون متطلبات الأمن السيبراني لحماية تطبيقات الويب الخارجية مدعومة من قبل الإدارة التنفيذية. وذلك من خلال اعتماد وموافقة رئيس الجهة أو من ينيبه.
	المخرجات المتوقعة: • وثيقة سياسة الأمن السيبراني التي تغطي متطلبات حماية تطبيقات الويب الخارجية للجهة من المخاطر السيبرانية (نسخة إلكترونية أو نسخة ورقية رسمية). • موافقة رسمية من قبل رئيس الجهة أو من ينيبه على الوثيقة (مثال: عن طريق البريد الإلكتروني الرسمي للجهة، أو التوقيع الورقي أو الإلكتروني).
٢-١٥-٢	يجب تطبيق متطلبات الأمن السيبراني لحماية تطبيقات الويب الخارجية للجهة.
	إرشادات تطبيق الضوابط: • العمل على تطبيق كافة متطلبات الأمن السيبراني عند تطبيق إجراءات حماية تطبيقات الويب الخارجية في الجهة، كما يجب أن تغطي إجراءات حماية تطبيقات الويب الخارجية للجهة بحد أدنى ما يلي وعلى سبيل المثال لا الحصر: ○ استخدام جدار الحماية لتطبيقات الويب (Web Application Firewall). ○ استخدام مبدأ المعمارية متعددة المستويات (Multi-tier Architecture). ○ استخدام بروتوكولات آمنة مثل بروتوكول(HTTPS). ○ توضيح سياسة الاستخدام الآمن للمستخدمين. ○ التحقق من الهوية متعدد العناصر (Multi-Factor Authentication) لعمليات دخول المستخدمين.

	• العمل على وضع خطة عمل لتطبيق كافة متطلبات الأمن السيبراني المتعلقة بحماية تطبيقات الويب الخارجية. • تضمين متطلبات الأمن السيبراني المتعلقة بحماية تطبيقات الويب الخارجية في إجراءات حماية التطبيقات في الجهة لضمان الالتزام بمتطلبات الأمن السيبراني لجميع أصحاب المصلحة الداخليين والخارجيين.
	المخرجات المتوقعة: • وثائق تؤكد تطبيق متطلبات الأمن السيبراني المتعلقة بحماية تطبيقات الويب الخارجية والتي تم توثيقها في وثيقة السياسات. • وثيقة خطة عمل لتطبيق متطلبات الأمن السيبراني لحماية تطبيقات الويب الخارجية للجهة. • دليل يوضح تطبيق ضوابط حماية تطبيقات الويب الجهة، على سبيل المثال لا الحصر: o لقطة شاشة لنظام جدار حماية التطبيقات WAF المستخدم بالجهة. o عينة من تصاميم تطبيقات الويب التي توضح استخدام مبدأ المعمارية متعددة المستويات لأحد تطبيقات الويب الخاصة بالجهة. o لقطة شاشة من تطبيق الويب يوضح فيه استخدام بروتوكول HTTPS في الرابط الخاص به. o لقطة شاشة من موقع الجهة يوضح فيه نشر سياسة الاستخدام الآمن للمستخدمين. o لقطات شاشة متعددة يوضح فيها عملية الدخول والتي تشمل التحقق من الهوية متعدد العناصر MFA.
٢-١٥-٣	يجب أن تغطي متطلبات الأمن السيبراني لحماية تطبيقات الويب الخارجية للجهة بحد أدنى ما يلي:
	٢-١٥-٣-١ استخدام جدار الحماية لتطبيقات الويب (Web Application Firewall).
	إرشادات تطبيق الضوابط: • العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية. • العمل على تحديد تطبيقات الويب والتي تشمل: o التطبيقات الخارجية التي تم شراؤها. o التطبيقات التي يتم تطويرها داخلياً. • في حال وجود تطبيقات ويب تم شراؤها وتشغيلها من طرف خارجي، يجب: o التأكد من التزام المورد بسياسات ومعايير الأمن السيبراني والتي تشمل استخدام نظام جدار حماية لتطبيقات الويب. • في حال وجود تطبيقات يتم تطويرها داخلياً أو تطبيقات ويب تم شراؤها من طرف خارجي ولكن يتم تشغيلها بالجهة، يجب: o العمل على تحديد تقنيات جدار الحماية التي ترغب الجهة في اقتناءها والتي تشمل على سبيل المثال لا الحصر: ▪ جدار حماية يحتوي على قواعد مُدارة مسبقًا ومُدارة من قِبل النظام نفسه.

	▪ جدار حماية يحتوي على خيار تخصيص القواعد من قبل الجهة. ○ العمل على تحديد وتعيين عدة أنظمة جدار حماية للتطبيقات تشمل التقنيات المرادة من قبل الجهة مع تخصيص الجوانب الإيجابية والسلبية لكل نظام على حدة. ○ العمل على تحديد وتعيين نظام جدار حماية معين ليتم استخدامه لتطبيقات الويب الخارجية للجهة ○ العمل على تطبيق وتنزيل نظام جدار الحماية لجميع تطبيقات الويب المُشغلة من قبل الجهة. ● العمل على إدراج تطبيق وتنزيل جدار الحماية في دورة حياة تطوير التطبيقات لضمان حماية التطبيقات المُراد تطويرها مستقبلاً.
	المخرجات المتوقعة: ● وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية) (مثال: نسخة إلكترونية أو نسخة ورقية رسمية). ● وثائق توضح تحديد وتوثيق متطلبات هذا الضابط بإجراءات الجهة المعتمدة من قبل صاحب الصلاحية (مثال: نسخة إلكترونية أو نسخة ورقية رسمية). ● لقطة شاشة لنظام جدار حماية التطبيقات WAF المستخدم بالجهة.
٢-١٥-٣-٢	استخدام مبدأ المعمارية متعددة المستويات (Multi-tier Architecture).
	إرشادات تطبيق الضوابط: ● العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية. ● العمل على تحديد تطبيقات الويب والتي تشمل: ○ التطبيقات الخارجية التي تم شراؤها. ○ التطبيقات التي يتم تطويرها داخلياً. ● تحديد تطبيقات الويب الحالية المستخدمة في الجهة. ● في حال وجود تطبيقات ويب تم شراؤها وتشغيلها من طرف خارجي، يجب: ○ التأكد من التزام المورد بسياسات ومعايير الأمن السيبراني والتي تشمل استخدام مبدأ المعمارية متعددة المستويات. ● في حال وجود تطبيقات يتم تطويرها داخلياً أو تطبيقات ويب تم شراؤها من طرف خارجي ولكن يتم تشغيلها بالجهة، يجب: ○ تحديد مستويات مبدأ المعمارية المناسبة لطبيعة تطبيق الويب والتي يجب ألّا تقل عن ثلاثة مستويات: ▪ طبقة قاعدة البيانات (Database Tier) ▪ طبقة الأعمال (Business Tier) ▪ طبقة العرض (Presentation/Client Tier) ○ العمل على تحديد الإدارات ذات الصلة لتطبيق مبدأ المعمارية متعددة المستويات.

	○ العمل على تطبيق مبدأ المعمارية متعددة المستويات والتي يجب ألّا تقل عن ثلاثة مستويات لجميع تطبيقات الويب الخاصة بالجهة. ● العمل على إدراج واستخدام مبدأ المعمارية متعدد المستويات في دورة حياة تطوير التطبيقات لضمان حماية التطبيقات المُراد تطويرها مستقبلاً.
	المخرجات المتوقعة: ● وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط بسياسات الجهة المعتمدة من قبل صاحب الصلاحية (مثال: نسخة إلكترونية أو نسخة ورقية رسمية). ● وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط بإجراءات الجهة المعتمدة من قبل صاحب الصلاحية (مثال: نسخة إلكترونية أو نسخة ورقية رسمية). ● عينة من تصاميم تطبيقات الويب التي توضح استخدام مبدأ المعمارية متعددة المستويات لأحد تطبيقات الويب الخاصة بالجهة التي تم تطويرها داخلياً. ● عينة من تصاميم تطبيقات الويب التي توضح استخدام مبدأ المعمارية متعددة المستويات لأحد تطبيقات الويب الخاصة بالجهة التي تم شراؤها من طرف خارجي.
٢-١٥-٣-٣	استخدام بروتوكولات آمنة مثل بروتوكول (HTTPS).
	إرشادات تطبيق الضوابط: ● العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية. ● العمل على تحديد تطبيقات الويب والتي تشمل: ○ التطبيقات الخارجية التي تم شراؤها. ○ التطبيقات التي يتم تطويرها داخلياً. ● تحديد تطبيقات الويب الحالية المستخدمة في الجهة. ● في حال وجود تطبيقات ويب تم شراؤها وتشغيلها من طرف خارجي، يجب: ○ التأكد من التزام المورد بسياسات ومعايير الأمن السيبراني والتي تشمل استخدام بروتوكولات آمنة. ● في حال وجود تطبيقات يتم تطويرها داخلياً أو تطبيقات ويب تم شراؤها من طرف خارجي ولكن يتم تشغيلها بالجهة، يجب: ○ العمل على تحديد بروتوكول الاتصالات الآمنة المُراد تطبيقها على تطبيقات الويب الخاصة بالجهة والتي تشمل على سبيل المثال لا الحصر: ■ بروتوكول نقل النص التشعبي الآمن (HTTPS) ■ بروتوكول نقل الملفات الآمن (SFTP) ■ بروتوكول أمن طبقة النقل (TLS)

○ العمل على تطبيق وتنزيل بروتوكولات الاتصالات الآمنة في تطبيقات الويب الخارجية الخاصة بالجهة لحمايتها. • العمل على إدراج تطبيق وتنزيل بروتوكولات الاتصالات الآمنة في دورة حياة تطوير التطبيقات لضمان حماية التطبيقات المُراد تطويرها مستقبلاً.	
المخرجات المتوقعة: • وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية) (مثال: نسخة إلكترونية أو نسخة ورقية رسمية). • لقطة شاشة من تطبيق الويب يوضح فيه استخدام بروتوكول HTTPS في الرابط الخاص به.	
توضيح سياسة الاستخدام الآمن للمستخدمين.	٢-١٥-٣-٤
إرشادات تطبيق الضوابط: • العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية. • العمل على توثيق سياسة الاستخدام آمن لتطبيقات الويب الخاصة بالجهة للمستخدمين. • التأكد من مشاركة سياسة الاستخدام الآمن للمستخدمين على تطبيقات الويب الخاصة بالجهة عن طريق الشبكة الخارجية (extranet) وليس الشبكة الداخلية (intranet).	
المخرجات المتوقعة: • وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية) (مثال: نسخة إلكترونية أو نسخة ورقية رسمية). • سياسة الاستخدام الآمن لمستخدمين تطبيقات الويب. • لقطة شاشة من موقع الجهة يوضح فيه نشر سياسة الاستخدام الآمن للمستخدمين.	
التحقق من الهوية متعدد العناصر (Multi-Factor Authentication) لعمليات دخول المستخدمين.	٢-١٥-٣-٥
إرشادات تطبيق الضوابط: • العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية. • استخدام التحقق من الهوية متعدد العناصر (Multi-Factor Authentication) لعمليات دخول المستخدمين لجميع تطبيقات الويب. (سواء كانت تطبيقات ويب تم شراؤها وتشغيلها من طرف خارجي أو تم تطويرها داخلياً أو تطبيقات ويب تم شراؤها من طرف خارجي ولكن يتم تشغيلها بالجهة). • العمل على تضمين متطلب تطبيق التحقق من الهوية متعدد العناصر في دورة حياة تطوير التطبيقات لضمان حماية التطبيقات المُراد تطويرها مستقبلاً.	

	المخرجات المتوقعة: • وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية) (مثال: نسخة إلكترونية أو نسخة ورقية رسمية). • لقطات شاشة متعددة يوضح فيها عملية الدخول والتي تشمل التحقق من الهوية متعدد العناصر MFA.
٢-١٥-٤	يجب مراجعة متطلبات الأمن السيبراني لحماية تطبيقات الويب الخارجية للجهة من المخاطر السيبرانية.
	إرشادات تطبيق الضوابط: • العمل على مراجعة تطبيق متطلبات الأمن السيبراني لحماية تطبيقات الويب الخارجية للجهة من خلال إجراء تقييم دوري (وذلك حسب خطة موثقة ومعتمدة للمراجعة، وبناء على فترة زمنية محددة "على سبيل المثال، بشكل ربع سنوي") لحماية تطبيقات الويب الخارجية من قبل الإدارة المعنية بالأمن السيبراني وبالتعاون مع الإدارات ذات العلاقة (كالإدارة المعنية بتقنية المعلومات). • مراجعة التطبيق قد تتم من خلال القنوات التقليدية (مثل البريد الإلكتروني) أو قد يكون مؤتمت باستخدام نظام لإدارة الالتزام. الجهة قد تضع خطة مراجعة توضح فيها جدول مراجعة تطبيق متطلبات الأمن السيبراني لحماية تطبيقات الويب الخارجية للجهة. • مراجعة وتحديث متطلبات الأمن السيبراني لحماية تطبيقات الويب الخارجية للجهة بشكل دوري حسب خطة موثقة ومعتمدة للمراجعة بناءً على فترة زمنية محددة أو في حالة حدوث تغييرات في المتطلبات التشريعية والتنظيمية ذات العلاقة. • توثيق المراجعة والتغييرات التي تتم على متطلبات الأمن السيبراني لحماية تطبيقات الويب الخارجية في الجهة واعتمادها من قبل رئيس الجهة أو من ينيبه.
	المخرجات المتوقعة: • نتائج مراجعة متطلبات الأمن السيبراني لحماية تطبيقات الويب الخارجية. • وثيقة تحدد دورة مراجعة تطبيق متطلبات الأمن السيبراني لحماية تطبيقات الويب الخارجية (جدول تقييم الالتزام). • وثيقة تقرير تقييم الالتزام توضح تقييم تطبيق متطلبات الأمن السيبراني لحماية تطبيقات الويب الخارجية. • 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. • 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).

٣ صمود الأمن السيبراني (Cybersecurity Resilience)

٣-١	جوانب صمود الأمن السيبراني في إدارة استمرارية الأعمال (Cybersecurity Resilience Aspects of Business Continuity Management "BCM")
الهدف	ضمان توافر متطلبات صمود الأمن السيبراني في إدارة استمرارية أعمال الجهة. وضمان معالجة وتقليل الآثار المترتبة على الاضطرابات في الخدمات الإلكترونية الحرجة للجهة وأنظمة وأجهزة معالجة معلوماتها جراء الكوارث الناتجة عن المخاطر السيبرانية.
الضوابط	
٣-١-١	يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني ضمن إدارة استمرارية أعمال الجهة.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني ضمن استمرارية الأعمال **إرشادات تطبيق الضوابط:** • العمل على تضمين وتوثيق متطلبات الأمن السيبراني ضمن إدارة استمرارية أعمال الجهة، ومن هذه المتطلبات وعلى سبيل المثال لا الحصر: ○ التأكد من استمرارية الأنظمة والإجراءات المتعلقة بالأمن السيبراني. ○ وضع خطط الاستجابة لحوادث الأمن السيبراني التي قد تؤثر على استمرارية أعمال الجهة. ○ وضع خطط التعافي من الكوارث (Disaster Recovery Plan). • العمل على أن تكون متطلبات الأمن السيبراني ضمن إدارة استمرارية الأعمال مدعومة من قبل الإدارة التنفيذية. وذلك من خلال اعتماد وموافقة رئيس الجهة أو من ينيبه.
	المخرجات المتوقعة: • وثيقة سياسة الأمن السيبراني التي تغطي متطلبات الأمن السيبراني ضمن إدارة استمرارية الأعمال (نسخة إلكترونية أو نسخة ورقية رسمية). • موافقة رسمية من قبل رئيس الجهة أو من ينيبه على الوثيقة (مثال: عن طريق البريد الإلكتروني الرسمي للجهة، أو التوقيع الورقي أو الإلكتروني).
٣-١-٢	يجب تطبيق متطلبات الأمن السيبراني ضمن إدارة استمرارية أعمال الجهة.
	إرشادات تطبيق الضوابط:

	• العمل على تطبيق متطلبات الأمن السيبراني ضمن إدارة استمرارية الأعمال والتي تم تحديد وتوثيقها واعتمادها في وثيقة السياسات. • العمل على وضع خطة عمل لتطبيق كافة متطلبات الأمن السيبراني المتعلقة بضمان إدارة استمرارية الأعمال في الجهة. • تضمين متطلبات الأمن السيبراني ضمن إدارة استمرارية الأعمال في إجراءات حمايتها لضمان الالتزام بمتطلبات الأمن السيبراني لجميع أصحاب المصلحة الداخليين والخارجيين.
	المخرجات المتوقعة: • وثائق تؤكد تطبيق كافة متطلبات الأمن السيبراني المتعلقة بضمان إدارة استمرارية الأعمال في الجهة والتي تم توثيقها في وثيقة السياسات. • وثيقة خطة عمل لتطبيق متطلبات الأمن السيبراني إدارة استمرارية الأعمال في الجهة. • إثبات يؤكد تطبيق ضوابط ضمان إدارة استمرارية الأعمال في الجهة، على سبيل المثال لا الحصر: o خطط استمرارية الأعمال الموثقة والمعتمدة للجهة. o الخطط المعتمدة للاستجابة لحوادث الأمن السيبراني التي قد تؤثر على استمرارية الأعمال في الجهة. o تقارير تنفيذ اختبارات خطط التعافي من الكوارث في الجهة.
٣-١-٣	يجب أن تغطي إدارة استمرارية الأعمال في الجهة بحد أدنى ما يلي:
١-٣-١-٣	التأكد من استمرارية الأنظمة والإجراءات المتعلقة بالأمن السيبراني.
	إرشادات تطبيق الضوابط: • العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية. • العمل على تحديد المتطلبات التشريعية والتنظيمية الخاصة باستمرارية الأعمال في الجهة. • العمل على تضمين حوادث الأمن السيبراني عالية الخطورة ضمن الأسباب الموجبة لتفعيل خطة استمرارية الأعمال في الجهة. • العمل على تطوير وثيقة لبرنامج إدارة استمرارية أعمال الجهة (Business Continuity Management (Program • العمل على توثيق واعتماد خطط لاستمرارية أعمال الجهة Business Continuity Plans)) والتي تشمل (على سبيل المثال لا الحصر): o إجراءات تقييم للمخاطر التي قد تؤثر على استمرارية أعمال الجهة. o إجراء تحليل التأثير على الأعمال (Business Impact Analysis) لأنظمة الجهة. o تحديد الأنظمة والإجراءات والأصول المتعلقة بالأمن السيبراني وأهميتها للجهة

	○ إجراءات استمرارية الأنظمة المتعلقة بالأمن السيبراني ومنها المتطلبات التقنية، مثل وجود خاصية التوافر العالي (high availability)، والمتطلبات التنظيمية، مثل وجود نائب يحل محل مشغلي أنظمة الأمن السيبراني عند الحاجة. ○ تحديد خدمات الأمن السيبراني وأهميتها للجهة، وتطوير خطة للتأكد من استمرارية هذه الخدمات. ● العمل على مراجعة خطط استمرارية أعمال الجهة بشكل دوري وتحديثها في حال لزم ذلك.
	المخرجات المتوقعة: ● وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية) (مثال: نسخة إلكترونية أو نسخة ورقية رسمية). ● وثيقة برنامج إدارة استمرارية الأعمال الموثقة والمعتمدة للجهة. ● خطط استمرارية الأعمال الموثقة والمعتمدة للجهة. ● موافقة رسمية من قبل رئيس الجهة أو من ينيبه على الوثائق (مثال: عن طريق البريد الإلكتروني الرسمي للجهة، أو التوقيع الورقي أو الإلكتروني). ● تقارير تنفيذ اختبارات خطط استمرارية الأعمال في الجهة. ● تقرير الاجتماعات الدورية لمشاركة خطط استمرارية الأعمال السيبرانية مع استمرارية الأعمال المؤسسية ومشاركة جميع أصحاب المصلحة في ذلك
٢-٣-١-٣	وضع خطط الاستجابة لحوادث الأمن السيبراني التي قد تؤثر على استمرارية أعمال الجهة.
	إرشادات تطبيق الضوابط: ● العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية. ● العمل على وضع خطط الاستجابة لحوادث الأمن السيبراني التي قد تؤثر على استمرارية أعمال الجهة والتي تشمل (على سبيل المثال لا الحصر): ○ إيضاح لأنواع الحوادث وتصنيفها حسب مدى تأثيرها على استمرارية أعمال الجهة. ○ تحديد الأدوار والمسؤوليات الخاصة بالاستجابة لحوادث الأمن السيبراني المؤثرة على استمرارية أعمال الجهة. ○ تحديد مراحل الاستجابة للحوادث، بحيث تشمل (على سبيل المثال لا الحصر): ■ التخطيط والتحضير (Planning and Preparation) ■ الاكتشاف والتحليل (Detection and Analysis) ■ الاحتواء والإزالة والتعافي من الحادثة (Containment, Eradication and Recovery) ■ المراجعة واستخلاص الدروس المستفادة (Review and Learn)

	○ الاستفادة من سيناريوات الاستجابة للحوادث المنشورة على صفحة الهيئة الوطنية للأمن السيبراني (Utilizing NCA published incident response playbooks)) ● العمل على تضمين حوادث الأمن السيبراني عالية الخطورة ضمن الأسباب الموجبة لتفعيل خطط الاستجابة لحوادث الأمن السيبراني. ● العمل على كتابة تقرير لحادثة الأمن السيبراني المؤثرة على استمرارية أعمال الجهة عند الانتهاء من الاستجابة بحيث يشمل (على سبيل المثال لا الحصر): ○ الأشخاص المشاركين لاستجابة الحادثة ووسيلة التواصل. ○ المعلومات الأساسية للحادثة، على سبيل المثال لا الحصر: ■ التاريخ والوقت. ■ نطاق الحادثة. ■ مستوى الخطورة. ○ ملخص الحادثة. ○ خطوات الاحتواء والإزالة. ○ التوصيات الحالية والمستقبلية. ● العمل على مراجعة خطط الاستجابة لحوادث الأمن السيبراني التي قد تؤثر على استمرارية أعمال الجهة بشكل دوري وتحديثها في حال لزم ذلك.
	المخرجات المتوقعة: ● وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية) (مثال: نسخة إلكترونية أو نسخة ورقية رسمية). ● الخطط المعتمدة للاستجابة لحوادث الأمن السيبراني التي قد تؤثر على استمرارية أعمال الجهة. ● موافقة رسمية من قبل رئيس الجهة أو من ينيبه على الوثائق (مثال: عن طريق البريد الإلكتروني الرسمي للجهة، أو التوقيع الورقي أو الإلكتروني).
٣-١-٣-٣	وضع خطط التعافي من الكوارث (Disaster Recovery Plan).
	إرشادات تطبيق الضوابط: ● العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية. ● العمل على وضع خطط التعافي من الكوارث والتي تشمل (على سبيل المثال لا الحصر): ○ تحديد فريق التعافي من الكوارث. ○ تحديد وتقييم مخاطر الكوارث.

	○ إجراء تحليل التأثير على الأعمال (Business Impact Analysis) لتحديد الأنظمة الحساسة في الجهة. ○ تحديد إجراءات النسخ الاحتياطي والتخزين الخارجي. ○ اختبار خطط التعافي من الكوارث. ● العمل على إنشاء مركز للتعافي من الكوارث للأنظمة الحساسة. ● العمل على إجراء اختبارات دورية للتأكد من فعالية خطط التعافي من الكوارث. ● العمل على تحديد متطلبات النسخ الدورية الخاصة بالأنظمة للجهة إلى مركز التعافي. **المخرجات المتوقعة:** ● وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية) (مثال: نسخة إلكترونية أو نسخة ورقية رسمية). ● الخطط المعتمدة للتعافي من الكوارث الخاصة بالجهة. ● تقارير تنفيذ اختبارات خطط التعافي من الكوارث في الجهة. ● موافقة رسمية من قبل رئيس الجهة أو من ينيبه على الوثائق (مثال: عن طريق البريد الإلكتروني الرسمي للجهة، أو التوقيع الورقي أو الإلكتروني)
٣-١-٤	يجب مراجعة متطلبات الأمن السيبراني ضمن إدارة استمرارية أعمال الجهة دورياً. **إرشادات تطبيق الضوابط:** ● مراجعة وتحديث متطلبات الأمن السيبراني ضمن إدارة استمرارية أعمال الجهة بشكل دوري حسب خطة موثقة ومعتمدة للمراجعة بناءً على فترة زمنية محددة أو في حالة حدوث تغييرات في المتطلبات التشريعية والتنظيمية ذات العلاقة. ● توثيق المراجعة والتغييرات التي تتم على متطلبات الأمن السيبراني ضمن إدارة استمرارية أعمال الجهة واعتمادها من قبل رئيس الجهة أو من ينيبه. **المخرجات المتوقعة:** ● وثيقة معتمدة تحدد جدول المراجعة للسياسة. ● وثيقة السياسة بما يوضح أن تكون محدثة وتم توثيق التغييرات على متطلبات الأمن السيبراني الخاصة باستمرارية الأعمال واعتمادها من قبل رئيس الجهة أو من ينيبه. ● موافقة رسمية من قبل رئيس الجهة أو من ينيبه على السياسة المحدثة (مثال: عن طريق البريد الإلكتروني الرسمي للجهة، أو التوقيع الورقي أو الإلكتروني).

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

٤-١	الأمن السيبراني المتعلق بالأطراف الخارجية
الهدف	ضمان حماية أصول الجهة من مخاطر الأمن السيبراني المتعلقة بالأطراف الخارجية (بما في ذلك خدمات الإسناد لتقنية المعلومات "Outsourcing" والخدمات المدارة "Managed Services"). وفقاً للسياسات والإجراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية ذات العلاقة.
الضوابط	
٤-١-١	يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني ضمن العقود والاتفاقيات مع الأطراف الخارجية للجهة.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني المتعلّق بالأطراف الخارجية **إرشادات تطبيق الضوابط:** • العمل على تطوير وتوثيق سياسة الأمن السيبراني المتعلق بالأطراف الخارجية في الجهة ومن هذه المتطلبات وعلى سبيل المثال لا الحصر: ○ متطلبات الأمن السيبراني ضمن العقود والاتفاقيات مع الأطراف الخارجية. ○ إجراءات تقييم المخاطر المتعلقة بالأطراف الخارجية. ○ حماية البيانات والمعلومات. ○ إدارة حوادث الأمن السيبراني. • العمل على أن تكون السياسة في الجهة مدعومة من قبل الإدارة التنفيذية. وذلك من خلال اعتماد وموافقة رئيس الجهة أو من ينيبه.
	المخرجات المتوقعة: • وثيقة سياسة الأمن السيبراني التي تغطي متطلبات العقود والاتفاقيات مع الأطراف الخارجية (مثال: نسخة إلكترونية أو نسخة ورقية رسمية). • موافقة رسمية من قبل رئيس الجهة أو من ينيبه على السياسة (مثال: عن طريق البريد الإلكتروني الرسمي للجهة، أو التوقيع الورقي أو الإلكتروني).
٤-١-٢	يجب أن تغطي متطلبات الأمن السيبراني ضمن العقود والاتفاقيات (مثل اتفاقية مستوى الخدمة SLA) الأطراف الخارجية التي قد تتأثر بإصابتها بيانات الجهة أو الخدمات المقدمة لها بحد أدنى ما يلي:

٤-١-٢-١	بنود المحافظة على سرية المعلومات (Non-Disclosure Clauses) و الحذف الآمن من قبَل الطرف الخارجي لبيانات الجهة عند انتهاء الخدمة.

إرشادات تطبيق الضوابط:

- العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية على أن تشمل متطلبات الأمن السيبراني بنود المحافظة على سرية المعلومات (Non-Disclosure Clauses) والحذف الآمن من قِبَل الطرف الخارجي لبيانات الجهة عند انتهاء الخدمة.
- احتواء عقود الجهة مع الأطراف الخارجية على بنود تنص على التزام الطرف الخارجي بالمحافظة على سرية المعلومات.
- احتواء عقود الجهة مع الأطراف الخارجية على بنود تنص بإلزام الطرف الخارجي بالحذف الآمن لبيانات الجهة عند انتهاء مدة العقد/الخدمة.

المخرجات المتوقعة:

- وثيقة سياسة الأمن السيبراني التي تغطي متطلبات العقود والاتفاقيات مع الأطراف الخارجية (مثال: نسخة إلكترونية أو نسخة ورقية رسمية).
- عينة موقعة من أحد العقود والاتفاقيات مع الأطراف الخارجية توضح تضمين بنود المحافظة على سرية المعلومات والحذف الآمن للبيانات (نسخة ورقية أو إلكترونية).

٤-١-٢-٢	إجراءات التواصل في حال حدوث حادثة أمن سيبراني.

إرشادات تطبيق الضوابط:

- العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية على أن تشمل متطلبات إجراءات التواصل في حال حدوث حادثة أمن سيبراني.
- احتواء عقود الجهة مع الأطراف الخارجية بنود تنص على إلزام الطرف الخارجي بتحديد إجراءات التواصل في حال حدوث حادثة أمن سيبراني.
- ضمان تطوير الأطراف الخارجية لإجراءات تواصل مع الجهة حيث تشمل على وسائل وبيانات التواصل في حال حدوث حادثة أمن سيبراني والتي من الممكن أن تؤثر على بيانات الجهة أو الخدمة المقدمة لها من قبل الطرف الخارجي ومن هذه المتطلبات ما يلي:
  - بيانات التواصل (كالبريد الإلكتروني).
  - آلية إبلاغ حادثة الأمن السيبراني للجهة مع تصنيف الحادثة.
  - آليات التصعيد.

المخرجات المتوقعة:

- وثيقة سياسة الأمن السيبراني التي تغطي متطلبات العقود والاتفاقيات مع الأطراف الخارجية (مثال: نسخة إلكترونية أو نسخة ورقية رسمية).

	• الإجراءات المعتمدة مع الأطراف الخارجية للتواصل في حال حدوث حادثة أمن سيبراني التي من الممكن أن تتأثر من خلالها بيانات الجهة أو الخدمة المقدمة لها.	
	٤-١-٢-٣	إلزام الطرف الخارجي بتطبيق متطلبات وسياسات الأمن السيبراني للجهة والمتطلبات التشريعية والتنظيمية ذات العلاقة.
	إرشادات تطبيق الضوابط: • العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية على أن تشمل متطلبات إلزام الطرف الخارجي بتطبيق متطلبات وسياسات الأمن السيبراني للجهة والمتطلبات التشريعية والتنظيمية ذات العلاقة. • احتواء عقود واتفاقيات الجهة مع الأطراف الخارجية على بنود تنص على التزام الطرف الخارجي بتطبيق متطلبات وسياسات الأمن السيبراني للجهة والمتطلبات التشريعية والتنظيمية ذات العلاقة.	
	المخرجات المتوقعة: • وثيقة سياسة الأمن السيبراني التي تغطي متطلبات العقود والاتفاقيات مع الأطراف الخارجية (مثال: نسخة إلكترونية أو نسخة ورقية رسمية). • عينة موقعة من أحد العقود أو الاتفاقيات مع الأطراف الخارجية توضح إلزام الطرف الخارجي من خلاله بتطبيق متطلبات وسياسات الأمن السيبراني للجهة والمتطلبات التشريعية والتنظيمية ذات العلاقة.	
٤-١-٣	يجب أن تغطي متطلبات الأمن السيبراني مع الأطراف الخارجية التي تقدم خدمات إسناد لتقنية المعلومات، أو خدمات مدارة بحد أدنى ما يلي:	
	٤-١-٣-١	إجراء تقييم لمخاطر الأمن السيبراني، والتأكد من وجود ما يضمن السيطرة على تلك المخاطر، قبل توقيع العقود والاتفاقيات أو عند تغيير المتطلبات التشريعية والتنظيمية ذات العلاقة.
	إرشادات تطبيق الضوابط: • العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية على أن تشمل متطلبات إجراء تقييم لمخاطر الأمن السيبراني، والتأكد من وجود ما يضمن السيطرة على تلك المخاطر، قبل توقيع العقود والاتفاقيات أو عند تغيير المتطلبات التشريعية والتنظيمية ذات العلاقة. • إجراء تقييم لمخاطر الأمن السيبراني المتعلق بالأطراف الخارجية من قبل الجهة في الحالات التالية: ○ قبل توقيع الجهة أية عقود أو اتفاقيات مع أطراف خارجية. ○ عند تغيير المتطلبات التشريعية والتنظيمية ذات العلاقة.	
	المخرجات المتوقعة:	

	• وثيقة سياسة الأمن السيبراني التي تغطي متطلبات العقود والاتفاقيات مع الأطراف الخارجية (مثال: نسخة إلكترونية أو نسخة ورقية رسمية). • عينة من تقرير تقييم المخاطر السيبرانية المتعلقة بالأطراف الخارجية قبل توقيع العقد أو عند حدوث تغيير في المتطلبات التشريعية والتنظيمية ذات العلاقة.	
٤-١-٣-٢	أن تكون مراكز عمليات خدمات الأمن السيبراني المدارة للتشغيل والمراقبة، والتي تستخدم طريقة الوصول عن بعد، موجودة بالكامل داخل المملكة.	
	إرشادات تطبيق الضوابط: • العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية على أن تشمل متطلبات أن تكون مراكز عمليات خدمات الأمن السيبراني المدارة للتشغيل والمراقبة، والتي تستخدم طريقة الوصول عن بعد، موجودة بالكامل داخل المملكة. • التأكد من أن مراكز عمليات خدمات الأمن السيبراني المدارة للتشغيل والمراقبة موجودة بالكامل داخل المملكة. • التأكد من أن الدخول عن بعد لمراكز عمليات خدمات الأمن السيبراني المدارة للتشغيل والمراقبة يتم بالكامل داخل المملكة. • تضمين بند ينص على إلزام الطرف الخارجي بوجود مراكز عمليات خدمات الأمن السيبراني المدارة للتشغيل والمراقبة، والتي تستخدم طريقة الوصول عن بعد داخل المملكة العربية السعودية كأحد بنود العقد الموقّع أو وجود اتفاقية مستوى الخدمة (SLA) موقعه بين الجهة ومقدم الخدمة.	
	المخرجات المتوقعة: • وثيقة سياسة الأمن السيبراني التي تغطي متطلبات العقود والاتفاقيات مع الأطراف الخارجية (مثال: نسخة إلكترونية أو نسخة ورقية رسمية). • عينة من إثبات استضافة أو إدارة مركز عمليات خدمات الأمن السيبراني داخل المملكة، (مثال: وجوده كأحد بنود العقد الموقع أو وجود اتفاقية مستوى الخدمة (SLA) موقعه بين الطرف الخارجي والجهة).	
٤-١-٤	يجب مراجعة متطلبات الأمن السيبراني مع الأطراف الخارجية دورياً.	
	إرشادات تطبيق الضوابط: • مراجعة وتحديث متطلبات الأمن السيبراني المتعلقة مع الأطراف الخارجية في الجهة بشكل دوري حسب خطة موثقة ومعتمدة للمراجعة بناءً على فترة زمنية محددة أو في حالة حدوث تغييرات في المتطلبات التشريعية والتنظيمية ذات العلاقة. • توثيق المراجعة والتغييرات التي تتم على متطلبات الأمن السيبراني الخاصة بالأطراف الخارجية في الجهة واعتمادها من قبل رئيس الجهة أو من ينيبه.	
	المخرجات المتوقعة:	

	• 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. • 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).

٢-٤	الأمن السيبراني المتعلق بالحوسبة السحابية والاستضافة
الهدف	ضمان معالجة المخاطر السيبرانية وتنفيذ متطلبات الأمن السيبراني للحوسبة السحابية والاستضافة بشكل ملائم وفعّال، وذلك وفقاً للسياسات والإجراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية والأوامر والقرارات ذات العلاقة. وضمان حماية الأصول المعلوماتية والتقنية للجهة على خدمات الحوسبة السحابية التي تتم استضافتها أو معالجتها أو إدارتها بواسطة أطراف خارجية.
الضوابط	
١-٢-٤	يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني الخاصة باستخدام خدمات الحوسبة السحابية والاستضافة.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني المتعلق بالحوسبة السحابية والاستضافة **إرشادات تطبيق الضوابط:** • العمل على تطوير وتوثيق سياسة الأمن السيبراني المتعلقة باستخدام خدمات الحوسبة السحابية والاستضافة في الجهة ومن هذه المتطلبات وعلى سبيل المثال لا الحصر: ○ متطلبات عقود مقدمي خدمات الحوسبة السحابية والاستضافة. ○ متطلبات موقع استضافة وتخزين أنظمة وبيانات الجهة. ○ متطلبات حذف واسترجاع بيانات الجهة. ○ تصنيف البيانات قبل استضافتها/تخزينها لدى مقدمي خدمات الحوسبة السحابية والاستضافة. ○ تضمين متطلبات الأمن السيبراني وبنود اتفاقية مستوى الخدمة (Service Level Agreement "SLA"). ○ تضمين بنود المحافظة على سرية المعلومات (Non-disclosure Clauses). • العمل على أن تكون السياسة في الجهة مدعومة من قبل الإدارة التنفيذية. وذلك من خلال اعتماد وموافقة رئيس الجهة أو من ينيبه.
	المخرجات المتوقعة:

	• وثيقة سياسة الأمن السيبراني التي تغطي متطلبات استخدام خدمات الحوسبة السحابية والاستضافة (مثال: نسخة إلكترونية أو نسخة ورقية رسمية). • موافقة رسمية من قبل رئيس الجهة أو من ينيبه على السياسة (مثال: عن طريق البريد الإلكتروني الرسمي للجهة، أو التوقيع الورقي أو الإلكتروني).
٤-٢-٢	يجب تطبيق متطلبات الأمن السيبراني الخاصة بخدمات الحوسبة السحابية والاستضافة للجهة.
	إرشادات تطبيق الضوابط: • العمل على تطبيق متطلبات الأمن السيبراني الخاصة بخدمات الحوسبة السحابية والاستضافة للجهة، وقد تشمل، على سبيل المثال لا الحصر: ○ التأكد من أن موقع استضافة وتخزين معلومات الجهة يكون داخل المملكة. ○ التأكد من تفعيل سجلات الأحداث على الأصول المعلوماتية المستضافة. ○ يجب على مقدمي خدمات الحوسبة السحابية والاستضافة إعادة البيانات (بصيغة قابلة للاستخدام) وحذفها بشكل غير قابل للاسترجاع عند إنهاء/انتهاء الخدمة. ○ التأكد من فصل البيئة الخاصة بالجهة (ويشمل ذلك الخوادم الافتراضية، والشبكات وقواعد البيانات) عن غيرها من البيئات التابعة لجهات أخرى في خدمات الحوسبة السحابية. ○ تشفير البيانات والمعلومات المنقولة إلى الخدمات السحابية، أو المخزنة فيها، أو المنقولة منها وفقاً للمتطلبات التشريعية والتنظيمية ذات العلاقة في الجهة. ○ التأكد من أن مقدم خدمات الحوسبة السحابية والاستضافة يقوم بعمل النسخ الاحتياطي دورياً وحماية النسخ الاحتياطية وفقاً لسياسة النسخ الاحتياطية المعتمدة في الجهة. • أيضاً قد تضع الجهة خطة عمل لتطبيق متطلبات الأمن السيبراني الخاصة بخدمات الحوسبة السحابية والاستضافة للجهة لضمان التزام الجهة بتطبيق كافة متطلبات الأمن السيبراني، وتشمل منسوبي الجهة والأطراف الخارجية، ومتابعتها ومراقبتها بشكل دوري لضمان التطبيق. • ضمان الالتزام الدائم والمستمر بضوابط الأمن السيبراني للحوسبة السحابية (CCC).
	المخرجات المتوقعة: • وثيقة خطة عمل لتطبيق متطلبات الأمن السيبراني الخاصة بخدمات الحوسبة السحابية والاستضافة. • عينة موقعة للاتفاقية أو العقد المبرم بين الجهة ومقدم خدمة الحوسبة السحابية. • إثبات من مقدم خدمة الحوسبة السحابية متضمن فيه تطبيق متطلبات الأمن السيبراني الخاصة بخدمات الحوسبة السحابية والاستضافة للجهة.
٤-٢-٣	بما يتوافق مع المتطلبات التشريعية والتنظيمية ذات العلاقة، وبالإضافة إلى ما ينطبق من الضوابط ضمن المكونات الرئيسية رقم (١) و(٢) و (٣) والمكون الفرعي رقم (٤-١) الضرورية لحماية بيانات الجهة أو الخدمات المقدمة لها، يجب أن تغطي متطلبات الأمن السيبراني الخاصة باستخدام خدمات الحوسبة السحابية والاستضافة بحد أدنى ما يلي:

٤-٢-٣-١	تصنيف البيانات قبل استضافتها لدى مقدمي خدمات الحوسبة السحابية والاستضافة، وإعادتها للجهة (بصيغة قابلة للاستخدام) عند انتهاء الخدمة.

إرشادات تطبيق الضوابط:

- التأكد من تصنيف البيانات قبل أن يتم استضافتها لدى مقدمي خدمات الحوسبة السحابية والاستضافة، بحيث يضمن أن يتم التعامل مع تلك البيانات بإجراءات على حسب ذلك التصنيف، وضمان إعادة تلك البيانات من قبل مقدم الخدمة عند انتهاء العقد/الخدمة مع الجهة عن طريق الخطوات التالية:
  - تحديد جميع البيانات التي سيتم إرسالها إلى مقدم خدمة الحوسبة السحابية.
  - تصنيف وترميز البيانات التي تم تحديدها بما يتوافق مع آلية تصنيف وترميز البيانات في الجهة والمتطلبات التشريعية والتنظيمية ذات العلاقة.
  - مشاركة هذه البيانات مع مقدم خدمة الحوسبة السحابية لاستضافتها في السحابة.
  - تطوير إجراءات لضمان إعادة البيانات من قبل مقدم خدمة الحوسبة السحابية (بصيغة قابلة للاستخدام) بعد انتهاء العقد/الخدمة.

المخرجات المتوقعة:

- وثيقة سياسة الأمن السيبراني التي تغطي متطلبات استخدام خدمات الحوسبة السحابية والاستضافة (مثال: نسخة إلكترونية أو نسخة ورقية رسمية).
- عينة من قائمة البيانات التي تم تصنيفها قبل استضافتها لدى مقدمي خدمات الحوسبة السحابية، وعلى سبيل المثال لا الحصر (ملف) موضح فيه البيانات التي تم تصنيفها. قبل مشاركتها مع مقدم خدمة الحوسبة السحابية
- عينة موقعة للاتفاقية أو العقد المبرم بين الجهة ومقدم خدمة الحوسبة السحابية.
- الإجراءات المعتمدة لإعادة البيانات بعد الانتهاء من خدمات الحوسبة السحابية.
- سياسات وإجراءات تصنيف البيانات المراد استضافتها على خدمات الحوسبة والاستضافة.
- قائمة حصر الخدمات المستضافة وتصنيفها على أن تكون محدثة.

٤-٢-٣-٢	فصل البيئة الخاصة بالجهة (وخصوصاً الخوادم الافتراضية) عن غيرها من البيئات التابعة لجهات أخرى في خدمات الحوسبة السحابية.

إرشادات تطبيق الضوابط:

- العمل على تحديد متطلبات فصل البيئة الخاصة بالجهة (وخصوصاً الخوادم الافتراضية) عن غيرها من البيئات التابعة لجهات أخرى في خدمات الحوسبة السحابية.
- احتواء عقود الجهة مع مقدمي الخدمة والاستضافة بنود تنص على فصل البيئة الخاصة بالجهة عن غيرها من البيئات التابعة لجهات أخرى في خدمات الحوسبة السحابية.

المخرجات المتوقعة:

		• وثيقة سياسة الأمن السيبراني التي تغطي متطلبات استخدام خدمات الحوسبة السحابية والاستضافة (مثال: نسخة إلكترونية أو نسخة ورقية رسمية). • إثبات يوضح فصل البيئة الخاصة بالجهة عن غيرها من البيئات التابعة لجهات أخرى في خدمات الحوسبة السحابية، (مثال: وجوده كأحد بنود العقد الموقع أو وجود اتفاقية موقعه بين مقدم الخدمة والجهة). • إثبات من مقدم خدمة الحوسبة السحابية يثبت فصل البيئة الخاصة بالجهة عن غيرها من البيئات التابعة لجهات أخرى في خدمات الحوسبة السحابية.
	٤-٢-٣-٣	موقع استضافة وتخزين معلومات الجهة يجب أن يكون داخل المملكة.
		إرشادات تطبيق الضوابط: • التأكد من أن السياسة الموثقة والمعتمدة تشمل على متطلبات موقع استضافة وتخزين معلومات الجهة ويجب أن تكون داخل المملكة. • التأكد من أن موقع استضافة وتخزين معلومات الجهة يكون داخل المملكة عن طريق وعلى سبيل المثال لا الحصر: ○ تضمين بند تواجد تخزين البيانات داخل المملكة العربية السعودية كأحد بنود العقد الموقع أو وجود اتفاقية مستوى الخدمة (SLA) موقعه بين الجهة ومقدم الخدمة. ○ تضمين بند التزام مقدم الخدمة بضوابط الهيئة الوطنية للأمن السيبراني المتعلقة بخدمات الحوسبة السحابية والاستضافة ، مع مراعاة تصنيف البيانات المستضافة.
		المخرجات المتوقعة: • وثيقة سياسة الأمن السيبراني التي تغطي متطلبات استخدام خدمات الحوسبة السحابية والاستضافة (مثال: نسخة إلكترونية أو نسخة ورقية رسمية). • إثبات تواجد موقع استضافة وتخزين معلومات الجهة داخل المملكة، (مثال: وجوده كأحد بنود العقد الموقع أو وجود اتفاقية مستوى الخدمة (SLA) موقع بين مقدم الخدمة والجهة). • إثبات من مقدم الخدمة يثبت تخزين البيانات داخل المملكة.
٤-٢-٤		يجب مراجعة متطلبات الأمن السيبراني الخاصة بخدمات الحوسبة السحابية والاستضافة دورياً.
		إرشادات تطبيق الضوابط: • العمل على مراجعة وتحديث سياسة الأمن السيبراني التي تغطي متطلبات استخدام خدمات الحوسبة السحابية والاستضافة للجهة بشكل دوري حسب خطة موثقة ومعتمدة للمراجعة بناءً على فترة زمنية محددة (على سبيل المثال، يتم اجراء المراجعة الدورية بشكل سنوي). • العمل على مراجعة وتحديث سياسة الأمن السيبراني التي تغطي متطلبات استخدام خدمات الحوسبة السحابية والاستضافة للجهة عند حدوث تغييرات في المتطلبات التشريعية والتنظيمية ذات العلاقة (على سبيل المثال، عند صدور تنظيم تشريعي جديد في الأمن السيبراني ينطبق على الجهة).

	• العمل على توثيق المراجعة والتغييرات التي تمت على متطلبات الأمن السيبراني المتعلقة باستخدام خدمات الحوسبة السحابية والاستضافة في الجهة واعتمادها من قبل رئيس الجهة أو من ينيبه.
	المخرجات المتوقعة: • وثيقة معتمدة تحدد جدول المراجعة للسياسة. • وثيقة السياسة بما يوضح أن تكون محدثة وتم توثيق التغييرات على متطلبات الأمن السيبراني الخاصة بخدمات الحوسبة السحابية والاستضافة واعتمادها من قبل رئيس الجهة أو من ينيبه. • موافقة رسمية من قبل رئيس الجهة أو من ينيبه على السياسة المحدثة (مثال: عن طريق البريد الإلكتروني الرسمي للجهة، أو التوقيع الورقي أو الإلكتروني).

0 الأمن السيبراني لأنظمة التحكم الصناعي
(Industrial Control Systems Cybersecurity)

٥-١	حماية أجهزة وأنظمة التحكم الصناعي
الهدف	ضمان إدارة الأمن السيبراني بشكل سليم وفعال لحماية توافر وسلامة وسرية أصول الجهة المتعلقة بأجهزة وأنظمة التحكم الصناعي (ICS/OT) ضد الهجوم السيبراني (مثل الوصول غير المصرح به والتخريب والتجسس والتلاعب) بما يتماشى مع استراتيجية الأمن السيبراني للجهة، وإدارة مخاطر الأمن السيبراني، والمتطلبات التشريعية والتنظيمية ذات العلاقة، وكذلك المتطلبات الدولية المقرة تنظيمياً على الجهة والمتعلقة بالأمن السيبراني.
الضوابط	
٥-١-١	يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني لحماية أجهزة وأنظمة التحكم الصناعي (ICS/OT) للجهة.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني لأنظمة التحكم الصناعي **إرشادات تطبيق الضوابط:** • العمل على تطوير وتوثيق سياسة الأمن السيبراني لحماية أجهزة وأنظمة التحكم الصناعي (ICS/OT) في الجهة ومن هذه المتطلبات وعلى سبيل المثال لا الحصر: ○ متطلبات حماية شبكات الإنتاج الصناعي ومتطلبات ربطها مع الشبكات الأخرى. ○ متطلبات حماية أنظمة التحكم الصناعي وتقييد الوصول والصلاحيات ○ متطلبات إدارة حوادث الأمن السيبراني المتعلقة بأنظمة التحكم الصناعي • العمل على ان تكون السياسة في الجهة مدعومة من قبل الإدارة التنفيذية. وذلك من خلال اعتماد وموافقة رئيس الجهة أو من ينيبه.
	المخرجات المتوقعة: • وثيقة سياسة الأمن السيبراني التي تغطي متطلبات لحماية أجهزة وأنظمة التحكم الصناعي (نسخة إلكترونية أو نسخة ورقية رسمية). • موافقة رسمية من قبل رئيس الجهة أو من ينيبه على السياسة (مثال: عن طريق البريد الإلكتروني الرسمي للجهة، أو التوقيع الورقي أو الإلكتروني).
٥-١-٢	يجب تطبيق متطلبات الأمن السيبراني لحماية أجهزة وأنظمة التحكم الصناعي (ICS/OT) للجهة.
	إرشادات تطبيق الضوابط:

	• العمل على تطبيق كافة متطلبات الأمن السيبراني لحماية أجهزة وأنظمة التحكم الصناعي (ICS/OT) للجهة، ومن ضمنها ضوابط الأمن السيبراني للأنظمة التشغيلية. • العمل على وضع خطة عمل لتطبيق كافة متطلبات الأمن السيبراني لحماية أجهزة وأنظمة التحكم الصناعي (ICS/OT) للجهة. • تضمين متطلبات الأمن السيبراني لحماية أجهزة وأنظمة التحكم الصناعي (ICS/OT) للجهة في إجراءات حمايتها لضمان الالتزام بمتطلبات الأمن السيبراني لجميع أصحاب المصلحة من منسوبي الجهة او الأطراف الخارجية.
	المخرجات المتوقعة: • وثيقة خطة عمل لتطبيق متطلبات الأمن السيبراني لحماية أجهزة وأنظمة التحكم الصناعي (ICS/OT). • عينة من مخطط تصميم شبكة الإنتاج الصناعي (نسخة إلكترونية أو نسخة ورقية). • إجراءات الحماية الخاصة بالأنظمة الصناعية.
٣-١-٥	بالإضافة إلى ما يمكن تطبيقه من الضوابط ضمن المكونات الرئيسية رقم (١) و (٢) و (٣) و (٤) الضرورية لحماية بيانات الجهة وخدماتها، فإن متطلبات الأمن السيبراني لحماية أجهزة وأنظمة التحكم الصناعي(ICS/OT) يجب أن تغطي بحد أدنى ما يلي:
١-٣-١-٥	التقييد الحازم والتقسيم المادي والمنطقي عند ربط شبكات الإنتاج الصناعية(ICS/OT) مع الشبكات الأخرى التابعة للجهة، مثل: شبكة الأعمال الداخلية للجهة "Corporate Network".
	إرشادات تطبيق الضوابط: • التأكد من أن السياسة الموثقة المعتمدة تشمل على متطلبات التقييد الحازم والتقسيم المادي والمنطقي عند ربط شبكات الإنتاج الصناعية (ICS/OT) مع الشبكات الأخرى التابعة للجهة. • العمل على تحديد جميع شبكات الإنتاج الصناعية (ICS/OT) في الجهة. • تحديد المخاطر السيبرانية المترتبة على ربط شبكات الإنتاج الصناعية مع الشبكات الأخرى • العمل على عزل شبكات الإنتاج الصناعية (ICS/OT) عن الشبكات الأخرى مادياً أو منطقياً بناءً على المخاطر السيبرانية، ومن هذه الشبكات: ○ شبكة الأعمال الداخلية للجهة (corporate network) ○ شبكة المنطقة المحايدة الصناعية (industrial demilitarized zone) • التأكد من عدم ربط شبكات الإنتاج الصناعية مع الشبكات الأخرى التابعة للجهة إلا للاتصالات الضرورية، والتأكد من التقييد الحازم والتقسيم المادي والمنطقي في حال تم الربط.
	المخرجات المتوقعة: • وثيقة سياسة الأمن السيبراني التي تغطي متطلبات لحماية أجهزة وأنظمة التحكم الصناعي (مثال: نسخة إلكترونية أو نسخة ورقية رسمية).

• مخطط تصميم شبكة الإنتاج الصناعي (نسخة إلكترونية أو نسخة ورقية) يوضح كيفية اتصالها بشبكة الأعمال الداخلية للجهة.	
٢-٣-١-٥	التقييد الحازم والتقسيم المادي والمنطقي عند ربط الأنظمة أو الشبكات الصناعية مع شبكات خارجية، مثل: الإنترنت أو الدخول عن بعد أو الاتصال اللاسلكي.

إرشادات تطبيق الضوابط:

- التأكد من أن السياسة الموثقة المعتمدة تشمل على متطلبات التقييد الحازم والتقسيم المادي والمنطقي عند ربط الأنظمة أو الشبكات الصناعية مع شبكات خارجية.
- العمل على تحديد جميع أنظمة وشبكات الإنتاج الصناعية (ICS/OT) في الجهة.
- تحديد وتقييم المخاطر السيبرانية المترتبة بربط الأنظمة والشبكات الصناعية مع شبكات خارجية
- العمل على عزل الأنظمة والشبكات الصناعية عن الشبكات الخارجية مادياً أو منطقياً بناءً على المخاطر السيبرانية، ومن هذه الشبكات:
  - الإنترنت
    - استخدام الوكيل (proxy) والوصول عبر المنطقة المحايدة (DMZ)
  - الدخول عن بعد
    - استخدام تقنيات الدخول عن بعد الآمنة (VPN) الخادم الوسيط (jump server) والتحقق من الهوية متعدد العناصر (MFA)
  - الشبكة اللاسلكية
    - استخدام البروتوكولات اللاسلكية الآمنة بناءً على المعايير الوطنية للتشفير (NCS-1:2020)
- التأكد من عدم ربط شبكات الإنتاج الصناعية مع الشبكات الخارجية إلا للاتصالات الضرورية، والتأكد من التقييد الحازم والتقسيم المادي والمنطقي في حال تم الربط.

المخرجات المتوقعة:

- وثيقة سياسة الأمن السيبراني التي تغطي متطلبات لحماية أجهزة وأنظمة التحكم الصناعي (مثال: نسخة إلكترونية أو نسخة ورقية رسمية).
- مخطط تصميم شبكة الإنتاج الصناعي (نسخة إلكترونية أو نسخة ورقية) يوضح كيفية اتصالها بالشبكات الخارجية.

٣-٣-١-٥	تفعيل سجلات الأحداث (Event logs) الخاصة بالأمن السيبراني للشبكة الصناعية والاتصالات المرتبطة بها ما أمكن ذلك، والمراقبة المستمرة لها.

إرشادات تطبيق الضوابط:

- التأكد من أن السياسة الموثقة المعتمدة تشمل على متطلبات تفعيل سجلات الأحداث(Event logs) الخاصة بالأمن السيبراني للشبكة الصناعية والاتصالات المرتبطة بها ما أمكن ذلك، والمراقبة المستمرة لها.
- العمل على تحديد جميع شبكات الإنتاج الصناعية (ICS/OT) في الجهة.
- العمل على تفعيل جمع سجلات الأحداث الخاصة بالأمن السيبراني للشبكة الصناعية والاتصالات المرتبطة بها ما أمكن ذلك.
- ربط سجلات الأحداث الخاصة بالأمن السيبراني للشبكة الصناعية والاتصالات المرتبطة بها بالنظام المركزي لتحليل ومراقبة السجلات (SIEM)، مع الأخذ بعين الاعتبار:
  - أن يكون النظام مؤهل من قبل موردي الأنظمة والشبكات الصناعية في الجهة
  - أن يكون النظام معزول (منطقياً على الأقل)
- العمل مع موردي الأنظمة والشبكات الصناعية في الجهة ومختصي الأنظمة والشبكات الصناعية لتحديد قواعد وحالات استخدام (use cases) لسجلات الأحداث الخاصة بالأمن السيبراني للشبكة الصناعية والاتصالات المرتبطة بها.
- تعيين فريق متخصص لمراقبة السجلات على مدار الساعة (٧/٢٤).

المخرجات المتوقعة

- وثيقة سياسة الأمن السيبراني التي تغطي متطلبات لحماية أجهزة وأنظمة التحكم الصناعي (مثال: نسخة إلكترونية أو نسخة ورقية رسمية).
- لقطة شاشة توضح تفعيل سجلات الأحداث الخاصة بالأمن السيبراني للشبكة الصناعية المرتبطة بها ما أمكن ذلك.
- إثبات المراقبة المستمرة لسجلات الأحداث، (مثال: الفريق المعتمد والمخصص للمتابعة والمراقبة لهذه السجلات).

٥-١-٣-٤	عزل أنظمة معدات السلامة (Safety Instrumented System "SIS").

إرشادات تطبيق الضوابط:

- التأكد من أن السياسة الموثقة المعتمدة تشمل على متطلبات عزل أنظمة معدات السلامة.
- العمل على تحديد جميع أنظمة معدات السلامة في الجهة.
- تحديد وتقييم المخاطر السيبرانية المترتبة بربط أنظمة معدات السلامة مع الأنظمة الأخرى.
- العمل على عزل أنظمة معدات السلامة عن الأنظمة الأخرى بناءً على التالي:
  - العزل المادي أو المنطقي بناءً على المخاطر السيبرانية وارشادات ومزودو أنظمة معدات السلامة.
  - تحديد نوع العزل الذي يتم تطبيقه ومنها:
    - عزل أنظمة معدات السلامة (SIS) عن أجهزة المستخدمين الهندسية (engineering workstations)
    - عزل أنظمة معدات السلامة عن الأنظمة الصناعية

▪ عزل أنظمة معدات السلامة عن الشبكات الأخرى	
المخرجات المتوقعة: • وثيقة سياسة الأمن السيبراني التي تغطي متطلبات لحماية أجهزة وأنظمة التحكم الصناعي (مثال: نسخة إلكترونية أو نسخة ورقية رسمية). • مخطط تصميم شبكة أنظمة معدات السلامة المعتمد (نسخة إلكترونية أو نسخة ورقية).	
٥-١-٣-٥	التقييد الحازم لاستخدام وسائط التخزين الخارجية.
إرشادات تطبيق الضوابط: • التأكد من أن السياسة الموثقة المعتمدة تشمل على متطلبات التقييد الحازم لاستخدام وسائط التخزين الخارجية. • العمل على إعداد الأنظمة والتقنيات لمنع استخدام وسائط التخزين الخارجية تلقائياً، وهذا قد يشمل: ○ إعداد تقنيات حماية الأنظمة الصناعية لمنع استخدام وسائط التخزين الخارجية تلقائياً، أو ○ إعداد النظام المركزي للخدمات (مثل Active Directory) لمنع استخدام وسائط التخزين الخارجية تلقائياً، أو ○ إعداد سجل الأجهزة (registry) لمنع استخدام وسائط التخزين الخارجية تلقائياً. • العمل على تطوير واعتماد إجراءات لمنح صلاحية استخدام وسائط التخزين الخارجية (على سبيل المثال لا الحصر: طلب الموافقات عن طريق البريد الإلكتروني، أو ورقياً، أو عن طريق نظام داخلي)، بحيث تحتوي على: ○ سبب طلب الموافقة على الاستخدام. ○ مدة الاستخدام. • العمل على تحديد آلية التعامل مع البيانات المخزنة في وسائط التخزين بحيث يتم فحصه قبل الاستخدام ومسح البيانات بعد الانتهاء.	
المخرجات المتوقعة: • وثيقة سياسة الأمن السيبراني التي تغطي متطلبات لحماية أجهزة وأنظمة التحكم الصناعي (مثال: نسخة إلكترونية أو نسخة ورقية رسمية). • لقطة شاشة توضح تقييد استخدام وسائط التخزين الخارجية على الأنظمة الصناعية. • إجراءات تقييد استخدام وسائط التخزين الخارجية على الأنظمة الصناعية، مع إثبات تطبيق هذه الإجراءات (مثال: إجراءات الموافقة على الاستخدام من خلال رسائل البريد الإلكتروني، نسخة ورقية أو إلكترونية من استمارة الموافقة على الاستخدام).	
٥-١-٣-٦	التقييد الحازم لتوصيل الأجهزة المحمولة على شبكة الإنتاج الصناعية.

إرشادات تطبيق الضوابط:

- التأكد من أن السياسة الموثقة المعتمدة تشمل على متطلبات التقييد الحازم لتوصيل الأجهزة المحمولة على شبكة الإنتاج الصناعية.
- تحديد وتطبيق وضبط التقنيات المناسبة لتقييد الوصول الى الشبكة الصناعية (network access control).
- العمل على تحديد التقنيات المناسبة للتحقق من الهوية للأجهزة المحمولة (مثل RADIUS أو باستخدام MAC Authentication).
- التأكد من أن امكانية توصيل الأجهزة المحمولة على شبكة الإنتاج الصناعية غير مفعلة بصورة أساسية، ويتم تقييد هذا التوصيل في حال وجود حاجه لتفعيله.
- العمل على تطوير واعتماد إجراءات لمنح صلاحية استخدام الأجهزة المحمولة (على سبيل المثال لا الحصر: طلب الموافقات عن طريق البريد الإلكتروني، أو ورقياً، أو عن طريق نظام داخلي)، بحيث تحتوي على:
  - سبب طلب الموافقة على الاستخدام.
  - مدة الاستخدام.
- العمل على تحديد آلية التعامل مع البيانات المخزنة في الأجهزة المحمولة بحيث يتم فحصه قبل الاستخدام ومسح البيانات بعد الانتهاء.

المخرجات المتوقعة:

- وثيقة سياسة الأمن السيبراني التي تغطي متطلبات لحماية أجهزة وأنظمة التحكم الصناعي (مثال: نسخة إلكترونية أو نسخة ورقية رسمية).
- لقطة شاشة توضح تقييد توصيل الأجهزة المحمولة على الأنظمة الصناعية.
- إجراءات تقييد توصيل الأجهزة المحمولة على شبكة الإنتاج الصناعية، مع إثبات تطبيق هذه الإجراءات (مثال: إجراءات الموافقة على التوصيل المحتمل من خلال رسائل البريد الإلكتروني، نسخة ورقية أو إلكترونية من استمارة الموافقة).

٥-١-٣-٧	مراجعة إعدادات وتحصين الأنظمة الصناعية، وأنظمة الدعم والأجهزة الآلية الصناعية (Secure Configuration and Hardening) دورياً.

إرشادات تطبيق الضوابط:

- التأكد من أن السياسة الموثقة المعتمدة تشمل على متطلبات مراجعة إعدادات وتحصين الأنظمة الصناعية، وأنظمة الدعم والأجهزة الآلية الصناعية دورياً.
- العمل على تحديد جميع الأنظمة الصناعية، وأنظمة الدعم والأجهزة الآلية الصناعية في الجهة.
- العمل على تطوير معايير للتحصين (hardening standards) للأنظمة الصناعية، وأنظمة الدعم والأجهزة الآلية الصناعية بالتعاون مع مزود الأنظمة والشركات الصانعة.

• توثيق وتنفيذ خطة عمل لمراجعة إعدادات وتحصين الأنظمة الصناعية، وأنظمة الدعم والأجهزة الآلية الصناعية بشكل دوري فردياً أو باستخدام أدوات آلية. • العمل مع الإدارات المعنية لتطوير خطة تصحيحية لنتائج مراجعة الإعدادات والتحصين	
المخرجات المتوقعة: • وثيقة سياسة الأمن السيبراني التي تغطي متطلبات لحماية أجهزة وأنظمة التحكم الصناعي (مثال: نسخة إلكترونية أو نسخة ورقية رسمية). • تقارير مراجعة إعدادات وتحصين الأنظمة الصناعية، وأنظمة الدعم والأجهزة الآلية الصناعية يوضح تطبيقها بشكل دوري.	
٥-١-٣-٨	إدارة ثغرات الأنظمة الصناعية (ICS/OT Vulnerability Management).
إرشادات تطبيق الضوابط: • التأكد من أن السياسة الموثقة المعتمدة تشمل على متطلبات إدارة ثغرات الأنظمة الصناعية. • العمل على تحديد الأنظمة الصناعية في الجهة. • تحديد التقنيات المناسبة لفحص الثغرات في الأنظمة الصناعية في الجهة، على أن تكون مؤهله من قبل مزودي الأنظمة الصناعية والشركات الصانعة. • تحليل مدى تأثير الفحص على الأنظمة الصناعية وتحديد نوع فحص الثغرات الذي يتم عمله على ان يكون اجتياحي (invasive) أم غير اجتياحي (non-invasive) مع تطوير خطة للاستمرارية في حالة طوارئ (contingency plan). • جدولة وعمل فحوصات الثغرات بناءً على الخطة المعتمدة. • العمل مع الإدارات المعنية لوضع خطة لمعالجة الثغرات.	
المخرجات المتوقعة: • وثيقة سياسة الأمن السيبراني التي تغطي متطلبات لحماية أجهزة وأنظمة التحكم الصناعي (مثال: نسخة إلكترونية أو نسخة ورقية رسمية). • تقرير مراجعة ثغرات الأنظمة الصناعية، يوضح الإجراءات المتبعة لإدارة الثغرات.	
٥-١-٣-٩	إدارة حزم التحديثات والإصلاحات الأمنية للأنظمة الصناعية (ICS/OT Patch Management).
إرشادات تطبيق الضوابط: • التأكد من أن السياسة الموثقة المعتمدة تشمل على متطلبات إدارة حزم التحديثات والإصلاحات الأمنية للأنظمة الصناعية. • العمل على تحديد الأنظمة الصناعية في الجهة، وتحديد حساسيتها، وفقا للمتطلبات التشريعية والتنظيمية ذات العلاقة.	

- تحديد قنوات اتصال معتمدة في الجهة مع موردي الأنظمة والشركات الصانعة لمعرفة أحدث حزم التحديثات والإصلاحات الأمنية للأنظمة الصناعية في جهة.
- العمل على تطوير إجراءات وخطة معتمدة لإدارة حزم التحديثات والإصلاحات الأمنية للأنظمة الصناعية.
- تحليل مدى تأثير تطبيق حزم التحديثات والإصلاحات على الأنظمة الصناعية مع تطوير خطة للاستمرارية في حالة طوارئ (contingency plan).
- العمل مع الإدارات المعنية لاختبار حزم التحديثات والإصلاحات الأمنية حسب الإجراءات المعتمدة.
- جدولة وتطبيق حزم التحديثات والإصلاحات الأمنية للأنظمة الصناعية بناءً على الخطة المعتمدة.

المخرجات المتوقعة:

- وثيقة سياسة الأمن السيبراني التي تغطي متطلبات لحماية أجهزة وأنظمة التحكم الصناعي (مثال: نسخة إلكترونية أو نسخة ورقية رسمية).
- تقرير مراجعة حزم التحديثات والإصلاحات الأمنية للأنظمة الصناعية، يوضح الإجراءات المتبعة لإدارة حزم التحديثات والإصلاحات.

١٠-٣-١-٥	إدارة البرامج الخاصة بالأمن السيبراني الصناعي للحماية من الفيروسات والبرمجيات المشبوهة والضارة.

إرشادات تطبيق الضوابط:

- التأكد من أن السياسة الموثقة المعتمدة تشمل على متطلبات إدارة البرامج الخاصة بالأمن السيبراني الصناعي للحماية من الفيروسات والبرمجيات المشبوهة والضارة.
- العمل على تحديد الأنظمة الصناعية في الجهة، وتحديد حساسيتها، وفقًا للمتطلبات التشريعية والتنظيمية ذات العلاقة.
- تحديد التقنيات المناسبة للحماية من الفيروسات والبرمجيات المشبوهة والضارة في الأنظمة الصناعية في الجهة، على أن تكون معتمدة من قبل مزودي الأنظمة الصناعية والشركات الصانعة.
- تطبيق وإعداد أدوات ا لحماية من الفيروسات والبرمجيات المشبوهة والضارة في الأنظمة الصناعية بناءً على إجراءات مزودي الأنظمة الصناعية والشركات الصانعة.
- العمل على مراجعة أدوات الحماية من الفيروسات والبرمجيات المشبوهة والضارة في الأنظمة الصناعية دورياً للتأكد من شمولية أدوات الحماية للأنظمة الصناعية.
- تطوير إجراءات للإدارة الآمنة لأدوات الحماية من الفيروسات والبرمجيات المشبوهة والضارة في الأنظمة الصناعية.

المخرجات المتوقعة:

- وثيقة سياسة الأمن السيبراني التي تغطي متطلبات لحماية أجهزة وأنظمة التحكم الصناعي (مثال: نسخة إلكترونية أو نسخة ورقية رسمية).
- القائمة المحدثة لأنظمة الحماية من الفيروسات والبرمجيات المشبوهة والضارة لحماية الأنظمة الصناعية.

	• تقارير تحديث أنظمة الحماية من الفيروسات والبرمجيات المشبوهة والضارة.
٤-١-٥	يجب مراجعة متطلبات الأمن السيبراني لحماية أجهزة وأنظمة التحكم الصناعي (ICS/OT) للجهة دورياً.
	إرشادات تطبيق الضوابط: • مراجعة وتحديث سياسة ومتطلبات الأمن السيبراني لحماية أجهزة وأنظمة التحكم الصناعي (ICS/OT) في الجهة بشكل دوري حسب خطة موثقة ومعتمدة للمراجعة بناءً على فترة زمنية محددة (بشكل سنوي على سبيل المثال)، أو في حالة حدوث تغييرات في المتطلبات التشريعية والتنظيمية ذات العلاقة. كما يجب توثيق المراجعة والتغييرات التي تمت على متطلبات الأمن السيبراني لحماية أجهزة وأنظمة التحكم الصناعي (ICS/OT) في الجهة واعتمادها من قبل رئيس الجهة أو من ينيبه.
	المخرجات المتوقعة: • وثيقة معتمدة تحدد جدول المراجعة للسياسة. • وثيقة السياسة بما يوضح أن تكون محدثة وتم توثيق التغييرات على متطلبات الأمن السيبراني لحماية أجهزة وأنظمة التحكم الصناعي (ICS/OT) واعتمادها من قبل رئيس الجهة أو من ينيبه. • موافقة رسمية من قبل رئيس الجهة أو من ينيبه على السياسة المحدثة (مثال: عن طريق البريد الإلكتروني الرسمي للجهة، أو التوقيع الورقي أو الإلكتروني).


الهيئة الوطنية
للأمن السيبراني
National Cybersecurity Authority