الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

الدليل الإرشادي لتطبيق ضوابط الأمن السيبراني للأنظمة التشغيلية

Guide to Operational Technology Cybersecurity Controls Implementation **(GOTCC-1:2023)**

إشارة المشاركة: أبيض
تصنيف الوثيقة: عام

إخلاء مسؤولية: طُور هذا الدليل الإرشادي عن طريق الهيئة الوطنية للأمن السيبراني لتمكين الجهات من تطبيق ضوابط الأمن السيبراني للأنظمة التشغيلية، 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 للاستلام.

برتقالي – مشاركة محدودة

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

أخضر – مشاركة في نفس المجتمع

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

أبيض – غير محدود

قائمة المحتويات

مقدمة..... ٥
الهدف..... ٥
نطاق العمل ٥
مكونات وهيكلية ضوابط للأمن السيبراني للأنظمة التشغيلية..... ٦
هيكلية الدليل الإرشادي..... ٧
إرشادات عامة لتطبيق ضوابط الأمن السيبراني للأنظمة التشغيلية..... ٨
إرشادات تطبيق ضوابط الأمن السيبراني للأنظمة التشغيلية ٩

قائمة الأشكال

شكل١: المكونات الأساسية والفرعية لضوابط الأمن السيبراني للأنظمة التشغيلية..... ٦
شكل ٢هيكلية الدليل الإرشادي لضوابط الأمن السيبراني للأنظمة التشغيلية..... ٧

مقدمة

طورت الهيئة الوطنية للأمن السيبراني (ويشار لها في هذه الوثيقة بـ "الهيئة") الدليل الإرشادي لتطبيق ضوابط الأمن السيبراني المنصوص عليها في ضوابط الأمن السيبراني للأنظمة التشغيلية (OTCC - 1: 2022) (ويشار لها في هذه الوثيقة بـ "الضوابط")، وذلك للمساهمة في تمكين الجهات الوطنية من تطبيق متطلبات الالتزام بضوابط الأمن السيبراني للأنظمة التشغيلية. حيث تم بناء هذا الدليل الإرشادي بالاعتماد على المعلومات والخبرات التي قامت الهيئة بجمعها وتحليلها منذ نشر الضوابط ومواءمة هذا الدليل الإرشادي مع أفضل الممارسات الرائدة في الأمن السيبراني لتسهيل تطبيق الضوابط في الجهات الوطنية.

الهدف

الهدف الرئيسي من هذا الدليل الإرشادي هو المساهمة في تمكين الجهات الوطنية لتحقيق متطلبات الالتزام بتطبيق ضوابط الأمن السيبراني للأنظمة التشغيلية 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 ضوابط الأمن السيبراني للأنظمة التشغيلية (OTCC-1:2022) هو:

- تنطبق هذه الضوابط على أنظمة التحكم الصناعي الموجودة في المرافق الحساسة – وفقاً للمعايير المذكورة بالوثيقة -من قبل الجهات المالكة، أو المشغلة، أو المستضيفة لهذه المرافق، سواء أكانت جهات حكومية (وتشمل وزارات وهيئات ومؤسسات وغيرها) أم جهات القطاع الخاص التي تملك بنى تحتية وطنية حساسة (CRITICAL NATIONAL INFRASTRUCRES "CNIs") أو تقوم بتشغيلها، أو استضافتها داخل المملكة العربية السعودية؛ أو خارجها، (ويشار لها جميعاً في هذه الوثيقة ب"الجهة").
- تشجع الهيئة الجهات الأخرى في المملكة وبشدة على الاستفادة من هذه الضوابط لتطبيق أفضل الممارسات في ما يتعلق بتحسن الأمن السيبراني وتطويره داخل الجهة.

مكونات وهيكلية ضوابط الأمن السيبراني للأنظمة التشغيلية

يوضح الشكل رقم (١) أدناه المكونات الأساسية والفرعية لضوابط الأمن السيبراني للأنظمة التشغيلية

١	حوكمة الأمن السيبراني Cybersecurity Governance	١-١	سياسات وإجراءات الأمن السيبراني Cybersecurity Policies and Procedures	١-٢	أدوار ومسؤوليات الأمن السيبراني Cybersecurity Roles and Responsibilities
		١-٣	إدارة مخاطر الأمن السيبراني Cybersecurity Risk Management	١-٤	الأمن السيبراني ضمن إدارة مشاريع أنظمة التحكم الصناعي Cybersecurity in Industrial Control System Project Management
		١-٥	الأمن السيبراني ضمن إدارة التغيير Cybersecurity in Change Management	١-٦	المراجعة والتدقيق الدوري للأمن السيبراني Periodical Cybersecurity Review and Audit
		١-٧	الأمن السيبراني المتعلق بالموارد البشرية Cybersecurity in Human Resources	١-٨	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 النظم ومرافق المعالجة System and Processing Facility Protection	٢-٤	إدارة أمن الشبكات Network Security Management
		٢-٥	أمن الأجهزة المحمولة Mobile Devices Security	٢-٦	حماية البيانات والمعلومات Data and Information Protection
		٢-٧	التشفير Cryptography	٢-٨	إدارة النسخ الاحتياطية Backup and Recovery Management
		٢-٩	إدارة الثغرات Vulnerability Management	٢-١٠	اختبار الاختراق Penetration Testing
		٢-١١	إدارة سجلات الأحداث ومراقبة الأمن السيبراني Cybersecurity Event Logs and Monitoring Management	٢-١٢	إدارة حوادث وتهديدات الأمن السيبراني Cybersecurity Incident and Threat Management
		٢-١٣	الأمن المادي Physical Security		
٣	صمود الأمن السيبراني Cybersecurity Resilience	٣-١	جوانب صمود الأمن السيبراني في إدارة استمرارية الأعمال Cybersecurity Resilience Aspects of Business Continuity Management (BCM)		
٤	الأمن السيبراني المتعلق بالأطراف الخارجية Third-Party Cybersecurity	٤-١	الأمن السيبراني المتعلق بالأطراف الخارجية Third-Party Cybersecurity		

شكل ١: المكونات الأساسية والفرعية لضوابط الأمن السيبراني للأنظمة التشغيلية

هيكلية الدليل الإرشادي

يوضح الشكل رقم (٢) أدناه هيكلية الدليل الإرشادي لضوابط الأمن السيبراني للأنظمة التشغيلية

١	اسم المكون الأساسي
الرقم المرجعي للمكون 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 ١: هيكلية الدليل الإرشادي لضوابط الأمن السيبراني للأنظمة التشغيلية

إرشادات عامة لتطبيق ضوابط الأمن السيبراني للأنظمة التشغيلية

إرشادات عامة
• حصر المرافق وتصنيفها حسب الآلية المعتمدة في أداة حصر وتحديد مستوى المرفق الصادرة عن الهيئة الوطنية للأمن السيبراني، ومراجعتها بشكل دوري. • حصر الأصول والأنظمة التشغيلية الموجودة في المرافق، ومراجعتها بشكل دوري. • حصر حسابات المستخدمين ذوي الصلاحيات الهامة والحساسة (Privileged Accounts) والذين لديهم القدرة على الوصول للأنظمة التشغيلية أو إداراتها، ومراجعتها بشكل دوري. • تحديد وتوثيق متطلبات الأمن السيبراني للأنظمة التشغيلية والأدوار والمسؤوليات المتعلقة بها، واعتمادها من قبل صاحب الصلاحية ومراجعتها بشكل دوري. • مراجعة الدليل الإرشادي لتطبيق الضوابط الأساسية للأمن السيبراني والعمل على تطبيق الضوابط ذات العلاقة بضوابط الأمن السيبراني للأنظمة التشغيلية. • وضع خطة لتطبيق ضوابط الأمن السيبراني للأنظمة التشغيلية، ومتابعتها بشكل مستمر.

إرشادات تطبيق ضوابط الأمن السيبراني للأنظمة التشغيلية

I حوكمة الأمن السيبراني (Cybersecurity Governance)

١-١	سياسات وإجراءات الأمن السيبراني (Cybersecurity Policies and Procedures)
الهدف	ضمان توثيق ونشر متطلبات الأمن السيبراني لأنظمة التحكم الصناعي (OT/ICS) والتزام الجهة بها، وذلك وفقاً لمتطلبات الأعمال التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية ذات العلاقة.
الضوابط	
١-١-١	رجوعاً للضابطين ١-٣-١ و ١-٣-٢ في الضوابط الأساسية للأمن السيبراني؛ يجب على الجهة توثيق مجموعة من سياسات وإجراءات الأمن السيبراني المخصصة لأنظمة التحكم الصناعي (OT/ICS) واعتمادها وتطبيقها.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج إجراء تطوير وثائق الأمن السيبراني • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية **إرشادات تطبيق الضوابط:** • العمل على تحديد متطلبات الأمن السيبراني الخاصة بأنظمة التحكم الصناعي (OT/ICS)، وتوثيقها في سياسات وإجراءات ومعايير الأمن السيبراني الخاصة بأنظمة التحكم الصناعي (OT/ICS)، بحيث يتم اعتمادها من قبل صاحب الصلاحية في الجهة بناء على دليل الصلاحيات المعتمد لدى الجهة. • التأكّد من نشر السياسات والإجراءات للعاملين والمتعاقدين في الجهة والأطراف المعنية بها الداخليين والخارجيين، من خلال قنوات الاتصال المعتمدة وذلك حسب النطاق المحدد في السياسة. • العمل على وضع خطة عمل لتطبيق سياسات وإجراءات ومعايير الأمن السيبراني وتشمل جميع أصحاب المصلحة الداخليين والخارجيين وكل 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.
	المخرجات المتوقعة: • جميع سياسات وإجراءات ومعايير الأمن السيبراني الخاصة بأنظمة التحكم الصناعي (OT/ICS) الموثقة والمعتمدة من قبل صاحب الصلاحية في الجهة أو من ينيبه. • إثبات يؤكد نشر سياسات وإجراءات ومعايير الأمن السيبراني الخاصة بأنظمة التحكم الصناعي (OT/ICS) للعاملين والأطراف المعنية.

١-١-٢	رجوعاً للضابط ١-٣-٣ في الضوابط الأساسية للأمن السيبراني؛ يجب أن تكون سياسات وإجراءات الأمن السيبراني لأنظمة التحكم الصناعي (OT/ICS) مدعومة بمتطلبات ومعايير للأمن السيبراني والمتطلبات التقنية ذات العلاقة. (مثل: توصيات الجهة المصنعة، إرشادات التطبيق والتنفيذ، إرشادات إدارة الإعدادات).
	أدوات الأمن السيبراني ذات العلاقة: • معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • **إرشادات تطبيق الضوابط:** • العمل على تحديد وتوثيق واعتماد المعايير التقنية بحيث تغطي الأصول الخاصة بأنظمة التحكم الصناعي (OT/ICS) في الجهة. (على سبيل المثال: توصيات الجهة المصنعة، إرشادات التطبيق والتنفيذ، إرشادات إدارة الإعدادات، إلخ..). • العمل على نشر المعايير التقنية للإدارات ذات العلاقة في الجهة (مثال: الإدارة المعنية بالأنظمة التشغيلية في المنشأة) والتأكد من تطبيقها بشكل دوري على الأصول الخاصة بأنظمة التحكم الصناعي (OT/ICS).
	المخرجات المتوقعة: • وثائق معايير الأمن السيبراني الخاصة بأنظمة التحكم الصناعي (OT/ICS) المعتمدة في الجهة. • إثبات يؤكد تطبيق سياسات وإجراءات الأمن السيبراني الخاصة بأنظمة التحكم الصناعي (OT/ICS) في الجهة.
١-١-٣	رجوعاً للضابط ١-٣-٤ في الضوابط الأساسية للأمن السيبراني؛ يجب مراجعة سياسات وإجراءات الأمن السيبراني لأنظمة التحكم الصناعي (OT/ICS) دوريا، أو عند حدوث تغييرات تؤثر على أمن وسلامة أنظمة التحكم الصناعي (OT/ICS). (مثل: حدوث تغييرات في مستوى وطبيعة المخاطر، أو تغيير في الهيكل التنظيمي للجهة، أو تغيرات في العمليات والإجراءات التشغيلية).
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • **إرشادات تطبيق الضوابط:** • العمل على مراجعة سياسات وإجراءات ومعايير الأمن السيبراني الخاصة بأنظمة التحكم الصناعي (OT/ICS) 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 الخاصة بأنظمة التحكم الصناعي (OT/ICS) 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 مراجعة وتحديث سياسات وإجراءات ومعايير الأمن السيبراني الخاصة بأنظمة التحكم الصناعي (OT/ICS) عند حدوث تغييرات تؤثر على أمن وسلامة أنظمة التحكم الصناعي (OT/ICS). (مثل: حدوث تغييرات في مستوى وطبيعة المخاطر، أو تغيرات في العمليات والإجراءات التشغيلية). • العمل على توثيق المراجعة والتغييرات التي تتم على سياسات وإجراءات ومعايير الأمن السيبراني الخاصة بأنظمة التحكم الصناعي (OT/ICS) واعتمادها من قبل رئيس الجهة أو من ينيبه.
	المخرجات المتوقعة: • وثيقة معتمدة تحدد جدول المراجعة. • وثيقة معتمدة توضح مراجعة سياسات وإجراءات ومعايير الأمن السيبراني الخاصة بأنظمة التحكم الصناعي (OT/ICS) بشكل دوري بناءً على الفترة الزمنية المحددة للمراجعة. • وثائق السياسات والإجراءات والمعايير والتي توضح مراجعة وتحديث وتوثيق التغييرات واعتمادها من قبل صاحب الصلاحية. • الموافقة الرسمية والاعتماد من قبل صاحب الصلاحية على السياسات والإجراءات والمعايير المحدثة.
١-٢	**أدوار ومسؤوليات الأمن السيبراني (Cybersecurity Roles and Responsibilities)**
الهدف	ضمان تحديد أدوار ومسؤوليات واضحة لجميع الأطراف المشاركة في تطبيق ضوابط الأمن السيبراني للأنظمة التشغيلية (OTCC) في الجهة.
الضوابط	
١-٢-١	بالإضافة للضوابط ضمن المكون الفرعي ١-٤ في الضوابط الأساسية للأمن السيبراني؛ يجب أن تغطي متطلبات الأمن السيبراني المتعلقة بأدوار ومسؤوليات الأمن السيبراني في بيئة أنظمة التحكم الصناعي (OT/ICS) بحد أدنى ما يلي:
	١-٢-١-١ يجب على صاحب الصلاحية، تحديد الأدوار والمسؤوليات الخاصة بالأمن السيبراني (RACI) وتوثيقها واعتمادها لجميع أصحاب المصلحة المعنيين بأنظمة التحكم الصناعي (OT/ICS)، مع الأخذ في الحسبان 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 الخاصة بأنظمة التحكم الصناعي (OT/ICS) على شكل مصفوفة تفصيلية (RACI Matrix) والتأكد من أن جميع الأطراف المشاركة في تطبيق ضوابط الأمن السيبراني في الجهة على دراية بمسؤولياتهم في تطبيق برامج ومتطلبات الأمن السيبراني، مع الأخذ بعين الاعتبار عدم تعارض المصالح.

	• العمل على أن يكون الهيكل التنظيمي والأدوار والمسؤوليات في الجهة مدعومة 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 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، إعداد وتطبيق برنامج التوعية بالأمن السيبراني، إلخ..) ○ الأدوار والمسؤوليات ذات العلاقة بالأمن السيبراني للإدارات الأخرى في الجهة (كالإدارة المعنية بالأنظمة التشغيلية، الإدارة المعنية بشؤون الموظفين، الإدارة المعنية بالأمن الصناعي، إلخ..) ○ الأدوار والمسؤوليات ذات العلاقة بالأمن السيبراني لكافة العاملين والمتعاقدين والمتعاقدين بالباطن.
	المخرجات المتوقعة: • وثيقة الهيكل التنظيمي. • وثيقة أدوار ومسؤوليات الأمن السيبراني (RACI Matrix) الخاصة بأنظمة التحكم الصناعي (OT/ICS) المعتمدة بالجهة (نسخة الكترونية أو نسخة ورقية رسمية). • إثبات يؤكد نشر وثيقة الأدوار والمسؤوليات الخاصة بالأمن السيبراني لذوي العلاقة في الجهة.
١-٢-١-٢	يجب إسناد أدوار الأمن السيبراني ومسؤولياته المتعلقة بأنظمة التحكم الصناعي (OT/ICS) للإدارة المعنية بالأمن السيبراني لدى الجهة؛ مع الأخذ في الحسبان عدم تعارض المصالح.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج أدوار ومسؤوليات الأمن السيبراني. **إرشادات تطبيق الضوابط:** • العمل على إسناد أدوار الأمن السيبراني ومسؤولياته المتعلقة بأنظمة التحكم الصناعي (OT/ICS) للإدارة المعنية بالأمن السيبراني لدى الجهة؛ مع الأخذ بالاعتبار عدم تعارض المصالح.
	المخرجات المتوقعة: • إثبات يؤكد إسناد أدوار الأمن السيبراني ومسؤولياته المتعلقة بأنظمة التحكم الصناعي للإدارة المعنية بالأمن السيبراني لدى الجهة؛ مع الأخذ في الحسبان عدم تعارض المصالح.
١-٣	**إدارة مخاطر الأمن السيبراني (Cybersecurity Risk Management)**

الهدف	ضمان إدارة مخاطر الأمن السيبراني على نحو ممنهج؛ يهدف إلى حماية الأصول المعلوماتية، وأنظمة التحكم الصناعي (OT/ICS)، وذلك وفقاً للسياسات والإجراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية ذات العلاقة.
الضوابط	
١-٣-١	بالإضافة للضوابط ضمن المكون الفرعي ١-٥ في الضوابط الأساسية للأمن السيبراني؛ يجب أن تغطي متطلبات إدارة مخاطر الأمن السيبراني المتعلقة بأنظمة التحكم الصناعي (OT/ICS) بحد أدنى ما يلي:
١-٣-١-١	وضع منهجية مخاطر الأمن السيبراني، المتعلقة بأنظمة التحكم الصناعي (OT/ICS) ضمن منهجية إدارة المخاطر و إدارة مخاطر السلامة وإجراءاتها في الجهة.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج إجراء إدارة مخاطر الأمن السيبراني • نموذج سجل مخاطر الأمن السيبراني **إرشادات تطبيق الضوابط:** • العمل على تطوير وتطبيق منهجية مخصصة لمخاطر الأمن السيبراني الخاصة بأنظمة التحكم الصناعي (OT/ICS) ضمن منهجية إدارة المخاطر وإدارة مخاطر السلامة وإجراءاتها في الجهة وفق ما يصدر من الهيئة الوطنية للأمن السيبراني. • التأكد من موائمة منهجية مخاطر الأمن السيبراني الخاصة بأنظمة التحكم الصناعي (OT/ICS) مع منهجية إدارة المخاطر الجهة وإدارة مخاطر السلامة وإجراءاتها في الجهة وأنها جزء منها. • العمل على تطوير خطة مراجعة بشكل دوري وعلى فترات زمنية محددة وتحضير تقرير موجز. **المخرجات المتوقعة:** • منهجية إدارة مخاطر الأمن السيبراني الخاصة بأنظمة التحكم الصناعي (OT/ICS) المعتمدة. • إثبات يؤكد بأن منهجية إدارة مخاطر الأمن السيبراني الخاصة بأنظمة التحكم الصناعي (OT/ICS) جزء من منهجية إدارة المخاطر الجهة وإدارة مخاطر السلامة.
١-٣-١-٢	يجب تقييم مخاطر الأمن السيبراني، لأنظمة التحكم الصناعي (OT/ICS) بشكل دوري، مع التأكد من تضمين مخاطر توقيع العقود والاتفاقيات، مع الأطراف الخارجية المتعلقة بأنظمة التحكم الصناعي (OT/ICS) و/أو عند حدوث تغييرات بالمتطلبات التشريعية والتنظيمية، ذات العلاقة بوصفها جزء من التقييم.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني لأنظمة التحكم الصناعي • نموذج إجراء إدارة مخاطر الأمن السيبراني

	• نموذج سجل مخاطر الأمن السيبراني **إرشادات تطبيق الضوابط:** • إجراء تقييم مخاطر الأمن السيبراني، لأنظمة التحكم الصناعي (OT/ICS) بشكل دوري (بناء على فترة زمنية محددة). • إجراء تقييم لمخاطر الأمن السيبراني قبل توقيع الجهة أية عقود أو اتفاقيات مع أطراف خارجية متعلقة بأنظمة التحكم الصناعي (OT/ICS). • إجراء تقييم لمخاطر الأمن السيبراني عند تغيير المتطلبات التشريعية والتنظيمية ذات العلاقة.
	المخرجات المتوقعة: • تقارير مخاطر الأمن السيبراني لأصول أنظمة التحكم الصناعي (OT/ICS). • سجل مخاطر الأمن السيبراني لأنظمة التحكم الصناعي (OT/ICS). • إثبات يؤكد قيام الجهة بتقييم مخاطر الأمن السيبراني لأنظمة التحكم الصناعي (OT/ICS) بشكل دوري وذلك عند تغيير المتطلبات التشريعية والتنظيمية ذات العلاقة وقبل توقيع الجهة أية عقود أو اتفاقيات مع أطراف خارجية.
١-٣-١-٣	تضمين سجل مخاطر الأمن السيبراني، المتعلقة بأنظمة التحكم الصناعي (OT/ICS) ضمن سجل المخاطر في الجهة.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج إجراء إدارة مخاطر الأمن السيبراني • نموذج سجل مخاطر الأمن السيبراني **إرشادات تطبيق الضوابط:** • العمل على انشاء سجل مخاطر الأمن السيبراني لأصول أنظمة التحكم الصناعي (OT/ICS). • العمل على تضمين سجل مخاطر الأمن السيبراني المتعلقة بأنظمة التحكم الصناعي (OT/ICS) ضمن سجل المخاطر في الجهة.
	المخرجات المتوقعة: • سجل مخاطر الأمن السيبراني لأنظمة التحكم الصناعي (OT/ICS). • إثبات يؤكد تضمين سجل مخاطر الأمن السيبراني المتعلقة بأنظمة التحكم الصناعي (OT/ICS) ضمن سجل المخاطر في الجهة.

١-٣-١-٤	تحديد المستويات الملائمة للمناطق، والمرافق التي تحتوي على أنظمة التحكم الصناعي (OT/ICS) بناءً على منهجية معتمدة.

أدوات الأمن السيبراني ذات العلاقة:

- نموذج سياسة الأمن السيبراني للأنظمة التشغيلية
- نموذج إجراء إدارة مخاطر الأمن السيبراني
- نموذج سجل مخاطر الأمن السيبراني

إرشادات تطبيق الضوابط:

- العمل على تطوير منهجية معتمدة لتحديد المستويات الملائمة للمناطق والمرافق التي تحتوي على أنظمة التحكم الصناعي (OT/ICS).
- التأكد من تطبيق المنهجية المعتمدة لتحديد المستويات الملائمة للمناطق والمرافق التي تحتوي على أنظمة التحكم الصناعي (OT/ICS).

المخرجات المتوقعة:

- المنهجية المعتمدة لتحديد المستويات الملائمة للمناطق والمرافق التي تحتوي على أنظمة التحكم الصناعي (OT/ICS).
- إثبات يؤكد تطبيق المنهجية المعتمدة لتحديد المستويات الملائمة للمناطق والمرافق التي تحتوي على أنظمة التحكم الصناعي (OT/ICS).

١-٣-١-٥	تضمين تحليل نوعي (Qualitative Analysis) لمخاطر الأمن السيبراني، ضمن إجراءات تحليل مخاطر العمليات (Process Hazard Analysis) الذي يطبق قبل أي تغيير في العمليات أو إجراءاتها في المصانع.

أدوات الأمن السيبراني ذات العلاقة:

- نموذج سياسة الأمن السيبراني للأنظمة التشغيلية
- نموذج إجراء إدارة مخاطر الأمن السيبراني
- نموذج سجل مخاطر الأمن السيبراني

إرشادات تطبيق الضوابط:

- تحديث إجراءات ومعايير تحليل مخاطر العمليات (Process Hazard Analysis) وتضمين مخاطر الأمن السيبراني ضمن الدراسات.
- التأكد من تضمين تحليل نوعي (Qualitative Analysis) لمخاطر الأمن السيبراني الخاصة بأنظمة التحكم الصناعي (OT/ICS) أثناء إجراء دراسة تحليل مخاطر العمليات (Process Hazard Analysis).

المخرجات المتوقعة:

	• إثبات يؤكد تحديث إجراءات ومعايير تحليل مخاطر العمليات (Process Hazard Analysis) وتضمين مخاطر الأمن السيبراني ضمن الدراسات. • تقرير لآخر دراسة تحليل مخاطر العمليات (Process Hazard Analysis).
١-٣-١-٦	في حال عدم التمكن من استيفاء متطلبات الأمن السيبراني داخل البيئة الخاصة بأنظمة التحكم الصناعي (OT/ICS)، فيجب توضيح المبررات اللازمة، مع توثيقها واعتمادها من قبل الجهة المعنية بالأمن السيبراني، وموافقة صاحب الصلاحية.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج إجراء إدارة مخاطر الأمن السيبراني • نموذج سجل مخاطر الأمن السيبراني **إرشادات تطبيق الضوابط:** • في حال عدم التمكن من استيفاء متطلبات الأمن السيبراني داخل البيئة الخاصة بأنظمة التحكم الصناعي (OT/ICS) فيجب تطبيق التالي: ○ توثيق وتوضيح المبررات اللازمة لعدم القدرة على استيفاء أي من المتطلبات؛ ويتضمن ذلك الحصول على خطاب رسمي (Official Letter) من المورد أو الشركة المصنعة (Vendor or OEM) في حال عدم توصيتهم بتطبيق أحد المتطلبات لأسباب تقنية أو فنية أو تشغيلية مع توضيح التفاصيل والمبررات التقنية. ○ إجراء تقييم مخاطر الأمن السيبراني لتحديد المخاطر في حال عدم تطبيق أحد المتطلبات ويتضمن ذلك وضع الضوابط البديلة لها وإتّباع المستوى المقبول للمخاطر في الجهة. ○ توثيق المبررات اللازمة واعتمادها من قبل الإدارة المعنية بالأمن السيبراني، وموافقة صاحب الصلاحية.
	المخرجات المتوقعة: • وثيقة المبررات اللازمة لعدم القدرة على استيفاء أي من المتطلبات؛ والتي تتضمن الخطاب الرسمي (Official Letter) من المورد أو الشركة المصنعة (Vendor or OEM) في حال عدم توصيتهم بتطبيق أحد المتطلبات لأسباب تقنية أو فنية أو تشغيلية مع توضيح التفاصيل والمبررات التقنية. • تقرير تقييم مخاطر الأمن السيبراني الخاص بتحديد المخاطر في حال عدم تطبيق أحد المتطلبات ويتضمن ذلك وضع الضوابط البديلة لها وإتّباع المستوى المقبول للمخاطر في الجهة. • موافقة الإدارة المعنية بالأمن السيبراني، وموافقة صاحب الصلاحية.

	١-٣-١-٧	في حال الموافقة على قبول المخاطر السيبرانية؛ فيجب تحديد الضوابط البديلة لها مع توثيقها، واعتمادها من قبل صاحب الصلاحية؛ مع التأكد من تطبيقها بفعالية في وقت محدد، مع الاستمرار في تقييم تلك المخاطر ومراجعتها بشكل مستمر.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج إجراء إدارة مخاطر الأمن السيبراني • نموذج سجل مخاطر الأمن السيبراني **إرشادات تطبيق الضوابط:** • في حال قبول المخاطر: ○ توضيح المخاطر المتبقية وتوثيقها وإقرار صاحب الصلاحية بها. ○ تحديد الضوابط البديلة لها مع توثيقها، واعتمادها من قبل صاحب الصلاحية وإدارة الأمن السيبراني. ○ التأكد من تطبيق الضوابط البديلة بفعالية وفي مدة زمنية محددة. ○ الاستمرار في تقييم الضوابط البديلة ومراجعتها بشكل مستمر.	
	المخرجات المتوقعة: • تقارير تقييم مخاطر الأمن السيبراني والتي توضّح تحديد الضوابط البديلة. • موافقة الإدارة المعنية بالأمن السيبراني، وموافقة صاحب الصلاحية. • إثبات يؤكد تطبيق الضوابط البديلة بفعالية ولمدة زمنية محددة. • إثبات يؤكد الاستمرار في تقييم الضوابط البديلة ومراجعتها بشكل مستمر.	
١-٤	**الأمن السيبراني ضمن إدارة مشاريع أنظمة التحكم الصناعي (Cybersecurity in Industrial Control System Project Management)**	
الهدف	التأكد من أن متطلبات الأمن السيبراني مضمنة في منهجية إدارة مشاريع الجهة وإجراءاتها لحماية السرية، وسلامة الأعمال التشغيلية، ودقتها، وتوافرها لأنظمة التحكم الصناعي (OT/ICS)، وذلك وفقاً للسياسات والإجراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية ذات العلاقة.	
الضوابط		
١-٤-١	بالإضافة للضوابط الفرعية ضمن الضابطين ١-٦-٢ و ١-٦-٣ من الضوابط الأساسية للأمن السيبراني؛ يجب أن تغطي متطلبات الأمن السيبراني ضمن إدارة مشاريع أنظمة التحكم الصناعي (OT/ICS) بحد أدنى ما يلي:	
	١-٤-١-١	تضمين متطلبات الأمن السيبراني بوصفه جزء من دورة حياة المشاريع المتعلقة بأنظمة التحكم الصناعي (OT/ICS).
	أدوات الأمن السيبراني ذات العلاقة:	

	• نموذج قائمة التحقق من متطلبات الأمن السيبراني لمشاريع تقنية المعلومات وإدارة التغيير • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية **إرشادات تطبيق الضوابط:** • العمل على تضمين متطلبات الأمن السيبراني في منهجية إدارة المشاريع الخاصة بأنظمة التحكم الصناعي (OT/ICS) والتأكد من تضمينها خلال دورة حياة المشاريع المتعلقة بأنظمة التحكم الصناعي (OT/ICS). • العمل على أن تكون متطلبات الأمن السيبراني في منهجية إدارة المشاريع الخاصة بأنظمة التحكم الصناعي (OT/ICS) والتي قد ضمنت خلال دورة حياة المشاريع المتعلقة بأنظمة التحكم الصناعي (OT/ICS) بأنها محدثة ومعتمدة من قبل صاحب الصلاحية أو من ينيبه. • التحقق والتأكد من أن جميع المشاريع المتعلقة بأنظمة التحكم الصناعي (OT/ICS) متماشية ومتوافقة مع متطلبات الأمن السيبراني المعتمدة في دورة حياة المشاريع المتعلقة بأنظمة التحكم الصناعي (OT/ICS).
	المخرجات المتوقعة: • وثيقة منهجية إدارة المشاريع الخاصة بأنظمة التحكم الصناعي (OT/ICS) والتي توضّح متطلبات الأمن السيبراني خلال دورة حياة المشاريع المتعلقة بأنظمة التحكم الصناعي (OT/ICS). • إثبات يؤكد بأن منهجية إدارة المشاريع الخاصة بأنظمة التحكم الصناعي (OT/ICS) والتي توضّح متطلبات الأمن السيبراني خلال دورة حياة المشاريع المتعلقة بأنظمة التحكم الصناعي (OT/ICS) محدثة ومعتمدة من قبل صاحب الصلاحية أو من ينيبه. • إثبات يؤكد أن جميع المشاريع المتعلقة بأنظمة التحكم الصناعي (OT/ICS) متماشية ومتوافقة مع متطلبات الأمن السيبراني المعتمدة في دورة حياة المشاريع المتعلقة بأنظمة التحكم الصناعي (OT/ICS).
١-٤-١-٢	تضمين متطلبات الأمن السيبراني ضمن اختبارات القبول (Acceptance Test) وعمليات التقييم (Evaluation Process). مثل: اختبارات قبول المصنع ((Factory Acceptance Tests (FAT) واختبارات القبول الميداني ((Site Acceptance Tests (SAT) واختبارات التشغيل (Commissioning Tests) واختبارات التغيير (Change Tests) واختبارات التكامل (Integration Tests) ومراجعة الشفرة المصدرية (Source Code Review).
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • قائمة التحقق من متطلبات الأمن السيبراني في تطوير البرمجيات **إرشادات تطبيق الضوابط:** • العمل على تطوير وتضمين متطلبات الأمن السيبراني ضمن اختبارات قبول المصنع ((Factory Acceptance Tests (FAT) واختبارات القبول الميداني ((Site Acceptance Tests (SAT) واختبارات التشغيل

	(Commissioning Tests) واختبارات التغيير (Change Tests) واختبارات التكامل (Integration Tests) ومراجعة الشفرة المصدرية (Source Code Review). • التأكد بأن جميع اختبارات قبول المصنع ((Factory Acceptance Tests (FAT) واختبارات القبول الميداني ((Site Acceptance Tests (SAT) واختبارات التشغيل (Commissioning Tests) واختبارات التغيير (Change Tests) واختبارات التكامل (Integration Tests) ومراجعة الشفرة المصدرية (Source Code Review) قد أجريت مع الأخذ بالاعتبار متطلبات الأمن السيبراني للأنظمة التشغيلية التي قد تم تطويرها.
	المخرجات المتوقعة: • إثبات يؤكد تطوير وتضمين متطلبات الأمن السيبراني ضمن اختبارات قبول المصنع (Factory Acceptance Tests (FAT)) واختبارات القبول الميداني (Site Acceptance Tests (SAT)) واختبارات التشغيل (Commissioning Tests) واختبارات التغيير (Change Tests) واختبارات التكامل (Integration Tests) ومراجعة الشفرة المصدرية (Source Code Review). • عينة من أحدث وثائق لاختبارات القبول المصنعية ((Factory Acceptance Tests (FAT)) ولاختبارات القبول الميداني ((Site Acceptance Tests (SAT)) ولاختبارات التشغيل (Commissioning Tests) ولاختبارات التغيير (Change Tests) ولاختبارات التكامل (Integration Tests) ومراجعة الشفرة المصدرية (Source Code Review) والتي توضّح تضمين متطلبات الأمن السيبراني للأنظمة التشغيلية بها.
١-٤-١-٣	تضمين مبدأ الأمن من خلال التصميم (Secure-By-Design) بوصفه جزء من الأمن المعماري لتصميم البيئة الخاصة بأنظمة التحكم الصناعي (OT/ICS).
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • نموذج قائمة التحقق من متطلبات الأمن السيبراني في تطوير البرمجيات **إرشادات تطبيق الضوابط:** • العمل على تحديد وتضمين مبدأ الأمن من خلال التصميم (Secure-By-Design) كجزء من الأمن المعماري لتصميم البيئة الخاصة بأنظمة التحكم الصناعي (OT/ICS). • تطبيق مبدأ الأمن من خلال التصميم (Secure-By-Design) للبيئة الخاصة بأنظمة التحكم الصناعي (OT/ICS). • التأكد من أن جميع البيئات الخاصة بأنظمة التحكم الصناعي (OT/ICS) قد تم تصميمها باستخدام مبدأ الأمن من خلال التصميم (Secure-By-Design).

	المخرجات المتوقعة: • وثائق المتطلبات الخاصة بمعمارية التصميم الآمن لبيئة أنظمة التحكم الصناعي (OT/ICS) والتي توضّح مبدأ الأمن من خلال التصميم (Secure-By-Design). • إثبات يؤكد أن جميع البيئات الخاصة بأنظمة التحكم الصناعي (OT/ICS) قد تم تصميمها باستخدام مبدأ الأمن من خلال التصميم (Secure-By-Design).
١-٤-١-٤	حماية الأنظمة في البيئة التطويرية (Development Environment)، وتشمل بيئات الاختبار (Testing Environment)، والمنصات التكاملية (Integration Platforms).
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • نموذج قائمة التحقق من العامة الأمن السيبراني في تطوير البرمجيات **إرشادات تطبيق الضوابط:** • تحديد إذا كان هناك بيئات تطويرية وتشمل بيئات الاختبار (Testing Environment)، والمنصات التكاملية (Integration Platforms). • العمل على تحديد وتوثيق إجراءات تتضمن المتطلبات المتعلقة بحماية البيئات المحددة والمعرفة مسبقاً. • اعتماد هذه الإجراءات من قبل مالك الأنظمة. • العمل على تطبيق الإجراءات المعتمدة المتعلقة بحماية البيئات المحددة والمعرفة مسبقاً.
	المخرجات المتوقعة: • قائمة البيئات التطويرية المحددة. • الإجراءات الموثقة والمعتمدة من قبل مالك الأنظمة. • إثبات يؤكد تطبيق الإجراءات المعتمدة المتعلقة بحماية البيئات المحددة والمعرفة مسبقاً.
٢-٤-١	يجب مراجعة متطلبات الأمن السيبراني، ضمن إدارة مشاريع أنظمة التحكم الصناعي (OT/ICS) وقياس فعالية تطبيقها وتقييمها دورياً.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • نموذج تقرير مؤشرات الأداء الرئيسية **إرشادات تطبيق الضوابط:**

	• العمل على مراجعة متطلبات الأمن السيبراني ضمن إدارة مشاريع أنظمة التحكم الصناعي (OT/ICS) بشكل دوري حسب خطة موثقة ومعتمدة للمراجعة بناءً على فترة زمنية محددة (على سبيل المثال، يتم إجراء المراجعة الدورية بشكل سنوي). • العمل على تطوير مؤشرات أداء رئيسية (KPIs) لكل الضوابط المتضمنة بداخل السياسات أو الإجراءات للتأكد من قياس فعالية تطبيقها، وتقييمها دورياً بناءً على فترة زمنية محددة (على سبيل المثال، يتم إجراء المراجعة الدورية بشكل سنوي).
	المخرجات المتوقعة: • إثبات يؤكد القيام بالمراجعة الدورية لمتطلبات الأمن السيبراني ضمن إدارة مشاريع أنظمة التحكم الصناعي (OT/ICS). • إثبات يؤكد القيام بقياس مؤشرات الأداء الرئيسية (KPIs) لكل الضوابط المتضمنة بداخل السياسات أو الإجراءات للتأكد من قياس فعالية تطبيقها، وتقييمها دورياً بناءً على فترة زمنية محددة.
٥-١	**الأمن السيبراني ضمن إدارة التغيير (Cybersecurity in Change Management)**
الهدف	التأكد من أن متطلبات الأمن السيبراني مضمنة في منهجية إدارة التغيير في الجهة وإجراءاتها لضمان سلامة تطبيق طلبات التغيير في بيئة أنظمة التحكم الصناعي (OT/ICS) وذلك بعد التحليل والتحكم بالتغييرات.
الضوابط	
١-٥-١	يجب تحديد متطلبات الأمن السيبراني وتوثيقها واعتمادها، ضمن إدارة التغيير لدى الجهة، ويجب التأكد من أن متطلبات الأمن السيبراني تمثل جزءاً لا يتجزأ من المتطلبات الأساسية لإدارة التغيير لأنظمة التحكم الصناعي (OT/ICS).
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) **إرشادات تطبيق الضوابط:** • تحديد وتوثيق واعتماد متطلبات الأمن السيبراني المتعلقة بإدارة التغيير لأنظمة التحكم الصناعي (OT/ICS).
	المخرجات المتوقعة: • الوثيقة المعتمدة لمتطلبات الأمن السيبراني المتعلقة بإدارة التغيير لأنظمة التحكم الصناعي (OT/ICS).
٢-٥-١	يجب تطبيق متطلبات الأمن السيبراني ضمن دورة حياة إدارة التغيير، المتعلقة بأنظمة التحكم الصناعي (OT/ICS) لدى الجهة.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية

		• نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) **إرشادات تطبيق الضوابط:** • العمل على تطبيق متطلبات الأمن السيبراني المعتمدة المتعلقة بإدارة التغيير لأنظمة التحكم الصناعي (OT/ICS). • التأكد من تطبيق متطلبات الأمن السيبراني المعتمدة والمعرفة مسبقاً عند حدوث أي تغيير على أنظمة التحكم الصناعي (OT/ICS). **المخرجات المتوقعة:** • إثبات يؤكد تطبيق متطلبات الأمن السيبراني المعتمدة المتعلقة بإدارة التغيير لأنظمة التحكم الصناعي (OT/ICS).
١-٥-٣	بالإضافة للضوابط الفرعية ضمن الضابطين ١-٦-٢ و ١-٦-٣ في الضوابط الأساسية للأمن السيبراني؛ يجب أن تغطي متطلبات الأمن السيبراني، ضمن إدارة التغيير لأنظمة التحكم الصناعي (OT/ICS) بحد أدنى ما يلي:	
	١-٥-٣-١	تضمين متطلبات الأمن السيبراني بوصفها جزء من دورة حياة إدارة التغيير.
		أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • قائمة التحقق من متطلبات الأمن السيبراني لمشاريع تقنية المعلومات وإدارة التغيير **إرشادات تطبيق الضوابط:** • العمل على تطوير واعتماد منهجية تتضمن متطلبات الأمن السيبراني أثناء دورة حياة إدارة التغيير لأنظمة التحكم الصناعي (OT/ICS). • تطبيق المنهجية المعتمدة عند حدوث أي تغيير في بيئة أنظمة التحكم الصناعي (OT/ICS). **المخرجات المتوقعة:** • وثيقة المنهجية المعتمدة لمتطلبات الأمن السيبراني أثناء دورة حياة إدارة التغيير لأنظمة التحكم الصناعي (OT/ICS). • إثبات يؤكد تطبيق المنهجية المعتمدة عند حدوث أي تغيير على بيئة أنظمة التحكم الصناعي (OT/ICS).
	١-٥-٣-٢	التحقق من صحة وسلامة التغييرات في بيئة منفصلة قبل تطبيقها على بيئة الإنتاج (Production Environment).
		أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) **إرشادات تطبيق الضوابط:**

	• تجهيز بيئة مخصصة ومنفصلة للتحقق من صحة وسلامة التغييرات قبل تطبيقها على بيئة الإنتاج على سبيل المثال لا الحصر؛ (بيئة تجريبية، بيئة اختبارية). • التأكد من أن جميع التغييرات يتم التحقق منها في البيئة المنفصلة التي تم تجهيزها.
	المخرجات المتوقعة: • عمل زيارة ميدانية للتحقق من وجود بيئات منفصلة عن بيئة الإنتاج. • إثبات يؤكد بأن جميع التغييرات يتم التحقق منها في بيئة مخصصة ومنفصلة عن بيئة الإنتاج.
١-٥-٣-٣	التحقق من كفاءة متطلبات الأمن السيبراني لأنظمة التحكم الصناعي (OT/ICS) في حال استبدالها بأجهزة مماثلة لها، سواء أكان ذلك في بيئات التصاميم؛ أم الاختبارات، أو التشغيلية، للتأكد من سلامتها، وذلك قبل تطبيقها في بيئة الإنتاج، أو البيئة التشغيلية.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) **إرشادات تطبيق الضوابط:** • العمل على تطوير قائمة مراجعة (Checklist) تحتوي على متطلبات الأمن السيبراني لأنظمة التحكم الصناعي (OT/ICS) للتحقق من كفاءتها في حال استبدالها بأجهزة مماثلة لها على سبيل المثال لا الحصر؛ (التأكد من إعدادات التحصين، التأكد من آخر تحديثات للنظام، التأكد من وجود مكافح فيروسات ...الخ). • التأكد من استخدام قائمة مراجعة (Checklist) على جميع الأجهزة الجديدة أو المستبدلة.
	المخرجات المتوقعة: • نموذج قائمة المراجعة (Checklist) والتي تحتوي على متطلبات الأمن السيبراني لأنظمة التحكم الصناعي (OT/ICS) للتحقق من كفاءتها في حال استبدالها بأجهزة مماثلة لها. • إثبات يؤكد استخدام قائمة مراجعة (Checklist) على جميع الأجهزة الجديدة أو المستبدلة.
١-٥-٣-٤	تطبيق إجراءات مقيدة، وآمنة للتغييرات الاستثنائية.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) **إرشادات تطبيق الضوابط:** • العمل على تطوير منهجية للموافقة على التغييرات الطارئة الخاصة بأنظمة التحكم الصناعي (OT/ICS). • التأكد من تطبيق المنهجية المطورة للموافقة على التغييرات الطارئة الخاصة بأنظمة التحكم الصناعي (OT/ICS).
	المخرجات المتوقعة:

		• وثيقة المنهجية المطورة للموافقة على التغييرات الطارئة الخاصة بأنظمة التحكم الصناعي (OT/ICS). • إثبات يؤكد تطبيق المنهجية المطورة للموافقة على التغييرات الطارئة الخاصة بأنظمة التحكم الصناعي (OT/ICS).
	١-٥-٣-٥	تطبيق آلية أتمتة الإعدادات (Automated Configuration) وآلية كشف التغييرات بالأصول (Assets Change Detection).
		أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) **إرشادات تطبيق الضوابط:** • تطبيق أحد الحلول التقنية لآلية أتمتة الإعدادات (Automated Configuration) وآلية كشف التغييرات بالأصول (Assets Change Detection). • التأكد من أن الحلول التقنية مثبّتة بشكل صحيح بحيث تغطي جميع الأصول الخاصة بأنظمة التحكم الصناعي (OT/ICS).
		المخرجات المتوقعة: • زيارة ميدانية لفحص الحلول التقنية لآلية أتمتة الإعدادات (Automated Configuration) وآلية كشف التغييرات بالأصول (Assets Change Detection). • إثبات يؤكد بأن الحلول التقنية مثبّتة بالشكل الصحيح بحيث تغطي جميع الأصول الخاصة بأنظمة التحكم الصناعي (OT/ICS).
١-٥-٤		يجب مراجعة متطلبات الأمن السيبراني، ضمن إدارة التغيير المتعلقة بأنظمة التحكم الصناعي (OT/ICS) وقياس فعالية تطبيقها وتقييمها دورياً.
		أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • نموذج تقرير مؤشرات الأداء الرئيسية **إرشادات تطبيق الضوابط:** • العمل على مراجعة متطلبات الأمن السيبراني ضمن إدارة التغيير المتعلقة بأنظمة التحكم الصناعي (OT/ICS) بشكل دوري حسب خطة موثقة ومعتمدة للمراجعة بناءً على فترة زمنية محددة (على سبيل المثال، يتم إجراء المراجعة الدورية بشكل سنوي). • العمل على تطوير مؤشرات أداء رئيسية (KPIs) لكل الضوابط المتضمنة بداخل السياسات أو الإجراءات للتأكد من قياس فعالية تطبيقها، وتقييمها دورياً بناءً على فترة زمنية محددة (على سبيل المثال، يتم إجراء المراجعة الدورية بشكل سنوي).

	المخرجات المتوقعة: • إثبات يؤكد القيام بالمراجعة الدورية لمتطلبات الأمن السيبراني ضمن إدارة التغيير المتعلقة بأنظمة التحكم الصناعي (OT/ICS). • إثبات يؤكد القيام بقياس مؤشرات الأداء الرئيسية (KPIs) لكل الضوابط المتضمنة بداخل السياسات أو الإجراءات للتأكد من قياس فعالية تطبيقها، وتقييمها دورياً بناءً على فترة زمنية محددة.
١-٦	**المراجعة والتدقيق الدوري للأمن السيبراني (Periodical Cybersecurity Review and Audit)**
الهدف	ضمان التأكد من أن ضوابط الأمن السيبراني لأنظمة التحكم الصناعي (OT/ICS) لدى الجهة، مطبقة، وتعمل وفقاً للسياسات والإجراءات التنظيمية للجهة، والمتطلبات التشريعية، والتنظيمية الوطنية ذات العلاقة، والمتطلبات الدولية المقرة تنظيمياً على الجهة.
الضوابط	
١-٦-١	رجوعاً للضابط ١-٨-١ في الضوابط الأساسية للأمن السيبراني؛ يجب على الإدارة المعنية بالأمن السيبراني في الجهة مراجعة تطبيق ضوابط الأمن السيبراني للأنظمة التشغيلية (OTCC-1:2022)، مرة واحدة سنوياً، على الأقل.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • نموذج إجراء تدقيق الأمن السيبراني • نموذج سجل خطة تدقيق الأمن السيبراني **إرشادات تطبيق الضوابط:** • العمل على مراجعة تطبيق متطلبات الأمن السيبراني للأنظمة التشغيلية (OTCC-1:2022)، وذلك بشكل سنوي على الأقل. • العمل على توثيق نتائج المراجعة ومشاركتها مع الإدارات ذات العلاقة.
	المخرجات المتوقعة: • تقارير المراجعة الدورية لتطبيق ضوابط الأمن السيبراني للأنظمة التشغيلية (OTCC-1:2022). • إثبات يؤكد توثيق نتائج المراجعة ومشاركتها مع الإدارات ذات العلاقة.
٢-٦-١	رجوعاً للضابط ١-٨-٢ في الضوابط الأساسية للأمن السيبراني؛ يجب مراجعة تطبيق ضوابط الأمن السيبراني للأنظمة التشغيلية (OTCC-1:2022) من قبل أطراف مستقلة عن الإدارة المعنية بالأمن السيبراني في الجهة، وذلك مرة واحدة كل ثلاث سنوات على الأقل.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية

	• نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • نموذج إجراء تدقيق الأمن السيبراني • نموذج سجل خطة تدقيق الأمن السيبراني **إرشادات تطبيق الضوابط:** • العمل على مراجعة وتدقيق تطبيق ضوابط الأمن السيبراني للأنظمة التشغيلية (OTCC-1:2022) في الجهة مرة كل ثلاث سنوات على الأقل، وذلك من قبل أطراف مستقلة عن الإدارة المعنية بالأمن السيبراني مثل الإدارة المعنية بالمراجعة في الجهة (Internal Audit)، أو من قبل أطراف خارجية يتم التعاون معها بشكل مستقل عن الإدارة المعنية بالأمن السيبراني بما يحقق مبدأ عدم تعارض المصالح عند مراجعة تطبيق متطلبات الأمن السيبراني للأنظمة التشغيلية. • العمل على توثيق نتائج المراجعة ومشاركتها مع الإدارات ذات العلاقة ومتابعة الملاحظات المرصودة حتى يتم معالجتها.
	المخرجات المتوقعة: • تقارير التدقيق (من قبل الإدارة المعنية بالمراجعة الداخلية أو من قبل مراجع خارجي مستقل) التي تمت على جميع متطلبات الأمن السيبراني للأنظمة التشغيلية (OTCC-1:2022). • إثبات يؤكد توثيق نتائج المراجعة ومشاركتها مع الإدارات ذات العلاقة ومتابعة الملاحظات المرصودة والتأكد من معالجتها.
١-٧	**الأمن السيبراني المتعلق بالموارد البشرية (Cybersecurity in Human Resources)**
الهدف	ضمان التأكد من أن مخاطر الأمن السيبراني ومتطلباته لأنظمة التحكم الصناعي (OT/ICS) المتعلقة بالعاملين (موظفين ومتعاقدين) في الجهة؛ تعالج بفعالية، قبل البدء في عملهم وأثنائه وعند الانتهاء منه، وذلك وفقاً للسياسات والإجراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية ذات العلاقة.
الضوابط	
١-٧-١	بالإضافة للضوابط الفرعية ضمن الضابط ١-٩-٣ في الضوابط الأساسية للأمن السيبراني؛ يجب أن تغطي متطلبات الأمن السيبراني، المتعلقة بالموارد البشرية لأنظمة التحكم الصناعي (OT/ICS)، بحد أدنى؛ إجراء عمل مسح أمني (Screening or Vetting) لجميع العاملين (ويشمل ذلك الموظفين والمتعاقدين) والذين يمكنهم الوصول إلى أصول أنظمة التحكم الصناعي (OT/ICS) أو استخدامها؛ وذلك قبل منحهم صلاحيات الوصول.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • نموذج سياسة الأمن السيبراني للموارد البشرية

	إرشادات تطبيق الضوابط: • تحديد قائمة بأسماء الأشخاص المخوّلين والذين يمكنهم الوصول إلى أصول أنظمة التحكم الصناعي (OT/ICS) أو استخدامها (ويشمل ذلك الموظفين والمتعاقدين والمتعاقدين بالباطن). • العمل مع الإدارات ذات العلاقة لضمان إجراء المسح الأمني لقائمة الأسماء المحددة قبل منحهم صلاحيات الوصول. **المخرجات المتوقعة:** • قائمة بأسماء الأشخاص المخوّلين والذين يمكنهم الوصول إلى أصول أنظمة التحكم الصناعي (OT/ICS) أو استخدامها (ويشمل ذلك الموظفين والمتعاقدين والمتعاقدين بالباطن). • إثبات يؤكد إجراء المسح الأمني لقائمة الأسماء المحددة.
١-٧-٢	رجوعاً للضابط ١-٩-٦ في الضوابط الأساسية للأمن السيبراني؛ يجب مراجعة متطلبات الأمن السيبراني لأنظمة التحكم الصناعي (OT/ICS) المتعلقة بالموارد البشرية، وقياس فعالية تطبيقها، وتقييمها دورياً. **أدوات الأمن السيبراني ذات العلاقة:** • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • نموذج سياسة الأمن السيبراني للموارد البشرية • نموذج تقرير مؤشرات الأداء الرئيسية **إرشادات تطبيق الضوابط:** • العمل على مراجعة متطلبات الأمن السيبراني لأنظمة التحكم الصناعي (OT/ICS) المتعلقة بالموارد البشرية بشكل دوري حسب خطة موثقة ومعتمدة للمراجعة بناءً على فترة زمنية محددة (على سبيل المثال، يتم إجراء المراجعة الدورية بشكل سنوي). • العمل على تطوير مؤشرات أداء رئيسية (KPIs) لكل الضوابط المتضمنة بداخل السياسات أو الإجراءات للتأكد من قياس فعالية تطبيقها، وتقييمها دورياً بناءً على فترة زمنية محددة (على سبيل المثال، يتم إجراء المراجعة الدورية بشكل سنوي). **المخرجات المتوقعة:** • إثبات يؤكد القيام بالمراجعة الدورية لمتطلبات الأمن السيبراني لأنظمة التحكم الصناعي (OT/ICS) المتعلقة بالموارد البشرية. • إثبات يؤكد القيام بقياس مؤشرات الأداء الرئيسية (KPIs) لكل الضوابط المتضمنة بداخل السياسات أو الإجراءات للتأكد من قياس فعالية تطبيقها، وتقييمها دورياً بناءً على فترة زمنية محددة.
١-٨	**برنامج التوعية والتدريب بالأمن السيبراني**

	(Cybersecurity Awareness and Training Program)
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، لأنظمة التحكم الصناعي (OT/ICS) لدى الجهة، والقيام بمسؤولياتهم تجاه الأمن السيبراني.
الضوابط	
١-٨-١	بالإضافة للضوابط الفرعية، ضمن الضابط ١-١٠-٣ في الضوابط الأساسية للأمن السيبراني؛ يجب أن يتضمن برنامج التوعية بالأمن السيبراني، التعامل الآمن مع أنظمة التحكم الصناعي (OT/ICS) في الجهة.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • خطة برنامج التوعية بالأمن السيبراني **إرشادات تطبيق الضوابط:** • تضمين التعامل الآمن مع أنظمة التحكم الصناعي (OT/ICS) بوصفه جزء من برنامج التوعية بالأمن السيبراني للجهة. • التأكد من تنفيذ المحتوى التوعوي والذي يحتوي على التعامل الآمن مع أنظمة التحكم الصناعي (OT/ICS).
	المخرجات المتوقعة: • وثيقة برنامج التوعية المعتمدة في الجهة والتي توضّح المحتوى الخاص بالتعامل الآمن مع أنظمة التحكم الصناعي (OT/ICS). • إثبات يؤكد تنفيذ المحتوى التوعوي والذي يحتوي على التعامل الآمن مع أنظمة التحكم الصناعي (OT/ICS).
٢-٨-١	بالإضافة للضوابط الفرعية، ضمن الضابط ١-١٠-٤ في الضوابط الأساسية للأمن السيبراني؛ يجب أن تغطي متطلبات الأمن السيبراني، المتعلقة ببرنامج التوعية والتدريب بالأمن السيبراني في بيئة أنظمة التحكم الصناعي (OT/ICS) بحد أدنى ما يلي:
١-٨-٢-١	يجب أن يتم توفير تمارين خاصة، وشهادات مهنية، ومهارات احترافية في مجال الأمن السيبراني، لجميع العاملين على الأصول المتعلقة بأنظمة التحكم الصناعي (OT/ICS). كما تشجع الهيئة الجهة على، الاستفادة من الإطار السعودي لكوادر الأمن السيبراني (سيوف) ليكون مرجع لها.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • خطة برنامج التوعية بالأمن السيبراني **إرشادات تطبيق الضوابط:**

	• تحديد قائمة بأسماء الأشخاص المخوّلين والذين يمكنهم الوصول إلى أصول أنظمة التحكم الصناعي (OT/ICS) أو استخدامها. • العمل على تحضير وتطوير تمارين خاصة، وشهادات مهنية، ومهارات احترافية في مجال الأمن السيبراني، لجميع العاملين على الأصول المتعلقة بأنظمة التحكم الصناعي (OT/ICS). • العمل على إعطاء تمارين خاصة، وشهادات مهنية، ومهارات احترافية في مجال الأمن السيبراني، لجميع العاملين على الأصول المتعلقة بأنظمة التحكم الصناعي (OT/ICS).
	المخرجات المتوقعة: • الوثائق المعتمدة والتي تتضمن تمارين خاصة، وشهادات مهنية، ومهارات احترافية في مجال الأمن السيبراني، لجميع العاملين على الأصول المتعلقة بأنظمة التحكم الصناعي (OT/ICS). • إثبات يؤكد إكمال الموظفين التمارين الخاصة، والشهادات المهنية، والمهارات الاحترافية في مجال الأمن السيبراني المتعلقة بأنظمة التحكم الصناعي (OT/ICS).
٢-٢-٨-١	يجب تشجيع الجهة للمشاركة مع الجهات المعتمدة و/أو ذات الاختصاص في مجال أنظمة التحكم الصناعي (OT/ICS) للتعرف على أحدث التقنيات والممارسات في مجال الأمن السيبراني لأنظمة التحكم الصناعي (OT/ICS).
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) **إرشادات تطبيق الضوابط:** • على الموظفين الذين يديرون أنظمة التحكم الصناعي (OT/ICS) المشاركة مع الجهات المعتمدة و/أو ذات الاختصاص في مجال أنظمة التحكم الصناعي (OT/ICS) للتعرف على أحدث التقنيات والممارسات في مجال الأمن السيبراني لأنظمة التحكم الصناعي (OT/ICS) ومن هذه الجهات على سبيل المثال لا الحصر (CySec conference, Dragos Industrial Security Conference).
	المخرجات المتوقعة: • إثبات يؤكد مشاركة الموظفين الذين يديرون أنظمة التحكم الصناعي (OT/ICS) مع الجهات المعتمدة و/أو ذات الاختصاص في مجال أنظمة التحكم الصناعي (OT/ICS) للتعرف على أحدث التقنيات والممارسات في مجال الأمن السيبراني لأنظمة التحكم الصناعي (OT/ICS).

٢ تعزيز الأمن السيبراني (Cybersecurity Defense)

٢-١	إدارة الأصول (Asset Management)
الهدف	التأكد من أن الجهة لديها قائمة جرد دقيقة، وحديثة للأصول؛ تشمل التفاصيل ذات العلاقة لجميع أصول أنظمة التحكم الصناعي (OT/ICS) المتاحة للجهة؛ من أجل دعم العمليات التشغيلية للجهة، ومتطلبات الأمن السيبراني، لتحقيق التشغيل الدائم (Production Uptime) لأصول أنظمة التحكم الصناعي (OT/ICS)، وسلامة عملياتها، وسريتها، وتوافرها ودقتها.
الضوابط	
٢-١-١	بالإضافة للضوابط، ضمن المكون الفرعي ٢-١ في الضوابط الأساسية للأمن السيبراني؛ يجب أن تغطي متطلبات الأمن السيبراني، المتعلقة بإدارة الأصول في بيئة أنظمة التحكم الصناعي (OT/ICS) بحد أدنى؛ ما يلي:
٢-١-١-١	إنشاء قائمة جرد إلكترونية، لجميع أصول أنظمة التحكم الصناعي (OT/ICS) ومراجعتها بشكل دوري.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • نموذج سياسة إدارة الأصول • نموذج معيار إدارة الأصول **إرشادات تطبيق الضوابط:** • العمل على تطوير واعتماد قائمة جرد إلكترونية (ملف اكسيل كحد أدنى)، لجميع أصول أنظمة التحكم الصناعي (OT/ICS). • العمل على تطوير خطة مراجعة دورية (بناء على فترة زمنية محددة). • مراجعة وتحديث قائمة الجرد الإلكترونية (بناء على فترة زمنية محددة). كما يجب أن توضح القائمة اسم المراجع وتاريخ المراجعة.
	المخرجات المتوقعة: • قائمة جرد إلكترونية لجميع أصول أنظمة التحكم الصناعي (OT/ICS). • إثبات يؤكد مراجعة وتحديث قائمة الجرد الإلكترونية (بناء على فترة زمنية محددة).
٢-١-١-٢	استخدام تقنيات الأتمتة لحصر الأصول.

أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • نموذج سياسة إدارة الأصول • نموذج معيار إدارة الأصول **إرشادات تطبيق الضوابط:** • العمل على توفير تقنيات الأتمتة لحصر الأصول على سبيل المثال (أداة لمسح الأصول الخاصة بأنظمة التحكم الصناعي). • التأكد من أن تقنيات الأتمتة لحصر الأصول لا تسبب تأثير على العمليات التشغيلية. **المخرجات المتوقعة:** • تقرير دوري (بناء على فترة زمنية محددة) يوضح فيه الأتمتة لأصول أنظمة التحكم الصناعي. • إثبات يؤكد توفير تقنيات الأتمتة لأنظمة التحكم الصناعي. • إثبات يؤكد بأن تقنيات الأتمتة لحصر الأصول لا تسبب تأثير على العمليات التشغيلية.	
٢-١-١-٣	حفظ معلومات أصول أنظمة التحكم الصناعي (OT/ICS) المحصورة بشكل آمن.
أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • نموذج سياسة إدارة الأصول • نموذج معيار إدارة الأصول **إرشادات تطبيق الضوابط:** • التأكد من اتباع إجراءات إدارة الصلاحيات والهويات لأنظمة وتقنيات الأتمتة. • التأكد بأن كل من تقنيات الأتمتة وسجل الأصول محمية بكلمات مرور مع منح الصلاحية للوصول لهذه البيانات للموظفين المصرح بهم فقط. **المخرجات المتوقعة:** • إثبات يؤكد اتباع إجراءات إدارة الصلاحيات والهويات لأنظمة وتقنيات الأتمتة. • إثبات يؤكد استخدام كلمة مرور عند الوصول لسجل الأصول.	
٢-١-١-٤	تحديد ملاك الأصول (Asset Owner) لجميع أصول أنظمة التحكم الصناعي (OT/ICS) والتأكد من مشاركتهم في دورة حياة إدارة جرد الأصول ذات العلاقة.
أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS)	

		• نموذج سياسة إدارة الأصول • نموذج معيار إدارة الأصول **إرشادات تطبيق الضوابط:** • تحديد وتوثيق كل ملاك الأصول لجميع الأصول الخاصة بأنظمة التحكم الصناعي (OT/ICS). تجهيز سجل أصول رسمي خاص بأنظمة التحكم الصناعي (OT/ICS) مع تحديد ملاك هذه الأصول. • التأكد والتحقق من مشاركة ملاك الأصول (Asset Owner) وأمناء الأصول (Asset Custodian) في دورة حياة إدارة جرد الأصول ذات العلاقة. **المخرجات المتوقعة:** • إثبات يؤكد تحديد وتوثيق كل ملاك الأصول لجميع الأصول الخاصة بأنظمة التحكم الصناعي (OT/ICS). • إثبات يؤكد مشاركة ملاك الأصول (Asset Owner) في دورة حياة إدارة جرد الأصول ذات العلاقة.
	٢-١-١-٥	تصنيف مستوى الحساسية (Criticality Rating) وتوثيقه واعتماده لجميع الأصول، من قبل ملاك الأصول. **أدوات الأمن السيبراني ذات العلاقة:** • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • نموذج سياسة إدارة الأصول • نموذج معيار إدارة الأصول بحيث يشمل إرشادات التصنيف **إرشادات تطبيق الضوابط:** • تحديد مبادئ وقواعد لآلية تصنيف مستوى الحساسية. • تحديد وتوثيق مستوى الحساسية (Criticality Rating) لجميع الأصول الخاصة بأنظمة التحكم الصناعي (OT/ICS) بناء على القواعد والمبادئ المعرفة. • التأكد من اعتماد مستوى الحساسية (Criticality Rating) لجميع الأصول، من قبل ملاك الأصول. **المخرجات المتوقعة:** • إثبات يؤكد اعتماد مستوى الحساسية (Criticality Rating) لجميع الأصول، من قبل ملاك الأصول. • إثبات يؤكد تحديد وتوثيق مستوى الحساسية (Criticality Rating) لجميع الأصول الخاصة بأنظمة التحكم الصناعي (OT/ICS).
٢-١-٢		رجوعاً للضابط ٢-١-٦ في الضوابط الأساسية للأمن السيبراني؛ يجب مراجعة متطلبات الأمن السيبراني المتعلقة بإدارة أصول أنظمة التحكم الصناعي (OT/ICS)، وقياس فعالية تطبيقها وتقييمها دورياً. **أدوات الأمن السيبراني ذات العلاقة:** • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية

	• نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • نموذج سياسة إدارة الأصول • نموذج تقرير مؤشرات الأداء الرئيسية **إرشادات تطبيق الضوابط:** • العمل على مراجعة متطلبات الأمن السيبراني المتعلقة بإدارة أصول أنظمة التحكم الصناعي (OT/ICS) بشكل دوري حسب خطة موثقة ومعتمدة للمراجعة بناءً على فترة زمنية محددة (على سبيل المثال، يتم إجراء المراجعة الدورية بشكل سنوي). • العمل على تطوير مؤشرات أداء رئيسية (KPIs) لكل الضوابط المتضمنة بداخل السياسات أو الإجراءات للتأكد من قياس فعالية تطبيقها، وتقييمها دورياً بناءً على فترة زمنية محددة (على سبيل المثال، يتم إجراء المراجعة الدورية بشكل سنوي). **المخرجات المتوقعة:** • إثبات يؤكد القيام بالمراجعة الدورية لمتطلبات الأمن السيبراني المتعلقة بإدارة أصول أنظمة التحكم الصناعي (OT/ICS). • إثبات يؤكد القيام بقياس مؤشرات الأداء الرئيسية (KPIs) لكل الضوابط المتضمنة بداخل السياسات أو الإجراءات للتأكد من قياس فعالية تطبيقها، وتقييمها دورياً بناءً على فترة زمنية محددة.
٢-٢	إدارة هويات الدخول والصلاحيات (Identity and Access Management)
الهدف	ضمان حماية الأمن السيبراني للوصول المنطقي (Logical Access) إلى أصول أنظمة التحكم الصناعي (OT/ICS) للجهة؛ من أجل منع الوصول غير المصرح به، وتقييد الوصول إلى ما هو مطلوب؛ لإنجاز الأعمال المتعلقة بالجهة.
الضوابط	
٢-٢-١	بالإضافة للضوابط الفرعية، ضمن الضابط ٢-٢-٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني المتعلقة بإدارة هويات الدخول، والصلاحيات في بيئة أنظمة التحكم الصناعي (OT/ICS) بحد أدنى ما يلي:
٢-٢-١-١	التأكد من أن دورة حياة إدارة هويات الدخول والصلاحيات، لأنظمة التحكم الصناعي (OT/ICS) مفصولة ومستقلة، عن تلك المتعلقة بتقنية المعلومات (IT) وذلك يشمل الحلول التقنية المستخدمة في الإدارة المركزية لهويات الدخول والصلاحيات.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • نموذج سياسة ادارة هويات الدخول والصلاحيات • نموذج معيار إدارة هويات الدخول والصلاحيات

إرشادات تطبيق الضوابط:

- تحديد آلية لإدارة هويات وصلاحيات أنظمة التحكم الصناعي (OT/ICS) بحيث تتضمن دورة حياة إدارة الهويات والصلاحيات وذلك عند (إنشاء مستخدم جديد، تجديد صلاحيات مستخدم، إزالة مستخدم).
- التأكد من أن دورة حياة إدارة هويات الدخول والصلاحيات، لأنظمة التحكم الصناعي (OT/ICS) مفصولة ومستقلة، عن تلك المتعلقة بتقنية المعلومات (IT).

المخرجات المتوقعة:

- وثيقة آلية إدارة الهويات والصلاحيات لأنظمة التحكم الصناعي (OT/ICS).
- زيارة ميدانية للتحقق من أن الدليل النشط (Active Directory) الخاص ببيئة أنظمة التحكم الصناعي (OT/ICS) مستقل ومفصول عن تقنية المعلومات (IT).

٢-١-٢-٢	الإدارة الآمنة لحسابات الخدمات (Service Accounts) المتعلقة بخدمات التحكم الصناعي (OT/ICS) وتطبيقاتها، وأنظمتها، وأجهزتها المعزولة وغير المتصلة بحسابات دخول المستخدمين التفاعلية (Interactive Login).

أدوات الأمن السيبراني ذات العلاقة:

- نموذج سياسة الأمن السيبراني للأنظمة التشغيلية
- نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS)
- نموذج سياسة ادارة هويات الدخول والصلاحيات
- نموذج معيار إدارة هويات الدخول والصلاحيات

إرشادات تطبيق الضوابط:

- العمل على تطوير إجراءات للإدارة الآمنة لحسابات الخدمات (Service Accounts) المتعلقة بخدمات التحكم الصناعي (OT/ICS) وتطبيقاتها، وأنظمتها، وأجهزتها المعزولة وغير المتصلة بحسابات دخول المستخدمين التفاعلية (Interactive Login) وذلك بالتنسيق مع الشركة المصنعة أو المورد (Vendor or OEM).
- التأكد من أن جميع حسابات الخدمات مدارة ومتماشية مع الإجراءات المعرفة.

المخرجات المتوقعة:

- قائمة بجميع حسابات الخدمات (Service Accounts) المتعلقة بخدمات التحكم الصناعي (OT/ICS).
- إجراءات إدارة حسابات الخدمات (Service Accounts).
- زيارة ميدانية للتحقق من أن جميع حسابات الخدمات مدارة ومتماشية مع الإجراءات المعرفة.

٢-٢-١-٣	تغيير الهويات المصنعية (Default Credentials) لجميع الأصول المتعلقة بأنظمة التحكم الصناعي (OT/ICS) أو تعطيلها، أو إزالتها.

أدوات الأمن السيبراني ذات العلاقة:

- نموذج سياسة الأمن السيبراني للأنظمة التشغيلية
- نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS)
- نموذج سياسة ادارة هويات الدخول والصلاحيات
- نموذج معيار إدارة هويات الدخول والصلاحيات

إرشادات تطبيق الضوابط

- التأكد من أن جميع الهويات المصنعية (Default Credentials) لجميع الأصول المتعلقة بأنظمة التحكم الصناعي (OT/ICS) تم تغييرها، أو تعطيلها، أو إزالتها وذلك بالتنسيق مع الشركة المصنعة أو المورد (Vendor or OEM).

المخرجات المتوقعة:

- إثبات من الشركة المصنعة يؤكد إزالة أو تعطيل أو تغيير جميع الهويات المصنعية (Default Credentials) للأصول الخاصة بأنظمة التحكم الصناعي (OT/ICS).
- زيارة ميدانية للتحقق من إزالة أو تعطيل أو تغيير جميع الهويات المصنعية (Default Credentials) للأصول الخاصة بأنظمة التحكم الصناعي (OT/ICS).

٢-٢-١-٤	الإدارة الآمنة لجلسات الاتصال، ويشمل ذلك موثوقية الجلسات (Authenticity)، وإقفالها (Lockout)، وإنهاء مهلتها (Timeout).

أدوات الأمن السيبراني ذات العلاقة:

- نموذج سياسة الأمن السيبراني للأنظمة التشغيلية
- نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS)
- نموذج سياسة ادارة هويات الدخول والصلاحيات
- نموذج معيار إدارة هويات الدخول والصلاحيات

إرشادات تطبيق الضوابط:

- العمل على تطوير إجراءات لإدارة الجلسات (Sessions Management Procedures) بالتعاون مع الشركة المصنعة وذلك لإدارة الجلسات بشكل آمن. وتتضمن هذه الإجراءات موثوقية الجلسات (Authenticity)، وإقفالها (Lockout)، وإنهاء مهلتها (Timeout) للأجهزة والخوادم.
- التأكد من تطبيق الإجراءات المعرفة والمعتمدة لإدارة الجلسات. ويتضمن ذلك موثوقية الجلسات (Authenticity)، و إقفالها (Lockout)، وإنهاء مهلتها (Timeout) للأجهزة والخوادم.

المخرجات المتوقعة: • وثيقة إجراءات إدارة الجلسات (Sessions Management Procedures). • زيارة ميدانية للتحقق من تطبيق الإجراءات المعرفة والمعتمدة لإدارة الجلسات. ويتضمن ذلك موثوقية الجلسات (Authenticity)، وإقفالها (Lockout)، وإنهاء مهلتها (Timeout) وذلك على الأجهزة والخوادم.	
٢-٢-١-٥	منع التعطيل، أو الإزالة التلقائية لحسابات الخدمات، أو البرامج، أو حسابات الأجهزة المتعلقة بأنظمة التحكم الصناعي (OT/ICS) باستثناء أنظمة المراقبة.
أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • نموذج سياسة ادارة هويات الدخول والصلاحيات • نموذج معيار إدارة هويات الدخول والصلاحيات **إرشادات تطبيق الضوابط:** • التأكد من أن كل الحسابات الخاصة بالمهندسين والمشغلين ليس لديها الصلاحية لإزالة البرامج. • إنشاء حسابات فردية للمهندسين مع وضع الصلاحيات المناسبة لكل مهندس. على سبيل المثال (إنشاء حساب فردي لكل مستخدم مع تحديد اسم مستخدم وكلمة مرور عندما يحتاج/تحتاج المهندس/ه للوصول إلى أجهزة المهندسين (Engineering Workstation)).	
المخرجات المتوقعة: • زيارة ميدانية للتأكد من صلاحيات المهندسين والمشغلين. • زيارة ميدانية للتأكد من أن الحسابات ذات الصلاحية تم إنشائها للأفراد.	
٢-٢-١-٦	استخدام إجراءات الاعتمادات الثنائية (Dual Approval) وآليات محددة لتصعيد الصلاحيات للإجراءات الحساسة، داخل بيئة أنظمة التحكم الصناعي (OT/ICS).
أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • نموذج سياسة ادارة هويات الدخول والصلاحيات • نموذج معيار إدارة هويات الدخول والصلاحيات	

	إرشادات تطبيق الضوابط: • تحديد وتوثيق آلية للإجراءات الحساسة في بيئة أنظمة التحكم الصناعي (OT/ICS). • تطبيق إجراءات الاعتمادات الثنائية (Dual Approval) وآليات تصعيد الصلاحيات بناء على الآلية الموثقة والمعرفة مسبقاً.
	المخرجات المتوقعة: • وثيقة آلية الإجراءات الحساسة في بيئة أنظمة التحكم الصناعي (OT/ICS). • إثبات يؤكد تطبيق إجراءات الاعتمادات الثنائية (Dual Approval) وآليات تصعيد بناء على الآلية الموثقة والمعرفة مسبقاً.
٢-٢-١-٧	تقييد الوصول عن بعد لشبكات أنظمة التحكم الصناعي (OT/ICS) وتمكينه بشكل استثنائي عند الضرورة، ووجود المبررات اللازمة، على أن يتم إجراء تقييم مخاطر الأمن السيبراني قبل منح الوصول عن بعد، ورصد المخاطر المتعلقة بذلك وإدارتها. وأن يكون الدخول المصرح به من خلال التحقق من الهوية ذات العناصر المتعددة ("MFA" Multi-Factor Authentication) وعبر قناة مشفرة لفترة زمنية محددة، وبصلاحيات محدودة. ويتم مراقبة جلسة الوصول عن بعد وتسجيلها، على أن تكون الصلاحيات الممنوحة للمستخدم، متوافقة مع تقييم مخاطر الأمن السيبراني.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • نموذج سياسة ادارة هويات الدخول والصلاحيات • نموذج معيار إدارة هويات الدخول والصلاحيات **إرشادات تطبيق الضوابط:** • تحديد وتوثيق واعتماد متطلبات الأمن السيبراني للوصول عن بعد لشبكات أنظمة التحكم الصناعي (OT/ICS). • إنشاء إجراءات لتقييم مخاطر ومراقبة مخاطر الوصول عن بعد لشبكات أنظمة التحكم الصناعي (OT/ICS). • العمل على توفير تقنيات التحقق من الهوية ذات العناصر المتعددة (Multi-Factor Authentication) وعبر قناة مشفرة لعمليات الدخول عن بعد. • مراقبة جلسة الوصول عن بعد وتسجيلها، على أن تكون الصلاحيات الممنوحة للمستخدم، متوافقة مع تقييم مخاطر الأمن السيبراني وذلك لفترة زمنية محددة.
	المخرجات المتوقعة: • وثيقة متطلبات الأمن السيبراني للوصول عن بعد لشبكات أنظمة التحكم الصناعي (OT/ICS).

	• إجراءات تقييم مخاطر. • تقارير تقييم المخاطر. • إثبات يؤكد توفير تقنيات التحقق من الهوية ذات العناصر المتعددة (Multi-Factor Authentication) وعبر قناة مشفرة لعمليات الدخول عن بعد. • تقارير المراقبة والتسجيل لعمليات الدخول عن بعد.
٢-٢-١-٨	تطبيق معايير آمنة ومعقدة لكلمات المرور.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • نموذج سياسة ادارة هويات الدخول والصلاحيات • نموذج معيار إدارة هويات الدخول والصلاحيات، بحيث يشمل إدارة كلمات المرور **إرشادات تطبيق الضوابط:** • تحديد وتوثيق واعتماد معايير كلمة المرور أخذًا بالاعتبار أفضل الممارسات. • تطبيق معايير كلمة المرور المعتمدة على أنظمة التحكم الصناعي (OT/ICS).
	المخرجات المتوقعة: • وثيقة معايير إدارة كلمة المرور. • زيارة ميدانية للتأكد من تطبيق معايير كلمة المرور على أنظمة التحكم الصناعي (OT/ICS).
٢-٢-١-٩	استخدام آليات آمنة لتخزين كلمات المرور، الخاصة بأصول أنظمة التحكم الصناعي (OT/ICS).
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • نموذج سياسة ادارة هويات الدخول والصلاحيات • نموذج معيار إدارة هويات الدخول والصلاحيات **إرشادات تطبيق الضوابط:** • توثيق وتحديد إجراءات تخزين كلمات المرور الخاصة بأصول أنظمة التحكم الصناعي (OT/ICS).

	• تطبيق الآليات الآمنة لتخزين كلمات المرور الخاصة بأصول أنظمة التحكم الصناعي (OT/ICS) على سبيل المثال لا الحصر (Secure Password Manager). • التأكد والتحقق من أن جميع كلمات المرور الخاصة بأصول أنظمة التحكم الصناعي (OT/ICS) مخزنة بآلية آمنة وذلك تماشياً مع الإجراءات الموثقة. • التأكد من جميع الحسابات الطارئة (Emergency Account) مخزنة بآلية آمنة وذلك تماشياً مع الإجراءات الموثقة.
	المخرجات المتوقعة: • وثيقة إجراءات تخزين كلمات المرور الخاصة بأصول أنظمة التحكم الصناعي (OT/ICS). • زيارة ميدانية للتحقق من أن كلمات المرور الخاصة بأصول أنظمة التحكم الصناعي (OT/ICS) والحسابات الطارئة (Emergency Account) مخزنة بآلية آمنة وذلك تماشياً مع الإجراءات الموثقة.
٢-٢-١-١٠	رجوعاً للضابط الفرعي ٢-٢-٣-٥ في الضوابط الأساسية للأمن السيبراني؛ يجب مراجعة هويات الدخول والصلاحيات، عند الاستجابة لحوادث الأمن السيبراني، وعند التغيير في أدوار العاملين، أو عند حدوث أي تغيير في الهيكلية المعمارية لأنظمة التحكم الصناعي (OT/ICS).
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • نموذج سياسة ادارة هويات الدخول والصلاحيات • نموذج معيار إدارة هويات الدخول والصلاحيات **إرشادات تطبيق الضوابط:** • تطوير وثيقة إجراءات معتمدة وخطة مراجعة دورية لهويات الدخول والصلاحيات، وذلك عند الاستجابة لحوادث الأمن السيبراني، وعند التغيير في أدوار العاملين، أو عند حدوث أي تغيير في الهيكلية المعمارية لأنظمة التحكم الصناعي (OT/ICS). • التأكد والتحقق من تطبيق خطة المراجعة الدورية لهويات الدخول والصلاحيات، وذلك عند الاستجابة لحوادث الأمن السيبراني، وعند التغيير في أدوار العاملين، أو عند حدوث أي تغيير في الهيكلية المعمارية لأنظمة التحكم الصناعي (OT/ICS).
	المخرجات المتوقعة: • وثيقة إجراءات وخطة المراجعة الدورية لهويات الدخول والصلاحيات. • إثبات يؤكد تطبيق الإجراءات وخطة المراجعة الدورية لهويات الدخول والصلاحيات، وذلك عند الاستجابة لحوادث الأمن السيبراني، وعند التغيير في أدوار العاملين، أو عند حدوث أي تغيير في الهيكلية المعمارية لأنظمة التحكم الصناعي (OT/ICS).

	٢-٢-١-١١	إلغاء صلاحيات الدخول مباشرة، عند انتهاء الحاجة لها.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • نموذج سياسة ادارة هويات الدخول والصلاحيات • نموذج معيار إدارة هويات الدخول والصلاحيات **إرشادات تطبيق الضوابط:** • إلغاء صلاحيات الدخول لجميع المستخدمين وذلك عند الانتهاء منها. • التأكد والتحقق أن جميع صلاحيات الدخول ملغية عند انتهاء الحاجة لها.	
	المخرجات المتوقعة: • توثيق متطلبات الضابط في سياسة إدارة الهويات والصلاحيات الخاصة بأنظمة التحكم الصناعي (OT/ICS). • إثبات يؤكد أن جميع صلاحيات الدخول ملغية عند انتهاء الحاجة لها.	
٢-٢-٢	رجوعاً للضابط ٢-٢-٤ في الضوابط الأساسية للأمن السيبراني؛ فأنه يجب مراجعة متطلبات الأمن السيبراني، المتعلقة بإدارة هويات الدخول والصلاحيات، في بيئة أنظمة التحكم الصناعي (OT/ICS)، وقياس فعالية تطبيقها وتقييمها دورياً.	
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • نموذج سياسة ادارة هويات الدخول والصلاحيات • نموذج معيار إدارة هويات الدخول والصلاحيات • نموذج تقرير مؤشرات الأداء الرئيسية **إرشادات تطبيق الضوابط:** • العمل على مراجعة متطلبات الأمن السيبراني المتعلقة بإدارة هويات الدخول والصلاحيات، في بيئة أنظمة التحكم الصناعي (OT/ICS) بشكل دوري حسب خطة موثقة ومعتمدة للمراجعة بناءً على فترة زمنية محددة (على سبيل المثال، يتم إجراء المراجعة الدورية بشكل سنوي). • العمل على تطوير مؤشرات أداء رئيسية (KPIs) لكل الضوابط المتضمنة بداخل السياسات أو الإجراءات للتأكد من قياس فعالية تطبيقها، وتقييمها دورياً بناءً على فترة زمنية محددة (على سبيل المثال، يتم إجراء المراجعة الدورية بشكل سنوي).	
	المخرجات المتوقعة:	

	• إثبات يؤكد القيام بالمراجعة الدورية لمتطلبات الأمن السيبراني المتعلقة بإدارة هويات الدخول والصلاحيات، في بيئة أنظمة التحكم الصناعي (OT/ICS). • إثبات يؤكد القيام بقياس مؤشرات الأداء الرئيسية (KPIs) لكل الضوابط المتضمنة بداخل السياسات أو الإجراءات للتأكد من قياس فعالية تطبيقها، وتقييمها دورياً بناءً على فترة زمنية محددة.
٢-٣	حماية النظم ومرافق المعالجة (System and Processing Facility Protection)
الهدف	ضمان حماية أنظمة التحكم الصناعي (OT/ICS) ومرافق المعالجة (بما في ذلك الأجهزة والخوادم وأنظمة معدات السلامة "SIS") من المخاطر السيبرانية.
الضوابط	
٢-٣-١	بالإضافة للضوابط الفرعية، ضمن الضابط ٢-٣-٣ في الضوابط الأساسية للأمن السيبراني؛ يجب أن تغطي متطلبات الأمن السيبراني، لحماية الأنظمة وأجهزة معالجة المعلومات، المتعلقة بأنظمة التحكم الصناعي (OT/ICS) بحد أدنى؛ ما يلي:
٢-٣-١-١	استخدام تقنيات وآليات الحماية الحديثة والمتقدمة، وإدارتها بشكل آمن، للحماية من الفيروسات، والبرامج، والأنشطة المشبوهة، والبرمجيات الضارة (Malware)، والتهديدات المتقدمة المستمرة (APT)، والملفات الضارة، وحظرها.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • نموذج معيار الحماية من البرمجيات الضارة • نموذج معيار امن الخوادم • نموذج معيار الحماية من التهديدات المتقدمة المستمرة **إرشادات تطبيق الضوابط:** • تطبيق تقنيات وآليات الحماية الحديثة والمتقدمة، وإدارتها بشكل آمن، للحماية من الفيروسات، والبرامج، والأنشطة المشبوهة، والبرمجيات الضارة (Malware) والتهديدات المتقدمة المستمرة (APT) والملفات الضارة، وحظرها. • تطبيق آخر اصدار من تقنيات وآليات الحماية الحديثة والمتقدمة وتحديث قواعد البيانات والتواقيع (Signatures) الخاصة بالحلول التقنية. • التأكد من إدارة الحلول التقنية بشكل آمن، للحماية من الفيروسات، والبرامج، والأنشطة المشبوهة، والبرمجيات الضارة (Malware) وتحديثها بشكل دوري (بناء على فترات زمنية محددة)، وتفعيل جدولة فحص الملفات، بالإضافة إلى حفظ سجلات الأحداث بما لا يقل عن ٣ أشهر.

المخرجات المتوقعة: • زيارة ميدانية للتحقق من التالي: o وجود حلول تقنيات وآليات الحماية الحديثة والمتقدمة المطبقة. o نطاق الحلول المطبقة (يجب أن يغطي جميع أصول التحكم الصناعي (OT/ICS)). o الحلول المطبقة، وقواعد بياناتها، وتواقيعها (Signatures). o الفحوصات المجدولة (Schedule Scanning). o سجل الأحداث الخاص بالفحوصات لجميع النهايات الطرفية.	
٢-١-٣-٢	إجراء مراجعة دورية للإعدادات والتحصين (Secure Configuration and Hardening) بما يتوافق مع إرشادات الأمن السيبراني، وأفضل الممارسات، والتوصيات الخاصة بالموردين (vendor)، وبما يتوافق مع آليات إدارة التغيير المتبعة في الجهة.
أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • نموذج معايير الإعدادات الآمنة والتحصين **إرشادات تطبيق الضوابط:** • العمل على تطوير قائمة مراجعة (Checklist) لمراجعة وتقييم الإعدادات والتحصين (Secure Configuration and Hardening) الخاصة بأنظمة التحكم الصناعي (OT/ICS). • يجب أن تتوافق قائمة المراجعة مع إرشادات الأمن السيبراني، وأفضل الممارسات، والتوصيات الخاصة بالموردين (Vendor Security Baselines).	
المخرجات المتوقعة: • وثيقة إجراءات المراجعة الدورية للإعدادات والتحصن (Secure Configuration and Hardening). • إثبات يؤكد تطبيق إجراءات المراجعة الدورية للإعدادات والتحصن (Secure Configuration and Hardening) بما يتوافق مع إرشادات الأمن السيبراني، وأفضل الممارسات، والتوصيات الخاصة بالموردين (Vendor).	
٢-١-٣-٣	تطبيق حزم التحديثات، والإصلاحات الأمنية بشكل دوري، على أنظمة التحكم الصناعي (OT/ICS) بما يتوافق مع إرشادات الأمن السيبراني، وأفضل الممارسات الخاصة بالموردين (vendor)، وبما يتوافق مع آليات إدارة التغيير المتبعة في الجهة.
أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية	

	• نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • سياسة ادارة حزم التحديثات والاصلاحات • معيار إدارة التحديثات والإصلاحات **إرشادات تطبيق الضوابط** • الحصول على تأكيد من الشركة المصنعة لآخر حزم تحديثات معتمدة (Approved Patches) بما يتوافق مع إرشادات الأمن السيبراني. • تحديد وتوثيق واعتماد إجراءات حزم التحديثات، والإصلاحات الأمنية بشكل دوري بما يتوافق مع الإرشادات أو التوصيات المجمعة فيما يتعلق بالأمن السيبراني وآليات إدارة التغيير المتبعة في الجهة. • التأكد من تطبيق حزم التحديثات، والإصلاحات الأمنية الدورية المعتمدة من قبل الشركة المصنعة. • التأكد من أن حزم التحديثات، والإصلاحات الأمنية تتوافق مع آليات إدارة التغيير المتبعة في الجهة. **المخرجات المتوقعة:** • وثيقة إجراءات حزم التحديثات والإصلاحات الأمنية الدورية. • زيارة ميدانية للتحقق من حزم التحديثات والإصلاحات الأمنية المطبقة. • تأكيد من الشركة المصنعة لآخر حزم التحديثات والإصلاحات الأمنية تم الموافقة عليها. • طلب التغيير الخاص بتطبيق حزم التحديثات والإصلاحات الأمنية.
٤-١-٣-٢	تطبيق مبدأ الحد الأدنى من الصلاحيات والامتيازات (Least Privilege) والحد الأدنى من الامكانيات (Least Functionality).
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) **إرشادات تطبيق الضوابط:** • تحديد الأدوار والمسؤوليات (Roles and Responsibilities) التي سيتم منحها الصلاحية ومن ثم توثيق مبدأ الحد الأدنى من الصلاحيات والامتيازات (Least Privilege) والحد الأدنى من الامكانيات (Least Functionality) للمسؤوليات المعرفة. • تطبيق مبدأ الحد الأدنى من الصلاحيات والامتيازات (Least Privilege) والحد الأدنى من الامكانيات (Least Functionality) على سبيل المثال لا الحصر (Privileged Access Management tool). • التحقق والتأكد من أن نطاق مبدأ الصلاحيات والامتيازات والحد الأدنى من الامكانيات يغطي جميع أصول أنظمة التحكم الصناعي (OT/ICS).

المخرجات المتوقعة: • وثيقة الأدوار المسؤوليات المعرفة. • زيارة ميدانية للتحقق من تطبيق مبدأ الحد الأدنى من الصلاحيات والامتيازات (Least Privilege) والحد الأدنى من الامكانيات (Least Functionality).	
٢-٣-١-٥	إعداد ووضع وحدات التحكم (Controllers) في أنظمة معدات السلامة (SIS) في الأوضاع الاعتيادية التشغيلية في جميع الأوقات؛ مما يمنع أي تغييرات غير مصرح بها، ولا يكون تغييرها الى الوضع غير الاعتيادي إلا بصفة استثنائية، ويكون ذلك مقيداً بفترة زمنية محددة.
أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) **إرشادات تطبيق الضوابط:** • التأكد من أن وحدات التحكم الخاصة بأنظمة معدات السلامة (SIS) في الأوضاع الاعتيادية التشغيلية. • تحديد إجراءات في حال الحاجة إلى تغيير وحدات التحكم الخاصة بأنظمة معدات السلامة (SIS) إلى الأوضاع الغير اعتيادية (improper modes). • التأكد من أن التغييرات للأوضاع الغير اعتيادية (improper modes) لا تتم إلا بصفة استثنائية، ويكون ذلك مقيداً بفترة زمنية محددة.	
المخرجات المتوقعة: • زيارة ميدانية للتحقق من أن وحدات التحكم الخاصة بأنظمة معدات السلامة (SIS) في الأوضاع الاعتيادية التشغيلية. • قائمة موثقة بالحالات الغير استثنائية في حال الحاجة إلى تغيير وحدات التحكم الخاصة بأنظمة معدات السلامة (SIS) إلى الأوضاع الغير اعتيادية (improper modes).	
٢-٣-١-٦	تحديد قوائم محددة من التطبيقات المسموح بتشغيلها في بيئة أنظمة التحكم الصناعي (OT/ICS) من خلال التقنيات المتاحة، مثل تقنية (Whitelisting).
أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) **إرشادات تطبيق الضوابط:**	

	• التأكد من استخدام تقنيات السماح بالتطبيقات مثل تقنية (Whitelisting) أو تقنيات مشابهة لها، وذلك لتحديد قوائم محددة من التطبيقات المسموح بتشغيلها في بيئة أنظمة التحكم الصناعي (OT/ICS).
	المخرجات المتوقعة: • زيارة ميدانية للتأكد من تطبيق تقنيات السماح بالتطبيقات مثل تقنية (Whitelisting) أو تقنيات مشابهة لها.
٢-٣-١-٧	إدارة أصول أنظمة التحكم الصناعي (OT/ICS) من خلال أجهزة المهندسين (Engineering Workstations) وأجهزة واجهات التعامل مع الأنظمة ("Human-Machine Interface "HMI")، والتأكد من أن تكون أجهزة إدارة الأصول وصيانتها؛ محصنة ومعزولة.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) **إرشادات تطبيق الضوابط:** • التحقق والتأكد من أن جميع أجهزة المهندسين (Engineering Workstations) وأجهزة واجهات التعامل مع الأنظمة ("Human-Machine Interface "HMI") معزولة. • التحقق والتأكد من أن جميع أجهزة المهندسين (Engineering Workstations) وأجهزة واجهات التعامل مع الأنظمة ("Human-Machine Interface "HMI") محصنة (hardened)، تماشياً مع المتطلبات والمبادئ المعتمدة ذات العلاقة.
	المخرجات المتوقعة: • زيارة ميدانية للتحقق من أن جميع الأصول الخاصة بأنظمة التحكم الصناعي (OT/ICS) تدار عن طريق أجهزة المهندسين (Engineering Workstations) وأجهزة واجهات التعامل مع الأنظمة ("Human-Machine Interface "HMI") مخصصة ومعزولة ومحصنة.
٢-٣-١-٨	فحص وسائط التخزين الخارجية، وتحليلها ضد البرامج الضارة، والتهديدات المتقدمة المستمرة (APT) في بيئة معزولة وآمنة.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • نموذج سياسة أمن وسائط التخزين **إرشادات تطبيق الضوابط:**

	• العمل على تطوير بيئة معزولة وآمنة لفحص وسائط التخزين الخارجية. • تحديد وتوثيق إجراءات للفحص والعمل على تطبيقها. • التأكد والتحقق من أن جميع وسائط التخزين الخارجية يتم فحصها وتحليلها ضد البرامج الضارة، والتهديدات المتقدمة المستمرة (APT).
	المخرجات المتوقعة: • وثيقة إجراءات فحص وسائط التخزين الخارجية. • إثبات يؤكد أن جميع وسائط التخزين الخارجية يتم فحصها وتحليلها ضد البرامج الضارة، والتهديدات المتقدمة المستمرة (APT).
٢-٣-١-٩	التقييد الحازم لاستخدام وسائط التخزين الخارجية في بيئة الإنتاج، ما لم يتم تطوير آليات آمنة وتطبيقها لنقل البيانات.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) **إرشادات تطبيق الضوابط:** • العمل على تقييد استخدام وسائط التخزين الخارجية في بيئة الإنتاج وذلك لتجنب الوصول غير المصرح به وغير المتوقع للعمليات التشغيلية. • العمل على تطوير آلية وإجراءات للنقل الآمن للبيانات في بيئة الإنتاج، على سبيل المثال لا الحصر (تخصيص مجلد مشاركة آمن (file server)، أو تخصيص وسائط تخزين خارجية (USBs and hard disks)، تستخدم في المنشأة فقط).
	المخرجات المتوقعة: • وثيقة إجراءات نقل البيانات في بيئة الإنتاج. • زيارة ميدانية للتحقق من تقييد استخدام وسائط التخزين الخارجية.
٢-٣-١-١٠	حماية سجلات الأحداث، والملفات الحساسة، من الدخول غير المصرح به، أو التلاعب، أو التغيير غير المصرح به، أو الحذف.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS)

إرشادات تطبيق الضوابط:

- التأكد من تفعيل جميع سجلات الأحداث الأمنية والخاصة بالأنظمة (system and security logs).
- التأكد من حماية سجلات الأحداث، والملفات الحساسة، من الدخول غير المصرح به، أو التلاعب، أو التغيير غير المصرح به، أو الحذف. وذلك من خلال إدارة الجلسات عن طريق إغلاقها (session lockout) وانتهائها (session timeout)، كما يجب تخصيص حساب لكل من المستخدمين في أجهزة المهندسين (workstation) مع وضع الصلاحيات المناسبة لكل حساب.

المخرجات المتوقعة:

- زيارة ميدانية للتحقق من التالي:
  - سجلات الأحداث الأمنية والخاصة بالأنظمة (system and security logs)
  - إدارة الجلسات
  - قائمة الحسابات

٢-٣-١-١١	اكتشاف التطبيقات والبرامج النصية (Scripts) والمهمات والتغييرات غير المصرح بها، وفحصها.

أدوات الأمن السيبراني ذات العلاقة:

- نموذج سياسة الأمن السيبراني للأنظمة التشغيلية
- نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS)

إرشادات تطبيق الضوابط:

- التأكد من تفعيل سجلات الاحداث (Event logs) التطبيقات والبرامج النصية (Scripts) والمهمات والتغييرات غير المصرح بها وتحويلها إلى نظام إدارة سجلات الاحداث والمراقبة (SIEM) أو مجمع سجلات الاحداث (Log collector)، ومن ثم يتم تحليل هذه الأحداث عن طريق مركز المراقبة الأمنية (SOC).

المخرجات المتوقعة:

- إثبات يؤكد اكتشاف التطبيقات والبرامج النصية (Scripts) والمهمات والتغييرات غير المصرح بها، وفحصها.
- قائمة الحالات المطورة (Use-cases) الخاصة بأنظمة التحكم الصناعي (OT/ICS) من مركز المراقبة الأمنية (SOC).

٢-٣-١-١٢	اكتشاف الأوامر المنفذة (Commands Execution) وجلسات الاتصالات الحديثة (New Communication Sessions)، وفحصها.

أدوات الأمن السيبراني ذات العلاقة:

- نموذج سياسة الأمن السيبراني للأنظمة التشغيلية
- نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS)

إرشادات تطبيق الضوابط:

- العمل على تطبيق تقنيات وأدوات لاكتشاف الأوامر المنفذة (Commands Execution) وجلسات الاتصالات الحديثة (New Communication Sessions)، مثل (network traffic monitoring tools or intrusion detection system).
- التأكد من تفعيل سجلات الأحداث (Event logs) الخاصة بالأوامر المنفذة (Commands Execution) وجلسات الاتصالات الحديثة (New Communication Sessions)، وتحويلها إلى نظام إدارة سجلات الأحداث والمراقبة (SIEM) أو مجمع سجلات الأحداث (Log collector)، ومن ثم يتم تحليل هذه الأحداث عن طريق مركز المراقبة الأمنية (SOC).

المخرجات المتوقعة:

- إثبات يؤكد اكتشاف الأوامر المنفذة (Commands Execution) وجلسات الاتصالات الحديثة (New Communication Sessions).
- قائمة الحالات المطورة (Use-cases) الخاصة بأنظمة التحكم الصناعي (OT/ICS) من مركز المراقبة الأمنية (SOC).

٢-٣-١-١٣	اكتشاف الاتصالات المباشرة بين بيئة شبكات أنظمة التحكم الصناعي (OT/ICS) والأطراف الخارجية (External Hosts)، وفحصها.

أدوات الأمن السيبراني ذات العلاقة:

- نموذج سياسة الأمن السيبراني للأنظمة التشغيلية
- نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS)

إرشادات تطبيق الضوابط:

- العمل على تطبيق تقنيات وأدوات لاكتشاف الاتصالات المباشرة بين بيئة شبكات أنظمة التحكم الصناعي (OT/ICS) الأطراف الخارجية (External Hosts)، مثل (network traffic monitoring tools).
- التأكد من تفعيل سجلات الأحداث (Event logs) الخاصة بالاتصالات المباشرة بين بيئة شبكات أنظمة التحكم الصناعي (OT/ICS) الأطراف الخارجية (External Hosts)، وتحويلها إلى نظام إدارة سجلات الأحداث والمراقبة (SIEM) أو مجمع سجلات الاحداث (Log collector)، ومن ثم يتم تحليل هذه الاحداث عن طريق مركز المراقبة الأمنية (SOC).

المخرجات المتوقعة:

- إثبات يؤكد اكتشاف الاتصالات المباشرة بين بيئة شبكات أنظمة التحكم الصناعي (OT/ICS) الأطراف الخارجية (External Hosts).
- قائمة الحالات المطورة (Use-cases) الخاصة بأنظمة التحكم الصناعي (OT/ICS) من مركز المراقبة الأمنية (SOC).

٢-٣-٢	رجوعاً للضابط ٢-٣-٤ في الضوابط الأساسية للأمن السيبراني؛ يجب مراجعة متطلبات الأمن السيبراني لحماية أنظمة معالجة المعلومات والأجهزة والمتعلقة بأنظمة التحكم الصناعي (OT/ICS)، وقياس فعالية تطبيقها وتقييمها دورياً.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • نموذج تقرير مؤشرات الأداء الرئيسية **إرشادات تطبيق الضوابط:** • العمل على مراجعة متطلبات الأمن السيبراني لحماية أنظمة معالجة المعلومات والأجهزة والمتعلقة بأنظمة التحكم الصناعي (OT/ICS) بشكل دوري حسب خطة موثقة ومعتمدة للمراجعة بناءً على فترة زمنية محددة (على سبيل المثال، يتم إجراء المراجعة الدورية بشكل سنوي). • العمل على تطوير مؤشرات أداء رئيسية (KPIs) لكل الضوابط المتضمنة بداخل السياسات أو الإجراءات للتأكد من قياس فعالية تطبيقها، وتقييمها دورياً بناءً على فترة زمنية محددة (على سبيل المثال، يتم إجراء المراجعة الدورية بشكل سنوي).
	المخرجات المتوقعة: • إثبات يؤكد القيام بالمراجعة الدورية لمتطلبات الأمن السيبراني لحماية أنظمة معالجة المعلومات والأجهزة والمتعلقة بأنظمة التحكم الصناعي (OT/ICS). • إثبات يؤكد القيام بقياس مؤشرات الأداء الرئيسية (KPIs) لكل الضوابط المتضمنة بداخل السياسات أو الإجراءات للتأكد من قياس فعالية تطبيقها، وتقييمها دورياً بناءً على فترة زمنية محددة.
٢-٤	**إدارة أمن الشبكات (Networks Security Management)**
الهدف	ضمان حماية شبكات أنظمة التحكم الصناعي (OT/ICS) الخاصة بالجهة من المخاطر السيبرانية.
الضوابط	
٢-٤-١	بالإضافة للضوابط الفرعية ضمن الضابط ٢-٥-٣ في الضوابط الأساسية للأمن السيبراني؛ يجب أن تغطي متطلبات الأمن السيبراني، لإدارة أمن الشبكات المتعلقة بأنظمة التحكم الصناعي (OT/ICS) بحد أدنى ما يلي:
٢-٤-١-١	تقسيم شبكات أنظمة التحكم الصناعي (OT/ICS) منطقياً أو مادياً عن الشبكات الأخرى.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • معيار أجهزة نقل البيانات في اتجاه واحد

	• نموذج سياسة أمن الشبكات • نموذج معيار امن الشبكات **إرشادات تطبيق الضوابط:** • العمل على تطبيق تقسيم شبكات أنظمة التحكم الصناعي (OT/ICS) منطقياً أو مادياً عن الشبكات الأخرى على سبيل المثال (العزل باستخدام VLANs, next-generation firewalls, Data diode). • التأكد والتحقق من الأصول الخاصة بأنظمة التحكم الصناعي (OT/ICS) لا تتفاعل مع باقي البيئات أو الشبكات. **المخرجات المتوقعة:** • المخطط البياني للشبكة والذي يوضّح تقسيم الشبكة. • زيارة ميدانية للتحقق من تقسيم شبكات أنظمة التحكم الصناعي (OT/ICS) منطقياً أو مادياً عن الشبكات الأخرى.
٢-١-٤-٢	تقسيم المناطق المختلفة (Zones) داخل بيئة أنظمة التحكم الصناعي (OT/ICS) منطقياً أو مادياً وفقاً للمستوى المناسب للمنطقة وعزل تدفق البيانات بين المناطق بحيث يتم الاتصال بين المناطق عبر نقاط اتصال محددة (Choke Points).
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • نموذج سياسة أمن الشبكات • نموذج معيار امن الشبكات **إرشادات تطبيق الضوابط:** • التأكد من أن الرسم البياني للشبكة العام (high level architecture) يحتوي على تقسيم المناطق المختلفة (Zones) داخل بيئة أنظمة التحكم الصناعي (OT/ICS)، كما يجب أن يوضح الرسم نوع وآلية الاتصال بين الشبكة الخاصة بأنظمة التحكم الصناعي (OT/ICS) وشبكة تقنية المعلومات (IT corporate network). • تطبيق تقسيم المناطق المختلفة (Zones) داخل بيئة أنظمة التحكم الصناعي (OT/ICS) منطقياً أو مادياً على سبيل المثال (التقسيم باستخدام VLANs, next-generation firewalls). **المخرجات المتوقعة:** • المخطط البياني للشبكة والذي يوضّح تقسيمات الشبكة.

• زيارة ميدانية للتحقق من تطبيق تقسيم المناطق المختلفة (Zones) داخل بيئة أنظمة التحكم الصناعي (OT/ICS) منطقياً أو مادياً للمستوى المناسب للمنطقة وعزل تدفق البيانات بين المناطق بحيث يتم الاتصال بين المناطق عبر نقاط اتصال محددة (Choke Points).	
٢-٤-١-٣	تقسيم أنظمة معدات السلامة ("Safety Instrumented System "SIS) منطقياً أو مادياً عن الشبكات الأخرى الخاصة بأنظمة التحكم الصناعي (OT/ICS).
أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • نموذج سياسة أمن الشبكات • نموذج معيار امن الشبكات **إرشادات تطبيق الضوابط** • التأكد من أن أنظمة معدات السلامة ("Safety Instrumented System "SIS) معزولة تماماً (stand-alone) ومقسمة منطقياً أو مادياً عن الشبكات الأخرى الخاصة بأنظمة التحكم الصناعي (OT/ICS). • التأكد والتحقق من أن الرسم البياني للشبكة يوضح تقسيم أنظمة معدات السلامة (Safety Instrumented System "SIS").	
المخرجات المتوقعة: • المخطط البياني للشبكة يوضح تقسيمات الشبكة. • زيارة ميدانية للتحقق من تقسيم أنظمة معدات السلامة ("Safety Instrumented System "SIS) منطقياً أو مادياً.	
٢-٤-١-٤	تقييد استخدام التقنيات اللاسلكية (مثل: Wi-Fi, Bluetooth, Cellular, Satellite, وغيرها)، على أن يكون استخدامها لتلبية متطلبات عمل محددة مع ضمان تأمينها بالشكل المناسب.
أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • نموذج سياسة أمن الشبكات • نموذج معيار امن الشبكات **إرشادات تطبيق الضوابط:** • تقييد استخدام التقنيات اللاسلكية (مثل: Wi-Fi, Bluetooth, Callular, Satellite, وغيرها). • تحديد وتوثيق المبررات اللازمة والمتطلبات الخاصة باستخدام التقنيات اللاسلكية.	

	• تحديد وتوثيق وتطبيق المتطلبات والمبادئ الخاصة باستخدام التقنيات اللاسلكية. • التأكد والتحقق من أن التقنيات اللاسلكية تتماشى مع المتطلبات والمبادئ الموثقة.	
	المخرجات المتوقعة: • المبررات اللازمة والمتطلبات الخاصة باستخدام التقنيات اللاسلكية (business justifications). • وثيقة المتطلبات والمبادئ الخاصة باستخدام التقنيات اللاسلكية. • زيارة ميدانية للتحقق من تقييد استخدام التقنيات اللاسلكية بالتماشي مع المتطلبات والمبادئ الموثقة عند استخدام التقنيات اللاسلكية.	
	٢-٤-١-٥	عزل التقنيات اللاسلكية منطقياً أو مادياً، عن الشبكات الخاصة بأنظمة التحكم الصناعي (OT/ICS).
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • نموذج سياسة أمن الشبكات • نموذج معيار امن الشبكات **إرشادات تطبيق الضوابط:** • تحديد قائمة بالتقنيات اللاسلكية المستخدمة. • تطبيق عزل التقنيات اللاسلكية منطقياً أو مادياً، عن الشبكات الخاصة بأنظمة التحكم الصناعي (OT/ICS) على سبيل المثال (التقسيم باستخدام VLANs, next-generation firewalls). • التأكد والتحقق من التقنيات اللاسلكية لا تتفاعل مع باقي البيئات أو الشبكات الخاصة بأنظمة التحكم الصناعي (OT/ICS).	
	المخرجات المتوقعة: • قائمة بالتقنيات اللاسلكية المستخدمة. • المخطط البياني للشبكة يوضح تقسيمات الشبكة. • زيارة ميدانية للتحقق من عزل التقنيات اللاسلكية منطقياً أو مادياً، عن الشبكات الخاصة بأنظمة التحكم الصناعي (OT/ICS).	
	٢-٤-١-٦	تقييد استخدام اتصالات الشبكة، والخدمات، ونقاط الاتصال بين المناطق المختلفة (Zones) وحصرها على الحد الأدنى؛ لتلبية متطلبات التشغيل والصيانة والسلامة.

	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • نموذج سياسة أمن الشبكات • نموذج معيار امن الشبكات **إرشادات تطبيق الضوابط:** • إدارة إعدادات جدار الحماية (Firewall Rules) من أجل تقييد استخدام اتصالات الشبكة، والخدمات، ونقاط الاتصال بين المناطق المختلفة (Zones) وحصرها على الحد الأدنى؛ لتلبية متطلبات التشغيل والصيانة والسلامة. **المخرجات المتوقعة:** • زيارة ميدانية للتحقق من تقييد استخدام اتصالات الشبكة، والخدمات، ونقاط الاتصال بين المناطق المختلفة (Zones) وحصرها على الحد الأدنى؛ لتلبية متطلبات التشغيل والصيانة والسلامة.
٢-٤-١-٧	منع الوصول المباشر لخدمات التحقق، و إدارة الدخول عن بعد (Remote Authentication and Access Management) على الأجهزة المتواجدة في الشبكة الخارجية للجهة (External-Facing Hosts).
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • معيار أجهزة نقل البيانات في اتجاه واحد • نموذج سياسة أمن الشبكات • نموذج معيار امن الشبكات **إرشادات تطبيق الضوابط:** • تجنب الوصول المباشر لخدمات التحقق على سبيل المثال تعطيل الخدمات على الأجهزة المتواجدة في الشبكة الخارجية للجهة (External-Facing Hosts). • التأكد والتحقق من منع الوصول المباشر لخدمات التحقق، و إدارة الدخول عن بعد (Remote Authentication and Access Management) على الأجهزة المتواجدة في الشبكة الخارجية للجهة (External-Facing Hosts). **المخرجات المتوقعة:** • رسم بياني للشبكة يؤكد العزل والتقسيم من البيئة الخاصة بأنظمة التحكم الصناعي (OT/ICS) إلى البيئات الاخرى.

٢-٤-١-٨	قصر الوصول لخدمات الأعمال الحساسة (Business Critical) المتعلقة بالشبكة الداخلية لأنظمة التحكم الصناعي (OT/ICS) على الخدمات المصرح بها، ويجب الحد من الوصول للخدمات ذات الثغرات الأمنية المعروفة إلى أقصى حد ممكن.

أدوات الأمن السيبراني ذات العلاقة:

- نموذج سياسة الأمن السيبراني للأنظمة التشغيلية
- نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS)
- نموذج سياسة أمن الشبكات
- نموذج معيار امن الشبكات

إرشادات تطبيق الضوابط:

- إجراء تقييم مخاطر للتأكد من أن مخاطر الأمن السيبراني مراقبة وتحت السيطرة.
- التأكد من أن الأنظمة الخارجة عن الدعم (Obsolete Systems) يقتصر استخدامها لخدمات الأعمال الحساسة (Business Critical) المصرح بها فقط مع تطبيق الضوابط البديلة (Compensating controls) على سبيل المثال لا الحصر (إزالة الخدمات الغير مستخدمة، تقييد الوصول لهذه الأنظمة، تقييد الاستخدام لعدد محدود من المستخدمين... الخ).

المخرجات المتوقعة:

- تقييم المخاطر.
- زيارة ميدانية للتحقق من أن الأنظمة الخارجة عن الدعم (Obsolete systems) يقتصر استخدامها لخدمات الأعمال الحساسة (Business Critical) المصرح بها فقط مع تطبيق الضوابط البديلة (Compensating controls).

٢-٤-١-٩	منع الوصول المباشر عن بعد، بين منطقة الجهة الداخلية (Corporate Zone) ومنطقة شبكات أنظمة التحكم الصناعي (OT/ICS)، وتوجيه جميع الاتصالات إلى نقاط الوصول عن بعد (Jump Hosts) بحيث تكون مخصصة لهذه العمليات، وآمنة ومحصنة في المنطقة المحايدة (DMZ).

أدوات الأمن السيبراني ذات العلاقة:

- نموذج سياسة الأمن السيبراني للأنظمة التشغيلية
- نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS)
- معيار أجهزة نقل البيانات في اتجاه واحد
- نموذج سياسة أمن الشبكات
- نموذج معيار امن الشبكات

إرشادات تطبيق الضوابط:

	• تجنب الوصول المباشر عن بعد، بين منطقة الجهة الداخلية (Corporate Zone) ومنطقة شبكات أنظمة التحكم الصناعي (OT/ICS). • في حال الحاجة لإرسال البيانات إلى منطقة الجهة الداخلية (Corporate Zone)، يجب توجيه جميع الاتصالات إلى نقاط الوصول عن بعد (Jump Hosts) بحيث تكون مخصصة لهذه العمليات، وآمنة ومحصنة في المنطقة المحايدة (DMZ).
	المخرجات المتوقعة: • رسم بياني للشبكة يؤكد وجود المنطقة المحايدة (DMZ). • زيارة ميدانية للتحقق من أن الاتصالات بين منطقة الجهة الداخلية (Corporate Zone) ومنطقة شبكات أنظمة التحكم الصناعي (OT/ICS) موجهة إلى نقاط الوصول عن بعد (Jump Hosts) بحيث تكون مخصصة لهذه العمليات، وآمنة ومحصنة في المنطقة المحايدة (DMZ).
٢-٤-١-١٠	عدم الاتصال بشبكات أنظمة التحكم الصناعي (OT/ICS) باستخدام نقطة الوصول عن بعد، المتواجدة في المنطقة المحايدة (DMZ) إلا عند الحاجة، مع ضمان تطبيق مبدأ التحقق من الهوية، ذات العناصر المتعددة (Multi-Factor Authentication "MFA") وتسجيل جلسات الاتصال (Session Recording) وأن يكون الاتصال لفترة زمنية محددة فحسب.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • نموذج سياسة أمن الشبكات • نموذج معيار امن الشبكات **إرشادات تطبيق الضوابط:** • التأكد من عدم الاتصال بشبكات أنظمة التحكم الصناعي (OT/ICS) باستخدام نقطة الوصول عن بعد، المتواجدة في المنطقة المحايدة (DMZ) إلا عند الحاجة. • تحديد إجراءات في حال الحاجة إلى الاتصال بشبكات أنظمة التحكم الصناعي (OT/ICS) باستخدام نقطة الوصول عن بعد، المتواجدة في المنطقة المحايدة (DMZ)، ويجب أن تحتوي الإجراءات على النقاط التالية: ○ تطبيق مبدأ التحقق من الهوية، ذات العناصر المتعددة ("MFA" Multi-Factor Authentication). ○ تسجيل جلسات الاتصال (Session Recording). ○ أن يكون الاتصال لفترة زمنية محددة فحسب.
	المخرجات المتوقعة: • زيارة ميدانية للتحقق من عدم الاتصال بشبكات أنظمة التحكم الصناعي (OT/ICS) باستخدام نقطة الوصول عن بعد، المتواجدة في المنطقة المحايدة (DMZ) دون الحاجة.

	• الإجراءات المعتمدة للوصول عن بعد. • إثبات يؤكد تطبيق مبدأ التحقق من الهوية، ذات العناصر المتعددة ("Multi-Factor Authentication "MFA) وتسجيل جلسات الاتصال (Session Recording) وأن يكون الاتصال لفترة زمنية محددة فحسب، في حال الحاجة للوصول عن بعد.
٢-٤-١-١١	استخدام الوكيل (Proxy) بين منطقة الجهة الداخلية (Corporate Zone) ومنطقة أنظمة التحكم الصناعي (OT/ICS) للتحكم بالحركة عند الاتصال ما بين الأجهزة (Machine-to-Machine).
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • معيار أجهزة نقل البيانات في اتجاه واحد • نموذج سياسة أمن الشبكات • نموذج معيار امن الشبكات • نموذج معيار أمن الخادم الوكيل **إرشادات تطبيق الضوابط:** • العمل على تطبيق الحلول التقنية الخاصة بالوكيل (Proxy Solution) بين منطقة الجهة الداخلية (Corporate Zone) ومنطقة أنظمة التحكم الصناعي (OT/ICS) للتحكم بالحركة عند الاتصال ما بين الأجهزة (Machine-to-Machine). • التأكد من جميع الاتصالات ما بين الأجهزة (Machine-to-Machine) بين منطقة الجهة الداخلية (Corporate Zone) ومنطقة أنظمة التحكم الصناعي (OT/ICS) تمر من خلال الوكيل (Proxy).
	المخرجات المتوقعة: • زيارة ميدانية للتحقق من أن جميع الاتصالات ما بين الأجهزة (Machine-to-Machine) بين منطقة الجهة الداخلية (Corporate Zone) ومنطقة أنظمة التحكم الصناعي (OT/ICS) تمر من خلال الوكيل (Proxy).
٢-٤-١-١٢	استخدام البوابات (Gateways) المخصصة؛ لتقسيم شبكات أنظمة التحكم الصناعي (OT/ICS) من الشبكة الداخلية (Corporate Zone).
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • معيار أجهزة نقل البيانات في اتجاه واحد • نموذج سياسة أمن الشبكات

	• نموذج معيار امن الشبكات **إرشادات تطبيق الضوابط:** • العمل على استخدام البوابات (Gateways) المخصصة؛ لتقسيم شبكات أنظمة التحكم الصناعي (OT/ICS) من الشبكة الداخلية (Corporate Zone). **المخرجات المتوقعة:** • زيارة ميدانية ورسم بياني للشبكة يوضح استخدام البوابات (Gateways) المخصصة؛ لتقسيم شبكات أنظمة التحكم الصناعي (OT/ICS) من الشبكة الداخلية (Corporate Zone).
٢-٤-١-١٣	استخدام منطقة محايدة (DMZ) لاستضافة أي نظام، يقدم خدمات بين منطقة الشبكة الداخلية (Corporate Zone) ومنطقة أنظمة التحكم الصناعي (OT/ICS).
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • معيار أجهزة نقل البيانات في اتجاه واحد • نموذج سياسة أمن الشبكات • نموذج معيار امن الشبكات **إرشادات تطبيق الضوابط:** • تحديد وتنفيذ استخدام منطقة محايدة (DMZ) بناء على المتطلبات ذات العلاقة بالأمن السيبراني. • تضمين جميع الأنظمة التي تقدم خدمات بين منطقة الشبكة الداخلية (Corporate Zone) ومنطقة أنظمة التحكم الصناعي (OT/ICS) بداخل المنطقة المحايدة (DMZ). **المخرجات المتوقعة:** • قائمة بالأنظمة التي تقدم خدمات بين منطقة الشبكة الداخلية (Corporate Zone) ومنطقة أنظمة التحكم الصناعي (OT/ICS). • زيارة ميدانية للتحقق من أنه يتم استخدام منطقة محايدة (DMZ) وذلك عند استخدام أي أنظمة تقدم خدمات بين منطقة الشبكة الداخلية (Corporate Zone) ومنطقة أنظمة التحكم الصناعي (OT/ICS).
٢-٤-١-١٤	التقييد الصارم على تمكين البروتوكولات الصناعية (Industrial protocols) والمنافذ (Ports) واستخدامها إلى الحد الأدنى، بالتوافق مع متطلبات التشغيل والصيانة والسلامة.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS)

	• معيار أجهزة نقل البيانات في اتجاه واحد • نموذج سياسة أمن الشبكات • نموذج معيار امن الشبكات **إرشادات تطبيق الضوابط:** • التحقق والتأكد من التقييد الصارم على تمكين البروتوكولات الصناعية (Industrial protocols) والمنافذ (Ports) واستخدامها إلى الحد الأدنى، بالتوافق مع متطلبات التشغيل والصيانة والسلامة. **المخرجات المتوقعة:** • زيارة ميدانية للتأكد من التقييد الصارم على تمكين البروتوكولات الصناعية (Industrial protocols) والمنافذ (Ports) واستخدامها إلى الحد الأدنى، بالتوافق مع متطلبات التشغيل والصيانة والسلامة.	
	اعتماد حزم التحديثات الدورية، والإصلاحات الأمنية للأصول في بيئة الإنتاج، من قبل الشركة المصنعة، وإجراء اختبار في بيئة تجريبية قبل تطبيقها على بيئة الإنتاج.	٢-٤-١-١٥
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • نموذج سياسة أمن الشبكات • نموذج معيار امن الشبكات • نموذج معيار ادارة حزم التحديثات والإصلاحات **إرشادات تطبيق الضوابط:** • التأكد من أن جميع حزم التحديثات الدورية، والإصلاحات الأمنية للأصول في بيئة الإنتاج معتمدة من قبل الشركة المصنعة. • إجراء اختبار في بيئة تجريبية قبل تطبيق حزم التحديثات الدورية، والإصلاحات الأمنية للأصول في بيئة الإنتاج. **المخرجات المتوقعة:** • شهادة (Certification) من الشركة المصنعة تؤكد بتطبيق حزم التحديثات الدورية، والإصلاحات الأمنية. • إثبات يؤكد وجود بيئة تجريبية معزولة ومنفصلة. • إثبات يؤكد إجراء اختبار في بيئة تجريبية قبل تطبيق جميع حزم التحديثات الدورية، والإصلاحات الأمنية للأصول في بيئة الإنتاج.	
	الحفاظ على الوثائق المفصلة، لهندسة الشبكة وتصميمها، وتقسيماتها، وتدفقات بيانات الشبكة، و نقاط ترابطها، واعتماديتها؛ وتوثيق، وتحديث الوثائق مع كل تغيير.	٢-٤-١-١٦

	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • نموذج سياسة أمن الشبكات • نموذج معيار امن الشبكات **إرشادات تطبيق الضوابط:** • الحفاظ على الوثائق المفصلة، لهندسة الشبكة وتصميمها، وتقسيماتها، وتدفقات بيانات الشبكة، ونقاط ترابطها، واعتماديتها. • التأكد من أن الرسوم البيانية للشبكات والوثائق المفصلة يتم تحديثها بشكل دوري. **المخرجات المتوقعة:** • آخر رسم بياني للشبكة محدث.
٢-٤-٢	رجوعاً للضابط ٢-٥-٤ في الضوابط الأساسية للأمن السيبراني؛ يجب مراجعة متطلبات الأمن السيبراني لإدارة أمن شبكات أنظمة التحكم الصناعي (OT/ICS) وقياس فعالية تطبيقها وتقييمها دورياً.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • نموذج سياسة أمن الشبكات • نموذج تقرير مؤشرات الأداء الرئيسية **إرشادات تطبيق الضوابط:** • العمل على مراجعة متطلبات الأمن السيبراني لإدارة أمن شبكات أنظمة التحكم الصناعي (OT/ICS) بشكل دوري حسب خطة موثقة ومعتمدة للمراجعة بناءً على فترة زمنية محددة (على سبيل المثال، يتم إجراء المراجعة الدورية بشكل سنوي). • العمل على تطوير مؤشرات أداء رئيسية (KPIs) لكل الضوابط المتضمنة بداخل السياسات أو الإجراءات للتأكد من قياس فعالية تطبيقها، وتقييمها دورياً بناءً على فترة زمنية محددة (على سبيل المثال، يتم إجراء المراجعة الدورية بشكل سنوي). **المخرجات المتوقعة:** • إثبات يؤكد القيام بالمراجعة الدورية لمتطلبات الأمن السيبراني لإدارة أمن شبكات أنظمة التحكم الصناعي (OT/ICS). • إثبات يؤكد القيام بقياس مؤشرات الأداء الرئيسية (KPIs) لكل الضوابط المتضمنة بداخل السياسات أو الإجراءات للتأكد من قياس فعالية تطبيقها، وتقييمها دورياً بناءً على فترة زمنية محددة.

٢-٥	أمن الأجهزة المحمولة (Mobile Devices Security)	
الهدف	ضمان حماية أجهزة الجهة المحمولة (بما في ذلك أجهزة الحاسب المحمول، أجهزة الإعدادات المحمولة، أجهزة اختبارات الشبكة) من المخاطر السيبرانية. وضمان التعامل بشكل آمن مع المعلومات الحساسة والمعلومات الخاصة بأعمال الجهة.	
الضوابط		
١-٥-٢	بالإضافة للضوابط الفرعية، ضمن الضابط ٢-٦-٣ في الضوابط الأساسية للأمن السيبراني؛ يجب أن تغطي متطلبات الأمن السيبراني لأمن الأجهزة المحمولة بحد أدنى، ما يلي:	
	٢-٥-١-١	تقييد استخدام الأجهزة المحمولة، لشبكات أنظمة التحكم الصناعي (OT/ICS) عند الحاجة لاستخدام الأجهزة المحمولة .ويجب إجراء تقييم مخاطر الأمن السيبراني، وتحديد المخاطر وإدارتها. يجب الحصول على موافقة الإدارة المعنية بالأمن السيبراني لفترة زمنية محددة فحسب، بما يتوافق مع آليات إدارة صلاحيات الوصول المتبعة في الجهة.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • نموذج معيار أمن الأجهزة المحمولة **إرشادات تطبيق الضوابط:** • تقييد استخدام الأجهزة المحمولة، لشبكات أنظمة التحكم الصناعي (OT/ICS) وذلك من اجل تجنب الوصول غير المصرح به على العمليات التشغيلية. • تحديد وتوثيق الحالات الاستثنائية عند الحاجة لاستخدام الأجهزة المحمولة. • إجراء تقييم مخاطر الأمن السيبراني، وتحديد المخاطر وإدارتها. وذلك بالتوافق مع الآليات الخاصة بالجهة. • تحديد وتوثيق وتطبيق متطلبات الأمن السيبراني الخاصة باستخدام الأجهزة المحمولة. • التأكد من أن جميع الأجهزة المحمولة المستخدمة تتوافق وتطبق المتطلبات المعرفة والمعتمدة.	
	المخرجات المتوقعة: • تقرير تقييم مخاطر الأمن السيبراني عند استخدام الأجهزة المحمولة. • وثيقة متطلبات الأمن السيبراني عند استخدام الأجهزة المحمولة. • زيارة ميدانية للتحقق من تقييد استخدام الأجهزة المحمولة، لشبكات أنظمة التحكم الصناعي (OT/ICS) عند الحاجة لاستخدام الأجهزة المحمولة.	
	٢-٥-١-٢	استخدام الأجهزة المحمولة المخصصة لأغراض العمل، وبما يتوافق مع متطلبات الأمن السيبراني، للمناطق الخاصة بها (Zones) قبل توصيلها ببيئة شبكات أنظمة التحكم الصناعي (OT/ICS). ويجب أن يتم تحصينها وتحديثها بالتحديثات الأمنية الحديثة؛ وفحصها من البرمجيات الضارة (Malware) والتهديدات المتقدمة المستمرة (APT).

أدوات الأمن السيبراني ذات العلاقة:

- نموذج سياسة الأمن السيبراني للأنظمة التشغيلية
- نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS)
- نموذج معيار أمن الأجهزة المحمولة
- نموذج معايير الإعدادات الآمنة والتحصين
- نموذج معيار أنظمة الحماية من التهديدات المستمرة المتقدمة

إرشادات تطبيق الضوابط:

- تحديد وتوثيق الإجراءات الخاصة بالتحصين وحزم الاصلاحيات وذلك عند استخدام الأجهزة المحمولة المخصصة لأغراض العمل.
- التأكد والتحقق من أن جميع الأجهزة المحمولة تستخدم فقط لأغراض العمل على سبيل المثال لا الحصر (من خلال: mobile devices management tools).
- التأكد والتحقق من أن جميع الأجهزة المحمولة يتم تحصينها وتحديثها بالتحديثات الأمنية الحديثة؛ وفحصها من البرمجيات الضارة (Malware) والتهديدات المتقدمة المستمرة (APT).

المخرجات المتوقعة:

- وثيقة الإجراءات الخاصة بالتحصين وحزم الاصلاحيات وذلك عند استخدام الأجهزة المحمولة المخصصة لأغراض العمل.
- زيارة ميدانية للتحقق من أن جميع الأجهزة المحمولة تستخدم فقط لأغراض العمل.
- تقارير التحديثات الأمنية الخاصة بالأجهزة المحمولة.
- تقارير فحص الأجهزة المحمولة.

٢-٥-١-٣	تحديد قائمة مقيدة بالأجهزة المحمولة المصرح بها مع ضمان إمكانية توصيل هذه الأجهزة المحمولة فحسب ببيئة التقنية التشغيلية وأنظمة التحكم الصناعي (OT/ICS)، واعتمادها.

أدوات الأمن السيبراني ذات العلاقة:

- نموذج سياسة الأمن السيبراني للأنظمة التشغيلية
- نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS)
- نموذج معيار أمن الأجهزة المحمولة

إرشادات تطبيق الضوابط:

- تحديد وتوثيق قائمة مقيدة بالأجهزة المحمولة المصرح بها بالاتصال بأنظمة التحكم الصناعي (OT/ICS).
- التأكد من توصيل الأجهزة المصرح بها فقط.

المخرجات المتوقعة:

- قائمة موثقة ومعتمدة توضّح الأجهزة المحمولة المصرح بها بالاتصال بأنظمة التحكم الصناعي (OT/ICS).
- زيارة ميدانية للتحقق من توصيل الأجهزة المصرح بها فقط.

	٢-٥-١-٤	تطبيق آلية لإدارة الأجهزة المحمولة، مركزياً ("Mobile Device Management "MDM).
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • نموذج معيار أمن الأجهزة المحمولة **إرشادات تطبيق الضوابط:** • تطبيق آلية لإدارة الأجهزة المحمولة، مركزياً ("Mobile Device Management "MDM). • التأكد من أن جميع الأجهزة المعرفة مسبقاً مدارة مركزياً من خلال التقنيات المطبقة.	
	المخرجات المتوقعة: • إثبات يؤكد تطبيق آلية لإدارة الأجهزة المحمولة، مركزياً ("Mobile Device Management "MDM). • إثبات يؤكد بأن جميع الأجهزة المعرفة مسبقاً مدارة مركزياً من خلال التقنيات المطبقة.	
	٢-٥-١-٥	تنفيذ عمليات التشفير على الأجهزة المحمولة المصرح باستخدامها للوصول إلى أصول أنظمة التحكم الصناعي (OT/ICS).
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • نموذج معيار التشفير • نموذج معيار أمن الأجهزة المحمولة **إرشادات تطبيق الضوابط:** • تحديد وتوثيق واعتماد آليات التشفير على الأجهزة المحمولة المصرح باستخدامها للوصول إلى أصول أنظمة التحكم الصناعي (OT/ICS). يجب أن تتوافق الآلية مع التشريعات ذات العلاقة في الجهة. • التأكد والتحقق من أن الأجهزة المحمولة المصرح باستخدامها للوصول إلى أصول أنظمة التحكم الصناعي (OT/ICS) مشفرة بناء على الآليات المعتمدة.	
	المخرجات المتوقعة: • إثبات يؤكد أن الأجهزة المحمولة المصرح باستخدامها للوصول إلى أصول أنظمة التحكم الصناعي (OT/ICS) مشفرة بناء على الآليات المعتمدة.	
٢-٥-٢	رجوعاً للضابط ٢-٦-٤ في الضوابط الأساسية للأمن السيبراني؛ يجب مراجعة متطلبات الأمن السيبراني لحماية استخدام الأجهزة المحمولة في بيئة شبكات أنظمة التحكم الصناعي (OT/ICS) وقياس فعالية تطبيقها، وتقييمها دورياً.	
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • نموذج معيار أمن الأجهزة المحمولة	

	• نموذج تقرير مؤشرات الأداء الرئيسية **إرشادات تطبيق الضوابط:** • العمل على مراجعة متطلبات الأمن السيبراني لحماية استخدام الأجهزة المحمولة في بيئة شبكات أنظمة التحكم الصناعي (OT/ICS) بشكل دوري حسب خطة موثقة ومعتمدة للمراجعة بناءً على فترة زمنية محددة (على سبيل المثال، يتم إجراء المراجعة الدورية بشكل سنوي). • العمل على تطوير مؤشرات أداء رئيسية (KPIs) لكل الضوابط المتضمنة بداخل السياسات أو الإجراءات للتأكد من قياس فعالية تطبيقها، وتقييمها دورياً بناءً على فترة زمنية محددة (على سبيل المثال، يتم إجراء المراجعة الدورية بشكل سنوي). **المخرجات المتوقعة:** • إثبات يؤكد القيام بالمراجعة الدورية لمتطلبات الأمن السيبراني لحماية استخدام الأجهزة المحمولة في بيئة شبكات أنظمة التحكم الصناعي (OT/ICS). • إثبات يؤكد القيام بقياس مؤشرات الأداء الرئيسية (KPIs) لكل الضوابط المتضمنة بداخل السياسات أو الإجراءات للتأكد من قياس فعالية تطبيقها، وتقييمها دورياً بناءً على فترة زمنية محددة.
٢-٦	**حماية البيانات والمعلومات (Data and Information Protection)**
الهدف	ضمان سرية بيانات الجهة ومعلوماتها وسلامتها وتوافرها وفقا للسياسات والإجراءات التنظيمية للجهة، والمتطلبات التشريعية ذات العلاقة.
الضوابط	
٢-٦-١	بالإضافة للضوابط الفرعية، ضمن الضابط ٢-٧-٣ في الضوابط الأساسية للأمن السيبراني؛ يجب أن تغطي متطلبات الأمن السيبراني لحماية البيانات والمعلومات المتعلقة بأنظمة التحكم الصناعي (OT/ICS) بحد أدنى ما يلي:
٢-٦-١-١	حماية البيانات الإلكترونية والمادية (في حال التخزين والنقل) بالمستوى الذي يتوافق مع تصنيف البيانات.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • نموذج سياسة الأمن السيبراني للبيانات • نموذج معيار الأمن السيبراني للبيانات **إرشادات تطبيق الضوابط:** • تحديد وتصنيف البيانات الإلكترونية والمادية في البيئة الخاصة بأنظمة التحكم الصناعي (OT/ICS). • التأكد من حماية البيانات المادية (في حال التخزين والنقل) وذلك عن طريق حصر الوصول للبيانات الحساسة والمصنفة مثل مخطط الشبكات (network diagrams) مخططات الأنابيب والأجهزة (P&ID diagrams) والملفات الهندسية (Engineering documents).

• التأكد من حماية البيانات الإلكترونية (في حال التخزين والنقل) وذلك عن طريق تطبيق الإجراءات الأمنية المناسبة على سبيل المثال لا الحصر (إدارة الجلسات وذلك عن طريق إغلاقها وانتهائها (session timeout and lockout)، ضبط اعدادات الوسائط الخارجية ... الخ).	
المخرجات المتوقعة: • زيارة ميدانية للتحقق من حماية البيانات الإلكترونية والمادية (في حال التخزين والنقل) بالمستوى الذي يتوافق مع تصنيف البيانات.	
حماية البيانات والمعلومات المصنفة من خلال تقنيات، منع تسريب البيانات ("DLP" Data Leakage Prevention).	٢-١-٦-٢
أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • نموذج معيار الحماية منع فقدان البيانات • نموذج سياسة الأمن السيبراني للبيانات • نموذج معيار الأمن السيبراني للبيانات **إرشادات تطبيق الضوابط:** • العمل على تطبيق تقنيات منع تسريب البيانات ("DLP" Data Leakage Prevention) على سبيل المثال لا الحصر (data transfer monitoring or data access management tools). • التأكد من حماية البيانات والمعلومات المصنفة من خلال تقنيات، منع تسريب البيانات ("DLP" Data Leakage Prevention).	
المخرجات المتوقعة: • زيارة ميدانية للتحقق من حماية البيانات والمعلومات المصنفة من خلال تقنيات منع تسريب البيانات ("DLP" Data Leakage Prevention).	
استخدام آليات الحذف الآمنة (Secure Wiping) لبيانات الإعدادات والبيانات المخزنة على أصول أنظمة التحكم الصناعي (OT/ICS)، وذلك عند الانتهاء منها.	٢-١-٦-٣
أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • نموذج سياسة الأمن السيبراني للبيانات • نموذج معيار الأمن السيبراني للبيانات **إرشادات تطبيق الضوابط:**	

		• تحديد وتوثيق إجراءات لاستخدام آليات الحذف الآمنة (Secure Wiping) على أصول أنظمة التحكم الصناعي (OT/ICS). • التأكد من استخدام آليات الحذف الآمنة (Secure Wiping) لبيانات الإعدادات والبيانات المخزنة على أصول أنظمة التحكم الصناعي (OT/ICS) عند الانتهاء منها وذلك بناء على الإجراءات المعتمدة.
		المخرجات المتوقعة: • وثيقة إجراءات استخدام آليات الحذف الآمنة (Secure Wiping). • إثبات يؤكد استخدام آليات الحذف الآمنة (Secure Wiping) لبيانات الإعدادات والبيانات المخزنة على أصول أنظمة التحكم الصناعي (OT/ICS) عند الانتهاء منها وذلك بناء على الإجراءات المعتمدة.
	٢-٦-١-٤	التقييد الحازم لنقل بيانات أنظمة التحكم الصناعي (OT/ICS) أو استخدامها خارج بيئة الإنتاج؛ إلى أن تطبق ضوابط صارمة لحماية تلك البيانات.
		أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • نموذج سياسة الأمن السيبراني للبيانات • نموذج معيار الأمن السيبراني للبيانات **إرشادات تطبيق الضوابط:** • التقييد الحازم لنقل بيانات أنظمة التحكم الصناعي (OT/ICS) أو استخدامها خارج بيئة الإنتاج. • التأكد من التقييد الحازم لنقل بيانات أنظمة التحكم الصناعي (OT/ICS) أو استخدامها خارج بيئة الإنتاج إلى أن تطبق ضوابط صارمة لحماية تلك البيانات على سبيل المثال لا الحصر؛ (من خلال فحص وسائط التخزين الخارجية، السماح بقائمة محددة من وسائط التخزين، استخدام خادم ملفات آمن (secure file server)).
		المخرجات المتوقعة: • زيارة ميدانية للتحقق من التقييد الحازم لنقل بيانات أنظمة التحكم الصناعي (OT/ICS) أو استخدامها خارج بيئة الإنتاج إلى أن تطبق ضوابط صارمة لحماية تلك البيانات.
٢-٦-٢		رجوعاً للضابط ٢-٧-٤ في الضوابط الأساسية للأمن السيبراني؛ يجب مراجعة متطلبات الأمن السيبراني لحماية البيانات والمعلومات في بيئة شبكات أنظمة التحكم الصناعي (OT/ICS)، وقياس فعالية تطبيقها وتقييمها دورياً.
		أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • نموذج سياسة حماية البيانات • نموذج تقرير مؤشرات الأداء الرئيسية **إرشادات تطبيق الضوابط:**

	• العمل على مراجعة متطلبات الأمن السيبراني لحماية البيانات والمعلومات في بيئة أنظمة التحكم الصناعي (OT/ICS) بشكل دوري حسب خطة موثقة ومعتمدة للمراجعة بناءً على فترة زمنية محددة (على سبيل المثال، يتم إجراء المراجعة الدورية بشكل سنوي). • العمل على تطوير مؤشرات أداء رئيسية (KPIs) لكل الضوابط المتضمنة بداخل السياسات أو الإجراءات للتأكد من قياس فعالية تطبيقها، وتقييمها دورياً بناءً على فترة زمنية محددة (على سبيل المثال، يتم إجراء المراجعة الدورية بشكل سنوي).
	المخرجات المتوقعة: • إثبات يؤكد القيام بالمراجعة الدورية لمتطلبات الأمن السيبراني لحماية البيانات والمعلومات في بيئة أنظمة التحكم الصناعي (OT/ICS). • إثبات يؤكد القيام بقياس مؤشرات الأداء الرئيسية (KPIs) لكل الضوابط المتضمنة بداخل السياسات أو الإجراءات للتأكد من قياس فعالية تطبيقها، وتقييمها دورياً بناءً على فترة زمنية محددة.
٢-٧	التشفير (Cryptography)
الهدف	ضمان الاستخدام السليم والفعال للتشفير لحماية أصول البيانات والمعلومات وفقاً للسياسات والإجراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية ذات العلاقة.
الضوابط	
٢-٧-١	بالإضافة للضوابط الفرعية، ضمن الضابط ٢-٨-٣ في الضوابط الأساسية للأمن السيبراني؛ يجب على الجهة أن تتأكد من مواءمة تقنيات التشفير المستخدمة في بيئة شبكات أنظمة التحكم الصناعي (OT/ICS) مع المعايير الوطنية للتشفير (NCS-1:2020).
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • نموذج سياسة التشفير • نموذج معيار التشفير • نموذج معيار إدارة مفاتيح التشفير **إرشادات تطبيق الضوابط:** • توثيق وتحديد جميع تقنيات التشفير المستخدمة في بيئة شبكات أنظمة التحكم الصناعي (OT/ICS). • التأكد والتحقق من أن تقنيات التشفير المستخدمة في بيئة شبكات أنظمة التحكم الصناعي (OT/ICS) متوائمة مع المعايير الوطنية للتشفير (NCS-1:2020).

	المخرجات المتوقعة: • قائمة بجميع تقنيات التشفير المستخدمة في بيئة شبكات أنظمة التحكم الصناعي (OT/ICS). • زيارة ميدانية للتحقق من أن تقنيات التشفير المستخدمة في بيئة شبكات أنظمة التحكم الصناعي (OT/ICS) متوائمة مع المعايير الوطنية للتشفير (NCS-1:2020).
٢-٧-٢	رجوعاً للضابط ٢-٨-٤ في الضوابط الأساسية للأمن السيبراني؛ فإنه يجب مراجعة متطلبات الأمن السيبراني للتشفير، في بيئة شبكات أنظمة التحكم الصناعي (OT/ICS)، وقياس فعالية تطبيقها وتقييمها دورياً.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • نموذج سياسة التشفير • نموذج تقرير مؤشرات الأداء الرئيسية **إرشادات تطبيق الضوابط:** • العمل على مراجعة متطلبات الأمن السيبراني للتشفير في بيئة أنظمة التحكم الصناعي (OT/ICS) بشكل دوري حسب خطة موثقة ومعتمدة للمراجعة بناءً على فترة زمنية محددة (على سبيل المثال، يتم إجراء المراجعة الدورية بشكل سنوي). • العمل على تطوير مؤشرات أداء رئيسية (KPIs) لكل الضوابط المتضمنة بداخل السياسات أو الإجراءات للتأكد من قياس فعالية تطبيقها، وتقييمها دورياً بناءً على فترة زمنية محددة (على سبيل المثال، يتم إجراء المراجعة الدورية بشكل سنوي).
	المخرجات المتوقعة: • إثبات يؤكد القيام بالمراجعة الدورية لمتطلبات الأمن السيبراني للتشفير في بيئة أنظمة التحكم الصناعي (OT/ICS). • إثبات يؤكد القيام بقياس مؤشرات الأداء الرئيسية (KPIs) لكل الضوابط المتضمنة بداخل السياسات أو الإجراءات للتأكد من قياس فعالية تطبيقها، وتقييمها دورياً بناءً على فترة زمنية محددة.
٢-٨	**إدارة النسخ الاحتياطية (Backup and Recovery Management)**
الهدف	ضمان حماية بيانات الجهة ومعلوماتها؛ بما في ذلك نظم المعلومات وإعدادات البرمجيات من المخاطر السيبرانية، وفقاً للسياسات والإجراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية ذات العلاقة.
الضوابط	
٢-٨-١	بالإضافة للضوابط الفرعية، ضمن الضابط ٢-٩-٣ في الضوابط الأساسية للأمن السيبراني؛ يجب أن تغطي متطلبات الأمن السيبراني لإدارة النسخ الاحتياطية المتعلقة بأنظمة التحكم الصناعي (OT/ICS) بحد أدنى ما يلي:

٢-٨-١-١	يجب أن تغطي النسخ الاحتياطية جميع أصول أنظمة التحكم الصناعي (OT/ICS)، كما يجب تخزينها بشكل مركزي (Location Centralized) وفي مواقع غير متصلة بالشبكة.	
أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • نموذج سياسة النسخ الاحتياطية • نموذج معيار النسخ الاحتياطية **إرشادات تطبيق الضوابط:** • التأكد والتحقق من أن نطاق النسخ الاحتياطي يغطي جميع أصول أنظمة التحكم الصناعي (OT/ICS)، كما يجب تخزينها بشكل مركزي (Location Centralized) وفي مواقع غير متصلة بالشبكة.		
المخرجات المتوقعة: • وثيقة خطة النسخ الاحتياطي الخاصة بأنظمة التحكم الصناعي (OT/ICS) ومبادئه ومتطلباته. • قائمة نطاق النسخ الاحتياطية الخاصة بأنظمة التحكم الصناعي (OT/ICS). • زيارة ميدانية للتحقق من أن نطاق النسخ الاحتياطية يغطي جميع أصول أنظمة التحكم الصناعي (OT/ICS)، والتحقق من تخزينها بشكل مركزي (Location Centralized) وفي مواقع غير متصلة بالشبكة.		
٢-٨-١-٢	التأكد من كون ملفات الإعدادات الحساسة والهندسية المختصة بأنظمة التحكم الصناعي (OT/ICS) مضمنه في النسخ الاحتياطية.	
أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • نموذج سياسة النسخ الاحتياطية • نموذج معيار النسخ الاحتياطية **إرشادات تطبيق الضوابط:** • التأكد والتحقق من أن ملفات الإعدادات الحساسة والهندسية المختصة بأنظمة التحكم الصناعي (OT/ICS) مضمنه في النسخ الاحتياطية.		
المخرجات المتوقعة: • قائمة ملفات الإعدادات الحساسة والهندسية المختصة بأنظمة التحكم الصناعي (OT/ICS). • زيارة ميدانية للتحقق من أن ملفات الإعدادات الحساسة والهندسية المختصة بأنظمة التحكم الصناعي (OT/ICS) مضمنه في النسخ الاحتياطية.		

	٢-٨-١-٣	إجراء عمليات النسخ الاحتياطي دورياً، وفقاً لتصنيف أصول أنظمة التحكم الصناعي (OT/ICS) والمخاطر المتعلقة بها.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • نموذج سياسة إدارة النسخ الاحتياطية • نموذج معيار الأمن السيبراني في إدارة النسخ الاحتياطية **إرشادات تطبيق الضوابط:** • التأكد والتحقق من إجراء عمليات النسخ الاحتياطي دورياً، بناء على فترات زمنية محددة.	
	المخرجات المتوقعة: • إثبات يؤكد إجراء عمليات النسخ الاحتياطي دورياً، بناء على فترات زمنية محددة.	
	٢-٨-١-٤	تأمين الوصول والتخزين والنقل للنسخ الاحتياطية ووسائطها، وضمان حمايتها من التلف، أو التغيير، أو الوصول غير المصرح به.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • نموذج سياسة النسخ الاحتياطية • نموذج معيار النسخ الاحتياطية **إرشادات تطبيق الضوابط:** • تحديد والعمل على تطبيق آليات آمنة لتأمين الوصول والتخزين والنقل للنسخ الاحتياطية ووسائطها. • التأكد والتحقق من أن المتطلبات والمبادئ الموثقة تتضمن الحماية ضد التلف أو التغيير أو الوصول غير المصرح به.	
	المخرجات المتوقعة: • زيارة ميدانية للتحقق تطبيق آليات آمنة لتأمين الوصول والتخزين والنقل للنسخ الاحتياطية ووسائطها. • زيارة ميدانية للتحقق من أن المتطلبات والمبادئ الموثقة تتضمن الحماية ضد التلف أو التغيير أو الوصول غير المصرح به.	
٢-٨-٢	رجوعاً للضابط ٢-٩-٤ في الضوابط الأساسية للأمن السيبراني؛ يجب مراجعة متطلبات الأمن السيبراني لإدارة النسخ الاحتياطية الخاصة بأنظمة التحكم الصناعي (OT/ICS)، وقياس فعالية تطبيقها وتقييمها دورياً.	
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • نموذج سياسة إدارة النسخ الاحتياطية • نموذج تقرير مؤشرات الأداء الرئيسية	

	إرشادات تطبيق الضوابط: • العمل على مراجعة متطلبات الأمن السيبراني لإدارة النسخ الاحتياطية الخاصة بأنظمة التحكم الصناعي (OT/ICS) بشكل دوري حسب خطة موثقة ومعتمدة للمراجعة بناءً على فترة زمنية محددة (على سبيل المثال، يتم إجراء المراجعة الدورية بشكل سنوي). • العمل على تطوير مؤشرات أداء رئيسية (KPIs) لكل الضوابط المتضمنة بداخل السياسات أو الإجراءات للتأكد من قياس فعالية تطبيقها، وتقييمها دورياً بناءً على فترة زمنية محددة (على سبيل المثال، يتم إجراء المراجعة الدورية بشكل سنوي).
	المخرجات المتوقعة: • إثبات يؤكد القيام بالمراجعة الدورية لمتطلبات الأمن السيبراني لإدارة النسخ الاحتياطية الخاصة بأنظمة التحكم الصناعي (OT/ICS). • إثبات يؤكد القيام بقياس مؤشرات الأداء الرئيسية (KPIs) لكل الضوابط المتضمنة بداخل السياسات أو الإجراءات للتأكد من قياس فعالية تطبيقها، وتقييمها دورياً بناءً على فترة زمنية محددة.
٢-٩	**إدارة الثغرات (Vulnerabilities Management)**
الهدف	ضمان الكشف عن الثغرات التقنية في الوقت المناسب، ومعالجتها بفعالية؛ لمنع استغلال هذه الثغرات أو تقليل احتماله؛ لشن هجمات إلكترونية ضد الجهة.
الضوابط	
	بالإضافة للضوابط الفرعية ضمن الضابط ٢-١٠-٣ في الضوابط الأساسية للأمن السيبراني؛ يجب أن تغطي متطلبات الأمن السيبراني لإدارة الثغرات المتعلقة بأنظمة التحكم الصناعي (OT/ICS) بحد أدنى ما يلي:
٢-٩-١-١	يجب تحديد نطاق عمليات تقييم الثغرات وأنشطتها لبيئة شبكات أنظمة التحكم الصناعي (OT/ICS) بوصفه جزء من الآليات الرسمية لإدارة الثغرات في الجهة، وضمان تأثير محدود أو غير محدود على بيئة الإنتاج.
٢-٩-١	**أدوات الأمن السيبراني ذات العلاقة:** • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • نموذج سياسة إدارة الثغرات • نموذج معيار إدارة الثغرات • نموذج عمليات واجراءات إدارة الثغرات السيبرانية ويشمل ذلك نموذج سجل لإدارة الثغرات المكتشفة **إرشادات تطبيق الضوابط:** • توثيق وتحديد نطاق عمليات تقييم الثغرات وأنشطتها لبيئة شبكات أنظمة التحكم الصناعي (OT/ICS)، وضمان تأثير محدود أو غير محدود على بيئة الإنتاج. • تضمين تقييم الثغرات بوصفه جزء من الآليات الرسمية لإدارة الثغرات في الجهة.

	• التأكد والتحقق من أن نطاق عمليات تقييم الثغرات يغطي جميع أصول أنظمة التحكم الصناعي (OT/ICS).
	المخرجات المتوقعة: • وثيقة نطاق وأنشطة عمليات تقييم الثغرات الخاصة بأنظمة التحكم الصناعي (OT/ICS). • إثبات يؤكد إجراء تقييم الثغرات بوصفه جزء من الآليات الرسمية لإدارة الثغرات في الجهة.
٢-١-٩-٢	رجوعاً للضابط الفرعي ٢-١٠-٣-٣ في الضوابط الأساسية للأمن السيبراني؛ يتم التأكد من ضمان المعالجة الفورية، للثغرات الحساسة المكتشفة حديثاً، والتي تشكل مخاطر كبيرة على بيئة شبكات أنظمة التحكم الصناعي (OT/ICS).
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • نموذج سياسة إدارة الثغرات • نموذج معيار إدارة الثغرات • نموذج إجراء تقييم الثغرات الأمنية ويشمل ذلك نموذج سجل لإدارة الثغرات المكتشفة • نموذج سجل الثغرات **إرشادات تطبيق الضوابط:** • تطوير إجراءات لضمان المعالجة الفورية، للثغرات الحساسة المكتشفة حديثاً. • التأكد من تطبيق إجراءات إدارة الثغرات.
	المخرجات المتوقعة: • الخطة المعتمدة لمعالجة الثغرات. • تقارير معالجة الثغرات. • إثبات يؤكد المعالجة الفورية، للثغرات الحساسة المكتشفة حديثاً، والتي تشكل مخاطر كبيرة على بيئة شبكات أنظمة التحكم الصناعي (OT/ICS).
٣-١-٩-٢	رجوعاً للضابط الفرعي ٢-١٠-٣-١ في الضوابط الأساسية للأمن السيبراني؛ يجب إجراء تقييم الثغرات لأنظمة التحكم الصناعي دورياً.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • نموذج سياسة إدارة الثغرات • نموذج معيار إدارة الثغرات • نموذج إجراء تقييم الثغرات الأمنية ويشمل ذلك نموذج سجل لإدارة الثغرات المكتشفة • نموذج سجل الثغرات **إرشادات تطبيق الضوابط:**

	• التأكد والتحقق من إجراء تقييم الثغرات لأنظمة التحكم الصناعي دورياً وفقاً لمستوى المرفق المصنف في وثيقة (OTCC-1:2022). **المخرجات المتوقعة:** • التقارير الدورية لتقييم الثغرات. • إثبات يؤكد إجراء تقييم الثغرات لأنظمة التحكم الصناعي دورياً وفقاً لمستوى المرفق المصنف في وثيقة (OTCC-1:2022).
٢-٩-٢	رجوعاً للضابط ٢-١٠-٤ في الضوابط الأساسية للأمن السيبراني؛ يجب مراجعة متطلبات الأمن السيبراني لإدارة الثغرات الخاصة بأنظمة التحكم الصناعي (OT/ICS)، وقياس فعالية تطبيقها وتقييمها دورياً. **أدوات الأمن السيبراني ذات العلاقة:** • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • نموذج سياسة إدارة الثغرات • نموذج تقرير مؤشرات الأداء الرئيسية **إرشادات تطبيق الضوابط:** • العمل على مراجعة متطلبات الأمن السيبراني الثغرات الخاصة بأنظمة التحكم الصناعي (OT/ICS) بشكل دوري حسب خطة موثقة ومعتمدة للمراجعة بناءً على فترة زمنية محددة (على سبيل المثال، يتم إجراء المراجعة الدورية بشكل سنوي). • العمل على تطوير مؤشرات أداء رئيسية (KPIs) لكل الضوابط المتضمنة بداخل السياسات أو الإجراءات للتأكد من قياس فعالية تطبيقها، وتقييمها دورياً بناءً على فترة زمنية محددة (على سبيل المثال، يتم إجراء المراجعة الدورية بشكل سنوي). **المخرجات المتوقعة:** • إثبات يؤكد القيام بالمراجعة الدورية لمتطلبات الأمن السيبراني الثغرات الخاصة بأنظمة التحكم الصناعي (OT/ICS). • إثبات يؤكد القيام بقياس مؤشرات الأداء الرئيسية (KPIs) لكل الضوابط المتضمنة بداخل السياسات أو الإجراءات للتأكد من قياس فعالية تطبيقها، وتقييمها دورياً بناءً على فترة زمنية محددة.
٢-١٠	**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 لاكتشاف الثغرات الأمنية، داخل البنية التحتية التقنية، والتي قد تؤدي إلى الاختراق السيبراني للجهة.
الضوابط	

٢-١٠-١	بالإضافة للضوابط الفرعية ضمن الضابط ٢-١١-٣ في الضوابط الأساسية للأمن السيبراني؛ يجب أن تغطي متطلبات الأمن السيبراني إجراء اختبارات اختراق على أنظمة التحكم الصناعي (OT/ICS) بحد أدنى ما يلي:	
	٢-١٠-١-١	رجوعاً للضابط الفرعي ٢-١١-٣-١ في الضوابط الأساسية للأمن السيبراني؛ يجب تحديد نطاق أنشطة اختبارات الاختراق، لتغطي بيئة شبكات أنظمة التحكم الصناعي (OT/ICS) والشبكات المرتبطة بالشبكة التشغيلية، وأن يتم عمل الاختبارات من قبل فريق ذي كفاءة عالية.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • نموذج سياسة اختبار الاختراق • نموذج معيار اختبار الاختراق **إرشادات تطبيق الضوابط:** • العمل على تحديد نطاق أنشطة اختبارات الاختراق. • التأكد من أن أنشطة اختبارات الاختراق يتم إجراءها من قبل فريق مؤهل.	
	المخرجات المتوقعة: • إثبات يؤكد إجراء أنشطة اختبارات الاختراق، لتغطي بيئة شبكات أنظمة التحكم الصناعي (OT/ICS) والشبكات المرتبطة بالشبكة التشغيلية، وأن يتم عمل الاختبارات من قبل فريق ذي كفاءة عالية.	
	٢-١٠-١-٢	رجوعاً للضابط الفرعي ٢-١١-٣-٢ في الضوابط الأساسية للأمن السيبراني؛ يجب إجراء اختبار الاختراق، بعد التأكد من أن تأثير الاختبار، محدود على بيئة الإنتاج، أو إجراء اختبار الاختراق، في بيئة منفصلة مماثلة.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • نموذج سياسة اختبار الاختراق • نموذج معيار اختبار الاختراق **إرشادات تطبيق الضوابط:** • العمل على إجراء اختبار الاختراق، بعد التأكد من أن تأثير الاختبار، محدود على بيئة الإنتاج، أو إجراء اختبار الاختراق، في بيئة منفصلة مماثلة، على سبيل المثال لا الحصر: بيئات الاختبار أو البيئات الخاصة بالتدريب.	
	المخرجات المتوقعة: • إثبات يؤكد إجراء اختبار الاختراق، بعد التأكد من أن تأثير الاختبار، محدود على بيئة الإنتاج، أو إجراء اختبار الاختراق، في بيئة منفصلة مماثلة، على سبيل المثال لا الحصر: بيئات الاختبار أو البيئات الخاصة بالتدريب.	

	٢-١٠-١-٣	رجوعاً للضابط الفرعي ٢-١١-٣-٢ في الضوابط الأساسية للأمن السيبراني؛ يجب إجراء اختبار الاختراق لأنظمة التحكم الصناعي دورياً.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • نموذج سياسة اختبار الاختراق • نموذج معيار اختبار الاختراق **إرشادات تطبيق الضوابط:** • التأكد من إجراء اختبار الاختراق لأنظمة التحكم الصناعي دورياً وفقاً لمستوى تصنيف المرفق في وثيقة (OTCC-1:2022). **المخرجات المتوقعة:** • إثبات يؤكد إجراء اختبار الاختراق لأنظمة التحكم الصناعي دورياً وفقاً لمستوى تصنيف المرفق في وثيقة (OTCC-1:2022).	
	٢-١٠-١-٤	يجب تحديد طرق اختبارات بديلة وتنفيذها مثل الاختبارات غير الفعالة (Passive Testing) لجمع المعلومات عندما يكون هنالك أثر محتمل على بيئة الإنتاج التشغيلية.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • نموذج سياسة اختبار الاختراق • نموذج معيار اختبار الاختراق **إرشادات تطبيق الضوابط:** • تحديد قائمة بأنظمة التحكم الصناعي (OT/ICS) التي تحتاج إلى طرق اختبارات بديلة لاختبارها. • تحديد وتوثيق طرق اختبارات بديلة وتنفيذها مثل الاختبارات غير الفعالة (Passive Testing)، عندما يكون هنالك أثر محتمل على بيئة الإنتاج التشغيلية. • العمل على تنفيذ طرق اختبارات بديلة مثل الاختبارات غير الفعالة (Passive Testing) للأنظمة المحددة، وذلك بناء على الإجراءات المعتمدة. • التأكد والتحقق من أن الاختبارات البديلة تسمح بجمع المعلومات عن الأصول الخاصة بأنظمة التحكم الصناعي (OT/ICS). **المخرجات المتوقعة:** • التقارير الدورية للاختبارات البديلة.	
	٢-١٠-٢	رجوعاً للضابط ٢-١١-٤ في الضوابط الأساسية للأمن السيبراني؛ يجب مراجعة متطلبات الأمن السيبراني لاختبارات الاختراق على أنظمة التحكم الصناعي (OT/ICS)، وقياس فعالية تطبيقها وتقييمها دورياً.
	أدوات الأمن السيبراني ذات العلاقة:	

	• نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • نموذج سياسة اختبار الاختراق • نموذج تقرير مؤشرات الأداء الرئيسية **إرشادات تطبيق الضوابط:** • العمل على مراجعة متطلبات الأمن السيبراني لاختبارات الاختراق على أنظمة التحكم الصناعي (OT/ICS) بشكل دوري حسب خطة موثقة ومعتمدة للمراجعة بناءً على فترة زمنية محددة (على سبيل المثال، يتم إجراء المراجعة الدورية بشكل سنوي). • العمل على تطوير مؤشرات أداء رئيسية (KPIs) لكل الضوابط المتضمنة بداخل السياسات أو الإجراءات للتأكد من قياس فعالية تطبيقها، وتقييمها دورياً بناءً على فترة زمنية محددة (على سبيل المثال، يتم إجراء المراجعة الدورية بشكل سنوي). **المخرجات المتوقعة:** • إثبات يؤكد القيام بالمراجعة الدورية لمتطلبات الأمن السيبراني لاختبارات الاختراق على أنظمة التحكم الصناعي (OT/ICS). • إثبات يؤكد القيام بقياس مؤشرات الأداء الرئيسية (KPIs) لكل الضوابط المتضمنة بداخل السياسات أو الإجراءات للتأكد من قياس فعالية تطبيقها، وتقييمها دورياً بناءً على فترة زمنية محددة.
٢-١١	إدارة سجلات الأحداث ومراقبة الأمن السيبراني (Cybersecurity Event Logs and Monitoring Management)
الهدف	ضمان جمع سجلات أحداث الأمن السيبراني في الوقت المناسب وتحليلها ومراقبتها للكشف المبكر عن الهجمات السيبرانية المحتملة وإدارة مخاطرها بفعالية، من أجل منع الآثار المترتبة على أعمال الجهة أو التقليل منها.
الضوابط	
٢-١١-١	بالإضافة للضوابط الفرعية، ضمن الضابط ٢-١٢-٣ في الضوابط الأساسية للأمن السيبراني؛ يجب أن تغطي متطلبات الأمن السيبراني لإدارة سجلات الأحداث ومراقبة الأمن السيبراني الخاصة بأنظمة التحكم الصناعي (OT/ICS) بحد أدنى ما يلي:
٢-١١-١-١	تفعيل سجلات الأحداث المتعلقة بالأمن السيبراني على جميع الأصول في بيئة شبكات أنظمة التحكم الصناعي (OT/ICS).
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • نموذج سياسة إدارة سجلات الأحداث ومراقبة الأمن السيبراني • نموذج معيار إدارة سجلات الأحداث ومراقبة الأمن السيبراني

إرشادات تطبيق الضوابط: • العمل على تفعيل سجلات الأحداث المتعلقة بالأمن السيبراني على جميع الأصول في بيئة شبكات أنظمة التحكم الصناعي (OT/ICS)، على سبيل المثال لا الحصر، أجهزة المشغّلين، والأجهزة الهندسية، والخوادم، وأجهزة الشبكة.	
المخرجات المتوقعة: • سجلات أحداث الأمن السيبراني ومسارات التدقيق التي يتلقاها نظام المراقبة. • إثبات يؤكد تفعيل سجلات الأحداث المتعلقة بالأمن السيبراني على جميع الأصول في بيئة شبكات أنظمة التحكم الصناعي (OT/ICS)، على سبيل المثال لا الحصر، أجهزة المشغّلين، والأجهزة الهندسية، والخوادم، وأجهزة الشبكة.	
٢-١-١١-٢	اكتشاف محاولات فشل الوصول إلى نظام المراقبة الخاص بالجهة، ورصدها.
أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • نموذج سياسة إدارة سجلات الأحداث ومراقبة الأمن السيبراني • نموذج معيار إدارة سجلات الأحداث ومراقبة الأمن السيبراني **إرشادات تطبيق الضوابط:** • تطبيق آليات لاكتشاف محاولات فشل الوصول إلى نظام المراقبة الخاص بالجهة، ورصدها على سبيل المثال (alerting system in case of unauthorized access). • التأكد من تفعيل سجلات الأحداث (Event logs) وتحويلها إلى نظام إدارة سجلات الأحداث والمراقبة (SIEM) أو مجمع سجلات الأحداث (Log collector)، ومن ثم يتم تحليل هذه الأحداث عن طريق مركز المراقبة الأمنية (SOC).	
المخرجات المتوقعة: • إثبات يؤكد تطبيق آليات لاكتشاف محاولات فشل الوصول إلى نظام المراقبة الخاص بالجهة، ورصدها. • قائمة الحالات المطورة (Use-cases) الخاصة بأنظمة التحكم الصناعي (OT/ICS) من مركز المراقبة الأمنية (SOC).	
٣-١-١١-٢	إجراء مراجعة ومراقبة مستمرة ودقيقة لسجلات الأحداث (Event Logs) والتدقيق (Audit Trails) المتعلقة بالأمن السيبراني، على أصول أنظمة التحكم الصناعي (OT/ICS)

	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • نموذج سياسة إدارة سجلات الأحداث ومراقبة الأمن السيبراني • نموذج معيار إدارة سجلات الأحداث ومراقبة الأمن السيبراني **إرشادات تطبيق الضوابط:** • التأكد من إجراء مراجعة ومراقبة مستمرة ودقيقة لسجلات الأحداث (Event Logs) والتدقيق (Audit Trails) المتعلقة بالأمن السيبراني، على أصول أنظمة التحكم الصناعي (OT/ICS) عن طريق قدرات مركز المراقبة الأمنية (SOC). • التأكد من تفعيل سجلات الأحداث (Event logs) وتحويلها إلى نظام إدارة سجلات الأحداث والمراقبة (SIEM) أو مجمع سجلات الأحداث (Log collector)، ومن ثم يتم تحليل هذه الأحداث عن طريق مركز المراقبة الأمنية (SOC). **المخرجات المتوقعة:** • زيارة ميدانية لمركز المراقبة الأمنية (SOC). • قائمة الحالات المطورة (Use-cases) الخاصة بأنظمة التحكم الصناعي (OT/ICS) من مركز المراقبة الأمنية (SOC).
٢-١١-١-٤	إجراء مراقبة وكشف، وتحليل لسلوك المستخدم ("UBA" User Behaviors Analytics)
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • نموذج سياسة إدارة سجلات الأحداث ومراقبة الأمن السيبراني • نموذج معيار إدارة سجلات الأحداث ومراقبة الأمن السيبراني **إرشادات تطبيق الضوابط:** • تحديد وتطبيق تقنيات مراقبة وكشف، وتحليل لسلوك المستخدم (User Behaviors Analytics). • التأكد والتحقق من أن تقنيات مراقبة وكشف، وتحليل لسلوك المستخدم (User Behaviors Analytics) تغطي جميع المستخدمين. • التأكد من تفعيل سجلات الأحداث (Event logs) وتحويلها إلى نظام إدارة سجلات الأحداث والمراقبة (SIEM) أو مجمع سجلات الأحداث (Log collector)، ومن ثم يتم تحليل هذه الأحداث عن طريق مركز المراقبة الأمنية (SOC).

المخرجات المتوقعة: • إثبات يؤكد تطبيق تقنيات مراقبة وكشف، وتحليل لسلوك المستخدم (User Behaviors Analytics).	
٢-١١-١-٥	اكتشاف عمليات الرفع أو التنزيل على أجهزة وأنظمة التحكم الصناعي (OT/ICS)، بما في ذلك أنظمة السلامة (SIS).
أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • نموذج سياسة إدارة سجلات الأحداث ومراقبة الأمن السيبراني • نموذج معيار إدارة سجلات الأحداث ومراقبة الأمن السيبراني **إرشادات تطبيق الضوابط:** • تحديد قائمة بجميع أجهزة وأنظمة التحكم الصناعي (OT/ICS)، بما في ذلك أنظمة معدات السلامة (SIS). • تحديد وتطبيق الآليات المناسبة لاكتشاف عمليات الرفع أو التنزيل على أجهزة وأنظمة التحكم الصناعي (OT/ICS)، بما في ذلك أنظمة السلامة (SIS). • التأكد من أنه يتم اكتشاف عمليات الرفع أو التنزيل على أجهزة وأنظمة التحكم الصناعي (OT/ICS)، بما في ذلك أنظمة السلامة (SIS).	
المخرجات المتوقعة: • زيارة ميدانية للتحقق من اكتشاف عمليات الرفع أو التنزيل على أجهزة وأنظمة التحكم الصناعي (OT/ICS)، بما في ذلك أنظمة السلامة (SIS).	
٢-١١-١-٦	مراقبة جميع عمليات الوصول عن بعد (Remote Access Sessions).
أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • نموذج سياسة إدارة سجلات الأحداث ومراقبة الأمن السيبراني • نموذج معيار إدارة سجلات الأحداث ومراقبة الأمن السيبراني **إرشادات تطبيق الضوابط:** • التأكد من مراقبة جميع عمليات الوصول عن بعد (Remote Access Sessions).	

	• التأكد من تفعيل سجلات الأحداث (Event logs) وتحويلها إلى نظام إدارة سجلات الأحداث والمراقبة (SIEM) أو مجمع سجلات الأحداث (Log collector)، ومن ثم يتم تحليل هذه الأحداث عن طريق مركز المراقبة الأمنية (SOC).
	المخرجات المتوقعة: • إثبات يؤكد مراقبة جميع عمليات الوصول عن بعد (Remote Access Sessions). • قائمة الحالات المطورة (Use-cases) الخاصة بأنظمة التحكم الصناعي (OT/ICS) من مركز المراقبة الأمنية (SOC).
٢-١١-١-٧	اكتشاف الاحداث الضارة (Malicious Events) وفحصها.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • نموذج سياسة إدارة سجلات الأحداث ومراقبة الأمن السيبراني • نموذج معيار إدارة سجلات الأحداث ومراقبة الأمن السيبراني **إرشادات تطبيق الضوابط:** • التأكد من تمكين جدولة فحص مكافحة الفيروسات بشكل دوري. • التأكد من اكتشاف الأحداث الضارة (Malicious Events) وفحصها عن طريق قدرات مركز المراقبة الأمنية (SOC). • التأكد من تفعيل سجلات الأحداث (Event logs) وتحويلها إلى نظام إدارة سجلات الأحداث والمراقبة (SIEM) أو مجمع سجلات الأحداث (Log collector)، ومن ثم يتم تحليل هذه الأحداث عن طريق مركز المراقبة الأمنية (SOC).
	المخرجات المتوقعة: • إثبات يؤكد اكتشاف الأحداث الضارة (Malicious Events) وفحصها.
٢-١١-١-٨	تسجيل التنبيهات الحديثة ومراقبتها في حال اتصال أجهزة جديدة، أو غير مسموح بها بشبكات أنظمة التحكم الصناعي (OT/ICS).
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS)

	• نموذج سياسة إدارة سجلات الأحداث ومراقبة الأمن السيبراني • نموذج معيار إدارة سجلات الأحداث ومراقبة الأمن السيبراني **إرشادات تطبيق الضوابط:** • التأكد من تسجيل التنبيهات الحديثة ومراقبتها في حال اتصال أجهزة جديدة، أو غير مسموح بها بشبكات أنظمة التحكم الصناعي (OT/ICS)، وذلك عن طريق قدرات مركز المراقبة الأمنية (SOC). • التأكد من تفعيل سجلات الأحداث (Event logs) وتحويلها إلى نظام إدارة سجلات الأحداث والمراقبة (SIEM) أو مجمع سجلات الأحداث (Log collector)، ومن ثم يتم تحليل هذه الأحداث عن طريق مركز المراقبة الأمنية (SOC). **المخرجات المتوقعة:** • إثبات يؤكد تسجيل التنبيهات الحديثة ومراقبتها في حال اتصال أجهزة جديدة، أو غير مسموح بها بشبكات أنظمة التحكم الصناعي (OT/ICS).
٢-١١-١-٩	استخدام التهديدات الاستباقية (Threat Intelligence) المتعلقة بأنظمة التحكم الصناعي (OT/ICS) لضبط تنبيهات نظام إدارة سجلات الاحداث وتحديثها، ومراقبة الأمن السيبراني (SIEM) بشكل منتظم.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • نموذج سياسة إدارة سجلات الأحداث ومراقبة الأمن السيبراني • نموذج معيار إدارة سجلات الأحداث ومراقبة الأمن السيبراني **إرشادات تطبيق الضوابط:** • التأكد والتحقق من استخدام التهديدات الاستباقية (Threat Intelligence) المتعلقة بأنظمة التحكم الصناعي (OT/ICS) لضبط تنبيهات نظام إدارة سجلات الأحداث وتحديثها، ومراقبة الأمن السيبراني (SIEM) بشكل منتظم. **المخرجات المتوقعة:** • إثبات يؤكد استخدام التهديدات الاستباقية (Threat Intelligence) المتعلقة بأنظمة التحكم الصناعي (OT/ICS) لضبط تنبيهات نظام إدارة سجلات الأحداث وتحديثها، ومراقبة الأمن السيبراني (SIEM) بشكل منتظم.
٢-١١-١-١٠	مراقبة جميع نقاط التحكم بالدخول (Access Control Points) بين حدود الشبكة (Network Boundaries) والاتصالات الخارجية.

	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • نموذج سياسة إدارة سجلات الأحداث ومراقبة الأمن السيبراني • نموذج معيار إدارة سجلات الأحداث ومراقبة الأمن السيبراني **إرشادات تطبيق الضوابط:** • التأكد من مراقبة جميع نقاط التحكم بالدخول (Access Control Points) بين حدود الشبكة (Network Boundaries) والاتصالات الخارجية. • التأكد من تفعيل سجلات الأحداث (Event logs) وتحويلها إلى نظام إدارة سجلات الأحداث والمراقبة (SIEM) أو مجمع سجلات الأحداث (Log collector)، ومن ثم يتم تحليل هذه الأحداث عن طريق مركز المراقبة الأمنية (SOC). **المخرجات المتوقعة:** • إثبات يؤكد مراقبة جميع نقاط التحكم بالدخول (Access Control Points) بين حدود الشبكة (Network Boundaries) والاتصالات الخارجية.
٢-١١-٢	رجوعاً للضابط ٢-١٢-٤ في الضوابط الأساسية للأمن السيبراني؛ يجب مراجعة متطلبات الأمن السيبراني لإدارة سجلات الأحداث، ومراقبة الأمن السيبراني لأنظمة التحكم الصناعي (OT/ICS)، وقياس فعالية تطبيقها وتقييمها دورياً. **أدوات الأمن السيبراني ذات العلاقة:** • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • نموذج سياسة إدارة سجلات الأحداث ومراقبة الأمن السيبراني • نموذج تقرير مؤشرات الأداء الرئيسية **إرشادات تطبيق الضوابط:** • العمل على مراجعة متطلبات الأمن السيبراني لإدارة سجلات الأحداث ومراقبة الأمن السيبراني الخاصة بأنظمة التحكم الصناعي (OT/ICS) بشكل دوري حسب خطة موثقة ومعتمدة للمراجعة بناءً على فترة زمنية محددة (على سبيل المثال، يتم إجراء المراجعة الدورية بشكل سنوي). • العمل على تطوير مؤشرات أداء رئيسية (KPIs) لكل الضوابط المتضمنة بداخل السياسات أو الإجراءات للتأكد من قياس فعالية تطبيقها، وتقييمها دورياً بناءً على فترة زمنية محددة (على سبيل المثال، يتم إجراء المراجعة الدورية بشكل سنوي). **المخرجات المتوقعة:** • إثبات يؤكد القيام بالمراجعة الدورية لمتطلبات الأمن السيبراني لإدارة سجلات الأحداث ومراقبة الأمن السيبراني الخاصة بأنظمة التحكم الصناعي (OT/ICS).

	• إثبات يؤكد القيام بقياس مؤشرات الأداء الرئيسية (KPIs) لكل الضوابط المتضمنة بداخل السياسات أو الإجراءات للتأكد من قياس فعالية تطبيقها، وتقييمها دورياً بناءً على فترة زمنية محددة.
٢-١٢	إدارة حوادث وتهديدات الأمن السيبراني (Cybersecurity Incident and Threat Management)
الهدف	ضمان اكتشاف حوادث الأمن السيبراني وتحديدها في الوقت المناسب، وإدارتها بشكل فعال، والتعامل مع تهديدات الأمن السيبراني استباقياً من أجل منع الأثار المترتبة أو تقليلها على أعمال الجهة المتعلقة بأنظمة التحكم الصناعي (OT/ICS).
الضوابط	
١-١٢-٢	بالإضافة للضوابط الفرعية ضمن الضابط ٢-١٣-٣ في الضوابط الأساسية للأمن السيبراني؛ يجب أن تغطي متطلبات الأمن السيبراني لإدارة حوادث وتهديدات الأمن السيبراني المتعلقة بأنظمة التحكم الصناعي (OT/ICS) بحد أدنى ما يلي:
١-١-١٢-٢	التأكد من أن خطط الاستجابة للحوادث الأمنية، المتعلقة بأنظمة التحكم الصناعي (OT/ICS) مدمجة، ومتوائمة مع خطط الجهة وإجراءاتها؛ مثل خطط الاستجابة لحوادث تقنية المعلومات، وإدارة الأزمات، وخطط استمرارية الأعمال (Business Continuity Plan "BCP").
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • نموذج سياسة إدارة حوادث وتهديدات الأمن السيبراني • نموذج معيار إدارة حوادث وتهديدات الأمن السيبراني • الدليل الإرشادي للاستجابة لحوادث الأمن السيبراني • نماذج الخطط التفصيلية للاستجابة لحوادث الأمن السيبراني **إرشادات تطبيق الضوابط:** • تحديد وتوثيق واعتماد خطط الاستجابة لحوادث الأمن السيبراني المتعلقة بأنظمة التحكم الصناعي (OT/ICS). كما يجب أن تكون الخطط المعتمدة موثقة رسمياً (كإجراءات على سبيل المثال) وتستند إلى المعايير الحالية والمتاحة عالمياً. • تضمين خطط الاستجابة لحوادث الأمن السيبراني المتعلقة بأنظمة التحكم الصناعي (OT/ICS) المعتمدة مع خطط الجهة وإجراءاتها. • التأكد والتحقق من موائمة خطط الاستجابة لحوادث الأمن السيبراني المتعلقة بأنظمة التحكم الصناعي (OT/ICS) مع باقي خطط الجهة إجراءاتها. **المخرجات المتوقعة:** • وثيقة خطط الاستجابة لحوادث الأمن السيبراني المتعلقة بأنظمة التحكم الصناعي (OT/ICS) المعتمدة.

• إثبات يؤكد موائمة خطط الاستجابة لحوادث الأمن السيبراني المتعلقة بأنظمة التحكم الصناعي (OT/ICS) مع باقي خطط الجهة وإجراءاتها.	
٢-١٢-١-٢	إجراء تحليل للحوادث، وتحليل الأسباب الجذرية (Root Cause Analysis) لحوادث الأمن السيبراني، بطريقة منظمة، بعد اكتشاف الحوادث.
أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • نموذج سياسة إدارة حوادث وتهديدات الأمن السيبراني • نموذج معيار إدارة حوادث وتهديدات الأمن السيبراني • الدليل الإرشادي للاستجابة لحوادث الأمن السيبراني • نماذج الخطط التفصيلية للاستجابة لحوادث الأمن السيبراني **إرشادات تطبيق الضوابط:** • تحديد وتوثيق إجراءات ومنهجيات لتحليل الحوادث (root cause analysis procedure) بعد اكتشاف الحوادث. • تنفيذ خطط الاستجابة لحوادث الأمن السيبراني المتعلقة بأنظمة التحكم الصناعي (OT/ICS) والتعامل مع الحوادث حسب المراحل المحددة بالخطة. • إجراء تحليل للحوادث، وتحليل الأسباب الجذرية (Root Cause Analysis) لحوادث الأمن السيبراني، بطريقة منظمة، بعد اكتشاف الحوادث.	
المخرجات المتوقعة: • وثيقة إجراءات ومنهجيات لتحليل الحوادث (root cause analysis procedure). • تقارير الاستجابة لحوادث الأمن السيبراني وتحليل الأسباب الجذرية (Root Cause Analysis). • إثبات يؤكد إجراء تحليل للحوادث، وتحليل الأسباب الجذرية (Root Cause Analysis) لجميع حوادث الأمن السيبراني، بعد اكتشافها.	
٢-١٢-١-٣	تحديد تسلسل أنشطة الاستجابة، لحوادث الأمن السيبراني اللازمة لاستعادة العمليات التشغيلية لطبيعتها.
أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • نموذج سياسة إدارة حوادث وتهديدات الأمن السيبراني • نموذج معيار إدارة حوادث وتهديدات الأمن السيبراني • الدليل الإرشادي للاستجابة لحوادث الأمن السيبراني	

	• نماذج الخطط التفصيلية للاستجابة لحوادث الأمن السيبراني **إرشادات تطبيق الضوابط:** • تحديد وتوثيق واعتماد تسلسل أنشطة الاستجابة، لحوادث الأمن السيبراني اللازمة لاستعادة العمليات التشغيلية لطبيعتها. يجب أن تكون الأنشطة المعتمدة موثقة رسمياً (على سبيل المثال كخطة أو إجراء). • تحديد وتوثيق خطة عمل استعادة العمليات. تحتوي على وصف مفصل خطوة بخطوة ودليل إرشادي. • التأكد والتحقق من استعادة العمليات التشغيلية لطبيعتها وذلك عند التعرض لحادث اختراق. **المخرجات المتوقعة:** • الوثيقة المعتمدة لتسلسل أنشطة الاستجابة، لحوادث الأمن السيبراني اللازمة لاستعادة العمليات التشغيلية لطبيعتها. • وثيقة خطة الاستعادة عند التعرض لحادث أمن سيبراني. • إثبات يؤكد استعادة العمليات التشغيلية لطبيعتها وذلك عند التعرض لحادث اختراق.
٢-١٢-١-٤	إنشاء خطط التواصل، عند وقوع الحوادث (Incident Communications Plan).
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • نموذج سياسة إدارة حوادث وتهديدات الأمن السيبراني • نموذج معيار إدارة حوادث وتهديدات الأمن السيبراني • الدليل الإرشادي للاستجابة لحوادث الأمن السيبراني • نماذج الخطط التفصيلية للاستجابة لحوادث الأمن السيبراني **إرشادات تطبيق الضوابط:** • تحديد وتوثيق خطط التواصل، عند وقوع الحوادث (Incident Communications Plan). • التأكد من تطبيق خطط التواصل، عند وقوع الحوادث (Incident Communications Plan). **المخرجات المتوقعة:** • وثيقة خطط التواصل، عند وقوع الحوادث (Incident Communications Plan). • إثبات يؤكد تطبيق خطط التواصل، عند وقوع الحوادث (Incident Communications Plan)
٢-١٢-١-٥	تضمين إجراءات التعافي لأنظمة التحكم الصناعي وتشمل أنظمة معدات السلامة (SIS) في خطط الاستجابة للحوادث، واستعادة النظام، واستمرارية الأعمال.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • نموذج سياسة إدارة حوادث وتهديدات الأمن السيبراني

	• نموذج معيار إدارة حوادث وتهديدات الأمن السيبراني • الدليل الإرشادي للاستجابة لحوادث الأمن السيبراني • نماذج الخطط التفصيلية للاستجابة لحوادث الأمن السيبراني **إرشادات تطبيق الضوابط:** • التأكد من تضمين إجراءات التعافي لأنظمة التحكم الصناعي وتشمل أنظمة معدات السلامة (SIS) في خطط الاستجابة للحوادث، واستعادة النظام، استمرارية الأعمال. **المخرجات المتوقعة:** • وثيقة إجراءات استعادة أنظمة التحكم الصناعي (OT/ICS). • وثيقة خطط الاستجابة لحوادث أنظمة التحكم الصناعي (OT/ICS). • وثيقة خطط استمرارية أعمال أنظمة التحكم الصناعي (OT/ICS).
٢-١٢-١-٦	تزويد العاملين بالجهة بالمهارات والدورات التدريبية المطلوبة (الموظفين والمتعاقدين)، للاستجابة لحوادث الأمن السيبراني المتعلقة بأنظمة التحكم الصناعي (OT/ICS).
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • نموذج سياسة إدارة حوادث وتهديدات الأمن السيبراني • نموذج معيار إدارة حوادث وتهديدات الأمن السيبراني **إرشادات تطبيق الضوابط:** • العمل على تدريب العاملين بالجهة بالمهارات والدورات المطلوبة (الموظفين والمتعاقدين)، للاستجابة لحوادث الأمن السيبراني المتعلقة بأنظمة التحكم الصناعي (OT/ICS). **المخرجات المتوقعة:** • قائمة موثقة بالعاملين المزودين بالمهارات والدورات، للاستجابة لحوادث الأمن السيبراني المتعلقة بأنظمة التحكم الصناعي (OT/ICS). • إثبات يؤكد تزويد جميع العاملين بالجهة بالمهارات والدورات المطلوبة (الموظفين والمتعاقدين)، للاستجابة لحوادث الأمن السيبراني المتعلقة بأنظمة التحكم الصناعي (OT/ICS).
٢-١٢-١-٧	اختبار قدرات الاستجابة لحوادث الأمن السيبراني ومستوى الجاهزية والخطة المعتمدة بشكل دوري من خلال إجراء تمارين محاكاة للهجمات السيبرانية (Attack Simulation Exercises).
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • نموذج سياسة إدارة حوادث وتهديدات الأمن السيبراني • نموذج معيار إدارة حوادث وتهديدات الأمن السيبراني

	إرشادات تطبيق الضوابط: • التأكد من اختبار قدرات الاستجابة لحوادث الأمن السيبراني ومستوى الجاهزية والخطة المعتمدة بشكل دوري من خلال إجراء تمارين محاكاة للهجمات السيبرانية (Attack Simulation Exercises).
	المخرجات المتوقعة: • قائمة موثقة بتمارين محاكاة للهجمات السيبرانية (cybersecurity drills, tabletop exercises). • إثبات يؤكد اختبار قدرات الاستجابة لحوادث الأمن السيبراني ومستوى الجاهزية والخطة المعتمدة بشكل دوري.
٢-١٢-١-٨	استخدام معلومات التهديدات الاستباقية (Threat Intelligence) لتحديد الخطط والأساليب والإجراءات (TTPs) المستخدمة من قبل المجموعات النشطة (Activity Groups) التي تستهدف أنظمة التحكم الصناعي (OT/ICS).
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • نموذج سياسة إدارة حوادث وتهديدات الأمن السيبراني • نموذج معيار إدارة حوادث وتهديدات الأمن السيبراني **إرشادات تطبيق الضوابط:** • الحصول على معلومات التهديدات الاستباقية (Threat Intelligence) لتحديد الخطط والأساليب والإجراءات (TTPs) المستخدمة من قبل المجموعات النشطة (Activity Groups) التي تستهدف أنظمة التحكم الصناعي (OT/ICS). • التأكد من الحصول على آخر المعلومات بخصوص التهديدات الاستباقية (Threat Intelligence).
	المخرجات المتوقعة: • تقارير التهديدات الاستباقية (Threat Intelligence). • إثبات يؤكد استخدام معلومات التهديدات الاستباقية (Threat Intelligence) لتحديد الخطط والأساليب والإجراءات (TTPs) المستخدمة من قبل المجموعات النشطة (Activity Groups) التي تستهدف أنظمة التحكم الصناعي (OT/ICS).
٢-١٢-٢	رجوعاً للضابط ٢-١٣-٤ في الضوابط الأساسية للأمن السيبراني؛ يجب مراجعة متطلبات الأمن السيبراني لإدارة حوادث وتهديدات الأمن السيبراني في بيئة أنظمة التحكم الصناعي (OT/ICS)، وقياس فعالية تطبيقها وتقييمها دورياً.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • نموذج سياسة إدارة حوادث وتهديدات الأمن السيبراني • نموذج تقرير مؤشرات الأداء الرئيسية **إرشادات تطبيق الضوابط:**

	• العمل على مراجعة متطلبات الأمن السيبراني لإدارة حوادث وتهديدات الأمن السيبراني في بيئة شبكات أنظمة التحكم الصناعي (OT/ICS) بشكل دوري حسب خطة موثقة ومعتمدة للمراجعة بناءً على فترة زمنية محددة (على سبيل المثال، يتم إجراء المراجعة الدورية بشكل سنوي). • العمل على تطوير مؤشرات أداء رئيسية (KPIs) لكل الضوابط المتضمنة بداخل السياسات أو الإجراءات للتأكد من قياس فعالية تطبيقها، وتقييمها دورياً بناءً على فترة زمنية محددة (على سبيل المثال، يتم إجراء المراجعة الدورية بشكل سنوي). **المخرجات المتوقعة:** • إثبات يؤكد القيام بالمراجعة الدورية لمتطلبات الأمن السيبراني لإدارة حوادث وتهديدات الأمن السيبراني في بيئة شبكات أنظمة التحكم الصناعي (OT/ICS). • إثبات يؤكد القيام بقياس مؤشرات الأداء الرئيسية (KPIs) لكل الضوابط المتضمنة بداخل السياسات أو الإجراءات للتأكد من قياس فعالية تطبيقها، وتقييمها دورياً بناءً على فترة زمنية محددة.
٢-١٣	الأمن المادي (Physical Security)
الهدف	ضمان حماية أنظمة التحكم الصناعي (OT/ICS) للجهة من الوصول المادي غير المصرح به والفقدان والسرقة والتخريب.
الضوابط	
٢-١٣-١	بالإضافة للضوابط الفرعية ضمن الضابط ٢-١٤-٣ في الضوابط الأساسية للأمن السيبراني؛ يجب أن تغطي متطلبات الأمن السيبراني للأمن المادي المتعلق بأنظمة التحكم الصناعي (OT/ICS) بحد أدنى ما يلي: ٢-١٣-١-١ الاحتفاظ بقائمة الأشخاص، الذين لديهم حق الوصول المادي المصرح به إلى المنشآت، والأماكن الحساسة، التي يتواجد بها أصول أنظمة التحكم الصناعي (OT/ICS). **أدوات الأمن السيبراني ذات العلاقة:** • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • نموذج سياسة الأمن المادي • نموذج معيار الأمن المادي **إرشادات تطبيق الضوابط:** • تحديد قائمة الأشخاص، الذين لديهم حق الوصول المادي المصرح به إلى المرافق، والأماكن الحساسة، التي يتواجد بها أصول أنظمة التحكم الصناعي (OT/ICS). • الاحتفاظ وتحديث القائمة بشكل مستمر وإدارتها بناء على الآليات والإجراءات المتبعة في الجهة. **المخرجات المتوقعة:** • قائمة موثقة بالأشخاص الذين لديهم حق الوصول المادي المصرح به إلى المرافق، والأماكن الحساسة، التي يتواجد بها أصول أنظمة التحكم الصناعي (OT/ICS).

• إثبات يؤكد تحديث القائمة بشكل دوري.	
٢-١٣-١-٢	تطبيق الآليات المناسبة للتنبيه، والكشف عن التسلل المادي (Physical Intrusion) والمراقبة (Surveillance) بشكل لحظي (Real Time)، للتعرف على محاولات الدخول المحتملة، وتطبيق إجراءات الاستجابة المعتمدة.
أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • نموذج سياسة الأمن المادي • نموذج معيار الأمن المادي **إرشادات تطبيق الضوابط:** • التأكد من تطبيق الآليات المناسبة للتنبيه، والكشف عن التسلل المادي (Physical Intrusion) والمراقبة (Surveillance) بشكل لحظي (Real Time)، للتعرف على محاولات الدخول المحتملة، وتطبيق إجراءات الاستجابة المعتمدة.	
المخرجات المتوقعة: • زيارة ميدانية للتحقق من تطبيق الآليات المناسبة للتنبيه، والكشف عن التسلل المادي (Physical Intrusion) والمراقبة (Surveillance) بشكل لحظي (Real Time).	
٢-١٣-١-٣	حماية نقاط الدخول المادية، والمحيط بالأماكن التي تحتوي على أنظمة التحكم الصناعي (OT/ICS) الحساسة، والتأكد من مراقبتها باستمرار.
أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • نموذج سياسة الأمن المادي • نموذج معيار الأمن المادي **إرشادات تطبيق الضوابط:** • تحديد قائمة بنقاط الدخول المادية، والمحيط بالأماكن التي تحتوي على أنظمة التحكم الصناعي (OT/ICS). • تطبيق آليات لحماية نقاط الدخول المادية، والمحيط بالأماكن التي تحتوي على أنظمة التحكم الصناعي (OT/ICS). الآلية المطبقة يجب أن تكون موثقة (خطة تطبيق أو إجراء على سبيل المثال). • التأكد والتحقق من مراقبة نقاط الدخول المادية باستمرار.	
المخرجات المتوقعة: • قائمة موثقة بنقاط الدخول المادية، والمحيط بالأماكن التي تحتوي على أنظمة التحكم الصناعي (OT/ICS). • زيارة ميدانية للتحقق من إدارة ومراقبة نقاط الدخول المادية باستمرار.	

٢-١٣-١-٤	استخدام إجراءات الحماية المناسبة؛ مثل الأقفال على جميع الخزائن (Cabinets) التي تحتوي على أنظمة تحكم (Control Systems) وأصول حساسة متعلقة بأنظمة التحكم الصناعي (OT/ICS)، وذلك لمنع الوصول غير المصرح به للأجهزة، التي يمكن أن توفر آلية لاختراق أصول أنظمة التحكم الصناعي (OT/ICS).

أدوات الأمن السيبراني ذات العلاقة:

- نموذج سياسة الأمن السيبراني للأنظمة التشغيلية
- نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS)
- نموذج سياسة الأمن المادي
- نموذج معيار الأمن المادي

إرشادات تطبيق الضوابط:

- التأكد والتحقق من استخدام إجراءات الحماية المناسبة؛ مثل الأقفال على جميع الخزائن (Cabinets) التي تحتوي على أنظمة تحكم (Control Systems).
- التأكد والتحقق من حماية جميع الأصول الخاصة بأنظمة التحكم الصناعي (OT/ICS) من الوصول المادي الغير مصرح به تماشياً مع الآليات المعتمدة في الجهة.

المخرجات المتوقعة:

- زيارة ميدانية للتحقق من استخدام إجراءات الحماية المناسبة للمواقع التالية:
  - الوصول المادي للمنشآت الصناعية.
  - الخزائن (Cabinets) التي تحتوي على أنظمة تحكم (Control Systems).
  - غرفة التحكم المركزية (CCR).

٢-١٣-١-٥	تطبيق قيود صارمة على صلاحيات الوصول المادي، لجميع أصول أجهزة وأنظمة التحكم الصناعي؛ بما في ذلك أنظمة معدات السلامة (SIS).

أدوات الأمن السيبراني ذات العلاقة:

- نموذج سياسة الأمن السيبراني للأنظمة التشغيلية
- نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS)
- نموذج سياسة الأمن المادي
- نموذج معيار الأمن المادي

إرشادات تطبيق الضوابط:

- التأكد والتحقق من تطبيق قيود صارمة على صلاحيات الوصول المادي، لجميع أصول أجهزة وأنظمة التحكم الصناعي؛ بما في ذلك أنظمة معدات السلامة (SIS).

المخرجات المتوقعة:

- زيارة ميدانية للتحقق من تطبيق قيود صارمة على صلاحيات الوصول المادي، لجميع أصول أجهزة وأنظمة التحكم الصناعي؛ بما في ذلك أنظمة معدات السلامة (SIS).

٢-١٣-١-٦	الاحتفاظ بسجلات دخول الزوار إلى المناطق الحساسة، والتي تحتوي على أنظمة التحكم الصناعي (OT/ICS).

أدوات الأمن السيبراني ذات العلاقة:

- نموذج سياسة الأمن السيبراني للأنظمة التشغيلية
- نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS)
- نموذج سياسة الأمن المادي
- نموذج معيار الأمن المادي

إرشادات تطبيق الضوابط:

- التأكد من الاحتفاظ بسجلات دخول الزوار إلى المناطق الحساسة، والتي تحتوي على أنظمة التحكم الصناعي (OT/ICS).
- التأكد من أن الزوار يقومون بتسجيل معلوماتهم أثناء الدخول إلى المناطق الحساسة، والتي تحتوي على أنظمة التحكم الصناعي (OT/ICS).

المخرجات المتوقعة:

- سجل الزوار الخاص بالمناطق الحساسة، والتي تحتوي على أنظمة التحكم الصناعي (OT/ICS).
- زيارة ميدانية للتحقق من الاحتفاظ بسجلات دخول الزوار إلى المناطق الحساسة، والتي تحتوي على أنظمة التحكم الصناعي (OT/ICS).

٢-١٣-١-٧	مراقبة الأعمال، التي يتم تأديتها من المقاولين، أو الموظفين التابعين للموردين، ومزودي الخدمات.

أدوات الأمن السيبراني ذات العلاقة:

- نموذج سياسة الأمن السيبراني للأنظمة التشغيلية
- نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS)
- نموذج سياسة الأمن المادي
- نموذج معيار الأمن المادي

إرشادات تطبيق الضوابط:

- تحديد المتطلبات الخاصة بمراقبة الأعمال، التي يتم تأديتها من قبل المقاولين. جميع المتطلبات يجب أن توثق وأن تكون متماشية مع الوثائق ذات العلاقة على سبيل المثال لا الحصر، وثائق تصاريح العمل (work permits).
- تحديد وتجهيز سجل مراقبة الأعمال، التي يتم تأديتها من المقاولين.
- التأكد والتحقق من مراقبة الأعمال، التي يتم تأديتها من المقاولين، أو الموظفين التابعين للموردين، ومزودي الخدمات.

المخرجات المتوقعة:

- وثيقة المتطلبات الخاصة بمراقبة الأعمال، التي يتم تأديتها من المقاولين.
- إثبات يؤكد مراقبة الأعمال، التي يتم تأديتها من المقاولين، أو الموظفين التابعين للموردين، ومزودي الخدمات.

	٢-١٣-١-٨	تزويد حراس الأمن بالمهارات المتخصصة، والتدريب اللازم، بما يتوافق مع المهمات والمسؤوليات المنوطة بهم؛ فيما يتعلق بالأمن المادي لأنظمة التحكم الصناعي (OT/ICS).
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • نموذج سياسة الأمن المادي • نموذج معيار الأمن المادي **إرشادات تطبيق الضوابط:** • التأكد من تزويد موظفي الأمن الصناعي (في المرافق والمعامل) بالمهارات المتخصصة، والتدريب اللازم، بما يتوافق مع المهمات والمسؤوليات المنوطة بهم؛ فيما يتعلق بالأمن المادي لأنظمة التحكم الصناعي (OT/ICS).	
	المخرجات المتوقعة: • قائمة موثقة بأسماء موظفي الأمن الصناعي الذين تم تزويدهم بالمهارات المتخصصة، والتدريب اللازم. • إثبات يؤكد تزويد موظفي الأمن الصناعي (في المرافق والمعامل) بالمهارات المتخصصة، والتدريب اللازم، بما يتوافق مع المهمات والمسؤوليات المنوطة بهم؛ فيما يتعلق بالأمن المادي لأنظمة التحكم الصناعي (OT/ICS).	
	٢-١٣-١-٩	اختبار إمكانيات الأمن المادي وجاهزيته بشكل دوري؛ من خلال عمل تمارين المحاكاة (مثل : الهندسة الاجتماعية).
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • نموذج سياسة الأمن المادي • نموذج معيار الأمن المادي **إرشادات تطبيق الضوابط:** • التأكد من اختبار إمكانيات الأمن المادي وجاهزيته بشكل دوري (بناء على فترات زمنية محددة)؛ من خلال عمل تمارين المحاكاة (مثل :الهندسة الاجتماعية).	
	المخرجات المتوقعة: • قائمة موثقة بتمارين محاكاة للهجمات السيبرانية (cybersecurity drills, tabletop exercises). • إثبات يؤكد اختبار إمكانيات الأمن المادي وجاهزيته بشكل دوري (بناء على فترات زمنية محددة)؛ من خلال عمل تمارين المحاكاة (مثل :الهندسة الاجتماعية).	
٢-١٣-٢	رجوعاً للضابط ٢-١٤-٤ في الضوابط الأساسية للأمن السيبراني؛ يجب مراجعة متطلبات الأمن السيبراني لإدارة الأمن المادي في بيئة أنظمة التحكم الصناعي (OT/ICS)، وقياس فعالية تطبيقها، وتقييمها دورياً.	
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS)	

	• نموذج سياسة الأمن المادي • نموذج تقرير مؤشرات الأداء الرئيسية **إرشادات تطبيق الضوابط:** • العمل على مراجعة متطلبات الأمن السيبراني لإدارة الأمن المادي في بيئة أنظمة التحكم الصناعي (OT/ICS) بشكل دوري حسب خطة موثقة ومعتمدة للمراجعة بناءً على فترة زمنية محددة (على سبيل المثال، يتم إجراء المراجعة الدورية بشكل سنوي). • العمل على تطوير مؤشرات أداء رئيسية (KPIs) لكل الضوابط المتضمنة بداخل السياسات أو الإجراءات للتأكد من قياس فعالية تطبيقها، وتقييمها دورياً بناءً على فترة زمنية محددة (على سبيل المثال، يتم إجراء المراجعة الدورية بشكل سنوي). **المخرجات المتوقعة:** • إثبات يؤكد القيام بالمراجعة الدورية لمتطلبات الأمن السيبراني لإدارة الأمن المادي في بيئة أنظمة التحكم الصناعي (OT/ICS). • إثبات يؤكد القيام بقياس مؤشرات الأداء الرئيسية (KPIs) لكل الضوابط المتضمنة بداخل السياسات أو الإجراءات للتأكد من قياس فعالية تطبيقها، وتقييمها دورياً بناءً على فترة زمنية محددة.

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 أنظمة التحكم الصناعي (OT/ICS) جراء الكوارث الناتجة عن المخاطر السيبرانية.	
الضوابط		
١-١-٣	بالإضافة للضوابط الفرعية ضمن الضابط ٣-١-٣ في الضوابط الأساسية للأمن السيبراني؛ يجب أن تغطي متطلبات صمود الأمن السيبراني في إدارة استمرارية الأعمال المتعلقة بأنظمة التحكم الصناعي (OT/ICS) بحد أدنى ما يلي:	
	١-١-١-٣	تحديد الأنشطة اللازمة، للمحافظة على الحد الأدنى من العمليات المتعلقة بأنظمة التحكم الصناعي (OT/ICS).
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • نموذج سياسة الأمن السيبراني في إدارة استمرارية الأعمال **إرشادات تطبيق الضوابط:** • تحديد قائمة بالأنظمة التشغيلية الحساسة والأنشطة اللازمة، للمحافظة على الحد الأدنى من عمل تلك الأنظمة وذلك بالتنسيق مع موظفي المرافق الصناعية. • القيام بالاختبارات اللازمة للتأكد من الأنشطة التي تم تحديدها ما إذا كانت كافية للمحافظة على الحد الأدنى من عمل الأنظمة التشغيلية الحساسة.	
	المخرجات المتوقعة: • قائمة موثقة بالأنظمة التشغيلية الحساسة لدى المرفق. • قائمة موثقة بالأنشطة الضرورية للمحافظة على الحد الأدنى من عمل الأنظمة التشغيلية الحساسة. • نماذج الاختبارات اللازمة للتأكد من الأنشطة التي تم تحديدها ما إذا كانت كافية للمحافظة على الحد الأدنى من عمل الأنظمة التشغيلية الحساسة.	
	٢-١-١-٣	تطبيق التوافر (Redundancy) للشبكات، والوسائط، والأجهزة الحساسة لأصول أنظمة التحكم الصناعي (OT/ICS) وفقاً للتقييم الدوري لمخاطر الأمن السيبراني، لأصول أنظمة التحكم الصناعي (OT/ICS).
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية	

	• نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • نموذج سياسة الأمن السيبراني في إدارة استمرارية الأعمال **إرشادات تطبيق الضوابط:** • إجراء تقييم مخاطر دوري وذلك بناء على الخطة الدورية لتقييم المخاطر. • بناء على تقييم المخاطر يتم تحديد وتوثيق المناطق والأنظمة التي من الضروري أن تطبق التوافرية (Redundancy). • تطبيق التوافرية (Redundancy) للشبكات، والوسائط، والأجهزة الحساسة لأصول أنظمة التحكم الصناعي (OT/ICS) وفقاً للتقييم الدوري لمخاطر الأمن السيبراني.
	المخرجات المتوقعة: • التقرير الدوري لتقييم المخاطر. • قائمة موثقة بالمناطق والأنظمة التي من الضروري أن تطبق التوافرية (Redundancy). • زيارة ميدانية للتحقق من تطبيق التوافرية (Redundancy) للشبكات، والوسائط، والأجهزة الحساسة لأصول أنظمة التحكم الصناعي (OT/ICS) وفقاً للتقييم الدوري لمخاطر الأمن السيبراني.
٣-١-١-٣	تضمين متطلبات الأمن السيبراني، المتعلقة بأنظمة التحكم الصناعي (OT/ICS) إلى خطة استمرارية الأعمال (BCP)؛ تحليل التأثر على الأعمال (BIA)، ووقت الاستعادة المستهدف (RTO)، ونقطة الاستعادة المستهدفة (RPO).
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • نموذج سياسة الأمن السيبراني في إدارة استمرارية الأعمال **إرشادات تطبيق الضوابط:** • تحديد وتوثيق متطلبات الأمن السيبراني، المتعلقة بأنظمة التحكم الصناعي (OT/ICS) إلى خطة استمرارية الأعمال (BCP)؛ تحليل التأثر على الأعمال (BIA)، ووقت الاستعادة المستهدف (RTO)، ونقطة الاستعادة المستهدفة (RPO). • تضمين المتطلبات المحددة والمعرفة إلى خطة استمرارية الأعمال (BCP)؛ تحليل التأثر على الأعمال (BIA)، ووقت الاستعادة المستهدف (RTO)، ونقطة الاستعادة المستهدفة (RPO). • التأكد والتحقق من أن متطلبات الأمن السيبراني، المتعلقة بأنظمة التحكم الصناعي (OT/ICS) توائم وتتوافق مع المتطلبات العامة للجهة.
	المخرجات المتوقعة: • وثيقة متطلبات الأمن السيبراني، المتعلقة بأنظمة التحكم الصناعي (OT/ICS). • إثبات يؤكد تضمين المتطلبات المحددة والمعرفة إلى خطة استمرارية الأعمال (BCP)؛ تحليل التأثر على الأعمال (BIA)، ووقت الاستعادة المستهدف (RTO)، ونقطة الاستعادة المستهدفة (RPO).

٣-١-١-٤	تضمين متطلبات الأمن السيبراني المتعلقة بأنظمة التحكم الصناعي (OT/ICS) ضمن خطط التعافي من الكوارث (DRP)، بحيث تشمل سيناريوهات الكوارث المتعلقة بالأمن السيبراني، وإجراءات التعامل مع توقف النظام، وإجراءات إدارة العمليات التشغيلية.

أدوات الأمن السيبراني ذات العلاقة:

- نموذج سياسة الأمن السيبراني للأنظمة التشغيلية
- نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS)
- نموذج سياسة الأمن السيبراني في إدارة استمرارية الأعمال

إرشادات تطبيق الضوابط:

- تحديد وتوثيق متطلبات الأمن السيبراني المتعلقة بأنظمة التحكم الصناعي (OT/ICS) ضمن خطط التعافي من الكوارث (DRP).
- تضمين المتطلبات المحددة والمعرفة ضمن خطط التعافي من الكوارث (DRP)، بحيث تشمل التالي:
  - سيناريوهات الكوارث المتعلقة بالأمن السيبراني.
  - إجراءات التعامل مع توقف النظام.
  - إجراءات إدارة العمليات التشغيلية.

المخرجات المتوقعة:

- وثيقة متطلبات الأمن السيبراني، المتعلقة بأنظمة التحكم الصناعي (OT/ICS).
- إثبات يؤكد تضمين متطلبات الأمن السيبراني المتعلقة بأنظمة التحكم الصناعي (OT/ICS) ضمن خطط التعافي من الكوارث (DRP)، بحيث تشمل سيناريوهات الكوارث المتعلقة بالأمن السيبراني، وإجراءات التعامل مع توقف النظام، وإجراءات إدارة العمليات التشغيلية.

٣-١-١-٥	عند فشل الأنظمة بسبب حادثة أمن سيبراني؛ يجب أن تكون أنظمة التحكم الصناعي (OT/ICS) قادرة على العمل بمستوى أمان مقبول، أو بأوضاع تسمح باستمرارية العمل.

أدوات الأمن السيبراني ذات العلاقة:

- نموذج سياسة الأمن السيبراني للأنظمة التشغيلية
- نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS)
- نموذج سياسة الأمن السيبراني في إدارة استمرارية الأعمال

إرشادات تطبيق الضوابط:

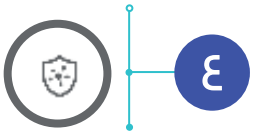
- تطوير وتطبيق إجراءات معالجة فشل الأنظمة.
- التأكد والتحقق من أن تكون أنظمة التحكم الصناعي (OT/ICS) قادرة على العمل بمستوى أمان مقبول، أو بأوضاع تسمح باستمرارية العمل.

المخرجات المتوقعة:

- وثيقة إجراءات معالجة فشل الأنظمة.
- إثبات يؤكد بأن تكون أنظمة التحكم الصناعي (OT/ICS) قادرة على العمل بمستوى أمان مقبول، أو بأوضاع تسمح باستمرارية العمل.

	٣-١-١-٦	إجراء اختبارات وتمارين المحاكاة، بشكل دوري (مثل "Tabletop Exercises "TTX) من أجل اختبار فعالية أنظمة التحكم الصناعي (OT/ICS) المتعلقة بخطط التعافي من الكوارث (DRP) وخطة استمرارية العمل (BCP) وإجراء تحليل الأسباب الجذرية (Root Cause Analysis) للحوادث.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • نموذج سياسة الأمن السيبراني في إدارة استمرارية الأعمال **إرشادات تطبيق الضوابط:** • إجراء اختبارات وتمارين المحاكاة، بشكل دوري (مثل "Tabletop Exercises "TTX) من أجل اختبار فعالية أنظمة التحكم الصناعي (OT/ICS) المتعلقة بخطط التعافي من الكوارث (DRP) وخطة استمرارية العمل (BCP) وإجراء تحليل الأسباب الجذرية (Root Cause Analysis) للحوادث. • توثيق التقارير الخاصة بنتائج اختبارات وتمارين المحاكاة.	
	المخرجات المتوقعة: • وثائق خطط استمرارية الأعمال وخطط الاستعادة من الكوارث وخطط إجراء اختبارات المحاكاة ذات العلاقة بأنظمة التحكم الصناعي (OT/ICS). • التقارير الدورية باختبارات وتمارين المحاكاة (مثل "Tabletop Exercises "TTX). • إثبات يؤكد فعالية أنظمة التحكم الصناعي (OT/ICS) المتعلقة بخطط التعافي من الكوارث (DRP) وخطة استمرارية العمل (BCP) وإجراء تحليل الأسباب الجذرية (Root Cause Analysis) للحوادث.	
٣-١-٢	رجوعاً للضابط ٣-١-٤ في الضوابط الأساسية للأمن السيبراني؛ يجب مراجعة متطلبات الأمن السيبراني لجوانب صمود الأمن السيبراني في إدارة استمرارية الأعمال لبيئة أنظمة التحكم الصناعي (OT/ICS)، وقياس فعالية تطبيقها وتقييمها دورياً.	
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • نموذج سياسة الأمن السيبراني في إدارة استمرارية الأعمال • نموذج تقرير مؤشرات الأداء الرئيسية **إرشادات تطبيق الضوابط:** • العمل على مراجعة متطلبات الأمن السيبراني لجوانب صمود الأمن السيبراني في إدارة استمرارية الأعمال لبيئة أنظمة التحكم الصناعي (OT/ICS) بشكل دوري حسب خطة موثقة ومعتمدة للمراجعة بناءً على فترة زمنية محددة (على سبيل المثال، يتم إجراء المراجعة الدورية بشكل سنوي). • العمل على تطوير مؤشرات أداء رئيسية (KPIs) لكل الضوابط المتضمنة بداخل السياسات أو الإجراءات للتأكد من قياس فعالية تطبيقها، وتقييمها دورياً بناءً على فترة زمنية محددة (على سبيل المثال، يتم إجراء المراجعة الدورية بشكل سنوي).	

	المخرجات المتوقعة: • إثبات يؤكد القيام بالمراجعة الدورية لمتطلبات الأمن السيبراني لجوانب صمود الأمن السيبراني في إدارة استمرارية الأعمال لبيئة أنظمة التحكم الصناعي (OT/ICS). • إثبات يؤكد القيام بقياس مؤشرات الأداء الرئيسية (KPIs) لكل الضوابط المتضمنة بداخل السياسات أو الإجراءات للتأكد من قياس فعالية تطبيقها، وتقييمها دورياً بناءً على فترة زمنية محددة.



٤ الأمن السيبراني المتعلق بالأطراف الخارجية
(Third-Party Cybersecurity)

٤-١	الأمن السيبراني المتعلق بالأطراف الخارجية (Third-Party Cybersecurity)	
الهدف	ضمان حماية أصول الجهة من مخاطر الأمن السيبراني، المتعلقة بالأطراف الخارجية؛ بما في ذلك مصنعو أجهزة وأنظمة التحكم الصناعي (OT/ICS)، ومقاولو منتجات أنظمة التحكم الصناعي (OT/ICS) وموردو خدمات أنظمة التحكم الصناعي (OT/ICS) وفقاً للسياسات والإجراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية ذات العلاقة.	
الضوابط		
٤-١-١	بالإضافة للضوابط الفرعية ضمن الضابط ٤-١-٢ و ٤-١-٣ في الضوابط الأساسية للأمن السيبراني؛ يجب أن تغطي متطلبات الأمن السيبراني للأطراف الخارجية، المتعلقة بأنظمة التحكم الصناعي (OT/ICS) بحد أدنى ما يلي:	
	٤-١-١-١	تضمين متطلبات الأمن السيبراني، أثناء دورة حياة المشتريات، لمنتجات وخدمات أنظمة التحكم الصناعي (OT/ICS).
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • نموذج سياسة الأمن السيبراني المتعلق بالأطراف الخارجية **إرشادات تطبيق الضوابط:** • تحديد وتوثيق واعتماد متطلبات الأمن السيبراني لمنتجات وخدمات أنظمة التحكم الصناعي (OT/ICS)، أثناء دورة حياة المشتريات (تحديد المتطلبات، اختيار المورد، التفاوض، التعاقد، تسليم الخدمات، مراقبة الأداء، التجديد/إغلاق العقد). • التأكد من تضمين متطلبات الأمن السيبراني، أثناء دورة حياة المشتريات، لمنتجات وخدمات أنظمة التحكم الصناعي (OT/ICS).	
	المخرجات المتوقعة: • وثيقة متطلبات الأمن السيبراني لمنتجات وخدمات أنظمة التحكم الصناعي (OT/ICS)، أثناء دورة حياة المشتريات. • إثبات يؤكد تضمين متطلبات الأمن السيبراني على جميع المشتريات الجديدة الخاصة بأنظمة التحكم الصناعي (OT/ICS).	
	٤-١-١-٢	تحديد متطلبات الأمن السيبراني، لتقييم الأطراف الخارجية واختيارهم ومشاركتهم المعلومات.

أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • نموذج سياسة الأمن السيبراني المتعلق بالأطراف الخارجية **إرشادات تطبيق الضوابط:** • تحديد وتوثيق واعتماد متطلبات الأمن السيبراني لتقييم الأطراف الخارجية واختيارهم ومشاركتهم المعلومات. • التأكد من تضمين متطلبات الأمن السيبراني في وثيقة المتطلبات التأهيلية (Qualification requirements). **المخرجات المتوقعة:** • وثيقة متطلبات الأمن السيبراني لتقييم الأطراف الخارجية واختيارهم ومشاركتهم المعلومات. • وثيقة المتطلبات التأهيلية (Qualification requirements) موضحاً تضمين متطلبات الأمن السيبراني بها. • إثبات يؤكد تقييم الأطراف الخارجية واختيارهم ومشاركتهم المعلومات بناءً على المتطلبات المحددة والمعرّفة مسبقاً.	
٤-١-١-٣	استخدام المتعاقدين والموردين الخارجيين ممارسات رسمية وموثقة لدورة حياة التطوير الآمن (SDLC) للبرامج الخاصة بالأنظمة والأصول المصممة أو المطبقة في بيئة أنظمة التحكم الصناعي (OT/ICS).
أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • نموذج سياسة الأمن السيبراني المتعلق بالأطراف الخارجية **إرشادات تطبيق الضوابط:** • الحصول على شهادة من المقاولين والموردين الخارجيين التي تستخدم ممارسات رسمية وموثقة لدورة حياة التطوير الآمن (SDLC) للبرامج الخاصة بالأنظمة والأصول المصممة أو المطبقة في بيئة أنظمة التحكم الصناعي (OT/ICS). **المخرجات المتوقعة:** • شهادة من المقاولين والموردين الخارجيين المعتمدين تؤكد بأنهم يستخدمون ممارسات رسمية وموثقة لدورة حياة التطوير الآمن (SDLC) للبرامج الخاصة بالأنظمة والأصول المصممة أو المطبقة في بيئة أنظمة التحكم الصناعي (OT/ICS).	
٤-١-١-٤	إجراء تقييم للأمن السيبراني وتدقيق له، بشكل دوري للأطراف الخارجية؛ والتأكد من وجود ما يضمن السيطرة، على أي مخاطر سيبرانية تم رصدها.
أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية	

	• نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • نموذج سياسة الأمن السيبراني المتعلق بالأطراف الخارجية **إرشادات تطبيق الضوابط:** • إجراء تقييم للأمن السيبراني وتدقيق له، بشكل دوري للأطراف الخارجية؛ والتأكد من وجود ما يضمن السيطرة، على أي مخاطر سيبرانية تم رصدها. **المخرجات المتوقعة:** • تقارير التقييمات السيبرانية والتدقيق للأطراف الخارجية.
٤-١-٢	رجوعاً للضابط ٤-١-٤ في الضوابط الأساسية للأمن السيبراني؛ يجب مراجعة متطلبات الأمن السيبراني للأمن السيبراني للأطراف الخارجية، لبيئة أنظمة التحكم الصناعي (OT/ICS)، وقياس فعالية تطبيقها وتقييمها دورياً. **أدوات الأمن السيبراني ذات العلاقة:** • نموذج سياسة الأمن السيبراني للأنظمة التشغيلية • نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS) • نموذج سياسة الأمن السيبراني المتعلق بالأطراف الخارجية • نموذج تقرير مؤشرات الأداء الرئيسية **إرشادات تطبيق الضوابط:** • العمل على مراجعة متطلبات الأمن السيبراني للأمن السيبراني للأطراف الخارجية لبيئة أنظمة التحكم الصناعي (OT/ICS) بشكل دوري حسب خطة موثقة ومعتمدة للمراجعة بناءً على فترة زمنية محددة (على سبيل المثال، يتم إجراء المراجعة الدورية بشكل سنوي). • العمل على تطوير مؤشرات أداء رئيسية (KPIs) لكل الضوابط المتضمنة بداخل السياسات أو الإجراءات للتأكد من قياس فعالية تطبيقها، وتقييمها دورياً بناءً على فترة زمنية محددة (على سبيل المثال، يتم إجراء المراجعة الدورية بشكل سنوي). **المخرجات المتوقعة:** • إثبات يؤكد القيام بالمراجعة الدورية لمتطلبات الأمن السيبراني للأمن السيبراني للأطراف الخارجية لبيئة أنظمة التحكم الصناعي (OT/ICS). • إثبات يؤكد القيام بقياس مؤشرات الأداء الرئيسية (KPIs) لكل الضوابط المتضمنة بداخل السياسات أو الإجراءات للتأكد من قياس فعالية تطبيقها، وتقييمها دورياً بناءً على فترة زمنية محددة.


الهيئة الوطنية
للأمن السيبراني
National Cybersecurity Authority