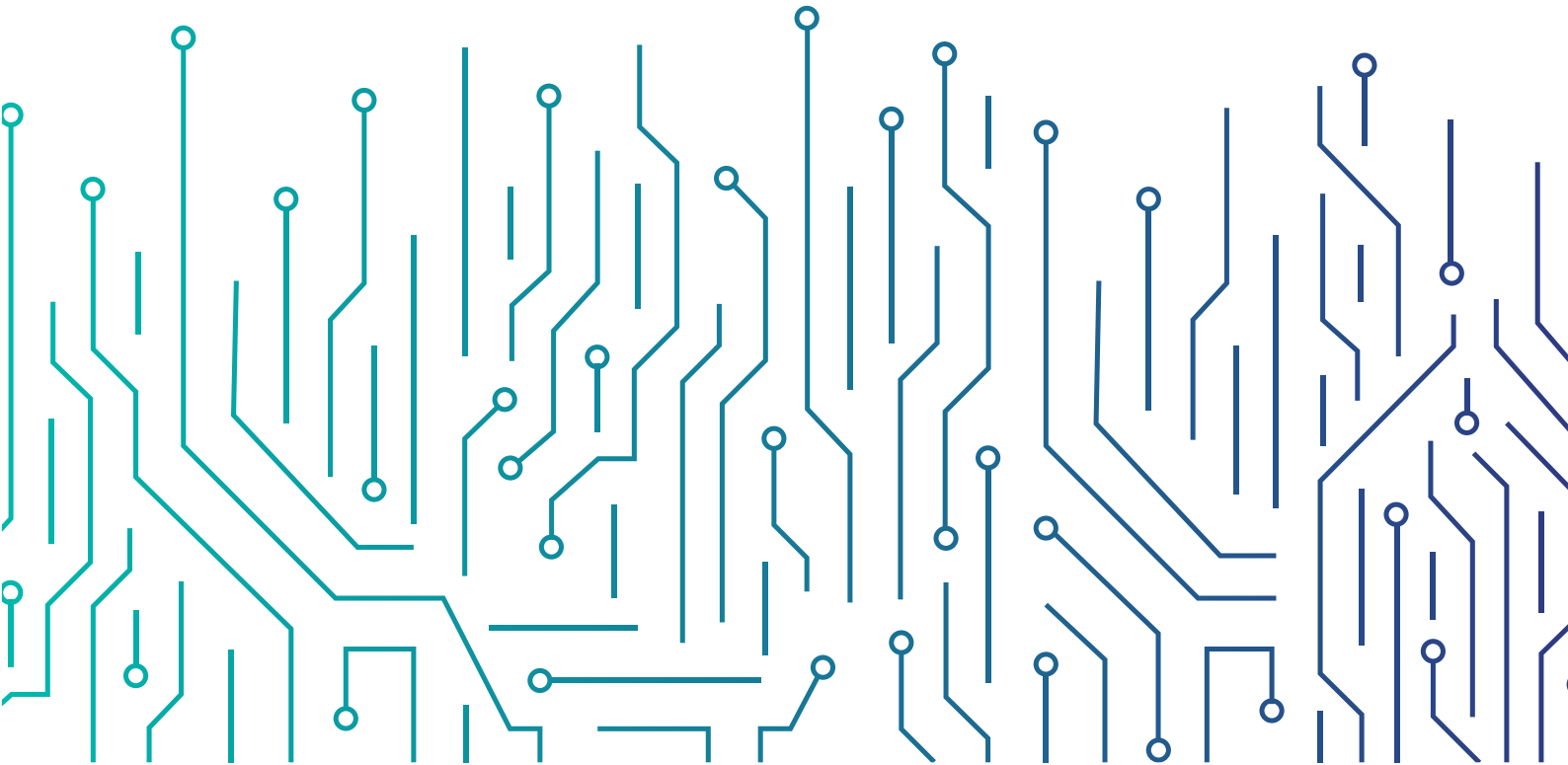
الهيئة الوطنية للأمن السيبـراني
National Cybersecurity Authority

ضوابط الأمن السيبراني
للأنظمة التشغيلية

Operational Technology Cybersecurity Controls
(OTCC -1: 2022)

إشـــارة المـــشـــاركـــة: أبـيـض
تـصـنـيـف الـوثـيـقـة: عـام



بسم الله الرحمن الرحيم

بروتوكول الإشارة الضوئية (TLP):

يستخدم هذا البروتوكول على نطاق واسع في العالم وهناك أربعة ألوان (إشارات ضوئية):

أحمر – شخصي وسري للمستلم فقط

المستلم لا يحق له مشاركة المصنف بالإشارة الحمراء مع أي فرد سواء من داخل أو خارج الجهة خارج النطاق المحدد للاستلام.

برتقالي – مشاركة محدودة

المستلم يمكنه مشاركة المعلومات في نفس الجهة مع الأشخاص المعنيين فقط، ومن يتطلب الأمر منه اتخاذ إجراء يخص المعلومة.

أخضر – مشاركة في نفس المجتمع

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

أبيض – غير محدود

قائمة المحتويات

قائمة الجداول

قائمة الأشكال والرسوم التوضيحية

الملخص التنفيذي

جاءت مهمات الهيئة الوطنية للأمن السيبراني واختصاصاتها، ملبيةً لجوانب وضع السياسات، وآليات الحوكمة، والأطر، والمعايير، والضوابط والإرشادات المتعلقة بالأمن السيبراني، وتعميمها على الجهات ذات العلاقة؛ بما يعزز الأمن السيبراني، وأهميته، والحاجة الملحة له، مع ازدياد التهديدات والمخاطر الأمنية في الفضاء السيبراني أكثر من أي وقت مضى.

يشـهد العالم تطوراً مستمراً في الأنظمة التشغيلية وأنظمة التحكم الصناعي، والتي يصاحبها تزايد مستمر في التهديدات السيبرانية لتلك الأنظمة. وأظهر ذلك، الحاجة لوجود ضوابط للأمن السيبراني، للتعامل مع هذه التهديدات، لحماية البنى التحتية الحساسة على ضوء أفضل الممارسات العالمية في هذا المجال.

وعلى هذا؛ فقد تم إصدار وثيقة ضوابط الأمن السيبراني للأنظمة التشغيلية (OTCC-1: 2022) التي تهدف للتقليل من المخاطر السيبرانية على الجهات ذات العلاقة. وتوضح هذه الوثيقة أهداف الضوابط، ونطاق عملها، وقابليتها للتطبيق، وآلية الالتزام؛ ولتكون بذلك امتداداً للضوابط الأساسية للأمن السيبراني (ECC-1:2018) وتابعة ومكملة لها. وتشمل أنظمة التحكم الصناعي جميع الأجهزة، والأنظمة، و الشبكات المستخدمة لتشغيل و/أو أتمتة العمليات الصناعية.

وعلى مختلف الجهات ضمن نطاق عمل هذه الضوابط تنفيذ ما يحقق الالتزام الدائم والمستمر بهذه الضوابط، تحقيقاً لما ورد في الفقرة الثالثة من المادة العاشرة في تنظيم الهيئة الوطنية للأمن السيبراني، وكـذلـك مـا ورد فـي الأمر السامي الكريم رقم (٥٧٢٣١) وتاريخ ١٤٣٩/١١/١٠ هـ.

المقدمة

قامت الهيئة الوطنية للأمن السيبراني (ويشار لها في الوثيقة بـ "الهيئة") بإصدار هذه الضوابط، بعد دراسة عدة معايير وأطر وضوابط أمن سيبراني؛ تم إعدادها من قِبل منظمات وجهات محلية ودولية، كما أطلعت على أفضل الممارسات، والتجارب ذات العلاقة في مجال الأمن السيبراني. وقد تم عمل دراسة مواءمة مع عدد من الضوابط والمعايير الدولية.

تتكون ضوابط الأمن السيبراني للأنظمة التشغيلية من:

- ٤ مكونات أساسية (4 Main Domains).
- ٢٣ مكوناً فرعياً (23 Subdomains).
- ٤٧ ضابطاً أساسياً (47 Main Controls).
- ١٢٢ ضابطاً فرعياً (122 Subcontrols).

الأهداف

تهدف هذه الضوابط إلى الإسهام في رفع مستويات الأمن السيبراني على المستوى الوطني من خلال التركيز على أنظمة التحكم الصناعي، وتحديد متطلبات الأمن السيبراني لها، مع الإسهام في تمكين الجهات ذات العلاقة؛ من العمل على تحقيق هذه المتطلبات، لتلبية الاحتياجات الأمنية، وحمايتاً للبنى التحتية الحساسة، ورفع مستوى جاهزيتها تجاه المخاطر السيبرانية.

وتأخذ هذه الضوابط في الحسبان المحاور الأربعة الأساسية التي يعتمد عليها الأمن السيبراني، وهي:

- الإستراتيجية (Strategy).
- الأشخاص (People).
- الإجراء (Process).
- التقنية (Technology).

نطاق العمل وقابلية التطبيق

نطاق عمل الضوابط

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 INFRASTRUCTURES "CNIs") أو تقوم بتشغيلها، أو استضافتها داخل المملكة العربية السعودية؛ أو خارجها، (ويشار لها جميعاً في هذه الوثيقة ب"الجهة"). ويتم تعريف المرافق الحساسة على أنها المرافق التي يكون في تعطلها أو وجود تغيير غير مشروع في أنظمتها أثر سلبي على توافر الخدمات، أو اعمال الجهة العامة، أو إحداث آثار اقتصادية أو أمنية، أو اجتماعية سلبية كبيرة، على المستوى الوطني. وتشمل أنظمة التحكم الصناعي جميع الأجهزة، والأنظمة، والشبكات المستخدمة لتشغيل العمليات الصناعية أو أتمتتها.

كما تشجع الهيئة الجهات الأخرى في المملكة وبشدة على الاستفادة من هذه الضوابط لتطبيق أفضل الممارسات فيما يتعلق برفع مستوى الأمن السيبراني وتطويره داخل الجهة.

قابلية التطبيق داخل الجهة

تم إعداد هذه الضوابط بحيث تكون ملائمة لاحتياجات الأمن السيبراني لأنظمة التحكم الصناعي ومتطلباته، ويجب على كل جهة في نطاق هذه الوثيقة الالتزام بجميع الضوابط القابلة للتطبيق، بعد قياس مدى التأثير، وإجراء الفحوصات اللازمة قبل التطبيق.

التنفيذ والالتزام

تحقيقاً لما ورد في الفقرة الثالثة من المادة العاشرة، من تنظيم الهيئة الوطنية للأمن السيبراني، وكـذلـك مـا ورد فـي الأمر السامي الكريم رقم (٥٧٢٣١) وتاريخ ١٤٣٩/١١/١٠ هـ؛ يجب على جميع الجهات، ضمن نطاق عمل هذه الضوابط؛ تنفيذ ما يحقق الالتزام الدائم والمستمر بهذه الضوابط، ولا يمكن تحقيق ذلك إلا من خلال تحقيق الالتزام الدائم، والمستمر بالضوابط الأساسية للأمن السيبراني (ECC-1:2018) وفقاً لقابلية تطبيقها في الجهة بحسب طبيعة أعمالها.

وتقوم الهيئة بتقييم التزام الجهات، بما ورد في هذه الضوابط، بطرق متعددة؛ منها: التقييم الذاتي للجهات، و/أو الزيارات الميدانية للتدقيق، وفقاً للآلية المناسبة التي تراها الهيئة.

أداة التقييم وقياس الالتزام

تقوم الهيئة بإصدار أداة (OTCC-1:2022 ASSESSMENT AND COMPLIANCE TOOL) لتنظيم عملية تقييم مدى التزام الجهات بتطبيق ضوابط الأمن السيبراني للأنظمة التشغيلية.

أداة حصر وتحديد مستوى المرفق

تقوم الهيئة بإصدار أداة (OTCC-1:2022 FACILITY LEVEL IDENTIFICATION TOOL) لتنظيم عملية الحصر وتحديد مستويات المرافق الحساسة، التي تتضمن أنظمة التحكم الصناعي.

التحديث والمراجعة

تتولى الهيئة التحديث والمراجعة الدورية، لضوابط الأمن السيبراني لأنظمة التحكم الصناعي، حسب متطلبات الأمن السيبراني، والمستجدات ذات العلاقة. كما تتولى الهيئة، إعلان الإصدار المحدث من الضوابط؛ لتطبيقه والالتزام به.

ملحق المنهجية والمواءمة لضوابط الأمن السيبراني للأنظمة التشغيلية

قامت الهيئة بتطوير وثيقة ملحق المنهجية والمواءمة لضوابط الأمن السيبراني للأنظمة التشغيلية. ويعد هذا الملحق جزءًا من وثيقة ضوابط الأمن السيبراني للأنظمة التشغيلية؛ ويحتوي على:

- مبادئ تصميم ضوابط الأمن السيبراني للأنظمة التشغيلية.
- العلاقة بين ضوابط الأمن السيبراني للأنظمة التشغيلية (OTCC-1:2022) والمكون الأساسي الخامس من الضوابط الأساسية للأمن السيبراني.
- العلاقة بين ضوابط الأمن السيبراني للأنظمة التشغيلية، والمعايير الدولية الأخرى.
- منهجية تصميم ضوابط الأمن السيبراني للأنظمة التشغيلية.
- منهجية تحديد المستويات الأساسية والفرعية، لضوابط الأمن السيبراني للأنظمة التشغيلية، وتحديد قابلية تطبيقها.

مستويات ضوابط الأمن السيبراني للأنظمة التشغيلية

تتكون ضوابط الأمن السيبراني للأنظمة التشغيلية، من ثلاثة مستويات محددة؛ وذلك اعتماداً على المعايير الآتية:

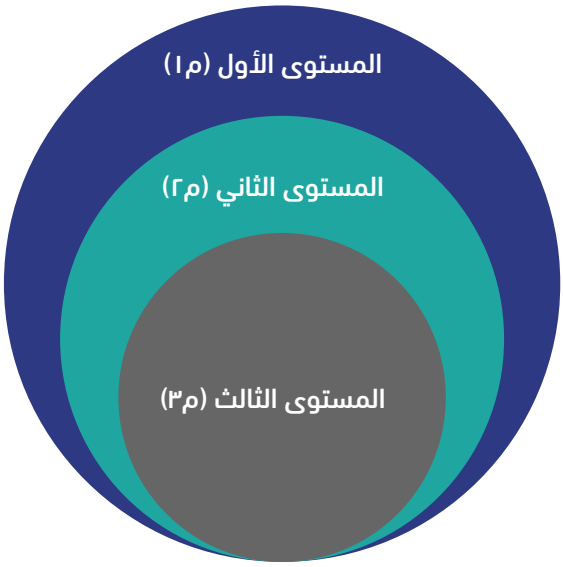
- مدى أثر المرافق على أعمال خدمات الجهة وتوافرها، وعواقب تأثرها؛ من الهجمات السيبرانية عليها.
- مدى التأثير السلبي للحوادث السيبرانية على الصحة، والسلامة، والبيئة لدى الجهة.
- مدى التأثير السلبي للحوادث السيبرانية للمرافق على الأمن الوطني، والاقتصاد الوطني، أو على الجانب الاجتماعي.

في حال أمتلكت الجهة أنظمة تحكم صناعي ذات مستويات مختلفة في نفس المرفق، فيتم تحديد مستوى المرفق بناءً على مستوى النظام الأعلى حساسية.

يوضح الجدول (١) الآتي المستويات الثلاثة للضوابط؛ بناءً على نتائج أداة حصر وتحديد مستوى المرفق:

المستوى	تعريف المستوى	عدد الضوابط
المستوى الأول (م١)	مرافق ذات حساسية عالية على الأصول، والبيئة التشغيلية، لدى الجهة من حيث الصحة، والسلامة، والبيئة.	١٥١ ضابط أساسي وفرعي (تشمل ضوابط المستوى الثاني والثالث)
المستوى الثاني (م٢)	مرافق ذات حساسية متوسطة على الأصول، والبيئة التشغيلية، لدى الجهة من حيث الصحة، والسلامة، والبيئة.	١١٧ ضابط أساسي وفرعي (تشمل ضوابط المستوى الثالث)
المستوى الثالث (م٣)	مرافق ذات حساسية منخفضة على الأصول، والبيئة التشغيلية، لدى الجهة من حيث الصحة، والسلامة، والبيئة.	٥٦ ضابط أساسي وفرعي

جدول رقم ١: مستويات ضوابط الأمن السيبراني للأنظمة التشغيلية



شكل ١: مستويات ضوابط الأمن السيبراني للأنظمة التشغيلية

يمكن الرجوع إلى وثيقة ملحق المنهجية والمواءمة، لضوابط الأمن السيبراني للأنظمة التشغيلية، للحصول على معلومات تفصيلية عن كيفية تحديد مستويات ضوابط الأمن السيبراني للأنظمة التشغيلية.

مكونات وهيكلية ضوابط الأمن السيبراني للأنظمة التشغيلية

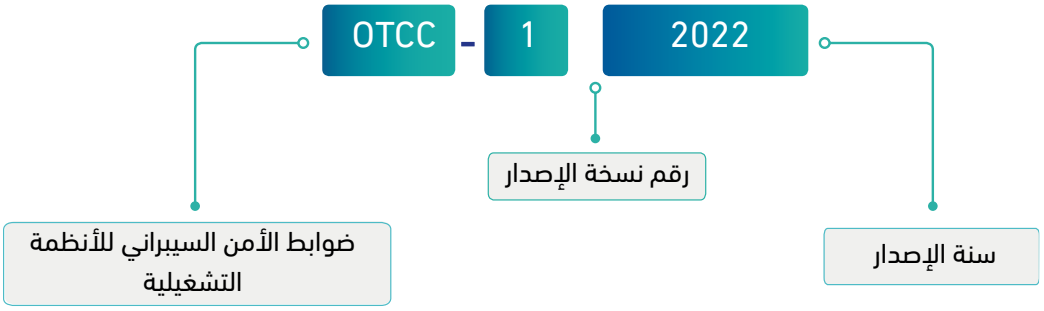
يوضح الشكل (2) الآتي المكونات الأساسية والفرعية، لضوابط الأمن السيبراني للأنظمة التشغيلية:

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

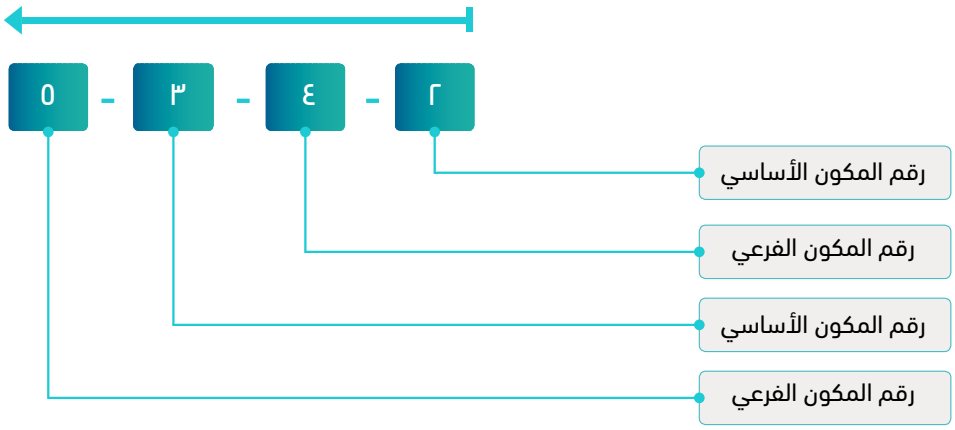
شكل ٢: المكونات الأساسية والفرعية لضوابط الأمن السيبراني للأنظمة التشغيلية

الهيكلية

يوضح الشكلان (٣) و (٤) أدناه معنى رموز ضوابط الأمن السيبراني للأنظمة التشغيلية.



شكل ٣ : معنى رموز ضوابط الأمن السيبراني لأنظمة التشغيلة



شكل ٤ : هيكلية ضوابط الأمن السيبراني للأنظمة التشغيلية

1	اسم المكون الأساسي	
رقم مرجعي للمكون الأساسي		
رقم مرجعي للمكون الفرعي	اسم المكون الفرعي	
الهدف		
الضوابط		مستوى الضابط
		١م ٢م ٣م
رقم مرجعي للضابط	بنود الضابط	✓ ✓ ✓

جدول ٢ : هيكلية ضوابط الأمن السيبراني للأنظمة التشغيلية

ضوابط الأمن السيبراني للأنظمة التشغيلية

١ حوكمة الامن 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		مستوى الضابط		
		م١	م٢	م٣
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 .	✔	✔	✔
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).	✔	✔	✔
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).	✔	✔	✔
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		مستوى الضابط		
		م١	م٢	م٣
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.	✔	✔	✔
	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.	✔	✔	
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 والإجـراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية ذات العلاقة.			
الضوابط		مستوى الضابط		
		م١	م٢	م٣
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.	✔	✔	✔

١-٣-١	١-٣-١-٢ يجب تقييم مخاطر الأمن السيبراني، لأنظمة التحكم الصناعي (OT/ICS) بشكل دوري، مع التأكد من تضمين مخاطر توقيع العقود و الاتفاقيات، مع الأطراف الخارجية المتعلقة بأنظمة التحكم الصناعي (OT/ICS) و/أو عند حدوث تغييرات بالمتطلبات التشريعية والتنظيمية، ذات العلاقة بوصفها جزء من التقييم.	✔	✔	✔
	١-٣-١-٣ 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.	✔	✔	✔
	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.	✔		
	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.	✔	✔	✔
	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.	✔	✔	✔
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 والإجـراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية ذات العلاقة.			

الضوابط		مستوى الضابط		
		م١	م٢	م٣
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).	✔	✔	✔
	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).	✔	✔	
	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).	✔	✔	✔
	١-٤-١-٤ حماية الأنظمة في البيئة التطويرية (Development Environment)، وتشمل بيئات الاختبار(Testing Environment) والمنصات التكاملية (Integration Platforms).	✔	✔	
١-٤-٢	يجب مراجعة متطلبات الأمن السيبراني، ضمن إدارة مشاريع أنظمة التحكم الصناعي (OT/ICS) وقياس فعالية تطبيقها وتقييمها دورياً.	✔	✔	
١-٥	**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		مستوى الضابط		
		م١	م٢	م٣
١-٥-١	يجب تحديد متطلبات الأمن السيبراني وتوثيقها واعتمادها، ضمن إدارة التغيير لدى الجهة، ويجب التأكد من أن متطلبات الأمن السيبراني تمثل جزءًا لا يتجزأ من المتطلبات الأساسية لإدارة التغيير لأنظمة التحكم الصناعي (OT/ICS).	✔	✔	✔
١-٥-٢	يجب تطبيق متطلبات الأمن السيبراني ضمن دورة حياة إدارة التغيير، المتعلقة بأنظمة التحكم الصناعي (OT/ICS) لدى الجهة.	✔	✔	✔

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.	✔	✔	✔
	١-٥-٣-٢ التحقق من صحة وسلامة التغييرات في بيئة منفصلة قبل تطبيقها على بيئة الإنتاج (Production Environment).	✔	✔	
	١-٥-٣-٣ التحقق من كفاءة متطلبات الأمن السيبراني لأنظمة التحكم الصناعي (OT/ICS) في حال استبدالها بأجهزة مماثلة لها، سواءً أكان ذلك في بيئات التصاميم؛ أم الاختبارات، أو التشغيلية، للتأكد من سلامتها، وذلك قبل تطبيقها في بيئة الإنتاج، أو البيئة التشغيلية.	✔	✔	
	١-٥-٣-٤ تطبيق إجراءات مقيدة، وآمنة للتغييرات الاستثنائية.	✔	✔	✔
	١-٥-٣-٥ تطبيق آلية أتمتة الإعدادات (Automated Configuration) وآلية كشف التغييرات بالأصول (Assets Change Detection).	✔	✔	
١-٥-٤	يجب مراجعة متطلبات الأمن السيبراني، ضمن إدارة التغيير المتعلقة بأنظمة التحكم الصناعي (OT/ICS)، و قياس فعالية تطبيقها وتقييمها دورياً.	✔	✔	
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		مستوى الضابط		
		م١	م٢	م٣
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.	✔	✔	✔
١-٦-٢	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.	✔	✔	✔

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		مستوى الضابط		
		م١	م٢	م٣
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.	✔	✔	
٢-٧-١	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.	✔	✔	
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		مستوى الضابط		
		م١	م٢	م٣
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.	✔	✔	✔

١-٨-٢	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.	✔	✔	
	١-٨-٢-٢ 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).	✔	✔	

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		مستوى الضابط			
		م١	م٢	م٣	
١-١-٢	بالإضافة للضوابط، ضمن المكون الفرعي ١-٢ 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:	✔	✔	✔	
	١-١-١-٢ إنشاء قائمة جرد إلكترونية، لجميع أصول أنظمة التحكم الصناعي (OT/ICS) ومراجعتها بشكل دوري.	✔			
	٢-١-١-٢ استخدام تقنيات الأتمتة لحصر الأصول.	✔	✔		
	٣-١-١-٢ حفظ معلومات أصول أنظمة التحكم الصناعي (OT/ICS) المحصورة بشكل آمن.	✔	✔		
	٤-١-١-٢ تحديد ملاك الأصول (Asset Owner) لجميع أصول أنظمة التحكم الصناعي (OT/ICS) والتأكد من مشاركتهم في دورة حياة إدارة جرد الأصول ذات العلاقة.	✔	✔		
	٥-١-١-٢ تصنيف مستوى الحساسية (Criticality Rating) وتوثيقه واعتماده لجميع الأصول، من قبل ملاك الأصول.	✔	✔		
٢-١-٢	رجوعاً للضابط ٦-١-٢ في الضوابط الأساسية للأمن السيبراني؛ يجب مراجعة متطلبات الأمن السيبراني المتعلقة بإدارة أصول أنظمة التحكم الصناعي (OT/ICS)، وقياس فعالية تطبيقها وتقييمها دورياً.	✔	✔		
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		مستوى الضابط		
		م١	م٢	م٣
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.	✔		
	٢-٢-١-٢ الإدارة الآمنة لحسابات الخدمات (Service Accounts) المتعلقة بخدمات التحكم الصناعي (OT/ICS) وتطبيقاتها، وأنظمتها، وأجهزتها المعزولة وغير المتصلة بحسابات دخول المستخدمين التفاعلية (Interactive Login).	✔	✔	
	٢-٢-١-٣ تغيير الهويات المصنعية (Default Credentials) لجميع الأصول المتعلقة بأنظمة التحكم الصناعي (OT/ICS) أو تعطيلها، أو إزالتها.	✔	✔	✔
	٢-٢-١-٤ الإدارة الآمنة لجلسات الاتصال، ويشمل ذلك موثوقية الجلسات (Authenticity)، و إقفالها (Lockout)، وإنهاء مهلتها (Timeout).	✔		
	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.	✔		
	٢-٢-١-٦ استخدام إجراءات الاعتمادات الثنائية (Dual Approval) وآليات محددة لتصعيد الصلاحيات للإجراءات الحساسة، داخل بيئة أنظمة التحكم الصناعي (OT/ICS).	✔		
	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 (Multi-Factor Authentication "MFA") 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.	✔	✔	

١-٢-٢	٢-١-٢-٨ تطبيق معايير آمنة ومعقدة لكلمات المرور.	✔	✔	
	٢-١-٢-٩ استخدام آليات آمنة لتخزين كلمات المرور، الخاصة بأصول أنظمة التحكم الصناعي (OT/ICS).	✔		
	٢-١-٢-١٠ 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).	✔	✔	
	٢-١-٢-١١ إلغاء صلاحيات الدخول مباشرة، عند انتهاء الحاجة لها.	✔	✔	
٢-٢-٢	رجوعاً للضابط ٢-٢-٤ في الضوابط الأساسية للأمن السيبراني؛ فإنه يجب مراجعة متطلبات الأمن السيبراني، المتعلقة بإدارة هويات الدخول والصلاحيات، في بيئة أنظمة التحكم الصناعي (OT/ICS)، وقياس فعالية تطبيقها وتقييمها دورياً.	✔	✔	
٢-٣	**حماية النظم ومرافق المعالجة (System and Processing Facilities Protection)**			
الهدف	ضمان حماية أنظمة التحكم الصناعي (OT/ICS) ومرافق المعالجة (بما في ذلك الأجهزة والخوادم وأنظمة معدات السلامة "SIS") من المخاطر السيبرانية.			
الضوابط		مستوى الضابط		
		١م	٢م	٣م
١-٣-٢	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: ٢-١-٣-١ 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.	✔	✔	
	٢-١-٣-٢ إجراء مراجعة دورية للإعدادات والتحصين (Secure Configuration and Hardening) بما يتوافق مع إرشادات الأمن السيبراني، وأفضل الممارسات، والتوصيات الخاصة بالموردين (Vendors)، وبما يتوافق مع آليات إدارة التغيير المتبعة في الجهة.	✔		
	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 (Vendors)، وبما يتوافق مع آليات إدارة التغيير المتبعة في الجهة.	✔		
	٢-١-٣-٤ تطبيق مبدأ الحد الأدنى من الصلاحيات والامتيازات (Least Privilege) والحد الأدنى من الامكانيات (Least Functionality).	✔	✔	

٢-٣-١	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.	✔	✔	
	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).	✔	✔	
	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 و صيانتها؛ محصنة ومعزولة.	✔		
	٢-٣-١-٨ فحص وسائط التخزين الخارجية، وتحليلها ضد البرامج الضارة، والتهديدات المتقدمة المستمرة (APT) في بيئة معزولة وآمنة.	✔	✔	
	٢-٣-١-٩ التقييد الحازم لاستخدام وسائط التخزين الخارجية في بيئة الإنتاج، ما لم يتم تطوير آليات آمنة وتطبيقها لنقل البيانات.	✔	✔	✔
	٢-٣-١-١٠ حماية سجلات الأحداث، والملفات الحساسة، من الدخول غير المصرح به، أو التلاعب، أو التغيير غير المصرح به، أو الحذف.	✔		
	٢-٣-١-١١ اكتشاف التطبيقات والبرامج النصية (Scripts) والمهمات والتغييرات غير المصرح بها، وفحصها.	✔	✔	
	٢-٣-١-١٢ اكتشاف الأوامر المنفذة (Commands Execution) وجلسات الاتصالات الحديثة (New Communication Sessions)، وفحصها.	✔	✔	
	٢-٣-١-١٣ اكتشاف الاتصالات المباشرة بين بيئة شبكات أنظمة التحكم الصناعي (OT/ICS) والأطراف الخارجية (External Hosts)، وفحصها.	✔	✔	✔
٢-٣-٢	رجوعاً للضابط ٢-٣-٤ في الضوابط الأساسية للأمن السيبراني؛ يجب مراجعة متطلبات الأمن السيبراني لحماية أنظمة معالجة المعلومات والأجهزة المتعلقة بأنظمة التحكم الصناعي (OT/ICS)، وقياس فعالية تطبيقها وتقييمها دورياً.	✔	✔	
٢-٤	**إدارة أمن الشبكات (Networks Security Management)**			
الهدف	ضمان حماية شبكات أنظمة التحكم الصناعي (OT/ICS) الخاصة بالجهة من المخاطر السيبرانية.			

الضوابط		مستوى الضابط		
		م١	م٢	م٣
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.			
	٢-٤-١-٢ 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).	✔		
	٢-٤-١-٣ تقسيم أنظمة معدات السلامة (Safety Instrumented Systems "SIS") منطقياً أو مادياً عن الشبكات الأخرى الخاصة بأنظمة التحكم الصناعي(OT/ICS).	✔	✔	✔
	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.	✔	✔	
	٢-٤-١-٥ عزل التقنيات اللاسلكية منطقيًا أو ماديًا، 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.	✔	✔	✔
	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).	✔	✔	✔
	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.	✔	✔	✔

١-٤-٢	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).	✔	✔	
	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.	✔	✔	
	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).	✔	✔	
	٢-٤-١-١٢ 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).	✔	✔	✔
	٢-٤-١-١٤ التقييد الصارم على تمكين البروتوكولات الصناعية (Industrial Protocols) والمنافذ (Ports) واستخدامها إلى الحد الأدنى، بالتوافق مع متطلبات التشغيل والصيانة والسلامة.	✔	✔	✔
	٢-٤-١-١٥ اعتماد حزم التحديثات الدورية، والإصلاحات الأمنية للأصول في بيئة الإنتاج، من قبل الشركة المصنعة، وإجراء اختبار في بيئة تجريبية قبل تطبيقها على بيئة الإنتاج.	✔	✔	
	٢-٤-١-١٦ الحفاظ على الوثائق المفصلة، لهندسة الشبكة وتصميمها، وتقسيماتها، وتدفقات بيانات الشبكة، و نقاط ترابطها، واعتماديتها؛ وتوثيق، وتحديث الوثائق مع كل تغيير.	✔	✔	✔
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.	✔	✔	
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		مستوى الضابط		
		م١	م٢	م٣
٢-٥-١	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.			
	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).	✔	✔	
	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.	✔	✔	
	٢-٥-١-٤ تطبيق آلية لإدارة الأجهزة المحمولة، مركزياً (Mobile Device Management "MDM").	✔		
	٢-٥-١-٥ تنفيذ عمليات التشفير على الأجهزة المحمولة المصرح باستخدامها للوصول إلى أصول أنظمة التحكم الصناعي (OT/ICS).	✔		
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.	✔	✔	
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		مستوى الضابط		
		م١	م٢	م٣
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: ٢-١-٦-١ حماية البيانات الإلكترونية والمادية (في حال التخزين والنقل) بالمستوى الذي يتوافق مع تصنيف البيانات.	✔	✔	✔
	٢-١-٦-٢ حماية البيانات والمعلومات المصنفة من خلال تقنيات، منع تسريب البيانات (Data Leakage Prevention "DLP").	✔	✔	
	٢-١-٦-٣ استخدام آليات الحذف الآمنة (Secure Wiping) لبيانات الإعدادات والبيانات المخزنة على أصول أنظمة التحكم الصناعي (OT/ICS)، وذلك عند الانتهاء منها.	✔	✔	
	٢-١-٦-٤ 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.	✔	✔	
٢-٧	**التشفير (Cryptography)**			
الهدف	ضمان الاستخدام السليم والفعال للتشفير لحماية أصول البيانات و المعلومات وفقاً للسياسات والإجراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية ذات العلاقة.			
الضوابط		مستوى الضابط		
		م١	م٢	م٣
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).	✔	✔	✔
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.	✔	✔	
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، وفقا للسياسات والإجراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية ذات العلاقة.			

الضوابط		مستوى الضابط		
		م١	م٢	م٣
١-٨-٢	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 (Centralized Location) 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.	✔	✔	✔
	٢-٨-١-٣ إجراء عمليات النسخ الاحتياطي دورياً، وفقاً لتصنيف أصول أنظمة التحكم الصناعي (OT/ICS) والمخاطر المتعلقة بها.	✔	✔	✔
	٢-٨-١-٤ تأمين الوصول والتخزين والنقل للنسخ الاحتياطية ووسائطها، وضمان حمايتها من 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.	✔	✔	

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		مستوى الضابط		
		م١	م٢	م٣
١-٩-٢	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.	✔	✔	✔
	٢-٩-١-٢ 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).	✔		
	٢-٩-١-٣ رجوعاً للضابط الفرعي ٢-١٠-٣-١ في الضوابط الأساسية للأمن السيبراني؛ يجب إجراء تقييم الثغرات لأنظمة التحكم الصناعي دورياً.	٣ أشهر	٦ أشهر	١٢ أشهر

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.	✔	✔	
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		مستوى الضابط		
		١م	٢م	٣م
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) و الشبكات 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.	✔		
	٢-١٠-١-٣ رجوعاً للضابط الفرعي ٢-١١-٣-٣ في الضوابط الأساسية للأمن السيبراني؛ يجب إجراء اختبار الاختراق لأنظمة التحكم الصناعي دورياً.	٣ أشهر	٦ أشهر	١٢ أشهر
	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.	✔		
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.	✔		

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		مستوى الضابط			
		م١	م٢	م٣	
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).	✓	✓	✓	
	٢-١١-١-٢ اكتشاف محاولات فشل الوصول إلى نظام المراقبة الخاص بالجهة، ورصدها.	✓	✓	✓	
	٢-١١-١-٣ إجراء مراجعة ومراقبة مستمرة ودقيقة لسجلات الأحداث (Event Logs) والتدقيق(Audit Trails) المتعلقة بالأمن السيبراني، على أصول أنظمة التحكم الصناعي (OT/ICS).	✓			
	٢-١١-١-٤ إجراء مراقبة وكشف، وتحليل لسلوك المستخدم (User Behaviors Analytics "UBA").	✓			
	٢-١١-١-٥ 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).	✓	✓		
	٢-١١-١-٧ اكتشاف الاحداث 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).	✓	✓	✓	
	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.	✓			
	٢-١١-١-١٠ 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.	✓	✓		

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		مستوى الضابط		
		م١	م٢	م٣
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: ٢-١٢-١-١ 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").	✔	✔	✔
	٢-١٢-١-٢ إجراء تحليل للحوادث، وتحليل الأسباب الجذرية (Root Cause Analysis) لحوادث الأمن السيبراني، بطريقة منظمة، بعد اكتشاف الحوادث.	✔	✔	✔
	٢-١٢-١-٣ تحديد تسلسل أنشطة الاستجابة، لحوادث الأمن السيبراني اللازمة لاستعادة العمليات التشغيلية لطبيعتها.	✔	✔	✔
	٢-١٢-١-٤ إنشاء 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.	✔		
	٢-١٢-١-٦ تزويد العاملين بالجهة بالمهارات والدورات التدريبية 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).	✔	✔	
	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).	✔		
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.	✔	✔	

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		مستوى الضابط		
		م١	م٢	م٣
٢-١٣-١	بالإضافة للضوابط الفرعية ضمن الضابط ٢-١٤-٣ في الضوابط الأساسية للأمن السيبراني؛ يجب أن تغطي متطلبات الأمن السيبراني للأمن المادي المتعلقة 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).	✔	✔	✔
	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.	✔		
	٢-١٣-١-٣ حماية نقاط الدخول المادية، والمحيط بالأماكن التي تحتوي على أنظمة التحكم الصناعي (OT/ICS) الحساسة، والتأكد من مراقبتها 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).	✔	✔	✔
	٢-١٣-١-٥ 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).	✔	✔	✔
	٢-١٣-١-٧ 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).	✔	✔	✔
	٢-١٣-١-٩ اختبار إمكانيات الأمن المادي وجاهزيته بشكل دوري؛ 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.	✔	✔	

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		مستوى الضابط		
		م١	م٢	م٣
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:	✔	✔	✔
	٣-١-١-١ تحديد الأنشطة اللازمة، للمحافظة على الحد الأدنى من العمليات المتعلقة بأنظمة التحكم الصناعي (OT/ICS).			
	٣-١-١-٢ 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).	✔	✔	
	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).	✔	✔	✔
	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.	✔	✔	✔
	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.	✔	✔	✔
	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.	✔	✔	

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.	✔	✔	

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

١-٤	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		مستوى الضابط		
		م١	م٢	م٣
١-١-٤	بالإضافة للضوابط الفرعية ضمن الضابطين 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).	✓	✓	
	٤-١-١-٢ تحديد متطلبات الأمن السيبراني، لتقييم الأطراف الخارجية واختيارهم ومشاركتهم المعلومات.	✓	✓	
	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).	✓	✓	
	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.	✓		
٢-١-٤	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.	✓	✓	

الملاحق

ملحق (أ): مصطلحات وتعريفات

يوضح الجدول (٣) الآتي بعض المصطلحات، التي ورد ذكرها في هذه الضوابط، وتعريفاتها.

المصطلح	التعريف
التحكم في الوصول/ الدخول Access Control	حماية موارد النظام من الوصول غير المصرح به. وهي عملية يتم من خلالها تنظيم استخدام موارد النظام، وفقاً لسياسة الأمن السيبراني، ويسمح به للمصرح لهم فحسب (المستخدمين أو البرامج أو العمليات أو الأنظمة الأخرى) وفقاً لتلك السياسة.
المجموعات النشطة Activity Groups	مجموعة متشابهة من الأنشطة الضارة، والتسلسلات والسلوكيات، أو العمليات والقدرات والبنية التحتية.
القائمة المحددة من التطبيقات Applications Whitelisting	ممارسة أمنية، تتمثل في تحديد قائمة التطبيقات المعتمدة التي يُسمح بتواجدها وتفعيلها على أجهزة المستخدمين وخوادمهم في الجهة. الهدف من القائمة المحددة هو حماية أجهزة المستخدمين وخوادمهم للجهة من التطبيقات التي قد تكون ضارة.
التوافر Availability	ضمان الوصول إلى المعلومات والبيانات والأنظمة والتطبيقات واستخدامها في الوقت المناسب.
الضوابط البديلة Alternative Controls	الضوابط الإدارية والتشغيلية والتقنية (على سبيل المثال، الإجراءات الوقائية أو المضادة) التي تستخدمها الجهة بدلاً من الضوابط الموصى بها، والتي توفر حماية كافية لأصول التقنية التشغيلية وأنظمة التحكم الصناعي (OT/ICS).
نقاط اتصال محددة Choke Point	نقاط اتصال محددة؛ هي نقاط اتصال يتم من خلالها توجيه جميع حركة مرور الشبكة الواردة والصادرة.
خطة التواصل Communication Plan	جزء من خطة الاستجابة للحوادث، تتضمن إجراءات التواصل مع أصحاب المصلحة؛ الداخليين والخارجيين في حال وقوع حادثة معينة.
السرية Confidentiality	الاحتفاظ بقيود مصرح بها للوصول إلى المعلومات، والإفصاح عنها، بما في ذلك وسائل حماية المعلومات.
الآثار المترتبة Consequence	الاثار المترتبة على حادثة؛ وتشمل الصحة والسلامة، والتأثيرات البيئية، وفقدان الممتلكات، وفقدان المعلومات (على سبيل المثال، الملكية الفكرية)، و/أو تكاليف انقطاع الأعمال.
الإجراءات المضادة Countermeasure	عمل أو اجراء أو جهاز، يقلل من تهديد، أو ثغرة أمنية، أو هجوم، وذلك عن طريق ازالته، أو منعه، أو تقليل الضرر الذي يمكن أن يسببه، أو عن طريق اكتشافه، والإبلاغ عنه؛ حتى يمكن اتخاذ الإجراء التصحيحي المناسب.
درجة الحساسية Criticality	مقياس لدرجة اعتماد الجهة على أصول تقنية تشغيلية، وأنظمة التحكم الصناعي (OT/ICS) لتحقيق رسالة، أو أهداف إدارة معينة للجهة.

المصطلح	التعريف
الأنظمة الحساسة Critical Systems	أي نظام أو شبكة قد يؤدي تعطلها، أو تغيير غير مصرح به في تشغيلها، أو وصول غير مصرح به إليها، أو إلى البيانات المخزنة بها، أو المعالجة بواسطتها؛ إلى تأثير سلبي على توافر أعمال وخدمات الجهة، أو التسبب في آثار سلبية اقتصادية، أو مالية أو أمنية، أو اجتماعية على المستوى الوطني.
الدفاع الأمني متعدد المراحل Defense in Depth	توفير ضوابط حماية أمنية متعددة المستويات للأمن السيبراني؛ كنوع من الدفاع لتأخير محاولة الاختراق او لمنعه.
المنطقة المحايدة Demilitarized Zone	هي منطقة محايدة معزولة؛ من خلال جدران حماية، ما بين الشبكات الداخلية والخارجية.
اختبار قبول المصنع Factory Acceptance Test	اختبار لمعدات التقنية التشغيلية، وأنظمة التحكم الصناعي (OT/ICS)، يتم إجراؤه في مقر مزود الخدمة، حيث يتم بناء المعدات، بعد الانتهاء من التجميع، وضبط الإعدادات، ويتم إجراؤه؛ للتحقق من الالتزام بالمواصفات الوظيفية المطلوبة. ويمكن حينئذ أن تحدد المشاكل إن وجدت فيه، ومعالجتها بسهولة أكبر.
التأثير Impact	مقياس الخسارة، أو الضرر النهائي، المرتبط بالآثار المترتبة.
أنظمة التحكم الصناعي Industrial Control Systems	مصطلح جامع يشير إلى أنواع مختلفة من أنظمة وأدوات التحكم، و تشمل الأجهزة والأنظمة، والشبكات المستخدمة، لتشغيل و/أو أتمتة العمليات الصناعية.
إنترنت الأشياء الصناعي Industrial Internet of Things	استخدام إنترنت الأشياء في القطاعات والانشطة الصناعية.
تقنية المعلومات Information Technology	التقنيات التي تُعنى بتطوير الأنظمة الحاسوبية والبرمجيات والشبكات وصيانتها واستخدامها في عمليات معالجة البيانات وتوزيعها. وتتمثل هذه التقنيات في الأنظمة الإدارية، وأنظمة الأعمال في الجهة.
سلامة المعلومة Integrity	الحماية ضد تعديل المعلومات أو تخريبها بشكل غير مصرح به، وتتضمن ضمان عدم الإنكار للمعلومات والموثوقية.
نقاط الوصول عن بعد Jump Hosts	نقاط مركزية للوصول عن بعد تمر من خلالها جميع عمليات الدخول إلى الشبكة بين منطقة عالية المستوى (Higher-Level Zone) ومنطقة منخفضة المستوى (Lower Level Zone).
تقسيم الشبكة Network Segmentation	عملية تقسيم شبكة جهاز الحاسب إلى شبكات فرعية؛ بحيث تشكل كل شبكة فرعية قسمًا من الشبكة الرئيسية.

المصطلح	التعريف
فصل الشبكة Network Segregation	عمليـة تطويـر مجموعـة مـن القواعـد وفرضها للتحكـم بالاتصالات بين المسـتضيفين والخوادم.
التقنية التشغيلية Operational Technology	مجموعة من المكونات التي تشمل أجهزة الشبكة، وأجهزة الحاسب والخوادم، وأجهزة الأمن السيبراني، ومعدات البنية التحتية، والتطبيقات التي تدعم عمليات التشغيل والصيانة والمراقبة، والأمن السيبراني للبيئات التشغيلية، وأنظمة التحكم الصناعي (OT/ICS).
تحليل مخاطر العمليات Process Hazard Analysis	مجموعة من التقييمات المنظمة للمخاطر، المحتملة، والمتعلقة بعملية صناعية محددة، حيث توضح هذه التقييمات المخاطر المعروفة، المرتبطة بالعملية المحددة، والحوادث السابقة، والضوابط الهندسية والإدارية المطبقة، والنتائج المترتبة على فشل هذه الضوابط. ويشمل ذلك تقييم جاهزية المنشأة، والعوامل البشرية، والتقييم النوعي لتأثيرات هذه العملية على الصحة والسلامة والبيئة.
مصفوفة توزيع المسؤوليات RACI Matrix	مصفوفة المسؤول، والخاضع للمساءلة، والمُستشار، والشخص الواجب اخباره. توضح هذه المصفوفة مهمة كل الأطراف المعنية في أي عملية، أو قسم، أو إدارة، مع توضيح درجة المشاركة والمسؤولية لكل الأطراف المعنية في الإجراء.
التحكم في الوصول بناءً على الأدوار Role-Based Access Control	وسيلة للتحكم في الوصول إلى الشبكة، بناءً على أدوار المستخدمين في الجهة. إذ يتم منح المستخدمين صلاحية الوصول إلى المعلومات، التي يحتاجونها؛ لتنفيذ مهماتهم فحسب، ولا يسمح لهم بالوصول إلى المعلومات التي لا يحتاجونها، أو التي لا تتعلق بأعمالهم.
مبدأ الأمن من خلال التصميم Secure by Design	منهجية لتطوير الأنظمة والتطبيقات، وتصميم الشبكات التي تسعى إلى جعلها خالية من نقاط الضعف، والثغرات الأمنية السيبرانية، ولديها المقدرة على صد الهجوم السيبراني قدر الإمكان؛ من خلال عدة تدابير. على سبيل المثال: الاختبار المستمر، وحماية المصادقة والتمسك بأفضل ممارسات البرمجة والتصميم، وغيرها.
اختبار قبول الموقع Site Acceptance Test	اختبار لمعدات التقنية التشغيلية، وأنظمة التحكم الصناعي (OT/ICS) يتم إجراؤه في مقر الجهة، بعد الانتهاء من تركيب المعدات وضبط إعداداتها وذلك للتحقق من الالتزام بالمواصفات الوظيفية، والتشغيل السليم للمعدات؛ بالتزامن مع مكونات أخرى. عندما لا يمكن التحقق من ذلك في اختبار قبول المصنع (Factory Acceptance Test "FAT"). وتشمل هذه المكونات الأدوات، وما يرتبط بها من معدات العمليات، التي قامت أطراف أخرى بتصميمها وتثبيتها.
مراجعة الشفرة المصدرية Source Code Review	عملية تتم بشكل مؤتمت، أو يدوي؛ لمراجعة الأوامر والتعليمات، المكتوبة بلغة برمجة معينة؛ للبحث عن نقاط الضعف الأمنية فيها.

المصطلح	التعريف
تمارين المحاكاة Tabletop Exercise	تمارين محاكاة مصممة لاختبار قدرات الكشف والاستجابة في البيئة التشغيلية للجهة. تشارك فرق الاستجابة التابعة للجهة في التمرين؛ من خلال مناقشة سيناريو واقعي يعني بالأحداث السيبرانية في بيئات التقنية التشغيلية، وأنظمة التحكم الصناعي (OT/ICS). وتهدف هذه التمارين إلى تحسين خطط الجهة؛ للاستجابة للحوادث، واستمرارية الأعمال، والتعافي من الكوارث، وتقديم التدريب اللازم لفرق الاستجابة في الجهة.
الخطط والأساليب و الإجراءات Tactics, Techniques, and Procedures	يشير هذا المصطلح إلى سلوكيات منفذي الهجمات السيبرانية. فيعني بالوصف العام لسلوكيات المنفذ، وتمثل (دافع) الهجوم (على سبيل المثال؛ الحصول على بيانات الدخول). وتمثل الأساليب (كيفية) تحقيق المهاجم لهدفه، من خلال تنفيذ نشاط معين (على سبيل المثال؛ استخراج بيانات الدخول للحصول على صلاحيات الوصول). ويقصد بالإجراءات الوسائل، والأدوات التي يستخدمها المهاجمون لتطبيق أساليبهم (على سبيل المثال؛ استخدام برمجيات (PwerShell) لحقن ملف "lsass.exe" لاستخراج بيانات الدخول).
تحليل سلوكيات المستخدم User Behaviors Analytics	هي عملية تتبع لبيانات المستخدم، وجمعها؛ والقيام بتحليلها، وتحديد أنماط أنشطة المستخدم؛ للكشف عن السلوكيات الضارة، أو غير الإعتيادية.
المنطقة Zone	مجموعة من الأصول المادية أو المنطقية التي تتوافر فيها متطلبات الأمن السيبراني نفسها.

جدول ٣: مصطلحات وتعريفات

ملحق (ب): قائمة الاختصارات

يوضح الجدول (٤) الآتي، معنى الاختصارات التي ورد ذكرها في هذه الضوابط.

المصطلح	التعريف
BCM	Business Continuity Management إدارة استمرارية الأعمال
BCP	Business Continuity Plan خطة استمرارية الأعمال
BIA	Business Impact Analysis تحليل التأثير على الأعمال
CNI	Critical National Infrastructure البنية التحتية الوطنية الحساسة
DMZ	Demilitarized Zone المطقة المحايدة
DRP	Disaster Recovery Plan خطة التعافي من الكوارث
ECC	Essential Cybersecurity Controls الضوابط الأساسية للأمن السيبراني
EWS	Engineering Workstation أجهزة المهندسين
FAT	Factory Acceptance Test اختبار قبول المصنع
HMI	Human-Machine Interface أجهزة واجهات التعامل مع الأنظمة
HSE	Health, Safety, and Environmental الصحة والسلامة والبيئة
ICS	Industrial Control System أنظمة التحكم الصناعي
I/O	Input/Output مدخل/مخرج
IRP	Incident Response Plan خطة الاستجابة للحوادث
IT	Information Technology تقنية المعلومات
MDM	Mobile Device Management إدارة الأجهزة المحمولة

المصطلح	التعريف
NCA	National Cybersecurity Authority الهيئة الوطنية للأمن السيبراني
NCS	National Cryptographic Standards المعايير الوطنية للتشفير
OT	Operational Technology الأنظمة التشغيلية
OTCC	Operational Technology Cybersecurity Controls ضوابط الأمن السيبراني للأنظمة التشغيلية
PHA	Process Hazard Analysis تحليل مخاطر العمليات
RACI	Responsible, Accountable, Consulted, and Informed المسؤولية والمحاسبة والاستشارة والتبليغ
RPO	Recovery Point Objective نقطة الاستعادة المستهدفة
RTO	Recovery Time Objective وقت الاستعادة المستهدف
SCyWF	Saudi Cybersecurity Workforce Framework الإطار السعودي لكوادر الأمن السيبراني (سيوف)
SDLC	Software Development Life Cycle دورة حياة تطوير البرنامج
SIEM	Security Information and Event Management نظام إدارة سجلات الأحداث ومراقبة الأمن السيبراني
SIS	Safety Instrumented System أنظمة معدات السلامة
TLP	Traffic Light Protocol بروتوكول الإشارة الضوئية
TTP	Tactics, Techniques, and Procedures الخطط والأساليب والإجراءات
TTX	Tabletop Exercise تمرين محاكاة افتراضي
VPN	Virtual Private Network الشبكة الافتراضية الخاصة

جدول ٤: قائمة الاختصارات

الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority