الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

مسودة ضوابط الأمن السيبراني للأنظمة التشغيلية

Operational Technology Cybersecurity Controls (OTCC -1: 2021)

إشارة المشاركة: أبيض
تصنيف الوثيقة: متاح

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 المعنين 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 الأشكال والرسوم التوضيحية

قائمة الجداول

الملخص التنفيذي

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

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

عليه فقد تم إصدار وثيقة ضوابط الأمن السيبراني للأنظمة التشغيلية (OTCC-1: 2021) والتي تهدف للتقليل من المخاطر السيبرانية على الجهات ذات العلاقة، وتوضح هذه الوثيقة أهداف الضوابط، ونطاق عملها، وقابليتها للتطبيق، وآلية الالتزام، ولتكون 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 الداخلة 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.

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).
- ٣١ ضابطاً أساسياً (31 Main Controls).
- ١٢٠ ضابطاً فرعياً (120 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 المساهمة في تمكين الجهات ذات العلاقة من العمل على تحقيق هذه المتطلبات لتلبية الاحتياجات الأمنية وحمايتاً للبنى التحتية الحساسة ورفع مستوى جاهزيتها اتجاه المخاطر السيبرانية.

وتأخذ هذه الضوابط بالاعتبار المحاور الأربعة الأساسية التي يرتكز عليها الأمن السيبراني، وهي:

- الاستراتيجية (Strategy)
- الأشخاص (People)
- الإجراء (Process)
- التقنية (Technology)

نطاق العمل وقابلية التطبيق

نطاق عمل الضوابط

تنطبق هذه الضوابط على أنظمة التحكم الصناعي المتواجدة 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، (ويشار لها جميعاً في هذه الوثيقة بـ"الجهة"). ويتم تعريف المرافق الحساسة على أنها المرافق التي في حال تعطلها أو التغيير غير المشروع في أنظمتها تؤدي إلى التأثير السلبي 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 و/أو أتمتة العمليات الصناعية.

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 ومتطلبات الأمن السيبراني لأنظمة التحكم الصناعي، 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، 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-1:2021 Assessment and Compliance Tool) لتنظيم عملية تقييم وقياس مدى التزام الجهات بتطبيق ضوابط الأمن السيبراني للأنظمة التشغيلية.

أداة تحديد مستويات المرافق

تقوم الهيئة بإصدار أداة (OTCC-1:2021 Facility Level Identification Tool) لتنظيم عملية تحديد 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 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-1:2021) 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 مستويات الأساسية والفرعية لضوابط الأمن السيبراني للأنظمة التشغيلية وتحديد قابلية تطبيقها.

مستويات ضوابط الأمن السيبراني للأنظمة التشغيلية

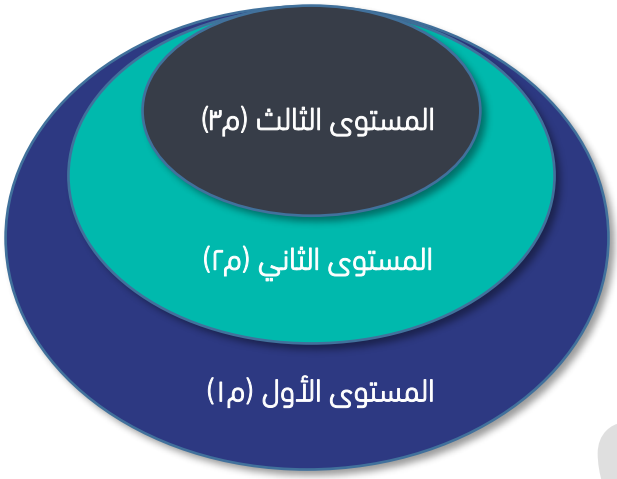
تتكون ضوابط الأمن السيبراني لأنظمة التحكم الصناعي من ثلاثة مستويات محددة وذلك اعتماداً على المعايير التالية:

- مدى حساسية المرافق على أعمال وتوافر خدمات الجهة 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 الجانب الاجتماعي.

يوضح الجدول رقم (١) أدناه المستويات الثلاثة للضوابط بناءً على نتائج أداة تحديد مستوى المرافق:

المستوى	تعريف المستوى	عدد الضوابط
المستوى الأول (م١)	مرافق ذات حساسية **عالية** على الأصول والبيئة التشغيلية لدى الجهة من حيث السلامة، والبيئة، و الأمان.	١٥١ ضابطاً أساسياً وفرعياً (تشمل ضوابط المستوى الثاني والثالث)
المستوى الثاني (م٢)	مرافق ذات حساسية **متوسطة** على الأصول والبيئة التشغيلية لدى الجهة من حيث السلامة، والبيئة، و الأمان.	١١٧ ضابطاً أساسياً وفرعياً (تشمل ضوابط المستوى الثالث)
المستوى الثالث (م٣)	مرافق ذات حساسية **منخفضة** على الأصول والبيئة التشغيلية لدى الجهة من حيث السلامة، والبيئة، و الأمان.	٥٦ ضابطاً أساسياً وفرعياً

جدول رقم (١): مستويات ضوابط الأمن السيبراني للأنظمة التشغيلية



شكل رقم (١): مستويات ضوابط الأمن السيبراني للأنظمة التشغيلية

ويمكن الرجوع إلى ملحق المنهجية والمواءمة لضوابط الأمن السيبراني للأنظمة التشغيلية للحصول على معلومات تفصيلية عن كيفية تحديد مستويات ضوابط الأمن السيبراني لأنظمة التحكم الصناعي.

هيكلية ضوابط الأمن السيبرانى للأنظمة التشغيلية

يوضح الجدول (٢) أدناه المكونات الأساسية والفرعية لضوابط الأمن السيبراني للأنظمة التشغيلية:

١. حوكمة الأمن السيبرانى	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	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 Device 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	٣-١	جوانب صمود الأمن السيبراني في إدارة استمرارية الأعمال Cyber Resilience Aspects of Business Continuity Management (BCM)		
٤. الأمن السيبرانى المتعلق بالأطراف الخارجية	٤-١	الأمن السيبراني للأطراف الخارجية Third-Party Cybersecurity		

الجدول رقم (٢): المكونات الأساسية والفرعية لضوابط الأمن السيبراني للأنظمة التشغيلية

ضوابط الأمن السيبراني للأنظمة التشغيلية

١ حوكمة الامن السيبراني (Cybersecurity Governance)

١-١	سياسات وإجراءات الأمن السيبرانى (Cybersecurity Policies and Procedures)			
الهدف	ضمان توثيق ونشر متطلبات الأمن السيبرانى لأنظمة التحكم الصناعى (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	بالإضافة للضابطين ١-٣-١ و ١-٣-٢ في الضوابط الأساسية للأمن السيبراني، يجب على الجهة توثيق واعتماد وتطبيق مجموعة من سياسات وإجراءات الأمن السيبراني المخصصة لأنظمة التحكم الصناعي (OT/ICS) .	✓	✓	✓
١-١-٢	بالإضافة 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	بالإضافة للضابط ١-٣-٤ في الضوابط الأساسية للأمن السيبراني، يجب مراجعة سياسات وإجراءات الأمن السيبراني لأنظمة التحكم الصناعي (OT/ICS) 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 فى تطبيق ضوابط الأمن السيبرانى لأنظمة التحكم الصناعى (OT/ICS) فى الجهة.			
	الضوابط	مستوى الضابط		
		م١	م٢	م٣
١-٢-١	بالإضافة للضابط ١-٤-1 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 وتوثيق واعتماد الأدوار والمسؤوليات الخاصة بالأمن السيبراني (RACI) لجميع أصحاب المصلحة المعنيين بأنظمة التحكم الصناعي (OT/ICS) ، مع الأخذ بالاعتبار عدم تعارض المصالح.	✓	✓	✓

	١-٢-١-٢ يجب إسناد أدوار ومسؤوليات الأمن السيبراني المتعلقة بأنظمة التحكم الصناعي (OT/ICS) للإدارة المعنية بالأمن السيبراني لدى الجهة; مع الأخذ بالاعتبار عدم تعارض المصالح.	✓	✓	
١-٣	إدارة مخاطر الأمن السيبراني(Cybersecurity Risk Management)			
الهدف	ضمان إدارة مخاطر الأمن السيبرانى على نحو ممنهج يهدف إلى حماية الأصول المعلوماتية وأنظمة التحكم الصناعى (OT/ICS)، وذلك وفقاً للسياسات والإجراءات 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 تضمين مخاطر الأمن السيبراني المتعلقة بأنظمة التحكم الصناعي (OT/ICS) ضمن منهجية وإجراءات إدارة مخاطر الأمن السيبراني في الجهة.	✓	✓	✓
	١-٣-١-٢ إجراء تقييم لمخاطر الأمن السيبراني لأنظمة التحكم الصناعي (OT/ICS) بشكل دوري، مع التأكد من تضمين الاتفاقيات والاعتماديات مع الأطراف الخارجية وسلاسل التوريد (Supply Chain) المتعلقة بأنظمة التحكم الصناعي (OT/ICS) كجزء من المخاطر و/أو عند حدوث تغييرات بالمتطلبات التشريعية والتنظيمية ذات العلاقة.	✓	✓	✓
	١-٣-١-٣ تضمين مخاطر الأمن السيبراني المتعلقة بأنظمة التحكم الصناعي (OT/ICS) ضمن سجل المخاطر الموحد للأمن السيبراني 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 إجراء تحليل وتقييم للمخاطر المرتبطة في الإجراءات والعمليات (Process Hazard Analysis) والذي يتضمن بحد أدنى، تحليلاً نوعياً لمخاطر الأمن السيبراني (Qualitative 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.	✓	✓	
	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 ومراجعة تلك المخاطر بشكل مستمر.	✓	✓	✓

١-٤	الأمن السيبرانى ضمن إدارة مشاريع أنظمة التحكم الصناعى (Cybersecurity in Industrial Control System Project Management)			
الهدف	التأكد من أن متطلبات الأمن السيبرانى مضمنة فى منهجية وإجراءات إدارة مشاريع الجهة لحماية السرية وسلامة الأعمال التشغيلية والتقنية ودقتها وتوافرها لأنظمة التحكم الصناعى (OT/ICS)، وذلك وفقاً للسياسات والإجراءات 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 في 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 كجزء من دورة حياة المشاريع المتعلقة بأنظمة التحكم الصناعي (OT/ICS) .	✓	✓	✓
	١-٤-١-٢ تضمين متطلبات الأمن السيبراني ضمن اختبارات القبول (Acceptance Test) و عمليات التقييم (Evaluation Process). (مثل: اختبارات قبول المصنع (Factory Acceptance Tests (FAT)) و اختبارات القبول الميداني (Site Acceptance Tests (SAT)) و اختبارات التشغيل (Commissioning Tests) و اختبارات التغيير (Change Tests) و مراجعة الشفرة المصدرية (Source Code Review).	✓	✓	
	١-٤-١-٣ تضمين مبدأ الأمن من خلال التصميم (Secure-By-Design) كجزء من الأمن المعماري لتصميم البيئة الخاصة بأنظمة التحكم الصناعي (OT/ICS) .	✓	✓	✓
	١-٤-١-٤ حماية الأنظمة في البيئة التطويرية (Development Environment)، بيئات الاختبار (Testing Environment)، المنصات التكاملية (Integration Platforms).	✓	✓	
١-٤-٢	يجب مراجعة متطلبات الأمن السيبراني ضمن إدارة مشاريع أنظمة التحكم الصناعي (OT/ICS) ، و قياس فعالية تطبيقها وتقييمها دورياً.	✓	✓	
١-٥	الأمن السيبرانى ضمن إدارة التغيير (Cybersecurity in Change Management)			
الهدف	التأكد من أن مستويات الأمن السيبرانى لا تتأثر حال تطبيق طلبات التغيير فى البيئة التى تحتوي على أنظمة التحكم الصناعى (OT/ICS) وذلك بعد التحليل والتحكم بالتغييرات.			
الضوابط		مستوى الضابط		
		م١	م٢	م٣
١-٥-١	يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني 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 كجزء 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 حالة استبدالها بأجهزة مماثلة لها سواءً في بيئات التصاميم، 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 استخدام آلية أتمته 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	بالإضافة للضابط ١-٨-١ في الضوابط الأساسية للأمن السيبراني، يجب على الإدارة المعنية في الجهة مراجعة تطبيق ضوابط الأمن السيبراني لأنظمة التحكم الصناعي (ICSCC-1:2021) ، مره واحدة سنوياً، على الأقل.	✓	✓	✓
١-٦-٢	بالإضافة للضابط ١-٨-٢ في الضوابط الأساسية للأمن السيبراني، يجب مراجعة تطبيق ضوابط الأمن السيبراني لأنظمة التحكم الصناعي (ICSCC-1: 2021) من قبل أطراف مستقلة عن الإدارة المعنية بالأمن السيبراني في الجهة، وذلك مره واحدة كل ثلاث سنوات على الأقل.	✓	✓	✓

١-٧	الأمن السيبرانى المتعلق بالموارد البشرية (Cybersecurity in Human Resources)			
الهدف	ضمان التأكد من أن مخاطر ومتطلبات الأمن السيبرانى لأنظمة التحكم الصناعى (OT/ICS) المتعلقة بالعاملين (موظفين ومتعاقدين) فى الجهة تعالج بفعالية قبل وأثناء وعند انتهاء/إنهاء عملهم، 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 فى الضوابط الأساسية للأمن السيبرانى، يجب أن تغطى متطلبات الأمن السيبراني المتعلقة بالموارد البشرية لأنظمة التحكم الصناعى (OT/ICS) ، بحد أدنى، إجراء عمل مسح أمنى (Screening or Vetting) لجميع العاملين (ويشمل ذلك الموظفين، المتعاقدين، والمقاولين، و المستشارين) والذين يمكنهم الوصول إلى أصول أنظمة التحكم الصناعى (OT/ICS) أو استخدامها، وذلك قبل منحهم صلاحيات الوصول.	✓	✓	
٢-٧-١	بالإضافة للضابط ١-٩-٦ فى الضوابط الأساسية للأمن السيبرانى، يجب مراجعة متطلبات الأمن السيبرانى لأنظمة التحكم الصناعى (OT/ICS) المتعلقة بالموارد البشرية، و قياس فعالية تطبيقها وتقييمها دورياً.	✓	✓	
٨-١	برنامج التوعية والتدريب بالأمن السيبرانى (Cybersecurity Awareness and Training Program)			
الهدف	ضمان التأكد من أن العاملين بالجهة لديهم التوعية الأمنية اللازمة وعلى دراية بمسؤولياتهم فى مجال الأمن السيبرانى. والتأكد من تزويد العاملين بالجهة بالمهارات والمؤهلات والدورات التدريبية المطلوبة فى مجال الأمن السيبرانى لحماية الأصول المعلوماتية والتقنية لأنظمة التحكم الصناعى (OT/ICS) لدى الجهة والقيام بمسؤولياتهم تجاه الأمن السيبرانى.			
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.	✓	✓	✓
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: ١-٢-٨-١ 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) كمرجع.	✓	✓	
	٢-٢-٨-١ 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) .	✓	✓	

٢ تعزيز الأمن السيبراني (Cybersecurity Defense)

1-2	إدارة الأصول Asset Management			
الهدف	للتأكد 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: ٢-١-١-١ إنشاء قائمة جرد إلكترونية لجميع أصول أنظمة التحكم الصناعي (OT/ICS) ومراجعتها بشكل دوري.	✓	✓	✓
	٢-١-١-٢ استخدم تقنيات الأتمتة لحصر الأصول.	✓		
	٢-١-١-٣ حفظ معلومات أصول أنظمة التحكم الصناعي (OT/ICS) المحصورة بشكل آمن.	✓		
	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.	✓	✓	
	٢-١-١-٥ تصنيف وتوثيق واعتماد مستوى الحساسية (Criticality Rating) لجميع الأصول من قبل ملاك الأصول.	✓	✓	
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.	✓	✓	

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) الخاصة بالتطبيقات، والأنظمة، والأجهزة المعزولة وغير المتصلة; وتعطيل الدخول البشري التفاعلي (interactive Login) إلى حسابات المستخدمين المتعلقة بأنظمة التحكم الصناعى (OT/ICS) .	✓	✓	
	٢-٢-١-٣ تغيير، أو تعطيل، أو إزالة الهويات المصنعية (Default Credentials) لجميع الأصول المتعلقة بأنظمة التحكم الصناعي (OT/ICS) .	✓	✓	✓
	٢-٢-١-٤ الإدارة الآمنة لجلسات الاتصال، ويشمل 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، بحيث يتم إجراء تقييم مخاطر الأمن السيبراني قبل منح الوصول عن بعد ورصد وإدارة المخاطر المتعلقة بذلك. وأن يكون الدخول المصرح به من خلال التحقق من الهوية متعدد العناصر "MFA" (Multi-Factor Authentication) و عبر قناة مشفرة لفترة زمنية محددة وبصلاحيات محدودة. ويتم مراقبة جلسة الوصول عن بعد وتسجيلها، وأن تكون الصلاحيات الممنوحة للمستخدم متوافقة مع تقييم مخاطر الأمن السيبرانى.	✓	✓	
	٢-٢-١-٨ تطبيق معايير آمنة ومعقدة لكلمات المرور.	✓	✓	
	٢-٢-١-٩ استخدام آليات آمنة لتخزين كلمات المرور الخاصة بأصول أنظمة التحكم الصناعي (OT/ICS) .	✓		
	٢-٢-١-١٠ رجوعاً للمكون 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 الصناعى (OT/ICS) .	✓	✓	
	٢-٢-١-١١ 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 الأنظمة وأجهزة معالجة المعلومات (System and Processing Facilities Protection)			
الهدف	ضمان حماية أنظمة التحكم الصناعى (OT/ICS) ومرافق المعالجة (بما فى ذلك شبكات الإنتاج الصناعى وأنظمة معدات السلامة "SIS") من المخاطر السيبرانية.			
الضوابط		مستوى الضابط		
		م١	م٢	م٣
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 يجب الحماية من الفيروسات والبرامج والأنشطة المشبوهة والبرمجيات الضارة (Malware) والتهديدات المتقدمة المستمرة (APT) للكشف عن الأنشطة الضارة وحظرها.	✓	✓	
	٢-٣-١-٢ 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 فى الجهة.	✓		
	٢-٣-١-٣ 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.	✓		
	٢-٣-١-٤ تطبيق مبدأ الحد الأدنى من الصلاحيات والامتيازات (Least Privilege) والحد الأدنى من الامكانيات (Least Functionality).	✓	✓	
	٢-٣-١-٥ إعداد وحدات التحكم (controllers) في أنظمة معدات السلامة (SIS) في الأوضاع المناسبة (Appropriate Modes) في جميع الأوقات، ومنع التغييرات على الإعدادات في حال كانت وحدات التحكم تعمل في الأوضاع غير المناسبة (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)).	✓		
	٢-٣-١-٧ إدارة أصول أنظمة التحكم الصناعي (OT/ICS) من خلال أجهزة المهندسين (Engineering Workstations) وأجهزة واجهات التعامل مع الأنظمة ("HMI" Human-Machine Interface)، والتأكد من أن الأجهزة محصنة ومعزولة لإدارة تنفيذ الأوامر وتطبيق الإعدادات وعمليات الصيانة.	✓		
	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 وتطبيق آليات آمنة 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.	✓		
٢-٣-٢	رجوعاً للضابط ٢-٣-٤ في الضوابط الأساسية للأمن السيبراني، يجب مراجعة متطلبات الأمن السيبراني لحماية أنظمة وأجهزة معالجة المعلومات 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) 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) ، واستخدامها يكون عند الحاجة وذلك بعد تقييم مخاطر الأمن السيبراني 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) 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 منع الوصول لخدمات الأعمال الحساسة (Business Critical) على شبكات أنظمة التحكم الصناعي (OT/ICS) من الشبكة الداخلية إلا للخدمات المصرح بالوصول لها, ويجب الحد من الوصول للخدمات ذات الثغرات الأمنية المعروفة إلى أقصى حد ممكن.	✓	✓	✓

	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 متعدد العناصر (Multi-Factor Authentication "MFA") وتسجيل جلسات الاتصال (Session Recording) وأن يكون الاتصال لفترة زمنية محددة فقط.	✓	✓	
	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 منطقة الشبكة الداخلية (Corporate Zone) مثل صمام الأمان (Data Diode).	✓		
	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 و استخدام البروتوكولات الصناعية (Industrial Protocols) والمنافذ (Ports) إلى الحد الأدنى بالتوافق مع متطلبات التشغيل والصيانة والسلامة.	✓	✓	✓
	٢-٤-١-١٥ إجراء اختبار لحزم التحديثات والإصلاحات الأمنية 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.	✓	✓	✓
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)			
	ضمان حماية أجهزة الجهة المحمولة (بما فى ذلك أجهزة الحاسب المحمول والهواتف الذكية والأجهزة الذكية اللوحية) من المخاطر السيبرانية. وضمان التعامل بشكل آمن مع المعلومات الحساسة والمعلومات الخاصة بأعمال الجهة وحمايتها أثناء النقل والتخزين عند استخدام الأجهزة الشخصية للعاملين فى الجهة (BYOD).			

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 فقط بما يتوافق مع آليات إدارة صلاحيات الوصول المتبعة في الجهة.	✓	✓	
	٢-٥-١-٢ استخدام الأجهزة المحمولة فقط 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 واعتماد قائمة بالأجهزة المحمولة المصرح بها مع ضمان إمكانية توصيل هذه الأجهزة المحمولة فقط ببيئة التقنية التشغيلية وأنظمة التحكم الصناعي (OT/ICS).	✓	✓	
	٢-٥-١-٤ تطبيق آلية لإدارة الأجهزة المحمولة مركزياً (Mobile Device Management "MDM").	✓		
	٢-٥-١-٥ تنفيذ عمليات التشفير على الأجهزة المحمولة المستخدمة للوصول إلى أصول شبكات 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 وسلامة وتوافر بيانات الجهة ومعلوماتها وفقا للسياسات والإجراءات التنظيمية ، وما يتصل بذلك من قوانين وأنظمة.			
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: ٢-٦-١-١ حماية البيانات الإلكترونية والمادية (في حالة التخزين والنقل) بالمستوى الذي يتوافق مع تصنيف البيانات.	✓	✓	✓
	٢-٦-١-٢ حماية البيانات والمعلومات المصنفة من خلال تقنيات، منع تسريب البيانات (Data Leakage Prevention "DLP").	✓	✓	
	٢-٦-١-٣ استخدام آليات الحذف الآمنة (Secure Wiping) لبيانات الإعدادات والبيانات المخزنة على أصول أنظمة التحكم الصناعي (OT/ICS) ، وذلك عند الانتهاء منها.	✓	✓	

	٢-٦-١-٤ التقييد الحازم لنقل أو استخدام بيانات أنظمة التحكم الصناعي (OT/ICS) خارج بيئة الإنتاج.	✓		
٢-٦-١	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، 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، 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 فى ذلك نظم المعلومات وإعدادات البرمجيات من المخاطر السيبرانية وفقا للسياسات والإجراءات التنظيمية ، والقوانين واللوائح ذات الصلة.			
الضوابط		مستوى الضابط		
		م١	م٢	م٣
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 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 بأن ملفات الإعدادات الحساسة والهندسية 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 الخاصة بالنسخ الاحتياطية ووسائطها وضمان حمايتها من التلف أو التعديل 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 أو تقليل احتمالية استغلال هذه الثغرات لشن هجمات إلكترونية ضد الجهة.			
الضوابط		مستوى الضابط		
		م١	م٢	م٣
٢-٩-١	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 تحديد نطاق وأنشطة عمليات تقييم الثغرات لبيئة شبكات أنظمة التحكم الصناعي (OT/ICS) كجزء من الآليات الرسمية لإدارة الثغرات في الجهة وضمان تأثير محدود أو غير محدود على بيئة الإنتاج.	✓	✓	✓
	٢-٩-١-٢ رجوعاً للضابط 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 إجراء تقييم الثغرات لأنظمة التحكم الصناعي دورياً.	٣ أشهر	٦ أشهر	١٢ شهر
	٢-٩-١-٤ فحص واكتشاف التطبيقات والبرامج النصية (Scripts) والمهام و التغييرات غير المصرح بها التي تم إجراؤها على الملفات أو الإعدادات (Configurations).	✓		
	٢-٩-١-٥ فحص و اكتشاف أوامر التنفيذ (Commands Execution) وجلسات الاتصالات الحديثة (New Communication Sessions).	✓	✓	
	٢-٩-١-٦ فحص واكتشاف الاتصالات المباشرة بين بيئة شبكات أنظمة التحكم الصناعي(OT/ICS) والإنترنت و الأطراف الخارجية (External Hosts).	✓		
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		
		م١	م٢	م٣
٢-١٠-١	بالإضافة للضوابط الفرعية ضمن الضابط ٢-١١-٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني لإجراء اختبارات اختراق على أنظمة التحكم الصناعي (OT/ICS) بحد أدنى ما يلي: ٢-١٠-١-١ رجوعاً للضابط ٢-١١-٣-١ في الضوابط الأساسية للأمن السيبراني، يجب تحديد نطاق أنشطة اختبارات الاختراق لتغطي بيئة شبكات أنظمة التحكم الصناعي (OT/ICS) ، وأن يتم عمل الاختبارات من قبل فريق ذو كفاءة عالية.	✓		

	٢-١٠-١-٢ رجوعاً للضابط 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 يجب تحديد وتنفيذ طرق اختبارات بديلة (مثل الاختبارات غير الفعالة (Passive Testing) لجمع المعلومات ذات العلاقة بالتأثيرات المحتملة على بيئة الإنتاج التشغيلي.	✓		
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 وتحليل ومراقبة سجلات أحداث الأمن السيبراني في الوقت المناسب للكشف المبكر عن الهجمات السيبرانية المحتملة وإدارة مخاطرها بفعالية، من أجل منع أو تقليل الآثار المترتبة على أعمال الجهة.

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 الكشف عن حالات فشل الوصول إلى نظام المراقبة 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 مراقبة جميع عمليات الوصول عن بعد (Remote Access Sessions).	✓	✓	
	٢-١١-١-٦ فحص واكتشاف الاحداث الضارة (Malicious Events) على مستوى الشبكة والأجهزة.	✓	✓	✓
	٢-١١-١-٧ تسجيل ومراقبة التنبيهات على سجلات الاحداث في حالة اتصال أجهزة جديدة أو غير مسموح بها بشبكات أنظمة التحكم الصناعي (OT/ICS) .	✓	✓	✓
	٢-١١-١-٨ استخدام التهديدات الاستباقية (Threat Intelligence) المتعلقة بأنظمة التحكم الصناعي (OT/ICS) لضبط وتحديث تنبيهات نظام إدارة سجلات الاحداث ومراقبة الأمن السيبراني (SIEM) بشكل دوري.	✓		

	٢-١١-١-٩ 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 السيبرانى Cybersecurity Incident and Threat Management			
الهدف	ضمان تحديد واكتشاف حوادث الأمن السيبرانى فى الوقت المناسب وإدارتها بشكل فعال والتعامل مع تهديدات الأمن السيبرانى استباقياً من أجل منع أو تقليل الأثار المترتبة على أعمال الجهة المتعلقة بأنظمة التحكم الصناعى (OT/ICS).			
الضوابط		مستوى الضابط		
		م١	م٢	م٣
٢-١٢-١	بالإضافة للضوابط الفرعية ضمن الضابط ٢-١٣-٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني لإدارة حوادث وتهديدات الأمن السيبراني 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 وإجراءات الجهة 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 تحديد خطط التواصل عند وقوع الحوادث (Incident Communications Plan).	✓	✓	✓
	٢-١٢-١-٥ تضمين إجراءات 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 والمقاولين والمستشارين) ، للاستجابة لحوادث الأمن السيبرانى المتعلقة بأنظمة التحكم الصناعى (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 التكتيكات والتقنيات و الإجراءات (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 الصناعى (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 الاشخاص 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 و الكشف 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 و المحيط بالأماكن التي تحتوي على أنظمة التحكم الصناعي (OT/ICS) الحساسة بحراس أمن 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 التكم الصناعي، بما في ذلك أنظمة معدات السلامة(SIS).	✓	✓	
	٢-١٣-١-٦ الاحتفاظ بسجلات دخول الزوار إلى مناطق أنظمة التحكم الصناعي (OT/ICS) الحساسة.	✓	✓	✓
	٢-١٣-١-٧ مراقبة الأعمال التي يتم تأديتها من المقاولين أو الموظفين التابعين للموردين و مزودي الخدمات.	✓	✓	
	٢-١٣-١-٨ تزويد حراس الأمن بالمهارات المتخصصة والتدريب اللازم بما يتماشى مع الأدوار والمسؤوليات فيما يتعلق بالأمن المادي لأنظمة التحكم الصناعي (OT/ICS) .	✓	✓	✓
	٢-١٣-١-٩ اختبار إمكانيات وجاهزية الأمن المادي 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)

١-٣	جوانب صمود الأمن السيبرانى فى إدارة استمرارية الأعمال Cybersecurity Resilience Aspects of Business Continuity Management (BCM)			
الهدف	ضمان توافر متطلبات صمود الأمن السيبرانى فى 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 فى الضوابط الأساسية للأمن السيبرانى، يجب أن تغطى متطلبات صمود الأمن السيبرانى فى إدارة استمرارية الأعمال المتعلقة بأنظمة التحكم الصناعى (OT/ICS) بحد أدنى ما يلى: 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 الصناعى (OT/ICS) وفقاً للتقييم الدوري لمخاطر الأمن السيبرانى لأصول أنظمة التحكم الصناعى (OT/ICS) .	✓	✓	
	٣-١-١-٣ تضمين متطلبات الأمن السيبرانى المتعلقة بأنظمة التحكم الصناعى (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 السيبرانى المتعلقة بأنظمة التحكم الصناعى (OT/ICS) ضمن خطط التعافى من الكوارث (DRP)، بحيث تشمل سيناريوهات الكوارث المتعلقة بالأمن السيبرانى، وإجراءات التعامل مع توقف النظام، وإجراءات إدارة العمليات التشغيلية.	✓	✓	✓
	٣-١-١-٥ عند فشل الأنظمة بسبب حادثة أمن سيبرانى, يجب أن تكون أنظمة التحكم الصناعى (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 الصناعى (OT/ICS) المتعلقة بخطط التعافى من الكوارث (DRP) وخطة استمرارية العمل (BCP) وإجراء تحليل الأسباب الجذرية (Root Cause Analysis) للحوادث.	✓	✓	
٢-١-٣	رجوعاً للضابط ٣-١-٤ فى الضوابط الأساسية للأمن السيبرانى ، يجب مراجعة متطلبات الأمن السيبرانى لجوانب صمود الأمن السيبرانى فى إدارة استمرارية الأعمال لبيئة أنظمة التحكم الصناعى (OT/ICS) ، وقياس فعالية تطبيقها وتقييمها دورياً.	✓	✓	

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

٤-١	الأمن السيبرانى للأطراف الخارجية Third-Party Cybersecurity			
الهدف	ضمان حماية أصول الجهة من مخاطر الأمن السيبرانى المتعلقة بالأطراف الخارجية ، بما فى ذلك مصنعو معدات أنظمة التحكم الصناعى (OT/ICS) ، ومقاولو منتجات أنظمة التحكم الصناعى (OT/ICS) وموردو خدمات أنظمة التحكم الصناعى (OT/ICS) وفقاً للسياسات والإجراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية ذات العلاقة.			
الضوابط		مستوى الضابط		
		م١	م٢	م٣
٤-١-١	بالإضافة للضوابط الفرعية ضمن الضابطين ٤-١-٢ و ٤-١-٣ فى الضوابط الأساسية للأمن السيبرانى، يجب أن تغطى متطلبات الأمن السيبرانى للأطراف الخارجية المتعلقة بأنظمة التحكم الصناعى (OT/ICS) بحد أدنى ما يلى: ٤-١-١-١ تضمين متطلبات الأمن السيبرانى فى متطلبات المشتريات لمنتجات وخدمات أنظمة التحكم الصناعي (OT/ICS) .	✓	✓	✓
	٤-١-١-٢ تحديد متطلبات الأمن السيبرانى لتقييم واختيار ومشاركة المعلومات مع الأطراف الخارجية.	✓	✓	
	٤-١-١-٣ استخدام المتعاقدون والموردون الخارجيون ممارسات آمنة لدورة حياة تطوير البرنامج (SDLC) الخاصة بالأنظمة والأصول المصممة أو المطبقة فى بيئة أنظمة التحكم الصناعي (OT/ICS) .	✓	✓	
	٤-١-١-٤ إجراء تقييم وتدقيق للأمن السيبرانى بشكل دوري للأطراف الخارجية والتأكد من وجود ما يضمن السيطرة على أي مخاطر سيبرانية تم رصدها.	✓		
٤-١-٢	رجوعاً للضابط ٤-١-٤ فى الضوابط الأساسية للأمن السيبرانى ، يجب مراجعة متطلبات الأمن السيبرانى للأمن السيبرانى للأطراف الخارجية لبيئة أنظمة التحكم الصناعى (OT/ICS) ، وقياس فعالية تطبيقها وتقييمها دورياً.	✓	✓	

الملاحق

ملحق (أ): مصطلحات وتعريفات

يوضح الجدول ٣ التالي 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 فقط للمصرح لهم (المستخدمين أو البرامج أو العمليات أو الأنظمة الأخرى) وفقاً لتلك السياسة.
مجموعة الأنشطة الضارة Activity Group	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 وخوادم المستخدمين للجهة. الهدف من القائمة المحددة هو حماية أجهزة وخوادم المستخدمين النهائيين 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).
نقطة التجمع Choke Point	نقطة التجمع هي نقطة واحدة 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 حالة وقوع حادثة معينة.
السرية Confidentiality	الاحتفاظ بقيود مصرح بها على الوصول إلى المعلومات والإفصاح عنها بما في ذلك وسائل حماية معلومات الخصوصية والملكية الشخصية
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 التي 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 امنية 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 حيث يمكن أن تحدد المشاكل ان 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 والتي 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 وصيانة واستخدام الأنظمة الحاسوبية والبرمجيات والشبكات في عمليات معالجة البيانات وتوزيعها. وتتمثل هذه التقنيات في الأنظمة الإدارية وأنظمة الأعمال في الجهة.
سلامة المعلومة Integrity	الحماية ضد تعديل أو تخريب المعلومات بشكل غير مصرح به، وتتضمن ضامن عدم الإنكار للمعلومات والموثوقية.
خادم القفز/الانتقال Jump Host	نقطة 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.
فصل الشبكة Network Segregation	عملية تطوير وفرض مجموعة من القواعد للتحكم بالاتصالات بين المستضيفين 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 Hazard Analysis Process	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.

المصطلح	التعريف
مصفوفة توزيع المسؤوليات RACI Matrix	مصفوفة المسؤول، والخاضع للمساءلة، والمُستشار، والشخص الواجب اخباره. توضح هذه المصفوفة دور كل الأطراف المعنية في أي عملية أو قسم أو إدارة مع توضيح درجة المشاركة والمسؤولية لكل الأطراف المعنية فى الإجراء.
التحكم في الوصول بناءً على الأدوار Role-Based Access Control	وسيلة للتحكم في الوصول إلى الشبكة بناءً على أدوار المستخدمين في الجهة، حيث يتم منح المستخدمين صلاحية الوصول إلى المعلومات التي يحتاجونها لتنفيذ مهامهم فقط ولا يسمح لهم بالوصول إلى المعلومات التي لا يحتاجونها أو التي لا تتعلق بأعمالهم.
مبدأ الامان من خلال التصميم Secure by Design	منهجية لتطوير الأنظمة والتطبيقات وتصميم الشبكات التي تسعى إلى جعلها خالية من نقاط الضعف والثغرات الأمنية السيبرانية، والمقدرة على صد الهجوم السيبراني قدر الإمكان من خلل عدة تدابير على سبيل المثال: الاختبار المستمر، وحماية المصادقة والتمسك بأفضل ممارسات البرمجة والتصميم، وغيرها
اختبار قبول المصنع Site Acceptance Test	اختبار لمعدات التقنية التشغيلية وأنظمة التحكم الصناعي (OT/ICS) يتم إجراؤه في مقر الجهة بعد الانتهاء من تركيب وضبط إعدادات المعدات وذلك للتحقق من الالتزام بالمواصفات الوظيفية والتشغيل السليم للمعدات بالتزامن مع مكونات أخرى حيث لا يمكن التحقق من ذلك في اختبار قبول المصنع (Factory Acceptance Test "FAT"). وتشمل هذه المكونات الأدوات وما يرتبط بها من معدات العمليات التى 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.
تمارين المحاكاة Tabletop Exercise	تمارين محاكاة مصممة لاختبار قدرات الكشف والاستجابة في البيئة التشغيلية للجهة، حيث تشارك فرق الاستجابة التابعة للجهة في التمرين من خلال مناقشة سيناريو واقعي يركز على الأحداث 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 فى الجهة.
الطرق والأساليب والإجراءات Tactics, Techniques, and Procedures	يشير هذا المصطلح إلى سلوكيات منفذي الهجمات السيبرانية، حيث تعتبر الطرق الوصف 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 المهاجمين 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 نفس متطلبات الأمن السيبرانى.

جدول (5) : مصطلحات وتعريفات

ملحق (ب): قائمة الاختصارات

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

الاختصار	معناه
A/V	Antivirus مكافح الفيروسات
BCM	Business Continuity Management إدارة استمرارية الأعمال
BCP	Business Continuity Plan خطة استمرارية الأعمال
BIA	Business Impact Analysis تحليل التأثير على الأعمال
CIP	Critical Infrastructure Protection حماية البنية التحتية الحساسة
CNI	Critical National Infrastructure البنية التحتية الوطنية الحساسة
CSF	[US NIST] Cybersecurity Framework إطار عمل الأمن السيبراني الأمريكي
DCS	Distributed Control System نظام تحكم موزع
DMZ	Demilitarized Zone المطقة المحايدة
DOE	[US] Department of Energy وزارة الطاقة الأمريكية
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
IEC	International Electrotechnical Commission اللجنة الكهروتقنية الدولية
IED	Intelligent Electronic Device الأجهزة الإلكترونية الذكية
IIoT	Industrial Internet of Things انترنت الأشياء الصناعي
I/O	Input/Output مدخل/مخرج
IRP	Incident Response Plan خطة الاستجابة للحوادث
ISA	International Society of Automation

	الجمعية الدولية للأتمتة
IT	Information Technology تقنية المعلومات
MDM	Mobile Device Management إدارة الأجهزة المحمولة
NCA	National Cybersecurity Authority الهيئة الوطنية للأمن السيبراني
NCS	National Cryptographic Standards المعايير الوطنية للتشفير
NERC CIP	North American Electric Reliability Corporation المعيار الأمريكي الخاص بقطاع الكهرباء
NIST	National Institute of Standards and Technology (US) المعهد الوطني للمعايير والتقنية
OT	Operational Technology التقنية التشغيلية
OTCC	Operational Technology Cybersecurity Controls ضوابط الأمن السيبراني للتقنية التشغيلية
PHA	Process Hazard Analysis تحليل مخاطر العمليات
PLC	Programmable Logic Controller التحكم المنطقي القابل للبرمجة
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 التكتيكات والتقنيات والإجراءات
TTX	Tabletop Exercise تمرين محاكاة افتراضي
VPN	Virtual Private Network الشبكة الافتراضية الخاصة

جدول (4) : قائمة الاختصارات