هذا المربع مخصّص لأغراض توجيهية. احذف جميع المربعات التوجيهية بعد تعبئة النموذج. يجب تحرير البنود الملوّنة باللون الأزرق بصورة مناسبة. ويجب إزالة التظليل الملون بعد إجراء التعديلات.

أدخل شعار الجهة بالضغط على الصورة الموضحة.

نموذج معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS)

اختر التصنيف

التاريخ: اضغط هنا لإضافة تاريخ

الإصدار: اضغط هنا لإضافة نص

المرجع: اضغط هنا لإضافة نص

استبدل <اسم الجهة> باسم الجهة في مجمل صفحات الوثيقة.
وللقيام بذلك، اتبع الخطوات التالية:

- اضغط على مفتاحي "Ctrl" و"H" في الوقت نفسه.
- أضف "<اسم الجهة>" في مربع البحث عن النص.
- أدخل الاسم الكامل لجهتك في مربع "استبدال" النص.
- اضغط على "المزيد" وتأكّد من اختيار "Match case".
- اضغط على "استبدل الكل".
- أغلق مربع الحوار.

إخلاء المسؤولية

طُور هذا النموذج عن طريق الهيئة الوطنية للأمن السيبراني كمثال توضيحي يمكن استخدامه كدليل ومرجع للجهات. يجب أن يتم تعديل هذا النموذج ومواءمته مع أعمال <اسم الجهة> والمتطلبات التشريعية والتنظيمية ذات العلاقة. كما يجب أن يُعتمد هذا النموذج من قبل رئيس الجهة أو من يقوم/تقوم بتفويضه. وتخلي الهيئة مسؤوليتها من استخدام هذا النموذج كما هو، وتؤكد على أن هذا النموذج ما هو إلا مثال توضيحي.

اعتماد الوثيقة

الدور	المسمى الوظيفي	الاسم	التاريخ	التوقيع
اختر الدور	<أدخل المسمى الوظيفي>	<أدخل الاسم الكامل للموظف>	اضغط هنا لإضافة تاريخ	<أدخل التوقيع>

نسخ الوثيقة

النسخة	التاريخ	عُدِّلَ بواسطة	أسباب التعديل
<أدخل رقم النسخة>	اضغط هنا لإضافة تاريخ	<أدخل الاسم الكامل للموظف>	<أدخل وصف التعديل>

جدول المراجعة

معدل المراجعة	التاريخ لأخر مراجعة	تاريخ المراجعة القادمة
مره واحدة كل سنة	اضغط هنا لإضافة تاريخ	اضغط هنا لإضافة تاريخ

اختر التصنيف

الإصدار <1.0>

قائمة المحتويات

الغرض

الغرض من هذا المعيار هو تحديد متطلبات الأمن السيبراني التفصيلية المتعلقة بأجهزة وأنظمة التحكم الصناعي (OT/ICS) لدى <اسم الجهة>. وتشمل أجهزة وأنظمة التحكم الصناعي (OT/ICS) كل الأصول والأجهزة والأنظمة المرتبطة بالبنية التحتية للأنظمة التشغيلية.

هذه المتطلبات تمت مواءمتها مع متطلبات الأمن السيبراني الصادرة عن الهيئة الوطنية للأمن السيبراني، ويشمل ذلك على سبيل المثال لا الحصر: الضوابط الأساسية للأمن السيبراني (ECC – 1: 2018) وضوابط الأمن السيبراني للأنظمة الحساسة (CSCC – 1: 2019) وضوابط الأمن السيبراني للحوسبة السحابية (CCC – 1: 2020) وضوابط الأمن السيبراني للأنظمة التشغيلية (OTCC-1: 2022) وغيرها من المتطلبات التشريعية والتنظيمية ذات العلاقة.

نطاق العمل

يغطي هذا المعيار جميع الأنظمة الموجودة ضمن شبكة أجهزة أنظمة التحكم الصناعي (OT/ICS) لدى <اسم الجهة> وينطبق على جميع العاملين (الموظفين والمتعاقدين) على تلك الأجهزة والأنظمة في <اسم الجهة>.

المعايير

1	المتطلبات العامة (General requirements)
الهدف	تحديد المتطلبات العامة لأجهزة وأنظمة التحكم الصناعي (OT/ICS) لضمان حماية توافرها وسلامتها وسريتها وإدارتها بشكل آمن واستخدامها بالشكل المناسب عند الحاجة.
المخاطر المحتملة	في حالة عدم استخدام أجهزة وأنظمة التحكم الصناعي (OT/ICS) بشكل صحيح وعدم إدارتها وفقًا لهذه المعايير الأمنية، فقد يؤدي ذلك إلى تداعيات وخيمة قد تتسبب في اختراق الأعمال والإخلال باستمرارية العمليات التشغيلية ووقوع خسائر مالية.
الإجراءات المطلوبة	
1-1	تثبيت كل أجهزة وأنظمة التحكم الصناعي (OT/ICS) في البنية التحتية لدى <اسم الجهة> وفقًا لسياسات ومعايير ومتطلبات الأمن السيبراني المعتمدة لضمان سلامة الأجهزة وأمنها وعملها بالشكل الصحيح.
2-1	تحديد كل أجهزة وأنظمة التحكم الصناعي (OT/ICS) وجردها وإدارتها وصيانتها وحمايتها وفقًا للمعايير المحددة مسبقًا والتوجيهات الصادرة عن الموردين وأفضل الممارسات ووفقًا للأنظمة واللوائح ذات العلاقة.

3-1	أن تشمل أجهزة وأنظمة التحكم الصناعي (OT/ICS) كل الأصول والأنظمة المسؤولة عن تنفيذ وصيانة العمليات التشغيلية لدى <اسم الجهة>، بما في ذلك وحدات التحكم في أجهزة أنظمة التحكم الصناعي (OT/ICS)، مثل أجهزة التحكم المنطقي القابلة للبرمجة (Programmable Logic Controllers)، ووحدات التحكم الطرفية (Remote Terminal Units)، وأنظمة التحكم الموزَّع (Distributed Controls Systems)، وأنظمة معدات السلامة (Safety Instrumented Systems) وغيرها من الأصول المسؤولة عن التحكم في العمليات التشغيلية لدى <اسم الجهة>.
4-1	إدارة جميع أجهزة وأنظمة التحكم الصناعي (OT/ICS) طوال دورة حياتها بالكامل وفقًا لمنهجية "الأمن من خلال التصميم" (Security-by-Design).
5-1	أن تكون جميع الوثائق المطلوبة بموجب معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS Security Standard) متوافقة مع هذا المعيار ومع ضوابط الأمن السيبراني للأنظمة التشغيلية (OTCC).
6-1	استخدام الأجزاء المشفرة أو المجموعات الاختبارية، إن أمكن، للتحقق من سلامة شفرة برامج وحدات التحكم في أجهزة وأنظمة التحكم الصناعي (OT/ICS) وإصدار إنذار في حالة تغييرها.
7-1	على مهندسي أنظمة التحكم في العمليات ضمان عدم قدرة المشغلين على إدخال بيانات أو ضبط إعدادات غير البيانات أو الإعدادات المطلوبة من الناحية العملية أو المادية في العملية.
2	التحكّم بالوصول (Access control)
الهدف	تحديد متطلبات عملية ضبط إعدادات الوصول إلى أجهزة وأنظمة التحكم الصناعي (OT/ICS) لضمان سير العملية بشكل سليم وآمن وفقًا للقواعد الأمنية المحددة.
المخاطر المحتملة	في حالة عدم تحديد ومراقبة صلاحيات الوصول إلى أجهزة وأنظمة التحكم الصناعي (OT/ICS) وإدارتها وفقًا للمعايير الأمنية لدى <اسم الجهة>، فقد يؤدي ذلك إلى انتهاكات تتعلق بصلاحيات الوصول وقد تتسبب في اختراق الأعمال والإخلال باستمرارية العمليات التشغيلية ووقوع خسائر مالية.
الإجراءات المطلوبة	
1-2	أن يقتصر استخدام موارد أجهزة وأنظمة التحكم الصناعي (OT/ICS) لدى <اسم الجهة> على المستخدمين المصرّح لهم أو البرامج أو العمليات أو الأنظمة الأخرى المصرَّح لها.
2-2	عدم منح صلاحية الوصول إلى أجهزة وأنظمة التحكم الصناعي (OT/ICS) إلا بعد تحديد هوية المستخدم ومنح التصريح له. ويجب على <اسم الجهة> تحديد وتوثيق أنواع الحسابات المستخدمة على تلك الأجهزة والأنظمة والامتيازات والصلاحيات الممنوحة لها.

3-2	إلغاء تفعيل الحسابات وكلمات المرور الافتراضية أو حذفها.
4-2	على <اسم الجهة> التأكّد من تطبيق آليات أو إجراءات لحماية الأنظمة وفقًا لمعايير إدارة الصلاحيات (Access Management) الخاصة بـ <اسم الجهة> والممارسات الأمنية العامة بناءً على معيار الجمعية الدولية للأتمتة / اللجنة الكهروتقنية الدولية (ISA/IEC 62443) أو المنشور الخاص للمعهد الوطني للمعايير والتقنية (NIST SP 800-82r2).
5-2	على <اسم الجهة> التأكد من عدم تأثير عملية تنفيذ صلاحيات الوصول المنطقي أو المادي إلى أجهزة وأنظمة التحكم الصناعي على استمرارية العمليات التشغيلية أو تعطيلها لها.
6-2	عدم منح المستخدمين سوى الحقوق والصلاحيات المطلوبة لهم تحديدًا لأداء المهام المطلوبة منهم (مبدأ الحد الأدنى من الصلاحيات والامتيازات). ويجب على وجه التحديد عدم منح صلاحيات مدير النظام، متى ما أمكن ذلك. ويجب إلغاء تفعيل الحسابات غير المطلوبة أو إزالتها، إن أمكن.
7-2	على <اسم الجهة> وضع وتوثيق القيود على الاستخدام ومتطلبات ضبط الإعدادات / الاتصال وإرشادات التنفيذ لكل نوع من أنواع الوصول عن بُعد المسموح بها.
8-2	تأمين جميع جلسات الوصول عن بُعد إلى أجهزة وأنظمة التحكم الصناعي (OT/ICS) وتشفيرها وتنفيذها بطريقة مقبولة لا تتداخل مع عمل تلك الأجهزة والأنظمة أو تؤثر عليه. ويجب مراقبة وتسجيل جميع اتصالات وأنشطة الوصول عن بُعد بصفة مستمرة.
9-2	يُحظر السماح بالوصول العام وغير الآمن إلى أجهزة وأنظمة التحكم الصناعي (OT/ICS). ويجب عدم السماح بالوصول إلى تلك الأجهزة والأنظمة من شبكات خارجية إلا عبر منطقة محايدة (DMZ) مخصصة لذلك.
10-2	على <اسم الجهة> توفير نقاط وصول عن بُعد (Jump Stations/Hosts) في منطقة محايدة (DMZ) لضمان التحكّم الصارم في وصول الاتصالات الخارجية إلى أجهزة وأنظمة التحكم الصناعي.
11-2	الفصل بين إعدادات وحدات التحكم و/ أو البرامج و/ أو بيانات التشغيل لأجهزة وأنظمة التحكم الصناعية (OT/ICS) بناءً على وسيط الوصول، مثل الواجهة المادية وبروتوكول الاتصال ونوع الأمر (على سبيل المثال، بدون صلاحيات (None) أو صلاحيات القراءة (Read) أو صلاحيات القراءة / الكتابة (Read/Write) للإعدادات / البرامج والشبكة الخارجية).
12-2	قصر صلاحيات الوصول إلى وحدات التحكم في أجهزة وأنظمة التحكم الصناعي لضبط إعداداتها أو صيانتها على مدير النظام المصرّح له فقط وحماية ذلك بحساب وكلمة مرور غير افتراضية.

3	التدقيق والمساءلة (Audit and accountability)
الهدف	تحديد متطلبات عمليات التدقيق والمساءلة لأجهزة وأنظمة التحكم الصناعي (OT/ICS) لضمان سيرها بشكل سليم وآمن وفقًا للقواعد الأمنية المحددة.
المخاطر المحتملة	في حالة عدم تحديد متطلبات التدقيق والمساءلة لأجهزة وأنظمة التحكم الصناعي (OT/ICS) بشكل صحيح وفقًا للمعايير الأمنية لدى <اسم الجهة>، فقد يؤدي ذلك إلى تداعيات وخيمة قد تتسبب في اختراق الأعمال والإخلال باستمرارية العمليات التشغيلية ووقوع خسائر مالية.
الإجراءات المطلوبة	
1-3	التحقق من أمن الشبكات والمكونات الأخرى لأجهزة وأنظمة التحكم الصناعي (OT/ICS) على فترات منتظمة. وفي حالة الأنظمة المعقدة، يجب تشكيل فرق متخصصة لتحديد سيناريوهات الهجمات المحتملة وتقييمها.
2-3	إجراء عمليات تدقيق دورية على أجهزة وأنظمة التحكم الصناعي (OT/ICS) للتحقق مما يلي: ● لا تزال الضوابط الأمنية التي كانت موجودة أثناء اختبار التحقق من الأنظمة موجودة وتعمل بشكل صحيح في نظام الإنتاج. ● خلو نظام الإنتاج من الثغرات الأمنية وتوفيره للمعلومات عن طبيعة الثغرات ونطاقها حال وجودها، قدر الإمكان. ● اتباع برنامج إدارة التغييرات بدقة بالغة، مع إجراء جولة لمراجعة جميع التغييرات واعتمادها.
3-3	في بعض الحالات، حينما لا يكون بإمكان أجهزة وأنظمة التحكم الصناعي (OT/ICS) دعم استخدام الآليات والإجراءات الآلية لإعداد سجلات التدقيق، يجب على <اسم الجهة> استخدام الآليات أو الإجراءات غير الآلية كضوابط بديلة وفقًا للممارسات الأمنية العامة بناءً على معيار الجمعية الدولية للأتمتة / اللجنة الكهروتقنية الدولية (ISA/IEC 62443) أو المنشور الخاص للمعهد الوطني للمعايير والتقنية (NIST SP 800-82r2).
4	التقييم والمراقبة (Assessment and monitoring)
الهدف	تحديد متطلبات عمليات تقييم ومراقبة أجهزة وأنظمة التحكم الصناعي (OT/ICS) لضمان سيرها بشكل سليم وآمن وفقًا للقواعد الأمنية المحددة.
المخاطر المحتملة	يمكن أن يؤدي عدم تقييم ومراقبة أجهزة وأنظمة التحكم الصناعي (OT/ICS) إلى عواقب وخيمة فيما يتعلق بالأمن. كما أن غياب المراقبة يمكن أن يؤدي إلى عدم إمكانية كشف التغييرات غير المصرّح بها، مما يضر باستمرارية العمليات والإجراءات.
الإجراءات المطلوبة	

1-4	إجراء عمليات تقييم أجهزة وأنظمة التحكم الصناعي (OT/ICS) من قبل مقيّمين مؤهلين ومفوضين من <اسم الجهة>.
2-4	قبل تطبيق أي ضوابط أمنية على أجهزة وأنظمة التحكم الصناعي (OT/ICS)، يجب إجراء تقييم مناسب للمخاطر لضمان عدم تأثير تطبيق تلك الضوابط على العمليات التشغيلية أو استمرارية الأعمال وعدم تقليله للقدرات الأمنية للأنظمة.
3-4	عند تقييم المخاطر، يجب على <اسم الجهة> التحقق من أن تطبيق أي ضوابط أمنية على أجهزة وأنظمة التحكم الصناعي (OT/ICS) لن يؤثر على مكونات الأنظمة الأخرى.
4-4	أن يكون لدى المقيّمين المسؤولين عن إجراء التقييم فهم كامل للسياسات والإجراءات الأمنية التنظيمية (خاصةً تلك المتعلقة بأجهزة وأنظمة التحكم الصناعي (OT/ICS)) وللمخاطر المحددة المتعلقة بالصحة والسلامة والبيئة والمرتبطة بمرفق و/ أو عملية معينة.
5-4	في حالة الحاجة إلى فصل أحد أجهزة وأنظمة التحكم الصناعي (OT/ICS) لإجراء تقييم معين عليه (مثل اختبارات الاختراق وعمليات مسح الثغرات)، يجب تحديد مواعيد التقييم و/ أو عمليات المسح بحيث يتم تنفيذها خلال أوقات توقف أجهزة وأنظمة التحكم الصناعي (OT/ICS) المخطط لها عند الإمكان.
6-4	استخدام مسح الثغرات واختبار الاختراق بعناية على شبكات أجهزة وأنظمة التحكم الصناعي (OT/ICS) لضمان عدم التأثير سلبًا على وظائف تلك الأجهزة والأنظمة بسبب عملية المسح.
7-4	حجب عمليات مسح الثغرات الناشئة من شبكة تقنيات المعلومات على مستوى حركة البيانات على الشبكة لضمان عدم مسحها لشبكة أجهزة وأنظمة التحكم الصناعي (OT/ICS).
5	إدارة النسخ الاحتياطي (Backup management)
الهدف	تحديد متطلبات عملية إدارة النسخ الاحتياطي لأجهزة وأنظمة التحكم الصناعي (OT/ICS) لضمان سير العملية بشكل سليم وآمن وفقًا للقواعد الأمنية المحددة.
المخاطر المحتملة	في حالة عدم تحديد متطلبات عملية إدارة النسخ الاحتياطي لأجهزة وأنظمة التحكم الصناعي (OT/ICS) وعدم تنفيذ تلك المتطلبات، فقد يؤدي ذلك إلى عواقب وخيمة قد تؤثر على استمرارية العمليات التشغيلية وتتسبب في وقوع خسائر مالية.
الإجراءات المطلوبة	
1-5	على <اسم الجهة> حفظ نسخ احتياطية من أجهزة وأنظمة التحكم الصناعي (OT/ICS) بصفة منتظمة بحسب الإجراءات المحددة لكل جهاز ونظام منها. ويجب ألا تؤثر عملية النسخ الاحتياطي على استمرارية العمليات التشغيلية أو الأعمال.

2-5	أن تشمل النسخ الاحتياطية جميع أجهزة وأنظمة التحكم الصناعي (OT/ICS) المخصصة للتحكم في العمليات ومراقبتها (ويجب ألا يقتصر ذلك على الأجهزة التي تعمل بنظام Windows ونظام Linux فقط).
3-5	أن تشمل عملية النسخ الاحتياطي لأجهزة وأنظمة التحكم الصناعي (OT/ICS) الأنظمة والبرامج والتراخيص المثبَّتة وإعدادات المكونات والقيم الحالية والأولية لمتغيرات العمليات.
4-5	تحديث النسخ الاحتياطية لأجهزة وأنظمة التحكم الصناعي (OT/ICS) بصفة منتظمة والتحقق منها في بيئة مخصصة بحيث لا تؤثر على استمرارية العمليات التشغيلية أو الأعمال.
5-5	في حالة عدم إمكانية تنفيذ النسخ الاحتياطي للأنظمة وهي قيد التشغيل، فيجب تنفيذه خلال فترات الصيانة والتخطيط لذلك مسبقًا.
6-5	على <اسم الجهة> ضمان الالتزام بقواعد الاحتفاظ بالنسخ الاحتياطية. يجب إعداد النسخ الاحتياطية بحيث تغطي حالة الأجهزة والأنظمة بعد اختبار القبول الميداني (Site Acceptance Test) وقبل جميع فترات صيانة أجهزة وأنظمة التحكم الصناعي (OT/ICS).
7-5	تحديد جميع عمليات النسخ الاحتياطي لأجهزة وأنظمة التحكم الصناعي (OT/ICS) مسبقًا وضبط إعداداتها وأتمتتها (إن أمكن).
8-5	على <اسم الجهة> توفير خادم مخصص للنسخ الاحتياطية لأجهزة وأنظمة التحكم الصناعي (OT/ICS).
9-5	عزل شبكة خادم النسخ الاحتياطية لأجهزة وأنظمة التحكم الصناعي (OT/ICS) ماديًا ومنطقيًا عن باقي شبكة أجهزة وأنظمة التحكم الصناعي (OT/ICS).
6	إدارة الإعدادات (Configuration management)
الهدف	تحديد متطلبات إدارة إعدادات أجهزة وأنظمة التحكم الصناعي (OT/ICS) لضمان سير العملية بشكل سليم وآمن وفقًا للقواعد الأمنية المحددة.
المخاطر المحتملة	في حالة عدم تحديد الإعدادات الأساسية لأجهزة وأنظمة التحكم الصناعي (OT/ICS) وتنفيذ عملية إدارة تلك الإعدادات وفقًا للمعايير الأمنية لدى <اسم الجهة>، فقد يؤدي ذلك إلى عواقب وخيمة قد تتسبب في الإخلال باستمرارية العمليات التشغيلية والأعمال ووقوع خسائر مالية.
الإجراءات المطلوبة	
1-6	توثيق إعدادات جميع أجهزة وأنظمة التحكم الصناعي (OT/ICS) المصرّح بها لدى <اسم الجهة> والاحتفاظ بها وإلزام جميع ملاك الأصول المعنيين باتباعها.

2-6	وضع سياسة وإجراءات إدارة الإعدادات واستخدامها للتحكم في التعديلات على الأجهزة والبرمجيات الثابتة والبرمجيات والوثائق لضمان حماية أجهزة وأنظمة التحكم الصناعي (OT/ICS) من التعديلات غير المناسبة قبل وأثناء وبعد تنفيذها على الأنظمة.
3-6	تطوير وتوثيق الإعدادات الأمنية الأساسية أجهزة وأنظمة التحكم الصناعي (OT/ICS)، بما يشمل جوانب الاتصالات والتشغيل والربط بالأنظمة، ومراجعتها بشكل رسمي.
4-6	ضبط إعدادات أجهزة وأنظمة التحكم الصناعي (OT/ICS) في أي بيئة حساسة بحيث لا يكون هناك سوى أقل عدد ممكن من نقاط الهجوم وبحيث تدعم الوظائف المطلوبة فقط. ويجب تعطيل جميع الوظائف والخدمات والبروتوكولات والمنافذ غير المستخدمة
5-6	تحديد وتنفيذ آليات للحماية من التلاعب في العمليات الجارية حاليًا، على أن يتم تعديل الآليات وتخصيصها بما يتناسب مع العملية ذات الصلة.
6-6	ضبط إعدادات أجهزة وأنظمة التحكم الصناعي (OT/ICS) وصيانتها وفقًا لمبدأ الحد الأدنى من الإمكانيات. ويجب أن يتبنى نظام إدارة التغيير المخصص التغييرات في إعدادات الأنظمة.
7-6	إلغاء تفعيل واجهات الأجهزة أو حمايتها من الوصول إليها أو إساءة استخدامها، ما لم تكن مطلوبة لاستمرارية العمليات.
8-6	استخدام أحدث أنظمة التشغيل المدعومة بالكامل فقط على جميع أجهزة وأنظمة التحكم الصناعي (OT/ICS).
9-6	تسجيل جميع التغييرات في الإعدادات ومراقبتها. ويجب ضبط إعدادات الحل المستخدم في إعداد السجلات بحيث لا يرسل سوى سجلات معينة إلى نظام السجلات المركزي باستخدام بروتوكول سجل النظام (syslog) وأن تكون بتنسيق CEF أو LEEF أو RFC 5425 المحدد للسجلات.
10-6	على <اسم الجهة> تحصين أجهزة وأنظمة التحكم الصناعي (OT/ICS) بصفة منتظمة لمعالجة المخاطر والثغرات فيها. وتشمل عملية التحصين تلك (على سبيل المثال لا الحصر) ما يلي: ● تثبيت التحديثات والإصلاحات لأنظمة التشغيل والتطبيقات والبرمجيات ● تحديث البرمجيات الثابتة ● تأمين الإعدادات ● تقييد الوصول إلى المستخدمين والحسابات ● إزالة البرمجيات والمكونات غير الضرورية
11-6	على <اسم الجهة> تحديد وتحليل المخاطر المرتبطة بأجهزة وأنظمة التحكم الصناعي (OT/ICS) القديمة التي تعمل على شبكة <اسم الجهة> باستمرار. وبالنسبة لجميع الأجهزة القديمة التي لا يمكن تثبيت التحديثات والإصلاحات عليها، يجب على <اسم الجهة> تنفيذ ضوابط بديلة، مثل:

	• عزل الأجهزة • نقل الأجهزة إلى أجزاء آمنة من الشبكة • قصر الاتصال على الخدمات الضرورية فقط • تطبيق تقنية الحماية المعزولة (Sandbox) على الأجهزة / الأنظمة التي تبدو كالأصلية • استخدام آلية التجزئة الدقيقة (micro-segmentation)
12-6	إذا كانت وحدات التحكم في أجهزة وأنظمة التحكم الصناعي (OT/ICS) تتيح تعطيل المنافذ المادية وخدمات الشبكة والأوامر الفردية، فيجب تعطيل الميزات غير المستخدمة.
13-6	تعطيل الميزات التي يسهل استغلالها، مثل خادم الويب المدمج أو الميزات الأقل استخدامًا.
14-6	مزامنة كل ساعات أجهزة وأنظمة التحكم الصناعي (OT/ICS) باستخدام الآليات المناسبة، مثل بروتوكول وقت الشبكة (Network Time Protocol) أو بروتوكول الوقت الدقيق (Precision Time Protocol).
15-6	حماية أجهزة وأنظمة التحكم الصناعي (OT/ICS) من التلاعب في مفاتيح الأوضاع (mode switches) أو التغييرات في عنوان بروتوكول الإنترنت (IP address) أو التغييرات في الرقم التعريفي لعُقدة وحدة التحكم.
16-6	تقسيم رموز وحدات التحكم في أجهزة وأنظمة التحكم الصناعي (OT/ICS) إلى وحدات، باستخدام كتل الوظائف المختلفة.
17-6	إدخال المنطق التشغيلي مباشرةً في وحدات التحكم في أجهزة وأنظمة التحكم الصناعي (OT/ICS)، وليس في أجهزة واجهات التعامل مع الأنظمة (HMIs) أو أي واجهات أجهزة أخرى.
7	التخطيط للاستمرارية (Continuity planning)
الهدف	تحديد متطلبات إدارة استمرارية أجهزة وأنظمة التحكم الصناعي (OT/ICS) لضمان سير العملية بشكل سليم وآمن وفقًا للقواعد الأمنية المحددة.
المخاطر المحتملة	في حالة عدم التخطيط لاستمرارية أجهزة وأنظمة التحكم الصناعي (OT/ICS) وإدارتها بشكل صحيح وفقًا للمعايير الأمنية لدى <اسم الجهة>، فقد يؤدي ذلك إلى عواقب وخيمة قد تؤثر سلبيًا على استمرارية الأعمال والعمليات التشغيلية وتتسبب في وقوع خسائر مالية.
الإجراءات المطلوبة	
1-7	على <اسم الجهة> وضع خطط لاستمرارية أجهزة وأنظمة التحكم الصناعي (OT/ICS) وإجراءات للتعافي من الكوارث المصنفة ضمن فئات الاضطرابات أو الأعطال المحددة وفقًا لسياسة استمرارية أعمال الأمن السيبراني لدى <اسم الجهة> والممارسات العامة لاستمرارية الأعمال بناءً على معيار الجمعية الدولية للأتمتة / اللجنة

	الكهروتقنية الدولية (ISA/IEC 62443) أو المنشور الخاص للمعهد الوطني للمعايير والتقنية (NIST SP 800-82r2).
2-7	في حالة فقدان المعالجة داخل أجهزة وأنظمة التحكم الصناعي (OT/ICS) أو فقدان الاتصال مع المرافق التشغيلية، يجب أن تنفذ أجهزة وأنظمة التحكم الصناعي (OT/ICS) إجراءات محددة مسبقًا (تشمل استعادة متغيرات حالة النظام).
3-7	في الحالات التي لا يمكن فيها ل<اسم الجهة> اختبار خطة الاستمرارية أو خطة التعافي من الكوارث أو التمرين عليهما على أجهزة وأنظمة التحكم الصناعي (OT/ICS) في بيئة الإنتاج بسبب الآثار السلبية الكبيرة التي قد تحدث فيما يتعلق بالأداء أو السلامة أو الموثوقية، حينها يجب على <اسم الجهة> تطبيق الضوابط البديلة المناسبة وفقًا لسياسة استمرارية أعمال الأمن السيبراني وسياسة إدارة النسخ الاحتياطي والتعافي من الكوارث لدى <اسم الجهة> والممارسات الأمنية العامة بناءً على معيار الجمعية الدولية للأتمتة / اللجنة الكهروتقنية الدولية (ISA/IEC 62443) أو المنشور الخاص للمعهد الوطني للمعايير والتقنية (NIST SP 800-82r2).
8	الاستجابة للحوادث (Incident response)
الهدف	تحديد متطلبات الاستجابة لحوادث أجهزة وأنظمة التحكم الصناعي (OT/ICS) لضمان سير العملية بشكل سليم وآمن وفقًا للقواعد الأمنية المحددة.
المخاطر المحتملة	في حالة عدم وضع خطة الاستجابة لحوادث أجهزة وأنظمة التحكم الصناعي (OT/ICS) وإدارتها بشكل صحيح وفقًا للمعايير الأمنية لدى <اسم الجهة>، فقد يؤدي ذلك إلى عواقب وخيمة قد تؤثر سلبيًا على استمرارية الأعمال والعمليات التشغيلية وتتسبب في وقوع خسائر مالية.
الإجراءات المطلوبة	
1-8	على <اسم الجهة> وضع خطة للاستجابة لحوادث أجهزة وأنظمة التحكم الصناعي (OT/ICS) تتضمن الإجراءات المطلوب اتباعها في حالة وجود تسلل للحد من تأثيره. ويجب أن تكون خطط الاستجابة لحوادث أجهزة وأنظمة التحكم الصناعي (OT/ICS) المحددة متكاملة ومتوافقة مع الخطط المؤسسية والإجراءات المحددة فيها، مثل خطط الاستجابة لحوادث تقنية المعلومات وخطة إدارة الأزمات وخطة استمرارية الأعمال.
2-8	على <اسم الجهة> إعداد دليل إرشادي مخصص للتعامل مع الحوادث المتعلقة بأجهزة وأنظمة التحكم الصناعي (OT/ICS).
3-8	إعداد جميع الخطط والأدلة الإرشادية بطريقة تحول دون التأثير أو الإخلال باستمرارية العمليات التشغيلية والإجراءات والأعمال.

9	الصيانة (Maintenance)
الهدف	تحديد متطلبات صيانة أجهزة وأنظمة التحكم الصناعي (OT/ICS) لضمان سير العملية بشكل سليم وآمن وفقًا للقواعد الأمنية المحددة.
المخاطر المحتملة	في حالة عدم تحديد متطلبات صيانة أجهزة وأنظمة التحكم الصناعي (OT/ICS) وإرساء عملية لإدارتها بشكل صحيح وتنفيذ تلك العملية وفقًا للمعايير الأمنية لدى <اسم الجهة>، فقد يؤدي ذلك إلى عواقب وخيمة قد تؤثر سلبيًا على استمرارية الأعمال والعمليات التشغيلية وتتسبب في وقوع خسائر مالية.
الإجراءات المطلوبة	
1-9	على <اسم الجهة> وضع سياسة وإجراءات لإجراء الصيانة الروتينية والوقائية لمكونات أجهزة وأنظمة التحكم الصناعي (OT/ICS).
2-9	على <اسم الجهة> تحديد مواعيد مسبقة لصيانة جميع أجهزة وأنظمة التحكم الصناعي (OT/ICS) حتى لا تؤثر على استمرارية العمليات أو الأعمال.
3-9	تحديد قواعد الصيانة واتفاقية مستوى الخدمة والاتفاق عليها مع مورّدي أجهزة وأنظمة التحكم الصناعي (OT/ICS) لتوضيح المسؤوليات المحددة وتلبية توقعات <اسم الجهة>.
4-9	دعم جميع أجهزة وأنظمة التحكم الصناعي (OT/ICS) وصيانتها طوال دورة حياتها بالكامل.
5-9	تحديث أجهزة وأنظمة التحكم الصناعي (OT/ICS) القديمة على الفور خلال الأوقات المحددة لإيقاف عمل تلك الأجهزة والأنظمة.
6-9	أجهزة وأنظمة التحكم الصناعي (OT/ICS) غير المدعمة أو ترحيلها على الفور أو تطبيق ضوابط أمنية مخصصة لها في حالات معينة.
10	أمن الشبكة (Network security)
الهدف	تحديد متطلبات أمن شبكة أجهزة وأنظمة التحكم الصناعي (OT/ICS) لضمان سير العملية بشكل سليم وآمن وفقًا للقواعد الأمنية المحددة.
المخاطر المحتملة	يمكن أن يؤدي القصور في حماية شبكة أجهزة وأنظمة التحكم الصناعي (OT/ICS) إلى تداعيات خطيرة تُفضي إلى اختراق بيئة العمل والعمليات، وهو ما قد يؤثر على استمرارية العمليات التشغيلية ويتسبب في وقوع خسائر مالية.
الإجراءات المطلوبة	

1-10	تقييد حركة مرور البيانات بين شبكة أجهزة وأنظمة التحكم الصناعي (OT/ICS) وشبكة تقنية المعلومات وأن تكون هناك نقطة اتصال واحدة بين هاتين الشبكتين وأن تمر جميع البيانات عبر جدار الحماية المحيط.
2-10	على <اسم الجهة> تنفيذ الهندسة المرجعية للشبكة بناءً على معيار الجمعية الدولية للأتمتة / اللجنة الكهروتقنية الدولية (ISA/IEC 62443) ونموذج الهندسة المرجعية (نموذج بوردو "Purdue model") لتمييز الطبقات التالية على الأقل: • شبكة تقنية المعلومات • المنطقة المحايدة (DMZ) لتقنية المعلومات / الأنظمة التشغيلية • الشبكة الإشرافية لأجهزة وأنظمة التحكم الصناعي (OT/ICS) • شبكة عمليات أجهزة وأنظمة التحكم الصناعي (OT/ICS)
3-10	ربط كل أصل من أصول أجهزة وأنظمة التحكم الصناعي (OT/ICS) بطبقة محددة في الشبكة.
4-10	مراقبة حركة مرور البيانات داخل شبكة أجهزة وأنظمة التحكم الصناعي (OT/ICS) وعبر محيط شبكة تقنية المعلومات / الأنظمة التشغيلية وإدارتها والتحكم فيها.
5-10	يجب على <اسم الجهة> استخدام أدوات مراقبة حركة مرور البيانات على شبكة أجهزة وأنظمة التحكم الصناعي (OT/ICS) المخصصة فقط، مع استخدام أساليب وآليات المراقبة غير المباشرة.
6-10	يجب أن تعتمد أنظمة الكشف عن التسلل إلى أجهزة وأنظمة التحكم الصناعي (OT/ICS) التي تستخدمها <اسم الجهة> فقط على المراقبة غير المباشرة لحركة مرور البيانات باستخدام توقيعات الهجمات المطورة لمختلف بروتوكولات أجهزة وأنظمة التحكم الصناعي (OT/ICS) وضمان ألا يؤثر استخدامها سلبًا على الأداء التشغيلي لتلك الأجهزة والأنظمة.
7-10	يجب على <اسم الجهة> استخدام الجيل الجديد من جدران الحماية كأجهزة حماية محيطية. ويجب أن يكون بإمكان جدران الحماية المستخدمة التعرف على بروتوكولات الشبكة الصناعية ودعمها.
8-10	بالنسبة للأنظمة الحساسة التي تتطلب مرور البيانات في اتجاه واحد على الشبكة، يجب استخدام أجهزة نقل البيانات في اتجاه واحد (Data diodes) وفقًا لمعيار أجهزة نقل البيانات في اتجاه واحد (Data diode standard) المطبق لدى <اسم الجهة>.
9-10	يجب على <اسم الجهة> تحديد متطلبات الإعدادات ومتطلبات الاتصال وإرشادات التنفيذ لكل نوع من أنواع الوصول اللاسلكي لأجهزة وأنظمة التحكم الصناعي (OT/ICS). يجب على <اسم الجهة> استخدام البروتوكولات المطورة والمعتمدة فقط للاتصال اللاسلكي بأجهزة وأنظمة التحكم الصناعي (OT/ICS) وفقًا للمنشور الخاص للمعهد الوطني للمعايير والتقنية (NIST SP 800-82r2).

11	الحماية المادية والبيئية (Physical and environmental protection)
الهدف	تحديد متطلبات الحماية المادية والبيئية لأجهزة وأنظمة التحكم الصناعي (OT/ICS) لضمان سير العملية بشكل سليم وآمن وفقًا للقواعد الأمنية المحددة.
المخاطر المحتملة	يمكن أن يؤدي القصور في الحماية المادية والبيئية لأجهزة وأنظمة التحكم الصناعي (OT/ICS) إلى تداعيات خطيرة تُفضي إلى اختراق بيئة العمل والعمليات، وهو ما قد يؤثر على استمرارية العمليات التشغيلية ويتسبب في وقوع خسائر مالية.
الإجراءات المطلوبة	
1-11	توفير الحماية المادية للمكونات السيبرانية والبيانات المتعلقة بأجهزة وأنظمة التحكم الصناعي (OT/ICS) في إطار توفير الأمن بوجه عام في الموقع.
2-11	على <اسم الجهة> توفير محيط أمني مادي (العديد من الحواجز، المباشرة وغير المباشرة، حول المباني أو المرافق أو الغرف أو المعدات أو أنظمة المعلومات الأخرى). وتشمل ضوابط الأمن المادي التي تهدف إلى حماية المواقع الفعلية الأسوار أو حواجز منع مرور المركبات أو الأرصفة أو الجدران أو الحواجز الخرسانية المسلحة أو البوابات أو غيرها من التدابير.
3-11	أن تضمن أنظمة التحكم بالوصول عدم وصول سوى الأشخاص المصرّح لهم فقط إلى المناطق الخاضعة للمراقبة. ويجب أن يتيح النظام التحقق من إمكانية التعرّف بوضوح وسرّية على الأشخاص الذين تم منحهم صلاحيات الوصول. ويجب أن تكون إجراءات التحكّم بالوصول موثوقة للغاية، وألا تؤثر على المهام الروتينية أو الطارئة للعاملين في المكان (الموظفون والمتعاقدون).
4-11	مراعاة جميع العوامل البيئية عند تلبية الاحتياجات الأمنية، على سبيل المثال: • إذا كان الموقع به غبار، فيجب وضع الأنظمة والأجهزة داخل خزائن خاصة بها فلاتر لتنقية الهواء، • إذا كان من المحتمل أن يشكل الاهتزاز مشكلة، فيجب تثبيت الأنظمة والأجهزة على بطانات مطاطية لتفادي مشاكل تعطل الأقراص وتوصيل الأسلاك، • يجب توفير درجة حرارة ورطوبة ثابتة للأنظمة والوسائط.
5-11	أن تدعم أنظمة التدفئة والتهوية والتكييف (HVAC) في غرف التحكم العاملين في الموقع (الموظفين والمتعاقدين) خلال ظروف العمل العادية وحالات الطوارئ.
6-11	من الضروري توفير مصدر طاقة موثوق لأجهزة وأنظمة التحكم الصناعي (OT/ICS)، لذلك يجب توفير مصادر طاقة متعددة وغير منقطعة أو مولّد احتياطي. ويجب ضبط القدرات بدقة، على أقل تقدير، حتى يمكن إيقاف تشغيل النظام بأمان.
7-11	يُحظر تمامًا السماح بخروج أجهزة وأنظمة التحكم الصناعي (OT/ICS) وغيرها من الأجهزة المستخدمة لأداء الوظائف المتعلقة بأجهزة وأنظمة التحكم الصناعي

	(OT/ICS) من المنطقة المخصصة لها واستخدامها خارج شبكة أجهزة وأنظمة التحكم الصناعي (OT/ICS).
12	تقييم المخاطر (Risk assessment)
الهدف	تحديد متطلبات تقييم المخاطر المتعلقة بأجهزة وأنظمة التحكم الصناعي (OT/ICS) لضمان سير العملية بشكل سليم وآمن وفقًا للقواعد الأمنية المحددة.
المخاطر المحتملة	في حالة عدم تحديد متطلبات تقييم المخاطر المتعلقة بأجهزة وأنظمة التحكم الصناعي (OT/ICS) وإدارتها بشكل صحيح وتنفيذ عملية إدارتها وفقًا للمعايير الأمنية لدى <اسم الجهة>، فقد يؤدي ذلك إلى عواقب وخيمة قد تؤثر سلبيًا على استمرارية الأعمال والعمليات التشغيلية وتتسبب في وقوع خسائر مالية.
الإجراءات المطلوبة	
1-12	على <اسم الجهة> وضع سياسات وإجراءات تقييم المخاطر المتعلقة بأجهزة وأنظمة التحكم الصناعي (OT/ICS) من أجل تحديد المخاطر وحجم الضرر الذي قد ينتج عن الوصول غير المصرح به إلى أنظمة المعلومات والبيانات أو استخدامها أو الإفصاح عنها أو الإخلال بها أو تعديلها أو إتلافها دون تصريح.
2-12	تقدير حجم المخاطر المحتملة لتدفق البيانات من شبكة أجهزة وأنظمة التحكم الصناعي (OT/ICS) إلى الشبكة المؤسسية على أساس قيمة البيانات.
3-12	أن يتضمن تقييم المخاطر المتعلقة بأجهزة وأنظمة التحكم الصناعي (OT/ICS) جميع العوامل المؤثرة على استمرارية الأعمال: الأمن السيبراني، والسلامة، والأمن المادي، واستمرارية العمليات.
13	حماية النظام والاتصالات وسلامة المعلومات (System, communication protection and information integrity)
الهدف	تحديد متطلبات حماية أجهزة وأنظمة التحكم الصناعي (OT/ICS) واتصالاتها وسلامة معلوماتها لضمان سير العملية بشكل سليم وآمن وفقًا للقواعد الأمنية المحددة.
المخاطر المحتملة	في حالة عدم تحديد متطلبات حماية أجهزة وأنظمة التحكم الصناعي (OT/ICS) واتصالاتها وسلامة معلوماتها وإدارة تنفيذ تلك المتطلبات وفقًا للمعايير الأمنية لدى <اسم الجهة>، فقد يؤدي ذلك إلى عواقب وخيمة قد تؤثر سلبًا على اتصالات الأنظمة وقد تهدد استمرارية العمليات التشغيلية وتتسبب في وقوع خسائر مالية.
الإجراءات المطلوبة	
1-13	يجب على <اسم الجهة> تحديد نمط العطل المحتمل (failure mode) لجميع أجهزة وأنظمة التحكم الصناعي (OT/ICS).

2-13	على مستوى التطبيق، يجب استخدام نسخ آمنة من البروتوكولات وكذلك من الآليات المصاحبة للتشفير والتحقق من السلامة والموثوقية.
3-13	تحديد مدى الحاجة إلى استخدام التشفير بعد تقييم المخاطر وتحليل الاحتياجات الأمنية والتداعيات المحتملة على أداء النظام. ويجب على <اسم الجهة> مراعاة ما إذا كان التأخير في الاستجابة الناتج عن استخدام التشفير سيؤثر سلبيًا على الأداء التشغيلية لأجهزة وأنظمة التحكم الصناعي (OT/ICS).
4-13	قبل نشر التشفير في بيئة أجهزة وأنظمة التحكم الصناعي (OT/ICS)، يجب إجراء اختبارات شاملة لأداء الحلول.
5-13	أن تكون جميع حلول التشفير المستخدمة والمطبقة على أجهزة وأنظمة التحكم الصناعي (OT/ICS) متوافقة مع سياسة ومعايير التشفير التي تم إعدادها.
6-13	في بعض الحالات، حينما لا يكون بإمكان أجهزة وأنظمة التحكم الصناعي (OT/ICS) حماية موثوقية جلسات الاتصالات، يجب على <اسم الجهة> استخدام ضوابط بديلة وفقًا للممارسات الأمنية العامة بناءً على معيار الجمعية الدولية للأتمتة / اللجنة الكهروتقنية الدولية (ISA/IEC 62443) أو المنشور الخاص للمعهد الوطني للمعايير والتقنية (NIST SP 800-82r2).
7-13	تطبيق ضوابط مخصصة لأجهزة وأنظمة التحكم الصناعي (OT/ICS) من أجل الكشف عن الشفرات الضارة والحماية من الرسائل الاقتحامية وبرمجيات التجسس وكشف التسلل.
8-13	تحديد مدى الحاجة للحماية من الشفرات الضارة بعد الدراسة المتأنية والتحقق من أنها لن تؤثر سلبيًا على الأداء التشغيلي لأجهزة وأنظمة التحكم الصناعي (OT/ICS).
9-13	على <اسم الجهة> استخدام نظام حماية الأجهزة الطرفية (Endpoint Protection System) الموصى به من مورّد أجهزة وأنظمة التحكم الصناعي (OT/ICS): • يجب تأمين أنظمة Windows وUnix وLinux وغيرها من الأنظمة المستخدمة كوحدات تشغيل ووحدات عمل هندسية وأجهزة لتسجيل وحفظ البيانات وأجهزة لواجهات التعامل مع الأنظمة (HMIs) وأنظمة للتحكم الإشرافي وتحصيل البيانات (SCADA) ذات أغراض عامة وخوادم للنسخ الاحتياطي وفقًا للممارسات الأمنية المعتادة بناءً على معيار أمن أجهزة المستخدمين (Workstations Security standard) لدى <اسم الجهة>. • كما يجب اتباع توصيات المورّد فيما يتعلق بجميع الخوادم وأجهزة المستخدمين الأخرى في بيئة أنظمة التحكم (أنظمة التحكم الموزّع (DCS) وأجهزة التحكم المنطقي القابلة للبرمجة (PLC) وغيرها من المعدات) ذات الشفرة المعتمدة على الوقت، والتي تعتمد على نظام تشغيل معدّل أو موسّع.
10-13	على <اسم الجهة> التأكد من عدم تأثير استخدام أدوات وأساليب المراقبة سلبًا على الأداء التشغيلي لأجهزة وأنظمة التحكم الصناعي (OT/ICS).

11-13	عدم إيقاف أو إعادة تشغيل أجهزة وأنظمة التحكم الصناعي (OT/ICS) بشكل آلي دون إذن من مسؤول النظام عند تحديد أي خلل.
12-13	دعم أجهزة وأنظمة التحكم الصناعي (OT/ICS) المصنفة باعتبارها حساسة بالنسبة إلى <اسم الجهة> من خلال أنظمة احتياطية وأنظمة لإيقاف التشغيل في حالة الطوارئ لحمايتها وضمان توافر العمليات بشكل كبير.
13-13	على <اسم الجهة> التأكد من عدم تأثير استخدام تطبيقات التحقق من السلامة سلبًا على الأداء التشغيلي لأجهزة وأنظمة التحكم الصناعي (OT/ICS).
14-13	مراقبة وحدات التحكم في أجهزة وأنظمة التحكم الصناعي (OT/ICS) من حيث تكرار الأنشطة غير الطبيعية ويجب اتخاذ الإجراءات المناسبة في حالة اكتشافها.
15-13	أن تكون بروتوكولات الاتصالات الصناعية المستخدمة في وحدات التحكم في أجهزة وأنظمة التحكم الصناعي (OT/ICS) معروفة وموثقة بشكل جيد.
16-13	أن تكون بروتوكولات الاتصال التي تستخدمها وحدات التحكم في أجهزة وأنظمة التحكم الصناعي (OT/ICS) لتبادل البيانات مع الأنظمة الموجودة خارج منطقة أجهزة وأنظمة التحكم الصناعي (OT/ICS) (الحلول الموجودة خارج تلك المنطقة) من الممكن التعرف عليها من خلال جدار الحماية الصناعي وأنظمة منع التسلل (IPS) / أنظمة كشف التسلل (IDS) المخصصة للأنشطة الصناعية.
17-13	تحديد الحالات الآمنة للعمليات في حالة إعادة تشغيل وحدات التحكم في أجهزة وأنظمة التحكم الصناعي (OT/ICS) (على سبيل المثال، توصيل الطاقة، أو فصل الطاقة، أو الحفاظ على الحالة السابقة).
18-13	الاحتفاظ بسجلات تشخيص وحدات التحكم في أجهزة وأنظمة التحكم الصناعي (OT/ICS) حتى تكون متاحة في حالة تحليلها. ويجب إرسال سجلات التشخيص إلى خوادم جمع السجلات الخارجية.
19-13	تسجيل حالات الإيقاف الإجباري لوحدات التحكم في أجهزة وأنظمة التحكم الصناعي (OT/ICS) نتيجة الأعطال أو إيقاف التشغيل ومراقبتها للرجوع إليها قبل إعادة تشغيل وحدات التحكم.
20-13	قياس استخدام الذاكرة بالنسبة لكل وحدة من وحدات التحكم في أجهزة وأنظمة التحكم الصناعي (OT/ICS) المستخدمة في بيئة الإنتاج وتحديد اتجاهها من أجل تشخيصها. ويجب وضع خط أساس لاستخدام الذاكرة.
14	إدارة أمن الموردين والأطراف الخارجية (Vendor and third-party security management)
الهدف	تحديد متطلبات إدارة أمن الأطراف الخارجية ومورّدي أجهزة وأنظمة التحكم الصناعي (OT/ICS) لضمان سير العملية بشكل سليم وآمن وفقًا للقواعد الأمنية المحددة.

اختر التصنيف

الإصدار <1.0>

المخاطر المحتملة	في حالة عدم ضمان مورّدي أجهزة وأنظمة التحكم الصناعي (OT/ICS) لتوافر الموارد الأمنية المناسبة وفقًا للمعايير الأمنية لدى <اسم الجهة>، فقد يؤدي ذلك إلى عواقب وخيمة قد تؤثر على استمرارية العمليات وتضر بالمؤسسة وتتسبب في وقوع خسائر مالية.
الإجراءات المطلوبة	
1-14	على مورّدي أجهزة وأنظمة التحكم الصناعي (OT/ICS) الحرص على تحديث التوصيات الأمنية بخصوص مكونات أجهزة وأنظمة التحكم الصناعي (OT/ICS) المستخدمة بانتظام.
2-14	على مورّدي أجهزة وأنظمة التحكم الصناعي (OT/ICS) ضمان توفير سجلات حديثة للثغرات بصفة منتظمة تتضمن جميع الثغرات المكتشفة والطرق المحتملة لإصلاحها.
3-14	مراقبة جميع مورّدي أجهزة وأنظمة التحكم الصناعي (OT/ICS) والمقاولين الخارجيين وتقييم أدائهم بصفة منتظمة وفقًا لمستوى الخطورة المحدد (بما في ذلك مخاطر سلسلة الإمداد) واتفاقية مستوى الخدمة المتفق عليها.
4-14	تقييم جميع مورّدي أجهزة وأنظمة التحكم الصناعي (OT/ICS) والمقاولين الخارجيين الجدد من حيث المخاطر المحتملة واتفاقية مستوى الخدمة.
15	الالتزام بالمعيار (Compliance)
الهدف	تحديد متطلبات ضمان الالتزام فيما يتعلق بأجهزة وأنظمة التحكم الصناعي (OT/ICS) لضمان سير العملية بشكل سليم وآمن وفقًا للقواعد الأمنية المحددة.
المخاطر المحتملة	يمكن أن يؤدي عدم الالتزام فيما يتعلق بأجهزة وأنظمة التحكم الصناعي (OT/ICS) إلى عواقب وخيمة قد تضر بالمؤسسة وتتسبب في وقوع خسائر مالية.
الإجراءات المطلوبة	
1-15	ضمان الالتزام بضوابط الأمن السيبراني للأنظمة التشغيلية (OTCC) والمعايير الصناعية المخصصة الأخرى، مثل معيار الجمعية الدولية للأتمتة / اللجنة الكهروتقنية الدولية (ISA/IEC 62443) أو المنشور الخاص للمعهد الوطني للمعايير والتقنية (NIST SP 800-82r2)، وغيرها من المتطلبات المحددة، بالنسبة لجميع أجهزة وأنظمة التحكم الصناعي (OT/ICS) والمسؤولين عن تحقيق التكامل بينها وموردّيها.
2-15	على <اسم الجهة> إجراء تقييمات منتظمة للتحقق من الالتزام.
3-15	مراجعة جميع الاتفاقيات مع مورّدي أجهزة وأنظمة التحكم الصناعي (OT/ICS) والمقاولين الخارجيين بصفة منتظمة من حيث المتطلبات التنظيمية والالتزام.

16	معايير أخرى (Other Standard controls)
الهدف	يجب ضبط إعدادات أجهزة وأنظمة التحكم الصناعي (OT/ICS) بشكل آمن ومراقبتها واستخدامها بشكل صحيح عند الحاجة.
المخاطر المحتملة	في حالة عدم التزام <اسم الجهة> بجميع معايير ومتطلبات <اسم الجهة> ، فقد يعرضها ذلك لتهديدات خطيرة.
الإجراءات المطلوبة	
1-16	تطبيق المعايير التالية فيما يتعلق بأمن أجهزة وأنظمة التحكم الصناعي (OT/ICS): 1. معيار أمن الشبكات 2. معيار أمن أجهزة المستخدمين 3. معيار إدارة هويات الدخول والصلاحيات 4. معيار الإعدادات والتحصين الآمن 5. معيار إدارة النسخ الاحتياطية والاسترجاع 6. معيار الأمن المادي 7. معيار إدارة الأصول 8. معيار تصنيف الأصول 9. معيار إدارة سجلات الأحداث ومراقبة الأمن السيبراني 10. معيار الاستجابة للحوادث

الأدوار والمسؤوليات

1- **مالك المعيار:** <رئيس الإدارة المعنية بالأمن السيبراني>.

2- **مراجعة المعيار وتحديثه:** <الإدارة المعنية بالأمن السيبراني>.

3- **تنفيذ المعيار وتطبيقه:** <الإدارة المعنية بأمن أجهزة وأنظمة التحكم الصناعي (OT/ICS)>.

4- **قياس الالتزام بالمعيار:** <الإدارة المعنية بالأمن السيبراني>.

التحديث والمراجعة

يجب على <الإدارة المعنية بالأمن السيبراني> مراجعة المعيار سنويًا على الأقل أو عند حدوث تغييرات تقنية جوهرية في البنية التحتية أو في حال حدوث تغييرات في السياسات أو الإجراءات التنظيمية في <اسم الجهة> أو المتطلبات التشريعية والتنظيمية ذات العلاقة.

اختر التصنيف

الإصدار <1.0>

الالتزام بالمعيار

1- يجب على <رئيس الإدارة المعنية بالأمن السيبراني> التأكد من التزام <اسم الجهة> بهذا المعيار دوريًا.

2- يجب على كافة العاملين في <اسم الجهة> الالتزام بهذا المعيار.

3- قد يعرض أي انتهاك لهذا المعيار صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في <اسم الجهة>.