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 سياسة الأمن السيبراني لأنظمة التحكم الصناعي

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

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

اختر التصنيف

التاريخ: اضغط هنا لإضافة نص

الإصدار: اضغط هنا لإضافة نص

المرجع: اضغط هنا لإضافة نص

اعتماد الوثيقة

الدور	الاسم	التاريخ	التوقيع
اختر الدور	<أدخل الاسم الكامل للشخص>	اضغط هنا لإضافة نص	<أدخل التوقيع>

نسخ الوثيقة

النسخة	التاريخ	عُدلَ بواسطة	أسباب التعديل
<أدخل رقم النسخة>	اضغط هنا لإضافة نص	<أدخل الاسم الكامل للشخص>	<أدخل وصف التعديل>

قائمة المحتويات

الأهداف

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بأجهزة وأنظمة التحكم الصناعي الخاصة بـ<اسم الجهة> بهدف تقليل المخاطر السيبرانية وحمايتها من التهديدات الداخلية والخارجية من خلال التركيز على الأهداف الأساسية للحماية وهي: سرية المعلومات، وسلامتها، وتوافرها.

وتهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم ١-١-٥ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع أجهزة وأنظمة التحكم الصناعي الخاصة بـ<اسم الجهة>، وتنطبق هذه السياسة على جميع العاملين في <اسم الجهة>.

بنود السياسة

1- المتطلبات العامة

1-1 يجب تطبيق جميع سياسات ومتطلبات الأمن السيبراني المعتمدة في <اسم الجهة> على أجهزة وأنظمة التحكم الصناعي.

2-1 يجب فرض قيود حازمة وتطبيق التقسيم المادي والمنطقي عند ربط شبكات الإنتاج الصناعي مع شبكة الأعمال الداخلية لـ<اسم الجهة>. (ECC-5-1-3-1)

3-1 يجب فرض قيود حازمة وتطبيق التقسيم المادي والمنطقي عند ربط شبكات الإنتاج الصناعي مع الشبكات الخارجية من خلال استخدام أنظمة تحكم أمنية مثل المنطقة المحايدة (DMZ). (ECC-5-1-3-2)

4-1 يجب تفعيل سجلات أحداث (Logs Files) الأمن السيبراني على الشبكات الصناعية والاتصالات المرتبطة بها ومراقبتها بشكل مستمر. (ECC-5-1-3-3)

5-1 يجب عزل أنظمة السلامة (Safety Instrumented System "SIS") منطقياً أو مادياً. (ECC-5-1-3-4)

6-1 يجب تنصيب حزم التحديثات والإصلاحات الأمنية للأنظمة الصناعية (OT/ICS Patch Management) دورياً وفقاً لسياسة إدارة حزم التحديثات والإصلاحات المعتمدة في <اسم الجهة>. (ECC-5-1-3-7)

7-1 يجب فحص واكتشاف الثغرات للأنظمة الصناعية (OT/ICS Vulnerability Management) دورياً، ومعالجة الثغرات بناءً على تصنيفها والمخاطر السيبرانية المترتبة عليها ووفقاً لسياسة إدارة الثغرات المعتمدة في <اسم الجهة>. (ECC-5-1-3-8)

8-1 يجب تقييد صلاحيات الدخول إلى مواقع أجهزة وأنظمة التحكم الصناعي داخل <اسم الجهة> ومنحها للعاملين المصرح لهم فقط ووفقاً لسياسة الأمن المادي في <اسم الجهة> وبناءً على متطلبات أعمالهم التشغيلية.

9-1 يجب إجراء فحص دوري لمدى فعالية استعادة النسخ الاحتياطية والتأكد من تطبيق متطلبات الأمن السيبراني لإدارة النسخ الاحتياطية وفقاً لسياسة النُسخ الاحتياطية المعتمدة في <اسم الجهة>.

10-1 يجب حماية البيانات والمعلومات في بيئة التحكم الصناعي والتعامل معها بناءً على تصنيفها ووفقاً لسياسة التصنيف المعتمدة في <اسم الجهة>.

2- حماية أنظمة التحكم الصناعي

1-2 يجب توفير تقنيات الحماية اللازمة لحماية أنظمة وأجهزة التحكم الصناعي من الفيروسات والبرمجيات المشبوهة والضارة وضبط إعداداتها وفقاً لأفضل المعايير الأمنية.

2-2 يجب ضبط إعدادات شبكات أنظمة التحكم الصناعي مثل الخوادم الوكيلة، وجدران الحماية، وأجهزة نقل البيانات باتجاه واحد (Data Diodes) لمنع نقل البيانات غير المصرح بها.

3-2 يُمنع توصيل وسائط التخزين الخارجية بأنظمة وأجهزة التحكم الصناعي أو مكوناتها التقنية إلا بإذن مسبق من <الإدارة المعنية بالأمن السيبراني>. (ECC-5-1-3-5)

4-2 يجب ضبط إعدادات مكونات أنظمة التحكم الصناعي القائمة على الويب على النحو التالي:

1-4-2 استخدام بروتوكول (HTTPS) للأجهزة المصرح لها فقط.

2-4-2 تحديد وتعيين قائمة محددة من التطبيقات (Whitelisting) للوصول إلى خدمات الويب.

5-2 يجب استخدام جدار الحماية لتطبيقات الويب (WAF) للحماية من هجمات الويب على أنظمة التحكم الصناعي الخارجية.

6-2 يجب استخدام التحقّق من الهوية متعدّد العناصر (Multi-Factor Authentication) لعمليات الدخول للمستخدمين ذوي الصلاحيات الهامة والحسّاسة على أنظمة وأجهزة التحكم الصناعي.

7-2 يجب تطبيق المعمارية متعددة المستويات (Multi-tier Architecture) في تطوير تطبيقات الويب الخاصة بأنظمة التحكم الصناعي.

8-2 يجب تقييم مخاطر الأمن السيبراني دورياً ووفقاً لسياسة إدارة مخاطر الأمن السيبراني المعتمدة في <اسم الجهة>.

3- إدارة حوادث وتهديدات الأمن السيبراني والتعافي من الكوارث

1-3 يجب تحديد خطط الاستجابة لحوادث الأمن السيبراني المتعلقة بأنظمة التحكم الصناعي وإجراءات التصعيد وفقاً لسياسة إدارة الحوادث وتهديدات الأمن السيبراني المعتمدة في <اسم الجهة>.

2-3 ينبغي تطوير واعتماد خطة طوارئ (Contingency Plan) تكون مصممة للحفاظ على سير الأعمال أو استعادتها من النسخ الاحتياطية المعتمدة في حال وقوع حوادث الأمن السيبراني والتأكد من استمرارية الأعمال بأقل تأثير ممكن.

3-3 يجب توثيق خطة التعافي من الكوارث المتعلقة بأنظمة التحكم الصناعي بحيث تشمل كحد أدنى ما يلي:

1-3-3 الاستجابة المطلوبة للأحداث بمختلف فتراتها وشدتها والتي تؤدي إلى تفعيل خطة التعافي من الكوارث من عدمها.

2-3-3 إجراءات إعادة تشغيل أنظمة التحكم الصناعي أو تشغيلها يدوياً.

3-3-3 أدوار ومسؤوليات فريق الاستجابة وقائمة العاملين المصرح لهم بالوصول المباشر أو غير المباشر إلى أنظمة التحكم الصناعي.

4-3-3 عمليات وإجراءات النُسخ الاحتياطية لنسخ الأصول المعلوماتية احتياطياً وتخزينها بشكل آمن.

5-3-3 مخطط شبكة منطقي مكتمل وحديث، ومعلومات الإعدادات الحالية للمكونات التقنية الخاصة بأجهزة وأنظمة التحكم الصناعي.

4- متطلبات أخرى

1-4 يجب مراجعة متطلبات الأمن السيبراني الخاصة بأنظمة التحكم الصناعي دورياً. (ECC-5-1-4)

2-4 يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر لإدارة الأمن السيبراني المتعلق بحماية أجهزة وأنظمة التحكم الصناعي.

3-4 يجب مراجعة هذه السياسة مرة واحدة في السنة؛ على الأقل.

الأدوار والمسؤوليات

1- **راعي ومالك وثيقة السياسة:** <رئيس الإدارة المعنية بالأمن السيبراني>.

2- **مراجعة السياسة وتحديثها:** <الإدارة المعنية بالأمن السيبراني>.

3- **تنفيذ السياسة وتطبيقها:** <الإدارة المعنية بتقنية المعلومات> و <الإدارة المعنية بالأمن السيبراني>.

الالتزام بالسياسة

1- يجب على <رئيس الإدارة المعنية بالأمن السيبراني> ضمان التزام <اسم الجهة> بهذه السياسة باستمرار.

2- يجب على كافة العاملين في <اسم الجهة> الالتزام بهذه السياسة.

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