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 للأنظمة التشغيلية

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.

اختر التصنيف

الإصدار <١,٠>

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 <١,٠>

قائمة المحتويات

اختر التصنيف

الإصدار <١,٠>

الغرض

الغرض من هذه السياسة هو تحديد متطلبات الأمن السيبراني المتعلقة بحماية الأصول المعلوماتية والتقنية المتعلقة بأجهزة وأنظمة التحكم الصناعي الخاصة في <اسم الجهة> لتقليل المخاطر السيبرانية الناتجة عن التهديدات الداخلية والخارجية في <اسم الجهة> وذلك لتحقيق الأهداف الرئيسية للحماية وهي: سرية المعلومات، وسلامة أنظمة المعلومات، وتوافرها.

تمت موائمة هذه السياسة مع الضوابط والمعايير الصادرة من الهيئة الوطنية للأمن السيبراني والمتطلبات التنظيمية والتشريعية ذات العلاقة.

نطاق العمل

تغطي هذه السياسة جميع الأصول المعلوماتية والتقنية (أجهزة وأنظمة التحكم الصناعي والأنظمة التشغيلية ومكوناتها) في <اسم الجهة>، وتنطبق على جميع العاملين (الموظفين والمتعاقدين) في <اسم الجهة>.

بنود السياسة

١- البنود العامة

١-١ يجب تحديد جميع سياسات ومتطلبات الأمن السيبراني المعتمدة في <اسم الجهة> وتطبيقها على الأنظمة التشغيلية وأنظمة التحكم الصناعي (OT/ICS) في <اسم الجهة>.

١-٢ يجب تقسيم المناطق المختلفة (Zones) داخل بيئة أنظمة التحكم الصناعي منطقيًا أو ماديًا وفقًا للمستوى المناسب للمنطقة وعزل تدفق البيانات بين المناطق بحيث يتم الاتصال بين المناطق عبر نقاط اتصال محددة (Choke Points).

١-٣ يجب فرض قيود حازمة وتطبيق التقسيم المادي والمنطقي عند ربط شبكات أنظمة التحكم الصناعي مع شبكة الأعمال الداخلية (Corporate Zone) والشبكات الأخرى في <اسم الجهة> ومنع الوصول لخدمات الأعمال الحساسة (Business Critical) على شبكات أنظمة التحكم الصناعي من الشبكة الداخلية وقصرها على الخدمات المصرح بالوصول لها.

١-٤ يجب فرض قيود حازمة وتطبيق التقسيم والفصل المادي والمنطقي عند ربط شبكات الأنظمة التشغيلية وأنظمة التحكم الصناعي مع الشبكات الخارجية من خلال استخدام أنظمة تحكم أمنية مثل المنطقة المحايدة (DMZ).

١-٥ يجب منع الوصول المباشر عن بعد لشبكات أنظمة التحكم الصناعي وتوجيه جميع الاتصالات إلى نقاط الوصول عن بعد (Jump Hosts) بحيث تكون مخصصة لهذه العمليات وآمنة ومحصنة في المنطقة المحايدة (DMZ)، ولا يتم استخدامها 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.

١-٦ يجب عزل أنظمة معدات السلامة (Safety Instrumented System - SIS) منطقيًا أو ماديًا عن الشبكات الأخرى الخاصة بأنظمة التحكم الصناعي.

١-٧ يجب تفعيل سجلات أحداث (Event Logs) الأمن السيبراني على شبكات الأنظمة التشغيلية وأنظمة التحكم الصناعي والاتصالات المرتبطة بها ومراقبتها بشكل مستمر.

١-٨ يجب تفعيل سجلات الأحداث المتعلقة بالأمن السيبراني على جميع الأصول في بيئة شبكات أنظمة التحكم الصناعي.

١-٩ يجب اكتشاف محاولات فشل الوصول إلى نظام المراقبة الخاص ب<اسم الجهة>، ورصدها.

١-١٠ يجب اجراء مراجعة ومراقبة مستمرة ودقيقة لسجلات الأحداث والتدقيق المتعلقة بالأمن السيبراني على جميع أصول أنظمة التحكم الصناعي.

١-١١ يجب إجراء مراقبة وكشف، وتحليل لسلوك المستخدم (User Behavior Analysis).

١-١٢ يجب اكتشاف عمليات الرفع أو التنزيل على أجهزة وأنظمة التحكم الصناعي بما في ذلك أنظمة السلامة.

١-١٣ يجب مراقبة جميع عمليات الوصول عن بعد.

١-١٤ يجب اكتشاف الأحداث الضارة وفحصها.

١-١٥ يجب تسجيل التنبيهات الحديثة ومراقبتها في حال اتصال أجهزة جديدة، أو غير مسموح بها بشبكات أنظمة التحكم الصناعي.

١-١٦ يجب استخدام التهديدات الاستباقية المتعلقة بأنظمة التحكم الصناعي لضبط تنبيهات نظام إدارة سجلات الاحداث.

١-١٧ يجب مراقبة جميع نقاط التحكم بالدخول بين حدود الشبكة والاتصالات الخارجية.

١-١٨ يجب إجراء مراجعة دورية للإعدادات الأمنية للأنظمة التشغيلية وأنظمة التحكم الصناعي.

١-١٩ يجب تحديد واعتماد وتطبيق المعايير التقنية الأمنية (Technical Security Standards) للأنظمة التشغيلية وأنظمة التحكم الصناعي مع الاخذ في الاعتبار التفضيلات من مصنعي ومطوري هذه الأنظمة وفقًا لسياسة الإعدادات والتحصين المعتمدة لدى <اسم الجهة>.

١-٢٠ يجب فحص واكتشاف الثغرات للأنظمة التشغيلية وأنظمة التحكم الصناعي (OT/ICS Vulnerability Management) دوريًا، ومعالجة الثغرات بناءً على تصنيفها والمخاطر السيبرانية المترتبة عليها ووفقًا لسياسة إدارة الثغرات المعتمدة لدى <اسم الجهة>.

١-٢١ يجب تحديد نطاق عمليات تقييم الثغرات وأنشطتها لبيئة شبكات أنظمة التحكم الصناعي (ICS/OT) بوصفه جزء من الآليات الرسمية لإدارة الثغرات في <اسم الجهة>، وضمان تأثير محدود أو غير محدود على بيئة الإنتاج.

١-٢٢ يجب التأكد من ضمان المعالجة الفورية، للثغرات الحساسة المكتشفة حديثاً، والتي تشكل مخاطر كبيرة على بيئة شبكات أنظمة التحكم الصناعي.

١-٢٣ يجب مراجعة متطلبات الأمن السيبراني لإدارة الثغرات الخاصة بأنظمة التحكم الصناعي (ICS/OT) وقياس فعالية تطبيقها وتقييمها دورياً.

١-٢٤ يجب تطبيق حزم التحديثات والإصلاحات الأمنية للأنظمة التشغيلية وأنظمة التحكم الصناعي (OT/ICS Patch Management) دوريًا وفقًا لسياسة إدارة حزم التحديثات والإصلاحات المعتمدة لدى <اسم الجهة>.

١-٢٥ يجب مراجعة الإعدادات التلقائية والمبدئية لهذه الأنظمة والتأكد من عدم احتوائها على إعدادات تسهل الدخول لأطراف خارجية أو صلاحيات دخول أو مرور محددة مسبقا.

١-٢٦ يجب تقييد صلاحيات الدخول إلى مواقع الأنظمة التشغيلية وأنظمة التحكم الصناعي داخل <اسم الجهة> ومنحها للعاملين المصرح لهم فقط وفقًا لسياسة إدارة هويات الدخول والصلاحيات وسياسة الأمن المادي المعتمدة لدى <اسم الجهة> وبناءً على متطلبات أعمالهم التشغيلية.

١-٢٧ يجب إجراء فحص دوري لمدى فعالية استعادة النسخ الاحتياطية والتأكد من تطبيق متطلبات الأمن السيبراني لإدارة النسخ الاحتياطية وفقًا لسياسة النُسخ الاحتياطية المعتمدة لدى <اسم الجهة>.

١-٢٨ يجب تحديد وتصنيف وحماية البيانات والمعلومات للبنية التحتية الوطنية الحساسة (CNI) التابعة للأنظمة التشغيلية وأنظمة التحكم الصناعي والتعامل معها بناءً على تصنيفها حسب التشريعات والأنظمة ذات العلاقة في <اسم الجهة>.

١-٢٩ يجب حماية البيانات الإلكترونية والمادية في حال التخزين والنقل بالمستوى الذي يتوافق مع تصنيف البيانات.

١-٣٠ يجب حماية البيانات والمعلومات المصنفة من خلال تقنيات، منع تسريب البيانات (Prevention Leakage Data" DLP).

١-٣١ يجب استخدام آليات الحذف الآمنة (Wiping Secure) لبيانات الإعدادات والبيانات المخزنة على أصول أنظمة التحكم الصناعي (ICS/OT) وذلك عند الانتهاء منها.

١-٣٢ يجب التقييد الحازم لنقل بيانات أنظمة التحكم الصناعي (ICS/OT) أو استخدامها خارج بيئة الإنتاج؛ إلى أن تطبق ضوابط صارمة لحامية تلك البيانات.

١-٣٣ يجب توفير التوعية الأمنية اللازمة للعاملين في <اسم الجهة> وتزويدهم بالمهارات والمؤهلات والدورات التدريبية المطلوبة في مجال الأمن السيبراني.

١-٣٤ يجب على <اسم الجهة> تطوير قائمة جرد دقيقة وحديثة لأصول الأنظمة التشغيلية وأنظمة التحكم الصناعي التابعة لها.

١-٣٥ يجب استخدام تقنيات الأتمتة لحصر الأصول.

١-٣٦ يجب حفظ معلومات أصول أنظمة التحكم الصناعي (ICS/OT) المحصورة بشكل آمن.

١-٣٧ يجب تحديد ملاك الأصول (Owner Asset) لجميع أصول أنظمة التحكم الصناعي (ICS/OT) والتأكد من مشاركتهم في دورة حياة إدارة جرد الأصول ذات العلاقة.

١-٣٨ يجب تصنيف مستوى الحساسية (Rating Criticality) وتوثيقه واعتماده لجميع الأصول، من قبل مالك الأصول.

١-٣٩ يجب تحديد وإسناد أدوار ومسؤوليات واضحة لجميع الأطراف المشاركة في تطبيق ضوابط الأمن السيبراني للأنظمة التشغيلية وأنظمة التحكم الصناعي في <اسم الجهة>.

١-٤٠ يجب تضمين متطلبات الأمن السيبراني في منهجية إدارة مشاريع <اسم الجهة> واجراءاتها، لحماية سرية وسلامة وتوافر الأعمال التشغيلية والتقنية للأنظمة التحكم الصناعي، وذلك وفقًا للسياسة العامة للأمن السيبراني المعتمدة لدى <اسم الجهة> والمتطلبات التشريعية والتنظيمية ذات علاقة.

١-٤١ يجب التأكد من أن مستويات الأمن السيبراني لا تتأثر حال تطبيق طلبات التغيير في البيئة التي تحتوي على أنظمة التحكم الصناعي وذلك بعد التحليل والتحكم بالثغرات.

١-٤٢ يجب على <اسم الجهة> تنظيم حملات توعية أمنية خاصة بالأنظمة التشغيلية وأنظمة التحكم الصناعي.

١-٤٣ يجب أن يتم توفير تمارين خاصة، وشهادات مهنية، ومهارات احترافية في مجال الأمن السيبراني، لجميع العاملين على الأصول المتعلقة بأنظمة التحكم الصناعي (ICS/OT)، كما تشجع الهيئة الوطنية للأمن السيبراني <اسم الجهة> على الاستفادة من الإطار السعودي لكوادر الأمن السيبراني (سيوف) ليكون مرجع لها.

١-٤٤ يجب تشجيع الجهة للمشاركة مع الجهات المعتمدة و/أو ذات الاختصاص في مجال أنظمة التحكم الصناعي (ICS/OT).

١-٤٥ يجب تطوير واعتماد إجراءات ومعايير خاصة بالأنظمة التشغيلية وأنظمة التحكم الصناعي بناءً على حاجة العمل.

١-٤٦ يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر والاستخدام الصحيح والفعال لمتطلبات الأمن السيبراني المتعلقة بحماية أجهزة وأنظمة التحكم الصناعي.

٢- حماية الأنظمة التشغيلية

٢-١ يجب توفير تقنيات الحماية اللازمة لحماية أنظمة وأجهزة التحكم الصناعي من الفيروسات والبرمجيات المشبوهة والضارة وضبط إعداداتها وفقًا لسياسة الحماية من البرمجيات الضارة المعتمدة في <اسم الجهة>، وأفضل المعايير الأمنية.

٢-٢ يجب ضبط إعدادات الأنظمة أو الأجهزة المرتبطة بشبكات أنظمة التحكم الصناعي مثل الخوادم الوكيلة، وجدران الحماية، وأجهزة نقل البيانات باتجاه واحد (Data Diodes) لمنع نقل البيانات غير المصرح بها.

٢-٣ يجب منع توصيل وسائط التخزين الخارجية والأجهزة المحمولة التابعة ل<اسم الجهة> بما في ذلك أجهزة الحاسب المحمول، أجهزة الإعدادات المحمولة، وأجهزة اختبارات الشبكة بالأنظمة التشغيلية وأنظمة التحكم الصناعي أو مكوناتها التقنية إلا بإذن مسبق من <اسم الجهة> وبعد دراسة المخاطر المحتملة.

٢-٤ يجب ضمان سرية البيانات المتعلقة بالأنظمة التشغيلية وأنظمة التحكم الصناعي ومعلوماتها وسلامتها وتوافرها وفقًا لسياسة حماية البيانات المعتمدة لدى <اسم الجهة>، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

٢-٥ يجب استخدام التشفير لحماية أصول البيانات والمعلومات وفقًا لسياسة التشفير المعتمدة في <اسم الجهة>، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

٢-٦ يجب تطبيق المعمارية متعددة المستويات (Multi-tier Architecture) في تطوير تطبيقات الويب الخاصة بالأنظمة التشغيلية وأنظمة التحكم الصناعي.

٢-٧ يجب استخدام معلومات التهديدات الاستباقية (Threat Intelligence) لتحديد التقنيات والإجراءات (TTPs) المستخدمة من قبل المجموعات النشطة (Activity Groups) الي تستهدف الأنظمة التشغيلية وأنظمة التحكم الصناعي.

٢-٨ يجب تقييم مخاطر الأمن السيبراني على الأنظمة التشغيلية وأنظمة التحكم الصناعي دوريًا وفقًا لسياسة إدارة مخاطر الأمن السيبراني المعتمدة في <اسم الجهة> والتشريعات الأخرى ذات العلاقة على أن تشمل هذه التقييمات تقييم مخاطر الأمن السيبراني المتعلقة بالأطراف الخارجية بما في ذلك مصنعو معدات الأنظمة التشغيلية وأنظمة التحكم الصناعي، وموردو منتجات وخدمات أنظمة التحكم الصناعي.

٢-٩ يجب التأكد من أن مخاطر الأمن السيبراني ومتطلباته للأنظمة التشغيلية وأنظمة التحكم الصناعي المتعلقة بالعاملين في <اسم الجهة> تعالج بفعالية قبل البدء في عملهم واثناءه وعند الانتهاء منه، وذلك وفقًا للسياسات أو الإجراءات التنظيمية المعتمدة لدى <اسم الجهة> والمتطلبات التشريعية والتنظيمية ذات العلاقة.

٢-١٠ يجب إجراء عمل مسح أمني (Vetting or Screening) لجميع العاملين ويشمل ذلك (الموظفين والمتعاقدين) والذين يمكنهم الوصول إلى أصول أنظمة التحكم الصناعي (ICS/OT) أو استخدامها؛ وذلك قبل منحهم صلاحيات الوصول.

٣- إدارة حوادث وتهديدات الأمن السيبراني والتعافي من الكوارث

٣-١ يجب تقييم واختبار مدى فعالية قدرات تعزيز الأمن السيبراني لأصول الأنظمة التشغيلية وأنظمة التحكم الصناعي (OT/ICS) في <اسم الجهة> من خلال اختبارات الاختراق.

٣-٢ يجب تحديد نطاق أنشطة اختبارات الاختراق، لتغطي بيئة شبكات أنظمة التحكم الصناعي (ICS/OT) والشبكات المرتبطة بالشبكة التشغيلية، وأن يتم عمل الاختبارات من قبل فريق ذي كفاءة عالية.

٣-٣ يجب إجراء اختبار الاختراق، بعد التأكد من أن تأثير الاختبار، محدود على بيئة الإنتاج، أو إجراء اختبار الاختراق، في بيئة منفصلة مماثلة.

٣-٤ يجب إجراء اختبار الاختراق لأنظمة التحكم الصناعي دورياً.

٣-٥ يجب تحديد طرق اختبارات بديلة وتنفيذها مثل الاختبارات غير الفعالة (Testing Passive) لجمع المعلومات عندما يكون هنالك أثر محتمل على بيئة الإنتاج التشغيلية.

٣-٦ يجب تطبيق التوافر (Redundancy) للشبكات والوسائط والأجهزة الحساسة لأصول الأنظمة التشغيلية وأنظمة التحكم الصناعي وفقا للتقييم الدوري لمخاطر الأمن السيبراني.

٣-٧ يجب تضمين متطلبات صمود الأمن السيبراني المتعلقة بالأنظمة التشغيلية وأنظمة التحكم الصناعي في خطة استمرارية الأعمال (Business Continuity Plan - BCP) ويشمل ذلك تحليل التأثير على الأعمال (BIA) ووقت الاستعادة المستهدف (RTO) ونقطة الاستعادة المستهدفة (RPO).

٣-٨ يجب تضمين متطلبات صمود الأمن السيبراني المتعلقة بالأنظمة التشغيلية وأنظمة التحكم الصناعي الى خطط التعافي من الكوارث (Disaster Recovery Plan - DRP).

٣-٩ يجب 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.

٣-١٠ يجب تحديد خطط الاستجابة لحوادث الأمن السيبراني المتعلقة بالأنظمة التشغيلية وأنظمة التحكم الصناعي وإجراءات التصعيد وفقًا لسياسة إدارة الحوادث وتهديدات الأمن السيبراني (Cybersecurity Incident and Threat Management) المعتمدة في <اسم الجهة> والتشريعات الأخرى ذات العلاقة وإجراء تمارين افتراضية على الخطط بشكل دوري.

٣-١١ يجب التأكد من أن خطط الاستجابة للحوادث الأمنية، المتعلقة بأنظمة التحكم الصناعي (ICS/OT) مدمجة ومتوائمة مع خطط الجهة وإجراءاتها.

٣-١٢ يجب إجراء تحليل للحوادث، وتحليل الأسباب الجذرية (Analysis Cause Root) لحوادث الأمن السيبراني، بطريقة منظمة، بعد اكتشاف الحوادث.

٣-١٣ يجب تحديد تسلسل أنشطة الاستجابة، لحوادث الأمن السيبراني اللازمة لاستعادة العمليات التشغيلية لطبيعتها.

٣-١٤ يجب إنشاء خطط التواصل، عند وقوع الحوادث (Plan Communications Incident).

٣-١٥ يجب تضمين إجراءات التعافي للأنظمة التشغيلية وأنظمة التحكم الصناعي بما في ذلك أنظمة معدات السلامة (SIS) في خطط الاستجابة للحوادث والتعافي من الكوارث واستمرارية الأعمال المعتمدة في <اسم الجهة>.

٣-١٦ يجب تزويد العاملين بالجهة بالمهارات والدورات التدريبية المطلوبة (الموظفين والمتعاقدين) للاستجابة لحوادث الأمن السيبراني المتعلقة بأنظمة التحكم الصناعي (ICS/OT).

٣-١٧ يجب اختبار قدرات الاستجابة لحوادث الأمن السيبراني ومستوى الجاهزية والخطة المعتمدة بشكل دوري من خلال إجراء تمارين محاكاة للهجمات السيبرانية (Exercises Simulation Attack).

٣-١٨ يجب استخدام معلومات التهديدات الاستباقية (Intelligence Threat) لتحديد الخطط والأساليب والإجراءات (TTPs) المستخدمة من قبل المجموعات النشطة (Groups Activity) التي تستهدف أنظمة التحكم الصناعي (ICS/OT).

٣-١٩ يجب التأكد من أن خطط الاستجابة لحوادث الأمن السيبراني المتعلقة بالأنظمة التشغيلية وأنظمة التحكم الصناعي متوائمة مع خطط الاستجابة لحوادث تقنية المعلومات وإدارة الأزمات وخطط استمرارية الأعمال المعتمدة في <اسم الجهة>.

٣-٢٠ يجب تحديد الأنشطة اللازمة للمحافظة على الحد الأدنى من العمليات المتعلقة بالأنظمة التشغيلية وأنظمة التحكم الصناعي كما يجب أن تكون الأنظمة قادرة على العمل بمستوى أمان مقبول عند فشلها بسبب حادثة أمن سيبراني.

٣-٢١ يجب إجراء تحليل للحوادث وتحليل الأسباب الجذرية (Root Cause Analysis) لحوادث الأمن السيبراني بطريقة منظمة بعد اكتشاف الحوادث.

٣-٢٢ يجب إنشاء خطط تواصل عند وقوع حوادث الأمن السيبراني (Incident Communications Plan).

٣-٢٣ يجب توعية الجهات المسؤولة وفرق الاستجابة على خطط الاستجابة لحوادث الأمن السيبراني المتعلقة بالأنظمة التشغيلية وأنظمة التحكم الصناعي من خلال تزويد العاملين بالجهة بالمهارات والدورات التدريبية المطلوبة.

٣-٢٤ يجب توثيق خطة التعافي من الكوارث المتعلقة بالأنظمة التشغيلية وأنظمة التحكم الصناعي بحيث تشمل كحد أدنى ما يلي:

٣-٢٤-١ تطوير خطة الاستجابة المطلوبة للأحداث بمختلف فتراتها وشدتها والتي تؤدي إلى تفعيل خطة التعافي من الكوارث أو عدمها.

٣-٢٤-٢ تحديد تسلسل أنشطة الاستجابة لحوادث الأمن السيبراني اللازمة لاستعادة العمليات التشغيلية لطبيعتها.

٣-٢٤-٣ تحديد إجراءات إعادة تشغيل الأنظمة التشغيلية وأنظمة التحكم الصناعي أو تشغيلها يدويًا.

٣-٢٤-٤ تحديد أدوار ومسؤوليات فريق الاستجابة وقائمة العاملين المصرح لهم بالوصول المباشر أو غير المباشر إلى أنظمة التحكم الصناعي.

٣-٢٤-٥ مراجعة عمليات وإجراءات النُسخ الاحتياطية لنسخ الأصول المعلوماتية احتياطيًا وتخزينها بشكل آمن.

٣-٢٤-٦ تطوير مخطط شبكة منطقي مكتمل وحديث، ومعلومات الإعدادات الحالية للمكونات التقنية الخاصة بأجهزة وأنظمة التحكم الصناعي.

٣-٢٥ يجب اختبار قدرات الاستجابة لحوادث الأمن السيبراني ومستوى الجاهزية والخطة المعتمدة بشكل دوري من خلال إجراء تمارين محاكاة للهجمات السيبرانية (Attack Simulation Exercises).

الأدوار والمسؤوليات

١- **مالك السياسة:** <رئيس الإدارة المعنية بالأمن السيبراني>.

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

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

٤- **قياس الالتزام بالسياسة:** <الإدارة المعنية بالأمن السيبراني>.

التحديث والمراجعة

يجب على <الإدارة المعنية بالأمن السيبراني> مراجعة السياسة سنويًا على الأقل أو في حال حدوث تغييرات في السياسات أو الإجراءات التنظيمية في <اسم الجهة> أو المتطلبات التشريعية والتنظيمية ذات العلاقة.

الالتزام بالسياسة

١- يجب على <رئيس الإدارة المعنية بالأمن السيبراني> التأكد من التزام <اسم الجهة> بهذه السياسة دوريًا.

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

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