سياسات توكيد المعلومات الوطنية القطرية

معيار تأمين أنظمة التحكم الإشرافي

مارس 2014

نسخة: **3.0**

التصنيف: **وثيقة عامة:**

الملحق (أ) جزئ من هذا المعيار الملحق (ب) يعرض معلومات فحسب.

قائمة المحتويات

1- مقدمة

ملحوظة: حيث ان هذه وثيقة مترجمة فأنه في حاله أي اختلاف تكون المرجعية للنص الإنجليزي لخصوصيه الموضوع فنيا.

لقد بدأت الجهات ذات البنى التحتية الهامة والتي تعتمد على أنظمة التحكم الإشرافي والحصول على البيانات (ICS) في استخدام التكنولوجيا التجارية الجاهزة (COTS) المطورة لنظم الأعمال في العمليات اليومية في تلك الجهات. وقد أدى ذلك إلى توفير فرصة كبيرة للهجمات الالكترونية ضد النظم الهامة التي تقوم تلك الجهات بتشغيلها. إن هذه النظم التجارية الجاهزية لا تتمتع بنفس القوة في العادة (في التعامل مع الهجمات الالكترونية) مثل النظم المصممة خصيصاً للبنية التحتية الهامة في التعامل مع الهجوم الالكتروني لأسباب عدة. وقد تؤدي نقاط الضعف هذه إلى تبعات تتعلق بالصحة والسلامة والبيئة قد يكون لها تأثير سيء على اقتصاد دولة قطر أو شعبها أو حكومتها.

ويحدد دليل تأمين أنظمة التحكم الإشرافي الأساسي الذي بين أيدينا الحد الأدنى من أنظمة التحكم التي يجب إضافتها إلى أي نظام للتحكم الإشرافي والحصول على البيانات هام وحيوي بالنسبة لدولة قطر. وقد تم إعداد هذا الدليل ليستخدم مع توثيق أمني مناسب قائم على المخاطر، أو مع سياسة تصنيف المعلومات الحكومية .

1-1 النطاق

يجب إضافة العوامل التالية عند تقييم أصول أي نظام هام للتحكم الإشرافي والحصول على المعلومات:

* مراكز التحكم ومراكز التحكم الاحتياطية، بما في ذلك النظم المتوفرة في المواقع الرئيسية والبعيدة.
* محطات النقل الفرعية التي تدعم التشغيل المعتمد عليه للنظم الكلية.
* النظم والمرافق الهامة لاستعادة النظام، بما في ذلك black start generators والمحطات الفرعية في المسار الكهربائي لخطوط النقل المستخدمة للاستعادة الأولية للنظام.
* النظم التي توفر المراقبة والتحكم والتحكم في التوليد التلقائي، وإعداد نماذج نظم الوقت الحقيقي، وتبادل البيانات بين المرافق في الوقت الحقيقي.

2- سياسة أمن أنظمة التحكم الإشرافي والحصول على البيانات/ نظم التحكم الموزع ICS

2-1 هدف السياسة

يتمثل الهدف من هذه السياسة في توفير التوجيه والدعم من الإدارة لأمن أنظمة التحكم الإشرافي والحصول على المعلومات/ نظم التحكم الموزع ICS وفقاً لمتطلبات الأعمال والقوانين واللوائح ذات الصلة.

2-2 السياسة وأنظمة التحكم الأساسية

2-2-1 وثيقة سياسة أمن أنظمة التحكم الإشرافي والحصول على البيانات/ نظم التحكم الموزع ICS

يجب اعتماد وثيقة سياسة أمن أنظمة التحكم الإشرافي والحصول على البيانات/ نظم التحكم الموزع ICS من الإدارة العليا، كما يجب نشرها وتعميمها على كافة الموظفين والأطراف الخارجية ذات الصلة سواءً كجزء من سياسة أمن معلومات الجهة، أو كسياسة منفصلة.

2-2-2 قيادة برنامج الأمن

يجب تعريف الإدارة العليا المسؤولة عن أمن أنظمة التحكم الإشرافي والحصول على المعلومات/ أنظمة التحكم الموزع ICS بالاسم والمسمى الويفي ورقم هاتف العمل وعنوان العمل وتاريخ التعيين. كما يجب توثيق التغيرات التي تطرأ على الإدارة العليا في غضون ثلاثين (30) يوماً تقويمياً من تاريخ سريان تلك التغييرات.

2-2-3 مراجعة سياسة الأمن

يجب مراجعة سياسة الأمن على فترات دورية محددة، أو ضمان استمرار ملاءمة وكفاية وفاعلية تلك السياسة في حال طرأت تغييرات مؤثرة عليها.

3- عملية شراء أنظمة التحكم

3-1 هدف السياسة

تهدف هذه السياسة إلى ضمان أخذ مبادئ الأمن بعين الاعتبار عند شراء منتجات أنظمة التحكم (البرمجيات والنظم والخدمات والشبكات).

3-2 السياسة وأنظمة التحكم الأساسية

3-2-1 لغة وعملية الشراء

يجب أن تتبع لغة الشراء وطلب العروض الإرشادات المنصوص عليها في الملحق (....)

3-2-2 قبول النظام

يجب وضع معايير قبول وتحديثات أنظمة التحكم الإشرافي والحصول على المعلومات/ أنظمة التحكم الموزع ICS والنسخ الجديدة منها، كما يجب إجراء اختبارات مناسبة للنظام (النظم) أثناء مرحلة التطوير وقبل القبول. يجب أن تكون كافة الأنظمة المشتراة مطابقة لأنظمة التحكم الواردة في هذا الدليل.

3-2-3 عقود الإسناد لجهات خارجية

يجب تناول متطلبات الأمن لأي جهة تقوم بإسناد إدارة و/أو التحكم في كافة أو بعض أنظمة التحكم الإشرافي والحصول على المعلومات/ أنظمة التحكم الموزع ICS وشبكاتها وبيئة سطح المكتب الخاصة بها في عقد يتم الاتفاق عليها بين الأطراف.

كما يتعين على الجهة أن تضمن وجود أنظمة التحكم الأساسية المحددة في هذا الدليل في اتفاقية أو عقد تقديم الخدمة الموقع مع الطرف الآخر. وينطبق ذلك أيضاً على المقاولين من الباطن الذين يستعين بهم الطرف الآخر.

4- الأمن المؤسسي

4-1 هدف السياسة

تهدف هذه السياسة إلى إيجاد أمن مؤسسي محدد بشكل جيد عند إدارة أنظمة التحكم الإشرافي والحصول على المعلومات/ أنظمة التحكم الموزع ICS.

4-2 السياسة وأنظمة التحكم الأساسية

4-2-1 إضافة أمن أنظمة التحكم الإشرافي والحصول على المعلومات/ أنظمة التحكم ICS

تلتزم الإدارة بإضافة إدارة أنظمة التحكم الإشرافي والحصول على المعلومات/ أنظمة التحكم ICS إلى نظام الحكومة التنظيمية/ الأمن التنظيمي، أو برنامج الأمن، والإقرار صراحةً بمسؤوليات الأمن الخاصة بتلك الأنظمة.

4-2-2 إدارة تغيير أنظمة التحكم الإشرافي والحصول على المعلومات/ أنظمة التحكم ICS

تلتزم الجهة بإنشاء لجنة خاصة لإدارة تغيير أنظمة التحكم الإشرافي والحصول على المعلومات/ أنظمة التحكم الموزع ICS تقوم بمراجعة واعتماد التغييرات المقترحة.

4-2-3 تنسيق أمن أنظمة التحكم الإشرافي والحصول على البيانات/ أنظمة التحكم الموزع ICS

يتم تنسيق أنشطة أمن أنظمة التحكم الإشرافي والحصول على البيانات/ أنظمة التحكم ICS من قبل ممثلين من مختلف أجزاء الجهة يحدد لكل منهم دور ووظيفة، مثل الأمن المادي، الاستجابة للطوارئ، تكنولوجيا المعلومات في الجهة... الخ

4-2-4 تحديد مسؤوليات أنظمة التحكم الإشرافي والحصول على البيانات/ أنظمة التحكم

يجب تحديد كافة المسؤوليات الخاصة بأنظمة التحكم الإشرافي والحصول على البيانات/ أنظمة التحكم الموزع

ICS	ICS بوضوح.
4–2–5 عملية التخويل لمرافق معالجة معلومات أنظمة التحكم الإشرافي والحصول على البيانات/ أنظمة التحكم ICS	يجب تعريف وتنفيذ عملية تخويل إدارة لمرافق معالجة المعلومات الخاصة بأنظمة ICS الجديدة.
4–2–6 اتفاقيات السرية الخاصة بمعلومات البنى التحتية الهامة CII	يجب تعريف متطلبات اتفاقيات السرية أو عدم الإفصاح التي تعكس حاجات الجهة لحماية معلومات البنى التحتية ومراجعتها بشكل دوري.
4–2–7 إبرام عقود مع السلطات	يجب إبرام العقود المناسبة مع السلطات المعنية، بما في ذلك كيو سيرت وخدمات الطوارئ.
4–2–8 الاتصال مع مجموعات الاهتمام الخاص	يجب الحفاظ على الاتصالات المناسبة مع مجموعات الاهتمام الخاص أو غيرها من منتديات الأمن المتخصصة المتعلقة بأنظمة ICS (مثل EN-IREC في قطر) والجمعيات المهنية.

5– الأمن المادي والبيئي

5–1 هدف السياسة

تهدف هذه السياسة إلى منع الوصول المادير غير المخول، أو إحداث تلف أو تشويش لمقار وأجهزة ومعلومات أنظمة التحكم الإشرافي والحصول على البيانات/ أنظمة التحكم ICS.

5–2 السياسة وأنظمة التحكم الأساسية

5–2–1 حدود الأمن المادي	يجب استخدام حدود مخصصة للأمن (حواجز مثل الجدران أو بوابات الدخول بالبطاقات أو مكاتب الاستقبال التي تعمل بموظفين) وذلك لحماية المناطق التي توجد بها مرافق المعالجة الخاصة بأنظمة التحكم الإشرافي والحصول على البيانات/ أنظمة التحكم ICS.
5–2–2 وسائل الاتصال	يجب وجود وسائل حماية مادية إضافية/ منفصلة لحماية خطوط التوزيع/ الاتصال الخاصة بأنظمة التحكم الإشرافي والحصول على البيانات/ أنظمة التحكم /ICSمن التلف أو العبث أو التجسس أو تعديل الاتصالات غير المشفرة أثناء عبورها. وتتضمن الإجراءات الوقائية ما

يلي: أماكن/ فتحات مقفلة لتمديد الأسلاك، قنوات أو أحواض محمية لتمديد الكيبلات... الخ

5-2-3 وسائل العرض يجب وجود أنظمة تحكم للوصول المادي للأجهزة التي تعرض معلومات ICS.

5-2-4 أمن الأجهزة المحمولة والمتنقلة داخل غرف التحكم يجب على الجهة وضع أنظمة تحكم لاستخدام الأجهزة المتنقلة والمحمولة داخل غرف التحكم، وتقييد استخدام تلك الأجهزة إلا إذا كانت مخولة أو سبق اعتمادها بشكل صريح، وكانت مملوكة للجهة وخاضعة للفحص من قبلها.

6- إدارة الاتصال والعمليات

6-1 هدف السياسة

تهدف هذه السياسة إلى ضمان التشغيل الصحيح والآمن لمرافق معالجة المعلومات الخاصة بأنظمة التحكم الإشرافي والحصول على البيانات/ أنظمة التحكم ICS.

6-2 السياسة وأجهزة التحكم الأساسية – الإجراءات والمسؤوليات التشغيلية

6-2-1 الإجراءات التشغيلية الموثقة يجب توثيق إجراءات التشغيل الخاصة بأنظمة التحكم الإشرافي والحصول على البيانات/ أنظمة التحكم ICSوالاحتفاظ بها وإتاحتها لكافة المستخدمين المخولين عند حاجتهم إليها. يلتزم الموردون بتزويد الجهة بكامل الوثائق الخاصة بأي إجراء تشغيلي مطلوب على النظم التابعة لهم.

6-2-2 إدارة التغيير يتم التحكم في التغيرات التي تطرأ على مرافق وأنظمة معالجة المعلومات الخاصة بأنظمة التحكم الإشرافي والحصول على البيانات/ أنظمة التحكم ICSواعتمادها مسبقاً من قبل لجنة إدارة التغيير الخاصة بأنظمة التحكم الإشرافي والحصول على البيانات/ أنظمة التحكم ICS.

6-2-3 فصل اختبار التطوير عن المرافق التشغيلية يجب فصل اختبار التشغيل والمرافق التشغيلية لتقليل مخاطر الوصول غير المخول أو غير المقصود، أو التغييرات غير المخولة أو غير المقصودة على النظم التشغيلية.

6–3 السياسة وأنظمة التحكم الأساسية – إدارة تقديم الخدمات المقدمة من أطراف أخرى

6–3–1 تقديم الخدمة

تلتزم الجهات بضمان تنفيذ وتشغيل وصيانة أنظمة التحكم الأمني وتعريفات الخدمة ومستويات تقديمها المنصوص عليها في اتفاقية تقديم الخدمة المقدمة من طرف آخر من قبل ذلك الطرف الآخر.

6–3–2 مراقبة ومراجعة خدمات الطرف الآخر

يتعين أن تخضع الخدمات والتقارير والسجلات التي يقدمها الطرف الآخر للمراقبة والمراجعة بصفة دورية، كما يجب القيام بعمليات فحص وتدقيق دورية عليها.

6–3–3 إدارة التغييرات التي تطرأ على خدمات الطرف الآخر

يجب إدارة التغييرات التي تطرأ على تقديم الخدمات، بما في ذلك صيانة وتحسين سياسات وإجراءات وأنظمة تحكم الأمن القائمة والخاصة بأنظمة التحكم الإشرافي والحصول على البيانات/ أنظمة التحكم ICS ؛ مع الأخذ بعين الاعتبار أهمية النظم والعمليات المعنية، وإعادة تقييم المخاطر المترتبة على ذلك.

6–4 السياسة وأنظمة التحكم الأساسية – الإصلاح والحماية من الرموز الخبيثة والمتنقلة

6–4–1 أجهزة التحكم للحماية من البرامج الخبيثة

يجب تنفيذ وتوثيق أنظمة التحكم الخاصة بالكشف والحماية والاسترداد للحماية من البرامج الخبيثة، بالإضافة إلى تنفيذ وتوثيق إجراءات وعي المستخدم المناسبة.

ويجب أن تتضمن أنظمة التحكم هذه تنصيب برنامج مكافحة البرامج الخبيثة، استخدام قوائم بيضاء للعمليات المعتمدة مسبقاً... الخ

6–4–2 حلول البرامج الضاره

يجب ان تكون محدثه باستمرار بأحدث الاصدارات المعتمده من الشركات المصنعه. و ينصح ايضا بأن يكون النظام المثبت من نوع اخر غير المثبت في شبكه و اجهزه الإداره.

6–4–3 أجهزة التحكم للحماية من البرامج المتنقلة

في حالة السماح باستخدام الرموز المتنقلة، يجب أن تضمن عملية الضبط أن الرمز المتنقل المصرح به يعمل وفقا لسياسة أمن محددة بوضوح، وأنه سيتم منع الرموز المتنقلة غير المصرح بها من التنفيذ.

6-4-4 إدارة تحديثات البرامج Patches

تلتزم الجهة المسؤولة بوضع وتوثيق برنامج لإدارة تحديثات البرامج Patches، سواءً كان ذلك البرنامج منفصلاً أو كأحد مكونات عملية إدارة التنصيب الموثقة، وذلك لمتابعة وتقييم واختبار وتنصيب تحديثات البرامج واجبة التطبيق لكافة أصول النظام في الوقت المناسب وفقاً لما يلي:

* تلتزم الجهة المسؤولة بتوثيق تقييم تحديثات الأمن وملفات إصلاح الأعطال للتطبيق خلال خمسة عشرة (15) يوما تقويميا من توفر التحديث أو ملف إصلاح الأعطال.

* تلتزم الجهة المعنية بتوثيق تنفيذ برامج تحديث الأمن وإصلاح أعطاله. وفي أي حالة لا يتم فيها تنصيب التحديث، تلتزم الجهة المسؤولة بتوثيق الإجراء (الإجراءات) التي تعوض ذلك والتي يتم تطبيقها للحد من التعرض للمخاطر أو قبول أي مخاطر.

* يجب تطوير الإجراءات الداخلية لتطبيق التحديثات الهامة/ التحديثات في حالة عدم تمكن المورد من نشر التحديثات الهامة في وقت مناسب.

6-4-5 الثغرات الفنية

يجب الحصول على معلومات عن الثغرات الفنية لأنظمة المعلومات في الوقت المناسب، كما يجب أن يتم تقييم تعرض الجهة لتلك الثغرات، واتخاذ الإجراءات الملائمة للتعامل مع الخطر المرتبط بها.

6-5 السياسة وأنظمة التحكم الأساسية – النسخ الاحتياطية

6-5-1 النسخ الاحتياطية للمعلومات

يجب أخذ نسخ احتياطية من معلومات وبرامجأنظمة التحكم الإشرافي والحصول على البيانات ICS، كما يجب اختبار الاسترداد بشكل دوري (سنويا علي الاقل) وفقاً لسياسة النسخ الاحتياطية المتفق عليها.

6-5-2 النسخ الاحتياطية خارج الموقع

كحد أدنى، يجب تخزين نسخ احتياطية شهرية كاملة خارج الموقع في مرفق آمن، مع توثيق كامل لعملية معالجة النسخ

الاحتياطي خارج الموقع.
يجب تشفير النسخ الاحتياطية إذا كان من المقرر تخزينها لدى طرف آخر أو خارج دولة قطر.

6-5-3 الاجهزه الاحتياطيه و قطع الغيار علي المؤسسه التأكد من توفر قطع غيار و بديل مناسب للأجهزه الهامه

6-6 السياسة وأنظمة التحكم الأساسية – أمن الشبكات وإدارتها

6-6-1 أنظمة الشبكة
يجب أن تخضع الشبكات للإدارة والتحكم الكافي بهدف حمايتها من التهديدات، وللحفاظ على أمن النظم والتطبيقات باستخدام شبكة أنظمة التحكم الإشرافي والحصول على البيانات/ أنظمة التحكم ICS ، بما في ذلك المعلومات العابرة.

6-6-2 أمن خدمات الشبكات
يجب تعريف خصائص الأمن ومستويات الخدمة ومتطلبات الإدارة لكافة خدمات الشبكة، وإضافتها إلى أي اتفاقية خدمات شبكات، سواءً كانت تلك الخدمات مقدمة داخل الجهة أو مسندة إلى جهة خارجية.

6-6-3 هندسة شبكة أنظمة التحكم الإشرافي ICS
يجب على الجهات استخدام هندسة ثلاثية الطبقات للشبكة تتضمن كل من المكونات التالية في طبقة منفصلة ماديا/ منطقيا:
* الشبكة المحلية LAN للشركة/ المشروع
* الشبكة الوسيطه DMZ المشتركة.
* أنظمة التحكم الإشرافي والحصول على البيانات/ أنظمة التحكم ICS
* علي التصميم ان يتجنب نقاط الضعف الواحده عن طريق استخدام الاجهزه عاليه الاعتماديه و الاجهزه المزدوجه و المسارات البديله
و في كل الاحوال يجب ان تفصل بين كل الشبكات المبينه اعلاه عن طريج جدار ناري.

6-6-4 عدم وجود اتصالات مباشرة من شبكة الإنترنت إلى شبكة أنظمة التحكم الإشرافي والحصول على البيانات/ أنظمة التحكم ICS والعكس	يجب ألا تنتهي اتصالات شبكة الإنترنت بشكل مباشر إلى شبكة أنظمة التحكم الإشرافي والحصول على البيانات ICS، ويجب استخدام جدار ناري لفصل شبكة أنظمة التحكم الإشرافي والحصول على البيانات ICS عن شبكة الإنترنت.
6-6-5 الوصول المحدود من شبكة المشروع لشبكة التحكم	يجب استخدام الجدران النارية لفصل شبكات المشروع عن شبكات التحكم. يكون مبدأ قاعدة الجدار الناري كالتالي: منع الكل، السماح بشكل صريح. يجب أن تكون الاتصالات الواردة إلى شبكات أنظمة التحكم الإشرافي والحصول على البيانات ICS محدودة. في حالات استثنائية عندما تكون الاتصالات الواردة ضرورية بشكل مطلق، يجب الحصول على موافقة الإدارة على هذه المخاطرة. يجب تقليل المرور الصادر من خلال الجدار الناري لأنظمة التحكم الإشرافي والحصول على البيانات/ أنظمة التحكم الموزع ICS بحيث يقتصر على الاتصالات الضرورية فقط. يجب تقييد مصدر ووجهة وصول كافة المرور الصادر من أنظمة التحكم الإشرافي والحصول على البيانات/ أنظمة التحكم الموزع ICS إلى شبكة المشروع وذلك عن طريق استخدام الخدمة والمنفذ لقواعد الجدارن النارية الثابتة.
6-6-6 انظمه الكشف عن و منع الاختراق	يجب تثبيت اجهزه منع و الكشف عن الاختراق في الشبكه او المنطقه الوسيطه الفاصله بين الشبكه الخاصه بالموؤسسه و شبكه التحكم الاشرافي. ينصح ايضا بتركيت تلك النظم داخل شبكات نظم التحكم الاشرافي ان امكن.
6-6-7 الطرق الآمنة للدعم المخول عن بعد لنظم التحكم	يجب أن تتم إدارة مرور البيانات عن طريق شبكة إدارة منفصلة وآمنة، أو على شبكة مشفرة مع توثيق ذو عاملين للاتصالات الصادرة من الشبكة المحلية LAN للشركة أو مع توثيق ذو ثلاثة عوامل من الشبكات الخارجية.

بالإضافة إلى ذلك، يجب قصر مرور البيانات عن طريق عنوان بروتوكول الانترنت IP على محطات إدارة خاصة.البيانات الصادره من هذا النظام تحفظ لمده 90 يوما.

6–6–8 الاتصال الآمن للأجهزة اللاسلكية

يجب تجنب الأجهزة اللاسلكية في أنظمة التحكم الإشرافي والحصول على البيانات ICS الهامة. في الحالات التي لا يمكن فيها ذلك، يجب على الجهة استخدام توثيق وتشفير لآليات الأمن المدعومة (على الأقل استخدام تشفير الوصول المحمي للشبكة اللاسلكية WPA لشبكات 802.11x) لمنع الوصول اللاسلكي غير المخول إلى أنظمة التحكم الإشرافي والحصول على البيانات ICS. ينصح باتباع المعيار ISA100 كلما امكن.

وتتضمن التكنولوجيا اللاسلكية على سبيل المثال لا الحصر الموجات الصغرى والأقمار الصناعية وراديو الحزمة (التردد فوق العالي UHF/ التردد العالي جدا VHF) وشبكات 802.11x.

6–6–9 القواعد المحددة التي تحدد نوع المرور المسموح به على الشبكة

يجب تعريف وتوثيق أنواع المرور المسموح بها (البروتوكول/ المنافذ).

6–6–10 مراقبة المرور الذي يحاول دخول شبكات أنظمة التحكم الإشرافي والحصول على البيانات/ أنظمة التحكم ICS

يجب على الجهات مراقبة وتسجيل المرور الداخل إلى شبكة أنظمة التحكم الإشرافي والحصول على البيانات ICS وذلك لتسجيل كافة أنشطة الشبكة غير المخولة أو عمليات الوصول المرفوضة بشكل مستمر و حفظ اليانات لمده 90 يوما.

6–6–11 أنظمة التحكم الإشرافي والحصول على البيانات ICS والبروتوكلات الصناعية (MODBUS/TCP, EtherNet/IP and DNP3)

يجب أن يقتصر السماح للبرتوكولات المتعلقة بأنظمة التحكم الإشرافي والحصول على البيانات مثل /ICS (MODBUS/TCP, EtherNet/IP, DNP3) على داخل شبكات أنظمة التحكم الإشرافي والحصول على البيانات/ أنظمة التحكم ICS؛ وألا يتم السماح لها بالعبور

إلى شبكة المشروع.

12-6-6 الاتصال الاسلكي

ZigBeeيجب أن يقتصر السماح للبرتوكولات المتعلقة بأنظمة التحكم الإشرافي والحصول على البيانات مثل /ICS MODBUS/TCP,) EtherNet/IP, DNP3) على داخل شبكات أنظمة التحكم الإشرافي والحصول على البيانات/ أنظمة التحكم ICS؛ وألا يتم السماح لها بالعبور إلى شبكة المشروع.

علي نظام الاتصال الاسلكي من هذا النوع تطبيق ما يلي/

- البنيه التحتيه للشبكه محميه بمفاتح للشبكه
- تشغيل خاصيه التشفير
- المنع يتم عن طريق عنوان الجهاز MAC Address
- تشغيل خاصيه التأكد من نقطه المصدر.

13-6-6 قواعد حفظ ومعالجة البيانات والخدمات ذات الصلة

يجب اعتماد تصميم ذي ثلاث مناطق عند إدخال قواعد حفظ ومعالجة البيانات عندما تستخدم الجهة نموذج ثنائي الخادم. يتم وضع خادم قواعد حفظ ومعالجة البيانات على شبكة أنظمة التحكم الإشرافي والحصول على البيانات/ أنظمة التحكم ICS لجمع البيانات من المراقبة/ وحدة تحكم الطرفيات البعيدة RTU، ويتم وضع خادم ثان على شبكة الشركة لنسخ الخادم الأول ودعم استفسارات العملاء.

14-6-6 أجهزة مودم (مرسل رقمي) الاتصال العادي

يجب على الجهة تحديد استخدام أجهزة المودم (المرسل الرقمي) المتصلة بشبكات أنظمة التحكم الإشرافي والحصول على البيانات ICS. وفي حالة عدم إمكانية استخدام بدائل أخرى، يتعين توفر الضوابط التالية:

* خصائص معاودة الاتصال.

يجب تغيير كلمات المرور الأساسية.

* تعريف أجهزة المودم المستخدمة بشكل مادي إلى مشغلي غرفة التحكم. والتأكد من أنها معدودة ومسجلة في قائمة الأجهزة المعتمدة.

* فصل أجهزة المودم في حالة عدم استخدامها، أو ضبطها بحيث تفصل تلقائياً بعد توقفها عن العمل لفترة زمنية محددة.

* في حالة استخدام أجهزة المودم للدعم عن بعد، تأكد من

إبلاغ موظفي الدعم بهذه الإرشادات بشكل جيد.

6-6-15 تعريف الأجهزة في الشبكات

يجب استخدام التعريف التلقائي للأجهزة كوسيلة لتوثيق الاتصالات من مواقع وأجهزة معينة و لتحديد الاتصالات الدخيله.

6-6-16 حماية منفذ التشخيص والضبط عن بعد

يجب التحكم في الوصول المادي والمنطقي لمنافذ التشخيص والضبط الخاصة بالنظم ومجالات الخدمة وأجهزة الاستشعار وأجهزة الاتصالات التابعة لأنظمة التحكم الإشرافي والحصول على البيانات/ أنظمة التحكم ICS.

6-6-17 الفصل في الشبكات

يجب فصل خدمات المعلومات والمستخدمين ونظم المعلومات على الشبكات.

6-6-18 الفصل في الادوار

يجب الفصل بين الادوار للمتعاملين مع النظام

6-6-19 التحكم في اتصالات الشبكات

بالنسبة للشبكات المشتركة، خاصة تلك الشبكات التي تمتد عبر الحدود المادية للجهة، يجب فصل قدرة المستخدمين على الاتصال بشبكة أنظمة التحكم الإشرافي والحصول على البيانات/ أنظمة التحكم /ICS. يجب أن تكون الاستثناءات المحددة متماشية مع سياسة التحكم في الوصول.

6-6-20 البيانات احاديه الاتجاه

ينصح بتثبيت تكنولوجيا البيانات احاديه الاتجاه كلما امكن

6-6-21 تثبيت الجدار الناري

ينصح بأن يكون الحائط الناري المستخدم في الشبكه نظام التحكم من نوع اخر غير المستخدم في شبكه الموؤسسه

6-7 السياسة وأنظمة التحكم الأساسية – معالجة الوسائط

6-7-1 إدارة الوسائط القابلة للإزالة

يجب عدم السماح باستخدام الوسائط القابلة للإزالة في غرفة التحكم الخاصة بأنظمة التحكم الإشرافي

والحصول على البيانات/ أنظمة التحكم الموزع /ICS DCS، أو استخدامها داخل النظام؛ إلا إذا كان ذلك الاستخدام مخولاً بشكل صريح من قبل الإدارة.

6-7-2 التخلص من الوسائط يجب التخلص من الوسائط عند زوال الحاجة إليها، وذلك باستخدام الإجراءات الرسمية للجهة.

6-7-3 **إجراءات معالجة المعلومات** يجب وضع إجراءات لمعالجة وتخزين معلومات أنظمة التحكم الإشرافي والحصول على البيانات/ أنظمة التحكم ICS وذلك لحماية هذه المعلومات من الإفصاح غير المخول أو إساءة الاستخدام.

6-7-4 أمن وثائق النظام يجب حماية وثائق أنظمة التحكم الإشرافي والحصول على البيانات/ أنظمة التحكم /ICSمن الوصول غير المخول.

6-8 السياسة وأنظمة التحكم الأساسية – تبادل معلومات أنظمة التحكم الإشرافي والحصول على البيانات/ أنظمة التحكم ICS

6-8-1 سياسات وإجراءات تبادل المعلومات يجب وضع سياسات وإجراءات وضوابط لعملية التبادل الرسمي وذلك لحماية تبادل المعلومات من خلال استخدام كافة أنواع مرافق الاتصالات (البريد الالكتروني، أجهزة الفاكس، PSTN، GSM... الخ)

6-8-2 اتفاقيات التبادل يجب إبرام اتفاقيات خاصة لتبادل معلومات وبرمجيات أنظمة التحكم الإشرافي والحصول على البيانات/ أنظمة التحكم ICS بين الجهة والجهات الخارجية.

6-8-3 الوسائط المادية أثناء مرحلة العبور يجب حماية الوسائط التي تحتوي على معلومات خاصة بأنظمة التحكم الإشرافي والحصول على البيانات/ أنظمة التحكم ICS من الوصول غير المخول (أي

باستخدام التشفير مثلاً)، ومن إساءة الاستخدام أو التلف أثناء النقل خارج الحدود المادية للجهة. وقد وردت تفاصيل البروتوكلات/ المفاتيح المقبولة للتشفير في الملحق (أ).

6-8-4 التراسل الالكتروني

يجب حماية معلومات أنظمة التحكم الإشرافي والحصول على البيانات/ أنظمة التحكم /ICSالتي ترسل عبر الوسائل الالكترونية بشكل ملائم.

6-9 السياسة وأنظمة التحكم الأساسية – المراقبة

6-9-1 تسجيل التدقيق

يجب إعداد سجلات للتدقيق لتسجيل أنشطة المستخدمين وحالات الاستثناء وأحداث أمن المعلومات، كما يجب حفظ تلك السجلات لمدة (90) تسعين يوماً تقويمياً للمساعدة في مراقبة/ توثيق الوصول ودعم أية عمليات بحث وتقصي.

يجب وضع إجراءات لمراقبة استخدام مرافق معالجة معلومات أنظمة التحكم الإشرافي والحصول على البيانات/ أنظمة التحكم /ICS ، وأن يتم مراجعة نتائج أنشطة المراقبة بشكل دوري.

6-9-2 التسجيل المركزي

ينصح بأن تكون السجلات محفوظه و تدار مركزيا من نظام منفصل.

6-9-3 مراقبه السجلات

يجب ان يكون هناك مراقبه دوريه و مراجعه لنتائج المراقبه

6-9-4 حمايه السجلات

يجب حمايه انظمه السجلات ضد العبث و الدخول الغير مصرح به و ان تكون السجلات منفصله عن انظمه السجلات الخاصه باداره تكنولوجيا المعلومات

6-9-5 سجلات المشرف و مهندسي التشغيل

يجب تسجيل نشاطات المشرفين و مشغلي انظمه التحكم الاشرافي

6-9-6 تسجيل الاخطاء

يجب تسجيل الاخطاء و دراستها

6-9-7 توحيد ساعه النظام

يجب توحيد التوقيت الخاص بالانظمه بدقه لتوافق التقويم العالمي UTC او المحلي لدوله قطر GMT+3

7- التحكم في الوصول

7-1 هدف السياسة

تهدف هذه السياسة إلى التحكم في الوصول إلى أنظمة ومعلومات أنظمة التحكم الإشرافي والحصول على البيانات/ أنظمة التحكم ICS وضمان توفر سجلات التحكم في الوصول إلى تلك الأنظمة، وكذلك التحكم في الوصول إلى وظيفة العملية ككل.

7-2 السياسة وأنظمة التحكم الأساسية – سياسة الوصول وإدارة وصول المستخدم

7-2-1 سياسة التحكم في الوصول

يجب وضع سياسة للتحكم في الوصول إلى أنظمة التحكم الإشرافي والحصول على البيانات/ أنظمة التحكم /ICS، وتوثيقها ومراجعتها بناءً على متطلبات الأعمال ومتطلبات الأمن الخاصة بالوصول. كما يتعين أن تعتمد تلك السياسة على مفاهيم أقل الامتيازات والمساءلة الشخصية/ المسماة.

ويجوز لإدارة الحساب أن تضم أنواع حسابات إضافية (كأن تكون حسابات تعتمد على الأدوار أو الأجهزة أو الخصائص).

7-2-2 تسجيل المستخدم

يجب أن يكون هناك إجراء رسمي لتسجيل وإلغاء تسجيل مستخدمي أنظمة التحكم الإشرافي والحصول على البيانات/ أنظمة التحكم /ICSوذلك لمنح وإلغاء الوصول لكافة الأنظمة والخدمات ذات الصلة.

كما يجب إبلاغ إدارة تكنولوجيا المعلومات وإدارة شؤون العاملين (الموارد البشرية) في الشركة بهذا الإجراء.

7-2-3 **إدارة الامتيازات**

يجب قصر توزيع واستخدام الامتيازات والتحكم فيها. كما تلتزم الجهة المسؤولة بضمان توافق الحسابات الفردية والمشتركة مع مفهوم الحاجة للمعرفة/ الحاجة للمشاركة فيما يتعلق بوظائف العمل التي يتم القيام بها.

7-2-4 إدارة كلمات مرور المستخدمين يجب التحكم في توزيع كلمات المرور من خلال عملية إدارة رسمية.

7-2-5 تعقد كلمة المرور يجب على الجهة أن تشترط وتستخدم كلمات مرور تخضع لما يلي (وفقاً لما يكون مجدياً من الناحية الفنية):
* يجب أن يكون الحد الأدنى لعدد رموز كل كلمة مرور/ جملة مرور اثنى عشر رمزاً.
* يجب تغيير كل كلمة مرور مرة واحدة سنوياً على الأقل، أو بمعدل أكثر تكراراً بناءً على تقييم المخاطر الذي تقره الجهة.

7-2-6 مراجعة حقوق الوصول الممنوحة للمستخدم يجب على الإدارة مراجعة حقوق الوصول الممنوحة للمستخدم على فترات دورية باستخدام عملية رسمية. ولا يجوز لموظفي الأمن الذين يقومون بوظائف التحكم في الوصول إجراء عملية المراجعة أو القيام بوظائف التدقيق.

7-2-7 **الاختبار** تلتزم الجهة المسؤولة بتنفيذ برنامج صيانة واختبار لضمان عمل كافة وظائف الأمن المدرجة تحت بند "التحكم في الوصول" بصورة جيدة.

7-3 السياسة وأنظمة التحكم الأساسية – التحكم في الوصول إلى الشبكة ونظام التشغيل

7-3-1 سياسة استخدام خدمات الشبكة الخاصة بأنظمة التحكم الإشرافي والحصول على البيانات/ أنظمة التحكم ICS/ يقتصر تزويد المستخدمين بالوصول إلى خدمات أنظمة التحكم الإشرافي والحصول على البيانات/ أنظمة التحكم ICSالتي تم تخويلهم باستخدامها بشكل خاص فقط.

7-3-2 **إجراء الدخول الآمن** يجب التحكم في الوصول إلى أنظمة التشغيل الخاصة بأنظمة التحكم الإشرافي والحصول على البيانات/ أنظمة التحكم /ICSمن خلال إجراء للدخول الآمن يتماشى مع سياسة التحكم في الوصول المتبعة في الجهة.

7-3-3 تعريف وتوثيق المستخدم

يحدد لكل المستخدمين أو لكافة العمليات "التي تعمل نيابة عن المستخدمين" رقم هوية فريد (هوية المستخدم) يقتصر استخدامه على الاستخدام الحصري والمقصود من قبل المستخدمين، كما يجب اختيار أسلوب توثيق مناسب للتثبت من الهوية التي يتم إدخالها للمستخدم/ العملية.

وباستثناء الحالات التي يستحيل فيها من الناحية الفنية استخدام هوية شخصية، يجب الحرص على وجود ما يلي:

* مبدأ الحاجة للمعرفة/ الحاجة للمشاركة ساري ومسجل، ويتم تحديده من خلال الواجبات الرسمية المسندة لكل شخص، على أن يراعي كافة المعايير الخاصة بأمن الموظفين.

* اجراءات تكميليه و تعويضيه مثل كاميرات المراقبه الامنيه او الكروت الذكيه.

* تقوم الجهة بترخيص ومراقبة استخدام الحسابات المحددة للضيوف/ الحسابات المشتركة/ الحسابات المغفلة (دون أسماء)، وإزالة أو فصل الحسابات غير الضرورية أو تأمينها بأي طريقة أخرى.

* تقوم الجهة بإزالة أو تغيير أو فصل الحسابات الافتراضية أو تأمينها بأي طريقة آخرى.

* يتم إبلاغ مدراء الحسابات/ الدوامات في حالة إنهاء خدمات المستخدمين أو نقلهم، ويتم إزالة أو فصل الحسابات الخاصة بهم أو تأمينها بأي طريقة أخرى.

* كما يتم إخطار مدراء الحسابات/ الدوامات عندما يطرأ تغيير على استخدام المستخدمين أو حاجتهم للمعرفة أو حاجتهم للمشاركة.

* في الحالات التي تكون فيها الحسابات قائمة على الأدوار، أي أن محطة العمل أو الجهاز و/أو الأجهزة الميدانية تحدد دور المستخدم، يجب أن يتضمن الوصول إلى أنظمة التحكم الإشرافي والحصول على البيانات/ أنظمة التحكم /ICSأنظمة تحكم أمني مادية مناسبة قادرة على تعريف المشغل وتسجيل وقت الدخول والمغادرة.

7-3-4 أنظمة إدارة كلمات المرور

يجب أن تكون أنظمة إدارة/ تخزين كلمات المرور الخاصة بأنظمة التحكم الإشرافي والحصول على البيانات/ أنظمة التحكم /ICS

تفاعلية، كما يجب أن تضمن جودة كلمات المرور.

7-3-5 **استخدام مرافق النظام** يجب أن يتم تقييد استخدام برامج المرافق التي قد تكون قادرة على تجاوز النظام وكذلك أجهزة التحكم في التطبيقات، وأن يتم التحكم فيها بشكل صارم.

7-3-6 **انتهاء وقت الجلسة** يجب أن تغلق تلقائياً جلسات أنظمة التحكم الإشرافي والحصول على البيانات/ أنظمة التحكم /ICSغير النشطة بعد فترة محددة من التوقف عن النشاط.

7-3-7 **التحكم في الجلسات المتزامنة** يجب أن تعمل أنظمة التحكم الإشرافي والحصول على البيانات/ أنظمة التحكم /ICSعلى تقييد عدد الجلسات المتزامنة لأي مستخدم محدد و/أو اسم مستخدم وذلك تماشياً مع سياسة الجهة بشأن الجلسات المتزامنة.

7-3-8 **تقييد وقت الاتصال** يجب استخدام قيود على أوقات الاتصال لتوفير أمن إضافي للتطبيقات عالية المخاطر.

7-4 السياسة وأنظمة التحكم الأساسية – وصول الأجهزة الميدانية ووحدات التحكم الطرفية RTU

7-4-1 وحدات التحكم الطرفية بالاتصال العادي لا تستخدم بروتوكولات قابلة للتحويل إن الأجهزة مثل وحدات التحكم الطرفية RTU التي لا تستخدم برتوكولات قابلة للتحويل لا يطلب غلقها في محيط الأمن المادي، ولكن يجب غلقها ومراقبتها في حدود محيط الأمن الالكتروني.

7-4-2 وحدات التحكم الطرفية RTU بالاتصال العادي التي تستخدم بروتوكولات قابلة للتحويل يجب غلق الأجهزة مثل وحدات التحكم الطرفية RTU التي تستخدم بروتوكولات قابلة للتحويل في حدود محيط الأمن المادي وكذلك في محيط الأمن الالكتروني.

ينصح بأن تستخدم أجهزة المجالات المؤمنة شهادات مشفرة صادرة

7-4-3 **توثيق وحدات التحكم الطرفية RTU** من قبل مصنع شهادات وذلك لتأكيد هوية الجهاز.

7-4-4 الوصول المباشر للأجهزة الميدانية التشغيلية

أي اتصال مباشر بأجهزة المجال التشغيلية يتم من قبل موظف ميداني يجب أن يتم إتمامه بطريقة تتضمن تطبيق فحوصات للسماح بإتمام ذلك الاتصال؛ أي أن هناك مساءلة شخصية (مثل الاحتفاظ بالسجلات مع هوية بشرية) لأي إجراء يتم عن طريق ذلك الوصول؛ وأن تظل حالة الجهاز متماشية مع أي نسخ من تلك الحالة يتم إخفائها بواسطة نظام التحكم.

7-4-5 تسجيل الوصول إلى وحدات التحكم الطرفية RTU

يجب أن تتيح الأجهزة الميدانية المؤمنة القدرة على كشف الرسائل المستلمة والتخلص منها، ونقصد هنا الرسائل التي يكون وقت استلامها بالنسبة للحظة المتوقعة لإرسالها، أو تتابعها، يمثل إخلالاً بخصائص جودة الخدمة الخاصة بجلسة الاتصالات.

7-4-6 واجهة اتصالات وحدات التحكم الطرفية RTUS

يجب تشفير روابط الاتصال بوحدات التحكم الطرفية على النحو المحدد في الملحق (أ). كما يجب ألا يعمل التشفير المستخدم على واجهة الاتصال على خفض درجة القدرة الوظيفية أو الأدائية للوظيفة التشغيلية التي تتمتع بالتخويل للوصول إلى وحدات التحكم الطرفية RTU.

8- إدارة حوادث أمن المعلومات

8-1 هدف السياسة

تهدف هذه السياسة إلى ضمان الإبلاغ عن أحداث ونقاط ضعف أمن المعلومات المرتبطة بنظم المعلومات الخاصة بأنظمة التحكم الإشرافي والحصول على البيانات/ أنظمة التحكم ICS على نحو يسمح باتخاذ الإجراء التصحيحي في الوقت المناسب.

8-2 السياسة وأنظمة التحكم الأساسية

8-2-1 خطة الاستجابة لحوادث أنظمة التحكم الإشرافي والحصول على البيانات/ أنظمة التحكم /ICS

تلتزم الجهة المسؤولة بتطوير وصيانة خطة للاستجابة لحوادث أمن معلومات أنظمة التحكم الإشرافي والحصول على البيانات/ أنظمة التحكم الموزع ICS على أن تتناول تلك الخطة الجوانب التالية كحد أدنى:

* إجراءات وصف وتصنيف الأحداث كحوادث أمن يجب الإبلاغ عنها.
* إجراءات الإبلاغ عن حوادث الأمن كما ينبغي وفي الوقت المناسب لقنوات الإدارة المناسبة.
* عملية تحديث خطة الاستجابة للحوادث خلال (30) ثلاثين يوماً تقويمياً تحسباً لأي تغييرات في آلية الإبلاغ أو التدرج الهرمي التنظيمي أو جهات الاتصال... الخ
* إجراءات اختبار خطة الاستجابة للحوادث، مرة واحدة سنوياً على الأقل. ويمكن أن تتراوح هذه الاختبارات من الاختبارات التشبيهية إلى سيناريوهات التشغيل الكامل للاستجابة لحادث فعلي.

8-2-2 الإبلاغ عن نقاط الضعف الأمنية

يجب على كافة الموظفين والمقاولين والأطراف الأخرى التي تستخدم نظم وخدمات المعلومات ملاحظة أي نقاط ضعف أمنية ملحوظة أو مشكوك فيها في الأنظمة أو الخدمات. ويمكن أن يتحقق ذلك من خلال إضافة هذا الشرط بشكل رسمي في العقود أو التوصيفات الوظيفية... الخ

8-2-3 الاتصال بالسلطات

يجب على الجهة المسؤولة إنشاء قنوات اتصال إلى الحد القابل للتطبيق مع كيو سرت وذلك للإبلاغ عن أية مشكلات قد تحدث نتيجة لأعمال التخريب أو ما شابهها.

9- دارة استمرارية الأعمال

9-1 هدف السياسة

تهدف هذه السياسة إلى مكافحة وتقليل انقطاع أنشطة الأعمال وحماية العمليات الحيوية في أنظمة التحكم الإشرافي والحصول على البيانات/ أنظمة التحكم /ICSمن آثار حالات التعطل الكبيرة في أنظمة المعلومات وانقطاع الشبكات أو الكوارث، بالإضافة إلى ضمان استعادة تلك الأنشطة في الوقت المناسب.

9-2 السياسة وأنظمة التحكم الأساسية

9-2-1 استمرار أعمال أنظمة التحكم الإشرافي والحصول على البيانات/ أنظمة التحكم الموزع ICS وخطة استعادة النظم بعد الكوارث

يجب أن تكون خطة استمرارية أعمال أنظمة التحكم الإشرافي والحصول على البيانات/ أنظمة التحكم /ICSأحد مكونات خطة استمرارية الأعمال في الشركة، كما يجب أن تشتمل على البنود التالية كحد أدنى:

* تصنيف تأثر الأعمال وتحديد أولويات أصول أنظمة التحكم الإشرافي والحصول على البيانات/ أنظمة التحكم الموزع /ICS
* الاستجابة اللازمة للحوادث التي ستعمل على تنشيط الخطة
* إجراءات تشغيل الوظائف الأساسية للأنظمة في وضع يدوي لحين استعادة الأوضاع التشغيلية الطبيعية
* أدوار ومسؤوليات المسؤولين عن الاستجابة لخطة استمرارية أعمال أنظمة التحكم الإشرافي والحصول على البيانات/ أنظمة التحكم /ICS
* وثائق حديثة مكتملة (أدلة، وثائق الضبط والتنصيب، الإجراءات، قوائم عقود الموردين، الرسومات البيانية للشبكة... الخ)
* قائمة الموظفين الخاصة بالوصول المادي والمنطقي المصرح به للأنظمة.
* ترتيب/ تتابع استعادة مكونات النظام.
* إجراءات استعادة واسترداد النسخ الاحتياطية المحفوظة خارج موقع العمل.
* إجراءات الاتصال مع السلطات المناسبة

10- الالتزام

10-1 هدف السياسة

تهدف هذه السياسة إلى تجنب خرق التزامات منصوص عليها في أي قانون أو لائحة أو عقد، وضمان التزام الأنظمة بالسياسات والمعايير الأمنية المحلية و/أو التنظيمية. كما تغطي هذه السياسة اعتبارات فحص الأنظمة.

10-2 السياسة وأنظمة التحكم الأساسية – الالتزام

10-2-1 تعريف التشريع واجب التطبيق

يجب تعريف وتوثيق وتحديث كافة المتطلبات القانونية والتنظيمية والتعاقدية وأسلوب الجهة في تلبية تلك المتطلبات بشكل صريح وذلك لكل نظام من أنظمة المعلومات بالجهة.

10-2-2 الالتزام بالسياسات والمعايير الأمنية

يلتزم المدراء بضمان تنفيذ كافة إجراءات الأمن في نطاق مسؤوليتهم بصورة صحيحة وذلك لتحقيق الالتزام بسياسات ومعايير الأمن، بما في ذلك هذه الوثيقة.

10-2-3 **الفحص الداخلي للالتزام الفني**

يجب أن تمر أنظمة التحكم الإشرافي والحصول على البيانات/ أنظمة التحكم /ICSبفحص ذاتي دوري للكشف عن الالتزام بمعايير تطبيق الأمن، بما في ذلك هذه الوثيقة، وذلك مرة واحدة سنوياً على الأقل.

10-2-4 مراقبة الالتزام والاحتفاظ ببيانات الفحص

يجب على الجهة الخاضعة للفحص الاحتفاظ بآخر تقرير للفحص وكافة الوثائق المتعلقة به لمدة عامين على الأقل من تاريخ استلام التقرير.

10-2-5 **مستويات عدم الالتزام**

تتطلب نتائج الفحص عملية تصحيح تماشياً مع النظام التالي:

* المستوى الأول: جوانب عدم مطابقة وملاحظات بسيطة يجب تصحيحها خلال (6) ستة أشهر.

* المستوى الثاني: جوانب عدم مطابقة مؤثرة ويجب تصحيحها خلال (3) ثلاثة أشهر.

10–3 السياسة وأنظمة التحكم الأساسية – فحص النظام

10-3-1 **ضوابط فحص نظم المعلومات**

يجب تخطيط متطلبات وأنشطة الفحص التي تتضمن إجراء فحوصات على النظم التشغيلية لأنظمة التحكم الإشرافي والحصول على البيانات/ أنظمة التحكم الموزع /ICSوالاتفاق عليها بعناية وذلك للحد من مخاطر توقف عمليات تشغيل الأعمال.

10–3–2 حماية أدوات فحص نظم المعلومات

يجب حماية الوصول إلى أدوات فحص نظم المعلومات الخاصة بأنظمة التحكم الإشرافي والحصول على البيانات/ أنظمة التحكم الموزع /ICSلمنع أي إساءة استخدام أو تعرض للمخاطر.

11– تقوية النظام

11–1 هدف السياسة

تهدف هذه السياسة إلى إلى ضمان فصل الخدمات غير المستخدمة في النظام التشغيلي المضيف / أنظمة التحكم الإشرافي والحصول على البيانات ICS. ويجب أن يقتصر التشغيل على الخدمات التي يستخدمها نظام التحكم الإشرافي والحصول على البيانات ICS وتشغيله وصيانته فقط وذلك للحد من نقاط الدخول أو الثغرات الممكنة.

11–2 السياسة وأنظمة التحكم الأساسية

11-2-1 **القائمة البيضاء لتطبيقات الموردين**

تلتزم الجهات بالحصول على قائمة بكافة التطبيقات والمرافق وخدمات النظم والحروف الطباعية وكافة البرمجيات الأخرى اللازمة للإبقاء على أنظمة التحكم الإشرافي والحصول على البيانات ICS في حالة تشغيل، والاحتفاظ بتلك القائمة.

يجب إزالة كافة البرمجيات/ الخدمات غير الضرورية، ويتضمن ذلك على سبيل المثال ما يلي:

11-2-2 **البرمجيات/ الخدمات الواجب إزالتها**

* الألعاب
* برامج التشغيل أو التعريف الخاصة بأجهزة غير مشمولة.
* خدمات التراسل.
* الخوادم أو العملاء لخدمات الانترنت غير المستخدمة

* أجهزة جمع البرمجيات (باستثناء آلات التطوير غير المنتجة)
* أجهزة جمع البرمجيات للغات غير المستخدمة
* البروتوكولات والخدمات غير المستخدمة بشكل عام
* المرافق الإدارية وبرامج التشخيص ووظائف إدارة الشبكات وإدارة النظم غير المستخدمة
* برامج الاختبار وعينات البرامج أو الحروف الطباعية
* باقات الإنتاجية ومرافق معالجة الكلمات غير المستخدمة، على سبيل المثال برنامج Word، برنامج Excel، برنامج Powerpoint، برنامج Adobe acrobat، برنامج Open Office... الخ
* البرامج الغير مرخصه و النسخ التجريبيه
* خدمات نظام UPnP

11-2-3 استخدام تقنيه البلوتوث

يجب حظر استخدام تكنولوجيا البلوتوث

11-2-4 **حماية نظام الإدخال والإخراج الأساسي)**

يجب أن يكون نظام الإدخال والإخراج الأساسي BIOS محمي عن طريقة كلمة مرور من إجراء أي تغييرات غير مخولة.

11-2-5 **فصل الحسابات المعروفة أو حسابات الضيوف**

يجب فصل الحسابات وكلمات المرور الافتراضية، أو تغييرها لتحقيق متطلبات التعقد في الجهة.

11-5-6 **اعتماد الاجهزه**

ينصح بأن تكون الاجهزه الخاصه بأمن المعلومات المستخدمه حاصله علي درجه الاعتماد +4 او اعلي الصادره من جهه التصنيف الموحد common criteria طبقا لنظام الايزو ISO 15408

الملحق (أ) (معياري) خوارزميات وبروتوكولات التشفير المعتمدة

المفتاح المتماثل/ المفتاح الخاص:

يجب أن تكون وظائف التشفير التي تستخدم أحد شفرات المفتاح المتماثل (ويشار إليها أحياناً باسم تشفير المفتاح الخاص) والتي توظف مفتاحاً سرياً مشتركاً مطابقة للمواصفات التالية:

اسم الخوارزمية	المراجع	الاستخدام المعتمد	الطول المطلوب للمفتاح
AES	معيار التشفير المتقدم، شفرة حجب تعتمد على خوارزمية تعرف باسم "Rijndael"	تشفير البيانات العامة	مفاتيح 256 بت
TDES /3DES	معيار تشفير البيانات الثلاثية (Triple DES) وهو شفرة حجب (SP800-67)	تشفير البيانات العامة	ثلاث مفاتيح فريدة 56 بت

ملاحظة: يجب استخدام خوارز AES إلا إذا كان ذلك غير ممكن من الناحية الفنية. يجب أن يقتصر استخدام خوارزمية TDES على النظم التي لا تدعم الخوارزمية AES.

المفتاح اللا متماثل/ المفتاح العام:

يجب أن تكون وظائف التشفير التي تستخدم شفرات المفتاح اللا متماثل (والذي يعرف أيضاً بالتشفير بالمفتاح العام) والتي توظف زوجاً من المفاتيح التشفيرية تتألف من مفتاح عام وآخر خاص، يجب أن تكون مطابقة للمواصفات التالية:

اسم الخوارزمية	المراجع	الاستخدام المعتمد	الطول المطلوب للمفتاح
RSA	"Rivest-Shamir-Adleman" خوارزمية للتشفير بالمفتاح العام RSA	التوقيعات الرقمية، نقل مفاتيح جلسة التشفير	مفاتيح 1024 بت
DSA	خوارزمية التوقيع الرقمي [FIP186-2]	التوقيعات الرقمية	مفاتيح 1024 بت

خوارزميات Hash

يمكن استخدام خوارزميات Hash الآمنة لدعم تنفيذ توثيق رسالة keyed-hash. وبصفة عامة، فإن وظائف Hash تستخدم لزيادة سرعة مهام مقارنة البيانات، مثل العثور على إحدى البيانات في قاعدة بيانات، أ, الكشف عن سجلات مكررة أو مشابهة في ملف أو نظام كبير.

اسم الخوارزمية	المراجع	الاستخدام المعتمد	الطول المطلوب للمفتاح
SHA-n	خوارزمية hash آمنة تنتج حجم hash بمقدار "n" مثل: SHA) 224, 256,384,512) [SHA]	كافة أغراض الاختزال	$n \geq 256$
MD5	Message Digest v5 [RFC 1321]	كافة أغراض الاختزال	حالة 128 بت المكررة

ملاحظة: يجب استخدام خوارزمية SHAn إلا إذا كان ذلك غير ممكن من الناحية الفنية. يجب أن يقتصر استخدام خوارزم MD5على النظم التي لا تدعم الخوارزم أسرة SHA.

الملحق (ب) – (تعليمي) – المرجع لإرشادات الشراء

يجب ان تحتوي مناقصات و اوامر الشراء علي المتطلبات الأمنيه للمؤسسه طبقا لهذا المعيار. علي سبيل المثال:

- **هندسه و تصميم الشبكات**
- **عدم تثبيت البرامج و الخدمات الغير مستخدمه**
- **برامج مكافحه الفيروسات و انظمه الكشف عن الاختراقات**
- **تقويه نظام التشغيل و نظام الملفات**
- **التطوير المستمر لاحدث الاصدارات لتلافي اي ثغرات أمنيه مكتشفه بما فيها برامج الطرف الثالث**
- **اسلوب تثبيت و اداره الجدار الناري و انظمه مكافحه الاختراقات**
- **تغيير الحسابات الاصليه و إمكانيه الحسابات الشخصيه**
- **إداره كلمات السر**
- **البنيه التحتيه لسجلات النظام**
- **إجراءات النسخ الاحتياطيه و استرداد النظام**

من اجل المزيد من المعلومات ممكن الرجوع الي الاصدار (لغة الشراء الخاصة بالأمن الالكتروني لأنظمة التحكم) الصادر من قبل مركز حماية البنية التحتية الهامة التابع للحكومه الامريكيه و الصادر في 2009.

المصدر:

http://ics-cert.us-cert.gov/pdf/FINAL-Procurement_Language_Rev4_100809.pdf

يجب أن يتضمن طلب تقديم العرض الصادر لمودري أنظمة التحكم العناصر التالية كإرشاد:

أساس الموضوع: أساس الموضوع عبارة عن ملخص لحالات التعرض والثغرات الممكنة المرتبطة بفئة معينة من المشكلات، أي السبب في إضافة الموضوع.

لغة الشراء: يقصد بها المصطلحات التي ورد شرحها في البند رقم 14 من الوثيقة (لغة الشراء الخاصة بالأمن الالكتروني لأنظمة التحكم).

إرشاد اللغة: معلومات إضافية تقدمها جهة البنية التحتية الهامة بشأن لغة الشراء وكيف يقصد منها تلبية الحاجات المبينة في الأساس.

إجراءات اختبارات القبول في المصنع: إن اختبار القبول في المصنع ضروري لضمان عمل الخصائص الأمنية كما ينبغي، وتقديم المستويات المطلوبة من أداء الوظائف. ويجب أن يتضمن كل موضوع في طلب تقديم العرض مهام اختبار القبول في

المصنع الخاصة بذلك الموضوع. لاحظ أن اختبار قبول المصنع عبارة عن عملية، وليس حدث، وقد تمتد في الواقع إلى أكثر من عدة أسابيع أو شهور.

إجراءات اختبارات القبول في الموقع: يكرر اختبار القبول في الموقع والذي يجريه مالك الأصل نوعاً فرعياً من اختبار القبول في المصنع بعد تركيب النظام، ولكن قبل التشغيل أو بدء العمل، وذلك لإثبات أن التركيب في الموقع مساو للنظام الذي تم اختباره في مصنع المورد، أو على النحو المبين بالوصف في أدلة الأنظمة. وكما هو الحال بالنسبة لاختبار القبول في المصنع، فإن اختبار القبول في الموقع قد يمتد لعدة أسابيع أو شهور، ويتم بالإضافة إلى ذلك في عدة مواقع مختلفة.

إرشاد الصيانة: يتناول هذا الإرشاد كيفية قيام المورد بالحفاظ على مستوى أمن النظام الذي تم إنشاؤه أثناء اختبار القبول في الموقع مع تطور عمل النظام أو تحديثه وإضافة برامج إصلاح الأعطال والتحديث. وقد يكون هذا البند الفرعي أفضل بند خاص بالأمن يمكن إضافته إلى أي عقد صيانة، وليس في مواصفات الشراء وذلك للحفاظ على دعم مستمر.

المراجع: إضافة المعلومات والممارسات والمعايير الخارجية الداعمة.