ضوابط الأمن السيبراني لموردي ومقاولي الخدمات المدارة

الهدف

تعتمد شركة الاتصالات الكويتية stc وشركة موردي/مقاولي الخدمات المدارة على الأداء الموثوق لبنيتها التحتية الحيوية. تستغل تهديدات أمن المعلومات التعقيد المتزايد والاتصال لأنظمة البنية التحتية الحيوية، مما يعرض أمن stc وموردي الخدمات المدارة والاقتصاد، وسلامة أصحاب المصلحة للخطر.

من المهم قيام مورد الخدمات المدارة بتنفيذ الضوابط الأساسية لأمن المعلومات الخاصة بـ stc لحماية وضع أنظمة معلومات مورد الخدمات المدارة، مما يضمن في النهاية السرية والسلامة والتوافر لموارد النظام الهامة.

تتمثل الأهداف الرئيسية للتوصية بالضوابط الأساسية لأمن المعلومات وتنفيذها فيما يلي:

أ. حماية سرية وسلامة وتوافر بيانات مورد الخدمات المدارة عبر عمليات الأشخاص والضوابط المتعلقة بالتكنولوجيا.
ب. النص على تطوير وتنفيذ ومراجعة وصيانة الحد الأدنى من ضوابط الأمن المطلوبة لحماية بيانات وأنظمة مورد الخدمات المدارة
ج. حماية مورد الخدمات المدارة التابع لـ stc موظفيه وعملائه من الاستخدام غير المشروع لبيانات وأنظمة الشركة.
د. ضمان فعالية الضوابط الأمنية على البيانات والأنظمة التي تدعم عمليات مورد الخدمات المدارة التابع لـ stc.
ه. تعزيز الوعي بأمن المعلومات بشأن مخاطر أمن المعلومات الحالية والناشئة.
و. أن تظل ملتزمة بالمتطلبات التشريعية والتنظيمية والمتطلبات المتعلقة بحقوق الملكية الفكرية المعمول بها.

ونظرًا لأن مخاطر كل مورد الخدمات المدارة وأولوياته وأنظمته فريدة من نوعها، فقد تختلف الأدوات والأساليب المستخدمة لتحقيق النتائج الموصوفة في خط الأساس.

تعريفات

تنطبق ضوابط الأمن السيبراني على جميع فرق stc التي تدير مقاولي stc وموردي الخدمات المدارة ومؤسسات الطرف الثالث.

تقع على عاتق كل موظف معني مسؤولية فهم قابلية تطبيق المبادئ التوجيهية وتوضيح الشكوك، إن وجدت، التي قد تكون لديهم.

الخطوات الإجرائية

هيكل الضوابط

رقم الضوابط - لكل عنصر ضوابط رقم فريد.

الهدف - يحدد هدف الأمن السيبراني الذي يتعين تحقيقه بغض النظر عن طريقة التنفيذ.

إرشادات التنفيذ - الوسائل المقترحة التي يمكن من خلالها تحقيق الهدف.

تم تضمين الأمثلة حسب الاقتضاء في جميع أقسام المستند الأساسي لتسهيل فهم ضوابط الأمن السيبراني لوثيقة موردي ومقاولي الخدمات المدارة التابعين لـ stc

يصف هذا المستند الأساسي مجموعة من ضوابط الأمن الإلزامية لموردي الخدمات المدارة التابعين لـ stc.

تضع ضوابط الأمن الإلزامية خطًا أساسيًا للأمن للمجتمع بأكمله ويجب أن يتم تنفيذها بواسطة جميع موردي الخدمات المدارة على البنية التحتية المحلية والبعيدة و/أو السحابية. اختارت stc إعطاء الأولوية لهذه الضوابط الإلزامية لتحديد هدف واقعي لتحقيق مكاسب أمنية ملموسة على المدى القريب وتقليل المخاطر.

الضوابط الإلزامية الأساسية للأمن السيبراني
لشركة الاتصالات الكويتية (stc)

ضوابط إدارة الأصول

نوع الضوابط: إلزامية	مرجع: ISMS-POL-04 سياسة إدارة الأصول

الهدف:
ضمان نشر ضوابط أمن المعلومات بدرجة كافية على المعلومات وأنظمة المعلومات، والتي تتناول المعلومات السرية.

إرشادات التنفيذ:
يجب أن يكون لدى موردي الخدمات المدارة في المستوى الأساسي الضوابط التالية فيما يتعلق بأمن إدارة الأصول.

1.1

أ. يجب على مالكي أصول المعلومات وأمناء المعلومات تحديد الأصول الخاضعة لسيطرتهم بما في ذلك المعلومات (الإلكترونية) والمادية والورقيّة والأفراد وأصول التطبيقات / البرامج وخدمات معالجة المعلومات. يجب الاحتفاظ بجرد رسمي لجميع الأصول التي تحت وصايتهم.

ب. يجب الإبلاغ عن فقدان الأصول أو سرقتها أو اختلاسها على الفور إلى إدارة stc. يتضمن الجدول التالي أمثلة على أنواع الأصول:

نوع الأصول	أمثلة (لا تقتصر على)
المعلومات (الإلكترونية)	قاعدة البيانات وملفات البيانات ووثائق التشغيل والدعم وما إلى ذلك.
الأصول المادية	الأصول المادية مثل الخوادم، وأجهزة الكمبيوتر المكتبية، وجدران الحماية، والطابعات، والآلات، والفاكسات، والهواتف، وأجهزة مانع انقطاع التيار الكهربائي، والتيار المتردد، وما إلى ذلك.
الأصول الورقية	أدلة وكتيبات المستخدم والعقود والاتفاقيات وإجراءات التشغيل والدعم، تشمل الموظفين اللازمين لدعم وتشغيل الأصول الأخرى.
الأفراد	الأفراد ومؤهلاتهم ومهاراتهم وخبراتهم
التطبيقات	برنامج التطبيقات، برنامج النظام
أصل البرمجيات	أدوات التطوير والمرافق
خدمات	تتضمن خدمات الكمبيوتر والاتصالات والمرافق العامة

1.2

أ. يجب على مالكي المعلومات وأمناء المعلومات توثيق وصيانة والتحقق من قوائم جرد الأصول بشكل دوري.
يجب تسجيل المعلومات التالية لتسهيل تخطيط النظام واسترداد الأصول في حالة الانقطاع أو الفساد أو الضياع أو الإتلاف:

1. نوع الأصل
2. المالك
3. الأمين
4. معلومات الترخيص
5. الوصف
6. تصنيف الأصول
7. موقع الأصول

1.3

يجب إدراج جميع أصول المعلومات والاحتفاظ بها في قائمة جرد أصول المعلومات التي تتم مراجعتها بشكل دوري.

الاستخدام المقبول لضوابط الأصول

نوع الضوابط: إلزامية	مرجع: SMS-POL-04 سياسة إدارة الأصول

الهدف:
التأكد من إنشاء استخدام مقبول وغير مقبول للأجهزة الإلكترونية وموارد الشبكة لدي موردي الخدمات المدارة بالتزامن مع الثقافة الراسخة للسلوك الأخلاقي والقانوني والانفتاح والثقة والنزاهة.

إرشادات التنفيذ:
يجب أن يكون لدى موردي الخدمات المدارة في المستوى الأساسي الضوابط التالية فيما يتعلق بالاستخدام المقبول

للأصول.

2.1

يجب وضع قواعد للاستخدام المقبول للمعلومات والأصول لما يلي:

- أصول المعلومات
- مرافق معالجة المعلومات
- الموظفين الذين يستخدمون أجهزتهم الخاصة التي يتم التحكم فيها بموجب إدارة الاستخدام المقبول لسياسة استخدام الأجهزة الخاصة في العمل.

2.2

أ. يجب على المستخدمين استخدام الأصول المتوفرة وموارد المعلومات الأخرى بشكل صارم لأغراض أعمال مشروعة، وحماية سرية أعمال stc والمعلومات التي يتم الحصول عليها أثناء أداء وظيفتهم.

ب. يحق لإدارة stc الوصول إلى جميع المعلومات المخزنة على أي جهاز تابع لشركة stc، ويجب أن تستند تصريحات تعطيل الخدمات أو الأجهزة أو البرامج الأمنية على أي من أجهزة stc إلى تفويض صريح.

ج. تحتفظ إدارة stc بالحق في إجراء مراجعة الامتثال على أساس دوري لضمان الامتثال لهذه السياسة. يجب على المستخدم الإبلاغ عن أي حوادث و/أو نقاط ضعف ملحوظة أو مشتبه بها في مجال الأمن السيبراني إلى قسم الأمن السيبراني في الشركة.

د. يجب ألا يتناقش المستخدمون مع الزملاء حول الضعف المشتبه به بمجرد إبلاغه إلى سلطة أعلى للتحقيق.

ه. يجب أن يكون استخدام موارد stc ضمن الحدود القانونية.

و. استخدام محطات العمل (أجهزة الكمبيوتر المحمولة / أجهزة الكمبيوتر المكتبية)، والإنترنت، والبريد الإلكتروني / وسيط اتصال آخر مملوك لـ stc أو مؤجر أو مُشغل من قبلها، والأصول المحمولة، وأنظمة الاتصالات الهاتفية والمعلومات، يجب أن يكون حسب الاستخدام المقبول المحدد.

2.3

أ. يتم تزويد المستخدمين بموارد تكنولوجية لتسهيل اتصالات وأنشطة الأعمال الإلكترونية الفعالة والآمنة والأخلاقية.

ب. لا يجوز استخدام موارد التكنولوجيا إلا بعد موافقة الإدارة، للأغراض المعتمدة ومن قبل المستخدمين المصرح لهم لغرض وحيد هو الوفاء بأي مسؤوليات وظيفية معينة.

ج. يقوم فريق تكنولوجيا المعلومات لدي stc بإزالة أي برامج غير مصرح بها في أنظمة المستخدم النهائي.

2.4

أ. يجب على المستخدمين التنازل إلى stc عن جميع حقوق الملكية الفكرية التي تنشأ أثناء أداء التزاماتهم بموجب الاتفاقية التعاقدية (بما في ذلك جميع حقوق النشر والعلامات التجارية وبراءات الاختراع الحالية والمستقبلية بالإضافة إلى تجديداتها وتمديداتها وجميع حقوق الملكية الفكرية في جميع مواد الملكية الفكرية).

ب. لا يجوز للمستخدمين والجهات الخارجية التي تتعامل مع الملكية الفكرية استخدام حقوق الملكية الفكرية ومواد الملكية الفكرية إلا لأداء التزامات العمل بموجب الاتفاقية ولا يجوز لهم الإفصاح عن أي مواد ملكية فكرية لأي طرف آخر دون الحصول على موافقة خطية مسبقة من إدارة stc.

ج. يجب على المستخدم أن ينقل على الفور إلى stc جميع مواد الملكية الفكرية والمعدات المملوكة للشركة التي في حوزته أو تحت سيطرته عند انتهاء صلاحية الاتفاقية التعاقدية أو إنهاؤها لأي سبب كان، أو في أي وقت تطلب الشركة النقل.

لا يجوز للمستخدم الاحتفاظ بأي نسخ أو أي سجل آخر لأي من مواد ملكية فكرية إلا بموافقة كتابية مسبقة من إدارة stc.

2.5

أ. لن يتم استخدام حسابات نظام وتطبيقات stc (رموز تسجيل الدخول وكلمات المرور) إلا لغرض العمل المطلوب والمصرح به. يجب عدم مشاركة كلمات المرور لأي سبب من الأسباب.

ب. لن يتم استخدام حساب المستخدم تحت أي ظرف من الظروف للمشاركة في نشاط مالي شخصي أو استثمار أو مسابقة ترويجية وما إلى ذلك.

ج. يتحمل المستخدمون مسؤولية حماية أي معلومات مستخدمة و/أو مخزنة / يمكن الوصول إليها من خلال حسابات المستخدمين الفردية الخاصة بهم.

د. لا يجوز للمستخدمين إفشاء معلومات stc لأي شخص خارج stc دون الحصول على إذن مناسب. سيتم اعتبار جميع المعلومات المتاحة للمستخدم بصفة عمله "داخلية" ما لم ينص صراحة على خلاف ذلك.

ه. لا يجوز للمستخدمين محاولة الوصول إلى أي بيانات أو برامج موجودة في أي نظام ليس لديهم إذن أو موافقة خطية صريحة من مالك النظام.

و. مرافق الاتصالات الإلكترونية (مثل البريد الإلكتروني وتصفح الإنترنت) مخصصة لاستخدام العمل المصرح به فقط. لا يجوز إرسال الرسائل و/أو المواد الاحتيالية أو المضايقة أو المخلة من أنظمة stc أو تخزينها عليها. تحظر هذه

السياسة صراحة تصفح مواقع الويب / الرسائل المخلة على مرافق الشركة. أي انتهاك لهذه الضوابط سيؤدي إلى اتخاذ إجراءات تأديبية صارمة بما في ذلك إنهاء العقد.

ز. يحظر نقل أي مادة تنتهك أي قانون أو نظام أو لائحة في الكويت.

ح. لا يجوز للمستخدمين تنزيل أي إصدارات مجانية / برامج تجريبية / برامج غير مرخصة من الإنترنت دون الحصول على إذن وموافقة مناسبة من إدارة الأمن السيبراني في stc.

2.6

الأنشطة التالية محظورة تمامًا ما لم يرد ذكرها في هذه السياسة:

أ. إحداث خروقات أمنية أو اضطرابات في اتصالات الشبكة. تشمل الانتهاكات الأمنية، على سبيل المثال لا الحصر، استخدام أي أداة / برنامج لتجاوز ضوابط أو سياسات النظام الحالية، أو المصادقة الجانبية، أو تعطيل التسجيل، أو الوصول إلى البيانات التي لا يكون المستخدم مستلمًا مقصودًا لها، أو تسجيل الدخول إلى خادم أو الحساب الذي لم يصرح للمستخدم صراحة بالوصول إليه، ما لم تكن هذه الأعمال ضمن نطاق المهام العادية، على النحو المحدد من قبل إدارة المستخدم. لأغراض هذه السياسة، يشمل "التعطيل"، على سبيل المثال لا الحصر، اختراق الشبكة بالتنصت على حركة مرور البيانات، والهجوم الفيضاني، وهجوم انتحال الشخصية، ورفض الخدمة، ومعلومات التوجيه المزورة لأغراض ضارة.

ب. يُحظر صراحة فحص المنافذ أو الفحص الأمني ما لم يتم إرسال إشعار مسبق إلى فريق تكنولوجيا المعلومات في stc ويُصرح به من قبل فريق تكنولوجيا المعلومات في حالة إجراء المسح كجزء من تقييم المراجعة السنوي.

ج. لا يمكن للمستخدمين بدون تصريح تنفيذ أي شكل من أشكال مراقبة الشبكة والذي سيعترض البيانات غير المخصصة لمضيف المستخدم.

د. لا يجوز للمستخدمين عمل نسخ من ملفات تكوين النظام لاستخدامهم الخاص أو غير المصرح به أو لتوفيرها لأشخاص / مستخدمين آخرين للاستخدام غير المصرح به.

ه. التدخل في الخدمة أو رفضها لأي مستخدم على سبيل المثال هجوم قطع الخدمة.

2.7

أ. تُعرِّف stc الاستخدام المقبول للأعمال على أنه الأنشطة التي تدعم أعمال stc بشكل مباشر أو غير مباشر.

ب. تُعرِّف stc الاستخدام الشخصي المقبول في وقت الشركة على أنه اتصال أو ترفيه شخصي معقول ومحدود، مثل القراءة أو ممارسة الألعاب، إن أمكن.

ج. يُمنع المستخدمون من الوصول إلى مواقع ويب معينة خلال ساعات العمل / أثناء الاتصال بشبكة الشركة وفقًا لتقدير الشركة.

د. لا يجوز استخدام الأجهزة في أي وقت من أجل:
- تخزين أو نقل المواد غير المشروعة
- تخزين أو نقل معلومات الملكية التي تنتمي إلى شركة أخرى
- مضايقة الآخرين
- الانخراط في أنشطة أعمال خارجية

ه. يجوز للمستخدمين استخدام أجهزتهم النقالة للوصول إلى الموارد التالية المملوكة لشركة stc: البريد الإلكتروني، والتقويمات، وجهات الاتصال، والمستندات، إلخ.

2.8

أ. يُسمح بالهواتف الذكية بما في ذلك هواتف الآيفون، والاندرويد، وبلاك بيري، وويندوز.

ب. يُسمح بالأجهزة اللوحية بما في ذلك، الآيباد، والاندرويد.

ج. يتم دعم مشكلات الاتصال من قبل قسم تكنولوجيا المعلومات في stc.

2.9

أ. من أجل منع الوصول غير المصرح به، يجب أن تكون الأجهزة محمية بكلمة مرور باستخدام ميزات الجهاز وكلمة مرور قوية للوصول إلى شبكة stc.

ب. سياسة كلمة المرور القوية لشركة stc هي: يجب أن تتكون كلمات المرور من ثمانية أحرف على الأقل ومجموعة من الأحرف الأبجدية (الصغيرة والكبيرة)، والأرقام، والأحرف الخاصة. ويتم تغيير كلمات المرور كل 45 يومًا ولا يمكن أن تكون كلمة المرور الجديدة واحدة من 5 كلمات مرور سابقة.

ج. يجب أن يقفل الجهاز نفسه بكلمة مرور أو رمز تحقق شخصي (PIN) أثناء وقت الخمول بناءً على إعدادات القفل الآمن للجهاز المعني.

د. بعد خمس محاولات فاشلة لتسجيل الدخول، سيتم قفل الجهاز. يجب على المستخدمين الاتصال بفريق تكنولوجيا المعلومات لدى الشركة لاستعادة الوصول.

ه. يُمنع منعًا باتًا الأجهزة المروتة (الاندرويد أو التي تم كسر حمايتها (آي أو إس) من الوصول إلى الشبكة.
و. يُمنع المستخدمون تلقائيًا من تنزيل وتثبيت واستخدام أي تطبيق لا يظهر في قائمة stc للتطبيقات المعتمدة.
ز. لا يُسمح للهواتف الذكية والأجهزة اللوحية غير المدرجة في قائمة الأجهزة المدعومة للشركة بالاتصال بالشبكة.
ح. يقتصر وصول المستخدمين إلى بيانات stc على ملفات تعريف المستخدمين المحددة من قبل قسم تكنولوجيا المعلومات في stc ويتم فرضه تلقائيًا.

2.10
أ. سيتخذ فريق تكنولوجيا المعلومات لدي stc كل الاحتياطات اللازمة لمنع ضياع بيانات المستخدم الشخصية في حالة وجوب مسح الجهاز عن بُعد.
ب. تحتفظ stc بالحق في فصل الأجهزة أو تعطيل الخدمات دون إخطار.
ج. يجب إبلاغ الشركة عن الأجهزة المفقودة أو المسروقة في غضون 24 ساعة.
د. يُتوقع دائمًا من المستخدمين استخدام أجهزتهم بطريقة أخلاقية والالتزام بسياسة الاستخدام المقبول لشركة stc كما هو موضح أعلاه.
ه. يتحمل المستخدم المسؤولية الكاملة عن المخاطر بما في ذلك، على سبيل المثال لا الحصر، الخسارة الجزئية أو الكاملة للشركة والبيانات الشخصية بسبب تعطل نظام التشغيل، والأخطاء، والخلل، والفيروسات، والبرامج الضارة، و/أو غيرها من أعطال البرامج أو الأجهزة، أو أخطاء البرمجة التي تجعل الجهاز غير قابل للاستخدام. تحتفظ stc بالحق في اتخاذ الإجراءات التأديبية المناسبة بما يصل إلى ويشمل الإنهاء التعاقدي لعدم الامتثال لهذه السياسة.

2.11
يجب على جميع المستخدمين إعادة أي أصول تخص الشركة في حوزتهم عند إنهاء الاتفاقية التعاقدية.

ضوابط تصنيف المعلومات

نوع الضوابط: إلزامية	مرجع: ISMS-POL-04 سياسة إدارة الأصول

الهدف:
ضمان أن بيانات الشركة مصنفة بشكل صحيح لتلقى مستوى مناسب من الحماية.

إرشادات التنفيذ:
يجب أن يكون لدى موردي الخدمات المدارة التابعين لـ stc في المستوى الأساسي الضوابط التالية المحددة فيما يتعلق بضوابط تصنيف المعلومات.

3.1
يجب تصنيف أصول المعلومات لدي stc بشكل مناسب على أنها مقيدة وسرية وعامة، بناءً على المقاييس التالية:
- أهمية المعلومات.
- المتطلبات القانونية لحماية المعلومات.
- قيمة المعلومات.
- حساسية المعلومات.
- متطلبات السرية والسلامة والتوافر للمعلومات المعنية.
- نوع الأصل.
- أثر الخرق الأمني.

3.2
يجب تصنيف جميع أصول المعلومات (المعدات، الأجهزة الطرفية، الوسائط البرمجية، المستندات الورقية، المعلومات المخزنة في أنظمة الكمبيوتر) ماديًا أو إلكترونيًا وفقًا لتصنيفها.

3.3
أ. يجب التعامل مع أصول المعلومات بطريقة تحمي أصول المعلومات من الكشف غير المصرح به أو العرضي، أو التعديل، و/أو الضياع.
ب. يجب أن يكون تناول ومعالجة وتخزين وإبلاغ المعلومات متسق مع تصنيف المعلومات من أجل حمايتها من الوصول غير المصرح به وسوء الاستخدام.

3.4

أ. لا يجوز استخدام الوسائط المقدمة من stc إلا لتخزين البيانات أو المعلومات أو معالجتها أو نقلها أو التخلص منها لأغراض العمل.
ب. لا يجوز استخدام أي وسائط لم توفرها stc.
ج. يجب تخزين معلومات stc المصنفة على أنها "سرية" في وسائط مشفرة.
د. عندما تكون الوسائط متصلة بنظام، على سبيل المثال أجهزة الكمبيوتر المكتبية / أجهزة الكمبيوتر المحمولة، يجب استخدام البرامج المضادة للفيروسات لفحص وإزالة فيروسات الكمبيوتر، إذا وجدت.
ه. يجب حفظ فقط بيانات stc المصرح بها واللازم نقلها على وسائط محمية.
و. يجب توخي العناية الخاصة لحماية الوسائط والبيانات المخزنة ماديًا من الضياع أو السرقة أو التلف.
ز. يجب تقييد الوصول إلى الوسائط لضمان الوصول المصرح به.

3.5
أ. يجب محو البيانات الموجودة على الوسائط قبل إتلافها أو إعادة استخدامها.
ب. قد تحتوي أجهزة التخزين التي تعرضت للتلف قبل التخلص منها على بيانات حساسة للغاية وتتطلب تدميرًا ماديًا إذا تعذر محوها بشكل آمن.
ج. يجب كسر أو خربشة الوسائط الضوئية عند عدم الحاجة إليها.

3.6
أ. يمكن إرسال الأصول المصنفة على أنها "عامة" في بريد مفتوح.
ب. لا يمكن إرسال الأصول المصنفة على أنها "سرية" أو "مقيدة للشركة" إلا باستخدام موظفين موثوق بهم أو من خلال خدمة البريد السريع المُبرم معها عقد.

ضوابط التحكم في الوصول

نوع الضوابط: إلزامية	مرجع:ISMS-POL-05 سياسة التحكم في الوصول

الهدف:
السماح بالوصول المصرح به فقط للمستخدمين (أو العمليات التي تعمل نيابة عن المستخدمين) والتي تعتبر ضرورية لإنجاز المهام المعينة وفقًا للمهام التنظيمية ووظائف العمل.

إرشادات التنفيذ:
يجب أن يكون لدى موردي الخدمات المدارة التابعين لـ stc في المستوى الأساسي الضوابط التالية فيما يتعلق بالتحكم في الوصول.

4.1 استخدم "." بعد الأفراد

يكون طلب وصول أفراد الجهات الخارجية إلى أصول معلومات stc والإلغاء من مسؤولية فريق المشروع المعني. يجب توفير الوصول للمقاولين أو الاستشاريين أو الموردين إلى أصول معلومات stc فقط على أساس عقد رسمي وتوقيع اتفاقية حماية المعلومات. جب أن تنص الاتفاقية على ما يلي:

- الشروط والأحكام التي بموجبها يتم توفير الوصول.
- مسؤوليات المقاولين والاستشاريين أو موظفي الموردين.
- موافقة المقاولين أو الاستشاريين أو الموردين على الالتزام بسياسة stc للأمن السيبراني. يجب أن تتضمن هذه التعليمات متطلبات أمنية، مثل الحاجة إلى الحفاظ على سرية المعلومات، ومتطلبات توزيع المعلومات خلال فترة الوصول.

4.2
يقتصر الوصول إلى أنظمة معلومات stc على المستخدمين المصرح لهم لدعم وتمكين متطلبات العمل. يجب التحكم في الوصول إلى نظم المعلومات على أساس ما يلي:
أ. تصنيف أمن المعلومات للأصل.
ب. الالتزام القانوني و/أو التعاقدي المعمول به لتقييد أو حماية الوصول إلى أصول المعلومات.
ج. معايير الوصول:
- الحاجة إلى المعرفة - يتم منح الوصول فقط إلى المعلومات المطلوبة لأداء عمل ما، وليس أكثر.
- الحاجة إلى الاستخدام - لن يتمكن المستخدمون إلا من الوصول إلى التسهيلات المادية والمنطقية المطلوبة لدورهم.
- الدفاع في العمق - يجب ألا يعتمد الأمن على أي عنصر تحكم واحد، بل يجب أن يكون مجموعة من عناصر التحكم التكميلية.

- أقل امتيازات - يجب أن يكون النهج الافتراضي المتبع هو افتراض أن الوصول غير مطلوب، بدلاً من افتراض أنه كذلك.

د. يجب التحكم في الوصول إلى أصول المعلومات وتفعيل حسابات المستخدمين للمقاولين أو المستشارين، أو العمال المؤقتين، أو موظفي الموردين المعتمدين / المخولين، ولا يكون ذلك ساريًا إلا عندما يقوم الفرد بأداء الخدمة بنشاط مع stc.

ه. لن يُسمح بالوصول عن بُعد إلى شبكة وموارد stc إلا بشرط مصادقة المستخدمين المصرح لهم وتقييد الامتيازات.

و. يجب أن يقتصر الوصول إلى أوامر نظام التشغيل على الأشخاص المصرح لهم بأداء وظائف إدارة الأنظمة.

ز. يتم منح حق الوصول مع ضمان الفصل بين الواجبات لتجنب "تعارض المصالح".

ح. يجب ضمان الفصل بين الواجبات في بيئات التطوير والاختبار والإنتاج.

4.3

أ. يُمنح الوصول إلى خدمات الشبكة حسب الحاجة لدعم متطلبات العمل.

ب. يجب أن يقتصر الوصول إلى الشبكة على المستخدمين والأنظمة المصرح لهم باستخدام مبدأ أقل امتياز.

4.4

أ. يجب على المستخدمين عن بُعد الاتصال بشبكة stc فقط من خلال خدمات الوصول عن بُعد المعتمدة والمخصصة والبوابات الآمنة، كما يتطلب ذلك تحديد المستخدم والترخيص.

ب. توفر stc خدمة الشبكة الافتراضية الخاصة (VPN) للمستخدمين بناءً على متطلبات العمل ومع الموافقات المناسبة.

4.5

تتم إدارة الوصول إلى موارد المعلومات باستخدام أنواع متعددة من الحسابات، بما في ذلك:

أ. الحسابات المنتظمة - تزويد الموظفين بالحد الأدنى من موارد المعلومات ووظائف النظام اللازمة لأداء واجباتهم ولا تحمل امتيازات خاصة أعلى من تلك المطلوبة لأداء وظيفة العمل.

ب. حسابات الامتياز / المدير - توفير مستويات أعلى من الوصول للأفراد الذين يؤدون وظائف إدارة النظام وصيانة حساب المستخدم أو الموظفين الذين يديرون موارد المعلومات المقيدة.

ج. يجب استخدام حسابات الامتياز وفقًا للإرشادات التالية:

- يجب أن يقتصر التخصيص على الأفراد الذين تتطلب واجباتهم امتيازات إضافية.
- يجب تخصيص حسابات الامتياز لفرد فريد.
- لا يجوز للمدير استخدام "المدير" أو "المسؤول" أو "الجذر" أو "المستخدم المتميز" أو أسماء مشابهة لحسابات الامتياز مثل معرف المستخدم لأداء الأنشطة الإدارية في الخوادم / قواعد البيانات / أجهزة الشبكة وما إلى ذلك. يجب عدم تسمية رموز التعريف التي تحمل امتياز على هذا نحو يمكن تحديد حقوق الوصول إلى الحساب بشكل صريح وقد لا يُسمح بها إلا في حالة وجود قيود / حدود على الاستخدام العادي لمعرف المستخدم أو بسبب مشكلات تشغيلية.

4.6

يجب أن يُطلب من المستخدمين التوقيع على بيان للحفاظ على سرية معلومات المصادقة الشخصية السرية وللحفاظ على معلومات المصادقة السرية للمجموعة (أي المشتركة) فقط داخل أعضاء المجموعة؛ قد يتم تضمين هذا البيان الموقع في شروط وأحكام الاتفاقية التعاقدية.

4.7

يجب تعطيل إزالة حسابات المستخدمين وامتيازات الوصول للموظفين الذين يتركون العمل من خلال العملية المناسبة قبل نهاية مدة العقد، اعتمادًا على مدى أهمية نطاق العمل.

4.8

يجب تخزين الوصول إلى الكود المصدري للبرنامج والعناصر المرتبطة به في شكل مكتبات مصدر البرنامج منفصلة عن بيئة التشغيل. يجب أن يضمن ذلك منع إدخال وظائف غير مصرح بها والتغييرات غير المقصودة بالإضافة إلى الحفاظ على قيمة الملكية الفكرية.

ضوابط استخدام التشفير

نوع الضوابط: إلزامية	مرجع: ISMS-POL-06 سياسة استخدام التشفير

الهدف:
ضمان الاستخدام المناسب والفعال للتشفير لحماية سرية و/أو صحة و/أو سلامة معلومات stc وعملائها والأطراف الخارجية.

إرشادات التنفيذ:
يجب أن يكون لدى موردي الخدمات المدارة التابعين لـ stc في المستوى الأساسي الضوابط التالية فيما يتعلق باستخدام التشفير.

5.1

أ. تمتلك stc مصادقة ثنائية سارية لتسجيل الدخول إلى أي خادم / شبكة مهمة وبنية تحتية لتكنولوجيا المعلومات.
ب. يجب وضع معايير وإجراءات لاستخدام ضوابط التشفير في جميع أنظمة تكنولوجيا المعلومات والشبكات الحساسة لحماية المعلومات الحساسة لشركة stc والعملاء والجهات الخارجية.
ج. يتم تنفيذ الأصول المحددة مع الضوابط اللازمة لضمان قابلية تطبيق التشفير. بشكل عام، يجب اعتماد تقنيات التشفير لعملية الأعمال أو الموقف ذي الصلة، كما هو موضح في الجدول أدناه:

العملية / الموقف	التقنية
أمن البريد الإلكتروني	حلول البريد الإلكتروني المعتمدة للشركة
حماية كلمات المرور على الأنظمة	تطبيقات إدارة كلمات المرور
حماية البيانات على التخزين	تشفير نقطة النهاية
الوصول عن بعد	الشبكة الافتراضية الخاصة (VPN)
الموجهات	الاتصالات المشفرة
المبدلات	الاتصالات المشفرة
جدران الحماية	الاتصالات المشفرة

5.2

أ. يجب أخذ ضوابط التشفير في الاعتبار، والتي تشمل على سبيل المثال، لا الحصر، ما يلي:
- التوصيلات الخارجية.
- المعلومات السرية التي تتم مشاركتها عبر شبكات الاتصال العامة و/أو المشتركة.

ب. يجب أن يتوافق استخدام ضوابط التشفير مع جميع القوانين والممارسات الصناعية الرائدة ذات الصلة ومراجعتها بشكل دوري امتثالا لأي لوائح جديدة.

ضوابط الأمن المادي والبيئي

نوع الضوابط: إلزامية	مرجع: SMS-POL-07 سياسة الأمن المادي والبيئي

الهدف:
نشر ضوابط أمن مادي وبيئي مناسبة لمنع الوصول غير المصرح به، أو المساومة، أو السرقة، أو الضرر، أو التدخل في مقار العمل، ومرافق معالجة المعلومات، ومرافق الاتصالات.

إرشادات التنفيذ:
يجب أن يكون لدى موردي الخدمات المدارة التابعين لـ stc في المستوى الأساسي الضوابط التالية فيما يتعلق بالأمن المادي والبيئي.

6.1

أ. يجب على الزوار (العملاء والموردين والمستثمرين وزوار الموقع والاستشاريين والمقاولين) الحصول على إذن قبل الدخول إلى مرافق معالجة المعلومات وغرف الخادم. يجب إصدار بطاقات هوية مؤقتة لزوار stc أو ضيوفها.
ب. يتم تقييد الوصول المادي إلى مناطق stc الآمنة مثل مركز البيانات أو المناطق التي يتم فيها تخزين المعلومات الحساسة ومرافق التحكم التشغيلي، وذلك لمنع أي وصول مادي غير مصرح به.
ج. لا ينبغي السماح بالتصوير الفوتوغرافي أو الفيديو أو الصوتي أو غيرها من معدات التسجيل دون إذن مسبق لتأمين المناطق (المناطق المحظورة).

6.2

أ. يجب إلغاء حقوق الوصول المادي إلى المناطق الآمنة على الفور أو وفقًا لما اعتمده رئيس الإدارة عند إنهاء/استقالة الموظفين أو الانتهاء من الأعمال الاستشارية أو اتفاقية المورد.

ب. يجب تجنب العمل غير الخاضع للإشراف في المناطق الآمنة من قبل موظفين وموردين تابعين لجهات خارجية لأسباب تتعلق بالسلامة ولمنع فرص الأنشطة الضارة.
ج. يجب منح موظفي الدعم / الخدمات التابعين للأطراف الخارجية وصولاً مقيدًا إلى المناطق الآمنة فقط عند الحاجة. ويتم دائمًا مرافقة هؤلاء الأفراد ومراقبتهم لأنشطتهم في المناطق الآمنة. ويتم تحديد الموظفين المناسبين لمرافقة أفراد خدمات الترتيب والنظافة أثناء التنظيف الروتيني للمناطق الآمنة.

6.3
أ. يجب صيانة المعدات وفقًا لمواصفات وفترات الخدمة الموصي بها من المورد. ويجب إبرام عقود الصيانة السنوية / عقود الصيانة الوقائية مع الموردين، عند الاقتضاء.
ب. ينبغي فقط لأفراد الصيانة المعتمدين إجراء الإصلاحات وصيانة المعدات. يجب الإشراف على أنشطة الصيانة في الموقع للتأكد من أن موظفي الدعم ليس لديهم وصول غير مصرح به إلى بيانات stc.

ضوابط أمن العمليات

نوع الضوابط: إلزامية	مرجع: ISMS-POL-08 سياسة أمن العمليات

الهدف:
ضمان العمليات الصحيحة والآمنة لأنظمة المعلومات، وأن أنظمة المعلومات تتم حمايتها من البرامج الضارة وفقدان البيانات، ويتم تسجيل الأحداث ومراقبة الامتثال، والتحكم في برنامج نظام التشغيل، ومنع استغلال الثغرات التقنية.

إرشادات التنفيذ:
يجب أن يكون لدى موردي الخدمات المدارة التابعين لـ stc في المستوى الأساسي الضوابط التالية فيما يتعلق بأمن العمليات.

7.1
يجب فصل بيئات التطوير والاختبار والتشغيل لتقليل مخاطر الوصول غير المصرح به أو التغييرات في بيئة التشغيل.

7.2
أ. يجب أن يتم تثبيت حلول مكافحة الفيروسات في جميع أنظمة المعلومات في stc بما في ذلك الخوادم وأجهزة الكمبيوتر المكتبية والمحمولة. تنفذ stc حلولاً وضوابط لمكافحة البرامج الضارة على مستويات مختلفة على النحو التالي:
- مستوى سطح المكتب.
- مستوى الخادم.
- نقاط الوصول الحرجة / البوابات المحددة حيث تدخل المعلومات من المجال العام إلى شبكة stc، على سبيل المثال البريد الإلكتروني وحركة مرور الويب.

ب. يجب إبلاغ مكتب خدمات تكنولوجيا المعلومات في stc عن جميع الفيروسات وفيروسات حصان طروادة وغيرها من حوادث البرامج الضارة. يجب إزالة أجهزة الكمبيوتر المصابة بالبرامج الضارة من الشبكة أو وضعها في قسم العزل بمجرد التعرف عليها، حتى يتم التحقق من خلوها من الفيروسات.

7.3
سيتم تسجيل نظام سجلات الأحداث والاستثناءات والأحداث ذات الصلة بالأمن على أنظمة تكنولوجيا المعلومات والشبكات وتخزينها وحمايتها بناءً على متطلبات العمل / المتطلبات التنظيمية. يجب متابعة مراجعة سجلات أحداث الأمن، وصيانة معلومات التسجيل، وسجلات مسؤولي النظام / المشغلين. ويتم مزامنة جميع الأنظمة المتصلة بشبكة stc بشكل آني للتأكد من أن سجلات الأحداث تحتوي على معلومات دقيقة. يجب أن تشمل الضوابط على ما يلي:
- ضمانات الأمن المادي.
- التصريح للمديرين والمشغلين بمسح السجلات أو إلغاء تنشيطها.
- مصادقة متعددة العوامل للوصول إلى الأصول الهامة عند الاقتضاء.
- النسخ الاحتياطي لسجلات التدقيق إلى مرافق خارج الموقع.
- أرشفة تلقائية للسجلات لتبقى ضمن سعة التخزين.

7.4
يتم إجراء تقييمات دورية للضعف التقني من قبل فريق الأمن السيبراني أو مقيمين خارجيين مؤهلين بموجب عقد محدد بشكل جيد واتفاقية حماية المعلومات؛ ويتم تقييم نقاط الضعف التقنية المحددة للمخاطر المحتملة وتصحيحها وفقًا لخطة العلاج.

7.5

أ. لا يُسمح للمستخدمين بتثبيت البرامج على أجهزة stc ما لم يتم التصريح بذلك على وجه التحديد.
ب. الموظفون المعتمدون مسؤولون عن تثبيت البرامج والتحديثات والتصحيحات.

ضوابط أمن الاتصالات

نوع الضوابط: إلزامية	مرجع: ISMS-POL-09 سياسة أمان الاتصالات

الهدف:
التأكد من حماية المعلومات في شبكات stc والحفاظ على أمن المعلومات المنقولة داخل المؤسسة ومع أي جهة خارجية.

إرشادات التنفيذ:
يجب أن يكون لدى موردي الخدمات المدارة التابعين لـ stc في المستوى الأساسي الضوابط التالية فيما يتعلق بأمن الاتصالات.

8.1

- يجب تحديد آليات الأمن ومستويات الخدمة ومتطلبات الإدارة لجميع خدمات الشبكة وإدراجها في اتفاقيات خدمات الشبكة. عند التعامل مع مزودي الخدمات الخارجيين أو الخدمات، يجب تنفيذ بروتوكولات الاسناد الخارجي.
- يجب فصل خدمات المعلومات داخل stc بشكل مناسب على الشبكة بما في ذلك الفصل بين الاختبار والإنتاج، وفصل الشبكات الهامة عن الإنترنت والشبكات الداخلية الأخرى الأقل حساسية باستخدام تقنيات الفصل المناسبة.
- يجب أن تضمن stc أن مستخدمي خدمات الشبكة لديهم فصل في الواجبات مع الحقوق المناسبة والتحكم في الوصول.

8.2

تضمن stc السياسات والإجراءات للحفاظ على أمن المعلومات المنقولة داخل الشركة ومع أي كيان خارجي، ويجب أن تشمل، على سبيل المثال لا الحصر، المجالات التالية:

- اتفاقيات أمن الشبكة
- اتفاقات السرية
- اتفاقيات حماية المعلومات
- استعمال الانترنت
- أمن البريد الإلكتروني
- مرشحات الويب

الاستخدام المقبول والاستخدام غير المقبول داخل شبكة stc أو داخل خدمات الشركة.

ضوابط دورة حياة تطوير النظام الآمن

نوع الضوابط: إلزامية	مرجع: ISMS-POL-10 سياسة دورة حياة تطوير النظام الآمن

الهدف:
التأكد من أن أمن المعلومات هو جزء لا يتجزأ من أنظمة المعلومات عبر دورة الحياة بأكملها بما في ذلك الخدمات عبر الشبكات العامة، والتدابير الأمنية لحماية التطبيق وشفرة مصدر التطبيق، أثناء تصميم الأنظمة وتطويرها وصيانتها وحمايتها أثناء الاختبار.

إرشادات التنفيذ:
يجب أن يكون لدى موردي الخدمات المدارة التابعين لـ stc في المستوى الأساسي الضوابط التالية المتعلقة بدورة حياة تطوير النظام الآمن.

9.1

يجب أن يتم الإشراف على تطوير مقابل البرامج الجاهزة الواردة من مصادر خارجية ومراقبتها من قبل stc من خلال اتفاقية حماية المعلومات، وتقييم المخاطر، والاتفاقيات التعاقدية، واجتماعات مراجعة الإدارة، أيهما ينطبق.

9.2

أي تطبيق مطور يتطلب تعميم إنتاجه، يجب اختباره بدقه على نحو شامل للامتثال لسياسات stc للأمن السيبراني.

9.3
يتعين الحصول على موافقة فريق الأمن السيبراني في stc قبل طرح أي منتج وتعميم إنتاجه. عند انتهاء صلاحية أحد التطبيقات، يجب التأكد من إزالة جميع الشفرات ذات الصلة بالتطبيق منتهي الصلاحية من بيئة الإنتاج. يجب دائمًا تمكين ميزات عمليات التدقيق في أنظمة التطبيق وقواعد البيانات.

ضوابط أمن علاقات الموردين

نوع الضوابط: إلزامية	مرجع:ISMS-POL-11 سياسة أمن علاقات الموردين

الهدف:
التأكد من حماية أصول الشركة التي يمكن للموردين الوصول إليها والحفاظ على مستوى متفق عليه من أمن المعلومات وتقديم الخدمات بما يتسق مع اتفاقيات الموردين.

إرشادات التنفيذ:
يجب أن يكون لدى موردي الخدمات المدارة التابعين لـ stc في المستوى الأساسي الضوابط التالية فيما يتعلق بأمن علاقات الموردين.

10.1
- يجب الاتفاق مع المورد على متطلبات أمن المعلومات للتخفيف من المخاطر المرتبطة بوصول الموردين إلى أصول معلومات stc وتوثيق هذا الاتفاق. يجب تنفيذ الضوابط الأمنية المتوافقة مع المعايير قبل السماح للموردين بالوصول إلى أصول معلومات stc. تشمل الضوابط العمليات والإجراءات التي يجب أن تنفذها stc وتلك التي يجب أن ينفذها المورد.
- يجب أن تستند الترتيبات مع الموردين التي تتضمن الوصول إلى أو معالجة أو تخزين أو نقل أو إدارة معلومات stc أو أنظمة المعلومات أو مرافق معالجة المعلومات الخاصة بـ stc إلى اتفاقية رسمية تتضمن متطلبات الأمن اللازمة.

10.2
يقوم فريق الأمن السيبراني في stc بالتنسيق مع إدارة الموردين المعنية بمراقبة ومراجعة الشروط والأحكام المتعلقة بالأمن السيبراني في الاتفاقيات مع الموردين. يجب التعامل مع العناصر غير المتعلقة بالأمن وفقًا لسياسات الشراء الخاصة بـ stc. يجب أن تشمل العمليات على:
- مراجعة تقارير الخدمة الصادرة عن المورد.
- إلزام الموردين وموردي الخدمات المدارة بعقد ورش عمل خاصة بالأمن السيبراني والتوعية لفرقهم على أساس سنوي وتقديم ما يثبت اعتمادهم.
- إلزام الموردين بقبول تثبيت برامج / وكلاء الأمن المناسبة على أجهزة فريقهم.
- فرض تفويضات التوجيه والتوعية للموردين وفريقهم لقراءة وفهم جميع سياسات وعمليات وإجراءات الأمن السيبراني.
- ضمان احتفاظ المورد بقدرة خدمة كافية، عند الاقتضاء.

ضوابط إدارة حوادث الأمن السيبراني

نوع الضوابط: إلزامية	الرقم المرجعي: • ISMS-POL-12 سياسة إدارة حوادث الأمن السيبراني • ISMS-PR01-p03 إجراءات عدم المطابقة والإجراءات التصحيحية • ISMS-PR10-p01 إجراءات إدارة حوادث الأمن السيبراني

الهدف:
ضمان اتباع نهج متسق وفعال لإدارة حوادث أمن المعلومات، بما في ذلك التواصل بشأن الأحداث الأمنية ونقاط الضعف.

إرشادات التنفيذ:
يجب أن يكون لدى موردي الخدمات المدارة في المستوى الأساسي stcالضوابط التالية فيما يتعلق بإدارة حوادث الأمن السيبراني.

11.1
أ. ستتبنى stc إطار عمل لإدارة حوادث أمن المعلومات من خلال وضع إجراءات لإدارة حوادث أمن المعلومات والتي تشمل الجوانب التالية:
- الإخطار الفوري بحوادث الأمن السيبراني.

- تحديد والاستجابة لأنواع مختلفة من حوادث الأمن السيبراني المحتملة.
- تنفيذ الإجراءات التصحيحية المناسبة.
- تقديم تقرير رسمي عن الحوادث الخطيرة يصف الحادث، والإجراءات المتخذة والتدابير الوقائية الموصي بها.

ب. سيؤسس تنفيذ هذه السياسة الآلية التالية:

- توعية الموظفين والمقاولين ومستخدمي نظم المعلومات الآخرين.
- قنوات الإبلاغ المعتمدة للموظفين للإبلاغ عن حوادث الأمن السيبراني (الانتهاكات الفعلية أو المشتبه بها).
- يجب توفير الموارد الداخلية أو الخارجية الكافية لإجراء تحقيقات القضائية، إذا لزم الأمر.
- يجب تحديد الإجراءات التصحيحية / الوقائية المناسبة للرد على الحادث.
- التوصية بتدابير استباقية لتجنب حوادث مماثلة في المستقبل بناءً على الدروس المستفادة.

11.2

يمكن تحديد حالات عدم المطابقة من أي مصدر وسيشجع مدير عام الأمن السيبراني في stc الموظفين والمستخدمين والعملاء والموردين على اقتراح طرق يمكن من خلالها معالجتها.

11.3

يمكن لأي شخص في stc اكتشاف أي حدث / واقعة تتعلق بالأمن السيبراني. من المهم بدرجة بالغة إبقاء الأشخاص المناسبين على اطلاع. ولهذا الغرض، يجب إطلاع جميع الأطراف الخارجية والمستخدمين الخارجيين، حيثما كان ذلك مناسبًا، على عملية الإبلاغ بهذه الأحداث / الوقائع ويجب التعامل مع النقاط التالية:

أ. يجب على الموظف / الطرف الخارجي / المستخدم التابع لجهة خارجية، الذي يلاحظ حدث / واقعة أو عطل في الأمن السيبراني، إبلاغ فريق الأمن السيبراني لدي stc في أقرب وقت ممكن عبر مكتب الخدمة.

ب. يجب وضع معلومات اتصال شاملة لضمان التواصل الفعال بين الموظفين المسؤولين. يجب تضمين معلومات الاتصال المحدثة مثل الخط الساخن لساعة العمل والخط الساخن في غير ساعات العمل وعنوان البريد الإلكتروني والنقال عند الضرورة.

11.4

قد يكون ضعف الأمن السيبراني خطأً أو ضعفًا في نظام المعلومات أو الخدمة التي إذا تُركت دون مراقبة / غير مُدارة قد تؤدي إلى أحداث / وقائع متعلقة بالأمن السيبراني. لهذا الغرض، يجب اتخاذ الإجراءات التالية:

أ. يجب على الأطراف الخارجية والمستخدمين التابعين لجهات خارجية الإبلاغ عن أي ضعف ملحوظ أو مشتبه به في الأمن السيبراني في أنظمة أو خدمات المعلومات الخاصة بهم إلى فريق الأمن السيبراني في stc عبر مكتب خدمة stc.

ب. يجوز لفريق الأمن السيبراني، بالتنسيق مع مدير عام تكنولوجيا المعلومات في stc، اتخاذ الإجراء المناسب مع مزود الخدمة / المورد المعني في أسرع وقت ممكن لمنع وقوع أي حوادث أمنية بسبب هذا الضعف الأمني في النظام أو الخدمة.

ضوابط الامتثال

نوع الضوابط: إلزامية	مرجع: ISMS-POL-14 سياسة الامتثال

الهدف:

التأكد من أن جميع المستخدمين على دراية كاملة بمسؤولياتهم القانونية فيما يتعلق باستخدامهم لأنظمة المعلومات والبيانات القائمة على الكمبيوتر.

إرشادات التنفيذ:

يجب أن يكون لدى موردي الخدمات المدارة التابعين لـ stc في المستوى الأساسي الضوابط التالية فيما يتعلق بسياسات الامتثال الخاصة بشركة stc.

12.1

تلتزم stc باتباع ممارسات الامتثال لحقوق الملكية الفكريةعلى النحو التالي:

- شراء أجهزة / برامج شرعية فقط من موردين مرخصين ومعتمدين.
- إعلام المستخدمين وتثقيفهم بأنهم لن يقوموا بتثبيت أي برامج غير مرخصة.
- إجراء عمليات التحقق من تثبيت البرنامج المصرح به فقط.
- عدم نسخ كتب أو مقالات أو مستندات بصورة كلية أو جزئية بخلاف ما يسمح به قانون حقوق النشر.
- الاحتفاظ بقائمة الجرد والسجلات ذات الصلة لإثبات ملكية التراخيص.

ضوابط كلمة المرور

نوع الضوابط: إلزامية	مرجع: ISMS-POL-15 سياسة كلمة المرور

الهدف:
التأكد من استخدام كلمات مرور معقدة للوصول إلى المعلومات وأصول المعلومات في البيئة.

إرشادات التنفيذ:
يجب أن يكون لدى موردي الخدمات المدارة التابعين stc في المستوى الأساسي إعدادات التكوين التالية المتعلقة بضوابط كلمة المرور.

13.1
يجب تهيئة الأنظمة لضمان تغيير كلمات المرور الأولية والمؤقتة للحسابات المخصصة حديثًا عند تسجيل الدخول الأول، ويجب الاحتفاظ بسجل لآخر خمس كلمات مرور للحساب لمنع إعادة استخدام كلمة المرور.

13.2
يجب أن تنتهي صلاحية كلمات المرور لأول مرة إذا لم يدخل المستخدم إلى حسابه بعد فترة محددة مسبقًا.

13.3
إذا تم تخزين بيانات اعتماد المستخدم في تطبيق / قاعدة بيانات، يكون مالك البيانات مسؤولاً عن تنفيذ إجراءات الحماية مثل تشفير ملفات بيانات الاعتماد / كلمات المرور. يجب على الإدارة المعنية التنسيق مع مورد التطبيق لضمان هذا الجانب.

13.4
يجب عدم إرسال كلمات المرور بصيغة نصية واضحة عبر أي نوع من الشبكات.

13.5
بشكل افتراضي، يجب تهيئة جميع التطبيقات والأنظمة بحيث لا تعرض كلمات المرور على الشاشة أثناء إدخالها.

13.6
يقدم فريق أمن المعلومات في stc تدريبات توعية لجميع المستخدمين (بما في ذلك موظفي الموردين الخارجيين والموظفي على نظام العقود) لضمان اتباع إجراءات وسياسات كلمة المرور من قبل جميع المستخدمين.

13.7
يجب ألا تستند كلمات المرور إلى اسم الشركة أو الموقع الجغرافي.

13.8
يجب حماية كلمة المرور من قبل المستخدمين ويكون المستخدمون مسؤولين عن الأنشطة التي يتم إجراؤها من خلال "رمز المستخدم" الخاص بهم.

13.9
يجب عدم مشاركة كلمات المرور.

13.10
لا يجوز استخدام كلمة مرور الشركة مطلقًا على حساب عبر الإنترنت لا يحتوي على تسجيل دخول آمن أو حيث يبدأ عنوان متصفح الويب بـ 'http://' بدلاً من 'https://'

13.11
يجب على موردي الجهات الخارجية الالتزام بسياسة كلمة مرور المطبقة لدي stc. ويجب أن تتضمن متطلبات التعقيد الحد الأدنى من النقاط التالية:

أ. يجب تحديد الحد الأدنى لعمر كلمة المرور ليوم واحد.
ب. يجب أن يكون الحد الأدنى لطول كلمة المرور ثمانية أحرف.
ج. يجب الاحتفاظ بسجل لآخر 5 كلمات مرور (سجل كلمة المرور) من أجل منع إعادة استخدامها.
د. يجب أن تحتوي كلمة المرور على مزيج من الأحرف الأبجدية وغير الأبجدية (رقم أو علامات ترقيم أو أحرف خاصة) أو مزيج من نوعين على الأقل من الأحرف غير الأبجدية.

ه. يجب أن تكون كلمة المرور حساسة لحالة الأحرف ويجب أن تحتوي على مزيج من الأحرف الكبيرة والصغيرة (على سبيل المثال، a-z، A-Z)
و. يجب تعيين الحد الأقصى لعمر كلمة المرور لحسابات المستخدمين لمدة 45 يومًا وحسابات المسؤول لمدة 90 يومًا على التوالي.
ز. يجب أن يكون حد قفل الحساب هو 5 محاولات متتالية غير صالحة لتسجيل الدخول.
ح. يجب تعيين مدة قفل الحساب وإعادة تعيين مدة قفل الحساب لمدة 0 دقيقة و 30 دقيقة على التوالي.

13.12.
يجب إبلاغ فريق الأمن السيبراني لدي stc في حالة تحديد أو الاشتباه في اختراق كلمة مرور أحد الأشخاص.

13.13
يجب ألا تعتمد كلمة المرور على ما يلي كما هو مذكور أدناه:
أ. أشهر السنة أو أيام الأسبوع أو أي جانب آخر من التاريخ (مثل تاريخ الميلاد وتاريخ الانضمام وما إلى ذلك).
ب. أسماء العائلة أو الأحرف الأولى من الأسماء.
ج. أرقام تسجيل السيارة.
د. رقم الموظف / هوية الموظف أو المسميات الوظيفية.
ه. مصطلحات والأسماء الكمبيوتر والأوامر والمواقع والشركات والأجهزة والبرامج.
و. اسم المشروع أو القسم أو المراجع.
ز. أسماء الشركات أو المعرفات أو المراجع أو كلمات المرور المعروفة للجمهور (مثل 123456، stc، stc1234، stc123، stc1234، admin، password، viva@1234، Viva 1234 وما إلى ذلك)
ح. أرقام الهواتف أو مجموعات رقمية متشابهة.
ط. معرف المستخدم أو اسم المستخدم أو معرف المجموعة أو معرف نظام آخر.
ي. مجموعات الإقام أو مجموعات الأبجدية.

13.14
يجب على مطوري التطبيقات التأكد من احتواء برامجهم على احتياطات أمن كلمة المرور التالية:
أ. ينبغي أن تدعم مصادقة المستخدمين الفرديين، وليس المجموعات.
ب. يجب عدم تخزين كلمات المرور في نص واضح أو في شكل يسهل استرجاعه.
ج. يجب أن توفر نوعًا من إدارة الأدوار، بحيث يمكن لمستخدم واحد تولي وظائف آخر دون الحاجة إلى معرفة كلمة مرور الطرف الآخر.
د. يجب أن تدعم نظام التحكم في الوصول إلى وحدة التحكم (TACACS +)، خدمة المستخدم لمصادقة الاتصال عن بُعد ((RADIUS، استرجاع خدمات الدليل النشط، حيثما أمكن ذلك.

13.15
يجب حفظ كلمات المرور وعدم تدوينها أو تسجيلها مطلقًا مع معلومات الحساب أو أسماء المستخدمين المقابلة.

ضوابط ضبط ومراقبة الوثائق

نوع الضوابط: إلزامية	مرجع: ISMS-PR02-p02-p02 إجراء ضبط ومراقبة الوثائق

الهدف:
التأكد من أن الضوابط والعمليات المطلوبة تُطبق أثناء إنشاء عناصر نظام إدارة أمن المعلومات والوصول إليها وتعديلها وتخزينها والتخلص منها.

إرشادات التنفيذ:
يجب أن يكون لدى موردي الخدمات المدارة التابعين لـ stc في المستوى الأساسي الضوابط التالية فيما يتعلق بضبط ومراقبة الوثائق.

14.1
أ. يجب أن يكون جميع المتعاقدين والموردين الخارجيين على دراية بمسؤولياتهم عند تحرير أو تطوير أو اعتماد مستند ما لشركة stc.
ب. يوضح هذا الدليل الإرشادي متطلبات التوثيق ويؤكد الالتزام الذي تتعامل به stc مع الوثائق والضوابط في إصدار الوثائق التي يتم كتابتها أو تطويرها أو اعتمادها.

ج. يُتوقع من المستخدمين مراقبة الترتيبات المنصوص عليها في هذا الدليل الإرشادي والإجراء والإبلاغ عن أي ظروف يعتقدون فيها أن هناك خرقًا يتعلق بضوابط أو استخدام المستندات بشكل مناسب.
د. قد يؤدي انتهاك المتطلبات القانونية للاحتفاظ بالبيانات / الاحتفاظ بالسجلات إلى تعريض الفرد لإجراءات تأديبية، فضلاً عن المسؤولية الشخصية عن العقوبات المدنية و/أو الجنائية من قبل المحاكم أو وكالات إنفاذ القانون.

14.2

أ. يجب اعتبار جميع الوثائق، التي تم إعدادها بشكل أولي، على أنه مسودات.
ب. عند مراجعة مسودة الوثيقة، يجب أن يتم إصدارها ثم الإضافة عليها لكل مراجعة حتى يتم اعتمادها.
ج. تصبح مسودة الوثيقة وثيقة معتمدة إذا تم اعتمادها من قبل السلطة المختصة.
د. يجب التعامل مع أي تغيير رئيسي في المستند على أنه تغيير في الإصدار، وإلا يجب معاملته كتغيير مراجعة.
ه. بإجراء تغيير في الإصدار/المراجعة، يجب وضع علامة على المستند السابق على أنه تم استبداله.
و. يجب إتلاف النسخ التي خضعت للمراقبة عند استبدالها بنسخة / مراجعة جديدة.
ز. يجب إدراج التغييرات في المستند الإلكتروني ويجب نسخ المستند بالكامل إلى المواقع التي تحتوي على النسخ التي خضعت للمراقبة.

ضوابط إدارة استمرارية أعمال الأمن السيبراني

نوع الضوابط: إلزامية	مرجع: ISMS-PR05-p01 إجراءات إدارة استمرارية أعمال الأمن السيبراني

الهدف:
وضع الخطط والإجراءات الواجب استخدامها في حالة الانقطاع، والتي تشمل خطط الطوارئ وخطط وإجراءات التعافي من الكوارث وخطة استمرارية الأعمال.

إرشادات التنفيذ:
يجب أن يكون لدى موردي الخدمات المدارة التابعين لـ stc في المستوى الأساسي الضوابط التالية فيما يتعلق بإدارة استمرارية أعمال الأمن السيبراني.

15.1

أ. يجب أن تتضمن إدارة استمرارية الأعمال ضوابط لتحديد وتقليل المخاطر على توافر الخدمات الهامة بالإضافة إلى عملية تقييم المخاطر العامة، والحد من عواقب الحوادث الضارة، والمعلومات المطلوبة لعمليات الأعمال متاحة بسهولة.
ب. يجب على مسؤولي عمليات الأعمال تحديد الأحداث الرئيسية التي يمكن أن تتسبب في تعطيل عملياتهم وتوثيق تأثيرها السلبي المحتمل، على سبيل المثال. فئات التأثير - الأثر المالي، وأثر جودة الصحة والسلامة والبيئة، وأثر السمعة والأثر التنظيمي
ج. يجب أن يكون مسؤول "خطة استمرارية الأعمال" مسؤولاً عن تنسيق تحديثات الخطة، بما في ذلك التوثيق والتحديثات الإجرائية. وهذا يشمل، على سبيل المثال لا الحد:
- الموقع الحالي ومعلومات الاتصال للأطراف ذات الصلة بالخطة.
- الإجراءات أو العمليات اللازمة لتنفيذ الخطة.
- اتفاقيات الطرف الثالث، حسب الاقتضاء.
- جرد الأصول أو متطلبات الخطة.
- مواد التدريب والتوعية والتعليم للمشاركين.
- التوثيق الخاص بمتطلبات الأمن السيبراني والضوابط.

ضوابط إدارة التغيير

نوع الضوابط: إلزامية	مرجع: ISMS-PR06-p01 إجراء إدارة التغيير

الهدف:
إنشاء ودعم نظام إدارة تغيير يتسم بالكفاءة والفعالية لضبط وإدارة جميع التغييرات بما في ذلك الصيانة الطارئة والتوثيق والتصحيحات الأمنية المتعلقة بالبنية التحتية والتطبيقات داخل بيئة الإنتاج وتقليل احتمالية الانقطاع بسبب التعديلات والأخطاء غير المصرح بها.

إرشادات التنفيذ:
يجب أن يكون لدى موردي الخدمات المدارة التابعين لـ stc في المستوى الأساسي الضوابط التالية فيما يتعلق بإجراءات إدارة التغيير.

16.1

أ. يجب أن تكون المستندات الخاصة بطلب التغيير مصحوبة بمتطلبات تغيير تفصيلية وإجراءات مناسبة لتنفيذ التغيير. يجب أن تتضمن أيضًا إجراءات / خطط مفصلة للعودة إلى الإصدار السابق، والأثر في حالة فشل التغيير و/أو عدم تحقيق النتيجة المرجوة. ب. يجب أن تسهل عملية إدارة التغيير التواصل والإخطار بجميع التغييرات لأصحاب المصلحة المعنيين الداخليين والخارجيين داخل stc. ج. يجب الحفاظ على الفصل المناسب بين المهام لضمان عدم إمكانية تنفيذ التغييرات في أنظمة الإنتاج على نحو فردي. د. يجب اختبار التغييرات في بيئة معزولة وخاضعة للرقابة وتمثيلية (حيث تكون هذه البيئة ممكنة) قبل التنفيذ لتقليل التأثير على عملية / عمليات العمل ذات الصلة. ه. يجب إجراء اختبار قبول المستخدم للتأكد من أن التغييرات المنفذة قد حققت الأهداف المتوقعة المحددة في طلب التغيير.

ضوابط تحديث النظام

نوع الضوابط: إلزامية	مرجع: ISMS-PR07-p01 إجراء تحديث النظام

الهدف:
تقديم المشورة بشأن تصحيح أنظمة تكنولوجيا المعلومات لتأمينها بشكل أفضل من الهجمات وتقييم نقاط الضعف المتعلقة بشبكة stc.

إرشادات التنفيذ:
يجب أن يكون لدى موردي الخدمات المدارة التابعين لـ stc في المستوى الأساسي الضوابط التالية فيما يتعلق بإجراءات تحديث النظام.

17.1

أ. يتعين على stc إنشاء عملية لتحديد الثغرات الأمنية المكتشفة حديثًا من خلال الوسائل التالية:
- الاشتراك في قوائم الاستشارات والتنبيهات التي تخطر بأي تحديثات أو تصحيحات جديدة للبرامج يتم إصدارها.
- إشعار مباشر من الموردين وموفري البرامج.
- تقارير تقييم الثغرات الأمنية من فريق الأمن السيبراني.

ب. يجب أن تحتوي جميع أنظمة تكنولوجيا المعلومات والشبكات على آخر التحديثات / التصحيحات / حزم الخدمة / الإصلاحات العاجلة المثبتة وفقًا للجداول المخطط لها.
ج. يجب أن تكون هناك آلية لاختبار التحديثات / التصحيحات / حزم الخدمة / الإصلاحات العاجلة لجميع الأنظمة والتطبيقات المهمة للأعمال في بيئة اختبار قبل تطبيقها على الأنظمة الحية.
د. ضمان إجراء التصحيح بانتظام وبطريقة خاضعة للرقابة ويمكن التنبؤ بها، يجب وضع جدول زمني للتصحيح.
ه. يجب تنفيذ عمليات التصحيح من خلال عملية إدارة التغيير حسب الاقتضاء.
و. يجب تقدير زمن التعطل، إن وجد، لإجراء التصحيحات لبيئات الإنتاج. يجب اتخاذ الترتيبات اللازمة لإبلاغ المستخدمين مسبقًا بالتوقف عن العمل أو يمكن التخطيط لوقت التوقف خارج ساعات العمل.
ز. يجب تطبيق آليات العودة إلى الإصدار السابق في حالة حدوث مشكلات غير متوقعة، بحيث يمكن إعادة النظام إلى الحالة السابقة.
ح. يجب نشر التصحيحات لإصلاح نقاط الضعف في النظام بمجرد إصدار التصحيح من قبل المورد ووفقًا للجداول الزمنية المنصوص عليها.
ط. في حالة عدم توفر التصحيحات، يجب على الموردين تنفيذ ضوابط / حلول وقتية للتخفيف من المخاطر ضمن اتفاقية مستوى الخدمة المتفق عليها.
ي. يُطلب من الفرق التي تطبق التصحيحات تجميع مقاييس الإبلاغ التي تسجل النسب المئوية للأنظمة التي تم تصحيحها بشكل فعال والإبلاغ بها والحفاظ عليها، مع تلخيص نتائج كل دورة تصحيح.
ك. يجب أن توثق السجلات التصحيحات والتحديثات التي تم تثبيتها على كل جهاز كمبيوتر محمول وكمبيوتر مكتبي وخادم بما في ذلك تفاصيل التصحيح وتاريخ التثبيت واسم الشخص المعين بتثبيت التصحيح.

ضوابط نقل المعلومات

نوع الضوابط: إلزامية	مرجع: ISMS-PR08-p01 إجراء نقل المعلومات

الهدف:
حماية المعلومات بشكل كافٍ لأسباب قانونية مثل السرية أو حماية البيانات، والحفاظ على ثقة مستخدمي الخدمة وشركائنا.

إرشادات التنفيذ:

ضوابط الأمن السيبراني
لموردي ومقاولي الخدمات المدارة

يجب أن يكون لدى موردي الخدمات المدارة التابعين لـ stc في المستوى الأساسي الضوابط التالية فيما يتعلق بإجراءات نقل المعلومات.

18.1

- نظام البريد الإلكتروني هو ملك لشركة stc وجميع نسخ الرسائل التي يتم إنشاؤها أو إرسالها أو استلامها أو تخزينها على النظام هي ملك لشركة stc.
- تحتفظ stc بالحق في مراجعة وتدقيق واعتراض والوصول إلى ومراقبة وحذف والكشف عن جميع الرسائل التي يتم إنشاؤها أو استلامها أو إرسالها أو تخزينها على نظام البريد الإلكتروني بناءً على موافقة لجنة الإدارة.
- توفر stc أنظمة معلومات واتصالات إلكترونية لتسهيل احتياجات ومصالح أعمال الشركة.
- يجب أن يقتصر الوصول إلى الرسائل الإلكترونية على الموظفين المصرح لهم بشكل صحيح.
- لا يجوز استخدام موارد معلومات stc لإرسال أو استقبال بيانات تحتوي على أي مواد مسيئة أو تشهيرية أو مهددة للآخرين.
- أي بيانات أو تعليقات يتم إجراؤها عبر البريد الإلكتروني والتي يجب تفسيرها بأي شكل من الأشكال على أنها إجراء من أعمال stc، يجب أن تحمل بيان إخلاء المسؤولية التالي:
  - قد تحتوي هذه الرسالة على معلومات تتعلق بشركة الاتصالات الكويتية (stc)، وبسبب عقد العمل الشخصي للمرسل مع stc، لا تتحمل stc أي مسؤولية عن محتوى هذه الرسالة، أو عن عواقب أي إجراءات يتم اتخاذها على أساس المعلومات المقدمة، ما لم يتم تأكيد هذه المعلومات لاحقًا كتابيًا من قبل stc.
- يجب تعطيل / إزالة معرّف البريد الإلكتروني الذي تم إنشاؤه للمورّد / الطرف الثالث / موظفي الخدمات المُدارة عند إنجاز الارتباط / الاتفاقية التعاقدية مع stc.
- يجب على كل مستخدم اتخاذ الاحتياطات اللازمة لمنع الاستخدام غير المصرح لحسابات البريد الإلكتروني. المستخدمون مسؤولون بشكل شخصي عن جميع رسائل البريد الإلكتروني من حساباتهم. لا يُسمح بتزوير معلومات العنوان الرأسي في البريد الإلكتروني (بما في ذلك عنوان المصدر وعنوان الوجهة والختم الزمني).
- لا يجوز استخدام أنظمة stc لنقل أو تلقي الأسرار التجارية أو المواد المحمية بحقوق الطبع والنشر أو المعلومات السرية أو ذات الملية الخاصة.
- لا يجوز إرسال أي معلومات تعتبر سرية، بما في ذلك الاتفاقيات القانونية أو التعاقدية أو المعلومات الفنية المتعلقة بعمليات stc أو الأمن وما إلى ذلك، عبر البريد الإلكتروني دون اتخاذ تدابير كافية لحماية المعلومات المرفقة من الوصول غير المصرح به.
- تحتفظ stc بالحق في مراقبة أو تقييد الوصول إلى رسائل البريد الإلكتروني الخاصة بها على شبكة الإنترنت. يتحمل المستخدمون مسؤولية ضمان عدم وصولهم إلى رسائل البريد الإلكتروني الخاصة بشركة stc من الأنظمة العامة مثل تلك الموجودة في مقاهي الإنترنت. في حالة الحاجة الماسة للوصول إلى بريد stc الإلكتروني من جهاز كمبيوتر عام، يحتاج المستخدم إلى التأكد من إزالة جميع النسخ المؤقتة / المحلية من رسائل البريد الإلكتروني والمرفقات من النظام وعدم تخزين بيانات المستخدم في النظام.

18.2

- حجم صندوق البريد الافتراضي لموظفي stc هو 1.1 جيجا بايت وبالنسبة لأي مقاول 110 ميجا بايت. ومع ذلك، يمكن للمستخدمين طلب أحجام إضافية لصندوق البريد الإلكتروني مع وجود سبب عمل مناسب، والاعتماد المناسب عل الطلب.
- يجب تهيئة حل فلترة المحتوى لحظر الرسائل المشبوهة في رسائل البريد الإلكتروني.

18.3

- يتم منح استخدام الإنترنت لغرض وحيد هو دعم الأنشطة التجارية اللازمة لتنفيذ وظائف العمل.
- لا يجوز للموظفين والمقاولين والعملاء والموردين والاستشاريين استخدام أي نوع آخر من الاتصالات عندما يكون النظام / الجهاز متصلاً بشبكة شركة stc.

18.4

- يجب فحص جميع المحتويات التي يتم تنزيلها من الإنترنت عند البوابة وعند العملاء للتأكد من خلوها من أي رموز برمجية ضارة مثل الفيروسات أو أحصنة طروادة أو الفيروسات المتنقلة.
- لا يُسمح للمستخدمين بتنزيل أو تحميل أي برنامج من/إلى الإنترنت دون موافقة مسبقة.
- يجب استخدام خدمة الإنترنت لتعزيز المساهمة المهنية للمستخدمين في الشركة. يجب على جميع المستخدمين أيضًا التأكد من أنهم يستخدمون خدمات الإنترنت بطريقة أخلاقية وقانونية لتجنب التعرض لإجراءات التقاضي.

18.5
يجب أن يدرك المستخدمون أن stc لن تتحمل أي مسؤولية عن تعرضهم للمواد المسيئة التي قد يصلون إليها عبر الإنترنت. يجب على المستخدمين عدم الوصول إلى المواقع المحجوبة من قبل الحكومة، كما يجب على المستخدمين عدم زيارة المواقع غير الرسمية أو المواقع المشبوهة. فيما يلي قائمة بأمثلة توضيحية للاستخدام غير المقبول لخدمات الإنترنت:

- نقل أي محتوى يتضمن إساءة أو تحرش أو احتيال أو يخالف القانون أو يسيء إلى الشركة أو السلطات الحاكمة.
- إجراء الأعمال الشخصية باستخدام موارد الشركة.
- تنزيل البرامج غير المرخصة.
- إرسال رسائل أو ملفات تهديد.
- إرسال رسائل أو ملفات تحرش جنسيًا أو عنصريًا.
- إرسال ملفات تحتوي على فيروسات كمبيوتر أو تعليمات برمجية ضارة أخرى.
- محاولة الوصول إلى الأنظمة دون الحصول على التراخيص المناسبة.
- إرسال أو نشر معلومات سرية لأشخاص غير مصرح لهم.
- نشر معلومات التهيئة أو تفاصيل الثغرات الأمنية المحتملة في البنية التحتية لتكنولوجيا المعلومات في stc على النطاقات العامة.
- الدخول إلى / تنزيل المواقع الإباحية أو العنصرية أو غير القانونية أو الصور أو الأغاني أو النكات أو الرسوم المتحركة أو الرسومات أو الأفلام أو أي مادة أخرى.
- استخدام الإنترنت للوصول إلى المواقع التي تروّج للمقامرة أو المنافع التجارية الشخصية أو غسل الأموال.
- إنشاء شبكة انترنت أو غيرها من اتصالات الشبكة الخارجية التي يمكن أن تسمح للمستخدمين غير التابعين لشركة stc بالوصول إلى أنظمة وتطبيقات stc.
- تعمد التدخل في التشغيل العادي لبوابة الإنترنت.
- لا يُسمح باتصالات الخدمة الطرفية الواردة والصادرة غير المضمونة عبر الإنترنت.
- يحظر خدمات الدردشة الداخلية وخدمات التراسل (P2P).

ضوابط حوكمة موردي الأمن السيبراني

نوع الضوابط: إلزامي	مرجع: SMS-PR09-p01 إجراءات حوكمة موردي الأمن السيبراني

الهدف:
وضع القواعد الأساسية لإدارة الأمن على الأطراف الخارجية (مثل الموردين والمستثمرين، إلخ) الذين لهم حق وصول مباشر أو غير مباشر إلى أنظمة وبيانات stc.

إرشادات التنفيذ:
يجب أن يكون لدى موردي الخدمات المدارة التابعين لـ stc في المستوى الأساسي الضوابط التالية فيما يتعلق بحوكمة موردي الأمن السيبراني.

19.1
يجب على موردي الخدمات المدارة استخدام ضوابط stc الأساسية وقائمة مراجعة التقييم لتطوير خطة تقييم أمني قابلة للتطبيق لإنتاج وتجميع المعلومات اللازمة لتحديد فعالية ضوابط الأمن المستخدمة في نظام المعلومات. عند تطوير خطط تقييم الأمن الفعالة، يجب على موردي الخدمات المدارة أن يأخذوا في الاعتبار المعلومات الموجودة بشأن الضوابط الأمنية التي سيتم تقييمها.

19.2
يمكن لموردي الخدمات المدارة استخدام المعلومات التي يتم إنتاجها أثناء تقييمات المراقبة الأمنية من أجل:

أ. تحديد نقاط الضعف والقصور في نظم المعلومات.
ب. التأكد من معالجة نقاط الضعف والقصور التي تم تحديدها في نظام المعلومات.
ج. دعم قرارات الميزانية والاستثمار الرأسمالي.

19.3
يلتزم موردو الخدمات المدارة تعاقديًا وعمليًا بالوفاء بالتزامات stc التجارية والأمنية وأي التزامات امتثال تنظيمي. يجب تضمين المتطلبات التالية في اتفاقيات الأطراف الخارجية:

أ. تخضع الأطراف الخارجية لاتفاقية حماية المعلومات تنص صراحةً على أنه لا يجوز للأشخاص الذين لديهم إمكانية الوصول إلى مرافق stc أو المعلومات الخاصة بها نشر أي معلومات بشأن stc أو قدراتها أو أنشطتها دون الحصول على إذن كتابي من stc.
ب. التزام الطرف الخارجي بإخطار stc في حالات الحوادث الأمنية التي تقع داخل مؤسسة الطرف الخارجي، والتي قد تؤثر على stc (على سبيل المثال، اختراق الفيروسات لبنية الطرف الخارجي، حدوث اختراق ناجح لشبكة الطرف الخارجي، وما شابه ذلك).
ج. التزام الطرف الخارجي بالحفاظ على سرية معلومات stc وتوافرها.
د. إمكانية إعادة التفاوض أو إنهاء العقد إذا لم يتم استيفاء الشروط والأحكام، على سبيل المثال وقوع حادثة أمنية لم يتم الكشف عنها أو فشل الطرف الخارجي في تلبية مستويات الخدمة المتفق عليها.
ه. مشكلات التعاقد من الباطن في حالة استخدام الأطراف الخارجية لموردين آخرين لتقديم الخدمات ويكونا لهؤلاء الموردين حق وصول مباشر أو غير مباشر إلى بيانات stc. يجب أن يلتزم الطرف الخارجي بأن يفي أي مورد بالتزامات stc الأمنية ومتطلبات الامتثال التنظيمي.
و. يجب وضع ضوابط لضمان أمن الاتصالات عن بعد بين الأطراف. يجب على الطرف الخارجي الاستفادة من البنية التحتية الأمنية الحالية لـ stc وتحمل مسؤولية الحفاظ على الضوابط الأمنية ذات الصلة التي وضعتها stc.
ز. يجب تحديد ملكية الترخيص والملكية الفكرية، بما في ذلك اتفاقيات الضمان بوضوح.
ح. إلى أقصى حد ممكن، تضمين بند "الحق في التدقيق" والذي يضمن قيام الإدارة و/أو ممثل معتمد عنها بإجراء تقييم مادي و/أو منطقي لبيئة الرقابة للطرف الخارجي.
ط. نوع وحجم وتكرار أي ملفات و/أو تقارير سيتم تبادلها بين الطرفين.
ي. ترتيبات استمرارية الأعمال والتعافي من الكوارث لاستئناف خدمات الطرف الخارجي في حالة انقطاع الخدمة أو فقدان / تدمير البيانات.

ضوابط النسخ الاحتياطي للمعلومات

نوع الضوابط: إلزامي	مرجع: ISMS-PR-12-p01 إجراء النسخ الاحتياطي

الهدف:
التأكد من عمل نسخ احتياطية للمعلومات على مستوى المستخدم، وبيانات الشركة التي تشمل رسائل البريد الإلكتروني، والمعاملات، وبيانات العملاء، وخطط واستراتيجيات الأعمال ومعلومات مستوى النظام الواردة في نظام المعلومات.

إرشادات التنفيذ:
يجب أن يكون لدى موردي الخدمات المدارة التابعين لـ stc في المستوى الأساسي الضوابط التالية فيما يتعلق بالنسخ الاحتياطي لنظام المعلومات.

20.1
تحديد وتوثيق وعمل نسخة احتياطية من بيانات الشركة الهامة، وتشمل على سبيل المثال لا الحصر ما يلي:
أ. بيانات مستوى المستخدم: مستخدمو النظام / التطبيقات وبيانات الموظفين وما إلى ذلك.
ب. بيانات مستوى النظام: نظام التشغيل، وبرامج التطبيقات، والتراخيص، وما إلى ذلك.
ج. بيانات العمل: بيانات العميل وخطط العمل ورسائل البريد الإلكتروني ومعلومات المنتج وما إلى ذلك.

20.2
تحديد وتوثيق استراتيجية النسخ الاحتياطي التي تنص على ما يلي:
أ. أنواع البيانات المطلوب نسخها احتياطيًا، على سبيل المثال بيانات الشركة أو المستخدم أو مستوى النظام وما إلى ذلك.
ب. أنواع طرق النسخ الاحتياطي التي سيتم استخدامها على سبيل المثال النسخ الاحتياطي الكامل الأسبوعي والشهري؛ النسخ الاحتياطي التفاضلي والتزايدي في أيام الأسبوع. راجع الجدول أدناه للتعرف على طريقة النسخ الاحتياطي التي يتم تنفيذها بناءً على احتياجات العمل المختلفة:

تنفيذ النسخ الاحتياطي	الحاجة
طلب النسخ الاحتياطي	إذا كانت هناك حاجة للعمل لتنفيذ نسخة احتياطية من أي معلومات، فيجب تقديم طلب؛ ويتم تفعيل هذا الإجراء.
طلب النسخ الاحتياطي في حالات الطوارئ / الاستجابة للكوارث	في حالة حدوث تغيير عاجل، يجب بدء طلب نسخ احتياطي للطوارئ في حالات الكوارث؛ ويتم تفعيل هذا الإجراء.
طلب النسخ الاحتياطي المشروط (طلب تغيير / تنفيذ تصحيح)	التأكد من تنفيذ إجراء النسخ الاحتياطي والاستعادة بشكل صحيح.
خطة النسخ الاحتياطي الدورية	إذا كان هناك طلب نسخ احتياطي دوري، يجب تفعيل هذا الإجراء.

إدارة التوفر للنسخ الاحتياطية	في حالة وقوع كارثة، يتم البدء في توفير نسخة احتياطية في حالات الطوارئ؛ ويتم تفعيل هذا الإجراء.

ج. فترة الاحتفاظ بالبيانات الاحتياطية. راجع الجدول أدناه للتعرف على سياسة Stc الخاصة بالاحتفاظ بالنسخة الاحتياطية:

خارج الموقع	في الموقع	عدد النسخ	مدة الاحتفاظ	المسؤول	التواتر	نوع النسخ الاحتياطي	النظام
نعم	نعم	2	1 شهر		تزايدي يوميا	قاعدة البيانات	كل الأنظمة
نعم	نعم	2	3 أشهر	مدير التطبيق	أسبوعي كامل		
لا	نعم	1	6 أشهر	مدير التطبيق	شهري كامل	نظام الملفات	
لا	نعم	1	1 شهر	مدير التطبيق	تزايدي يوميا		
نعم	نعم	2	لا حد له	مدير التطبيق	تزايدي يوميا	ملفات CDRS	
نعم	نعم	2	لا حد له	مدير التطبيق	تزايدي يوميا	ملفات سجلات الكلام	
نعم	نعم	2	3 أشهر	مدير التطبيق	تزايدي يوميا	التبادل	
نعم	نعم	2	لا حد له	مدير التطبيق	شهري كامل		

د. تأمين البيانات الاحتياطية على سبيل المثال التشفير، والتخزين خارج الموقع، واختبار الاسترداد، وغيرها.
ه. متطلبات النسخ الاحتياطي للأشرطة أو الأقراص أو كليهما.

20.3
إجراء النسخ الاحتياطي وفقًا لإستراتيجية النسخ الاحتياطي المحددة.

20.4
تخزين النسخ الاحتياطية في أماكن آمنة في الموقع على سبيل المثال في حالة استخدام الأشرطة الاحتياطية، فيجب حفظ الأشرطة في خزائن مقاومة للحريق.

20.5
حفظ نسخة ثانية من النسخة الاحتياطية في مكان بعيد إما إلكترونيًا أو عن طريق الشحن المادي لوسائط التخزين.

20.6
استخدام التوقيعات الرقمية والتجزئة المشفرة لحماية سلامة نُسخ نظام المعلومات الاحتياطية.

20.7
التأكد من توفر النسخ الاحتياطي لاستمرارية الأعمال عن طريق اختبار استعادة البيانات التي تم نسخها احتياطيًا باستخدام طريقة أخذ العينات.

ضوابط تصنيف المعلومات

نوع الضوابط: إلزامية	مرجع: ISMS-PR12-p03 إجراء تصنيف المعلومات

الهدف:
وضع إطار لتصنيف بيانات / معلومات stc بناءً على مستوى حساسيتها وقيمتها وأهميتها بالنسبة للشركة.

إرشادات التنفيذ:
يجب أن يكون لدى موردي الخدمات المدارة التابعين لـ stc في المستوى الأساسي الضوابط التالية فيما يتعلق بتصنيف المعلومات.

21.1
يعتمد تصنيف المعلومات في stc على سرية المعلومات أو سلامتها أو توفرها. يحدد الجدول أدناه مستويات تصنيف المعلومات

المستوى	البيان

معلومات عامة	ينطبق هذا التصنيف على المعلومات المتاحة لعامة الجمهور والمخصصة للتوزيع خارج الشركة. ويجوز نشر هذه المعلومات بحرية دون أي ضرر محتمل. على الرغم من عدم وجود قيود على الإفصاح لحماية البيانات العامة (لأن المعلومات متوفرة للوصول للعرض على نطاق واسع)، يجب تطبيق حماية كافية لمنع التعديل غير المصرح به على هذه المعلومات. ينطبق هذا التصنيف على المعلومات التي من المفترض أن يتم نشرها
معلومات مقصورة على الشركة	داخل أقسام الشركة. لا يُتوقع أن يؤثر الكشف غير المصرح به أو تعديل أو إتلاف هذه البيانات بشكل خطير أو سلبي على stc أو موظفيها أو أصحاب المصلحة. ينطبق هذا التصنيف على المعلومات التي تعتبر خاصة، أي لا يمكن الوصول إليها إلا من قبل عدد محدود من الموظفين المدرجين في هذا التصنيف.
معلومات سرية	الإفصاح غير المصرح به والذي يمكن أن يؤثر سلبًا على الشركة وموظفيها وأصحاب المصلحة. أصول المعلومات التي توجد لها متطلبات قانونية تحظر أو تفرض عقوبات مالية على الإفصاح غير المصرح به. المعلومات التي يغطيها القانون أو التشريع التنظيمي والخاص بالدولة. سجلات المخاطر، وتقارير التدقيق والمعلومات المالية تقع في هذه الفئة.

21.2

يحدد الجدول التالي معايير أمن المعلومات والضمانات المطلوبة لحماية المعلومات بناءً على تصنيفها. بالإضافة إلى معايير أمن المعلومات التالية ، يجب أن تفي أي معلومات تغطيها قوانين أو لوائح الدولة أو الاتفاقيات التعاقدية بمتطلبات الأمن التي تحددها تلك القوانين أو اللوائح أو العقود.

المعايير، أي معلومات تغطيها قوانين أو لوائح الولاية أو الاتفاقات التعاقدية يجب أن تفي بمتطلبات الأمان المحددة بواسطة تلك القوانين أو اللوائح أو العقود.

فئة ضوابط الأمن	تصنيف المعلومات – عامة	تصنيف المعلومات – مقصورة على الشركة	تصنيف المعلومات – سرية
ضوابط الوصول	لا قيود على العرض تصريح من قبل المسؤول عن المعلومات أو من ينوب عنه مطلوب لإجراء تعديل عليها. اعتماد المشرف مطلوب أيضًا إذا لم تكن وظيفة خدمة ذاتية	العرض والتعديل مقصوران على الأفراد المصرح لهم حسب الحاجة للأدوار المتعلقة بالأعمال. يمنح المسؤول عن المعلومات أو من ينوب عنه الإذن للوصول، بالإضافة إلى اعتماد المشرف المصادقة والتفويض مطلوبان للوصول إليها.	العرض والتعديل مقصوران على الأفراد المصرح لهم حسب الحاجة للأدوار المتعلقة بالأعمال. يمنح المسؤول عن المعلومات أو من ينوب عنه الإذن بالوصول، بالإضافة إلى اعتماد المشرف المصادقة والترخيص مطلوبان للوصول إلى اتفاقية السرية
النسخ / الطباعة (ينطبق على كل من النماذج الورقية والإلكترونية)	لا توجد قيود	يجب طباعة المعلومات فقط عندما تكون هناك حاجة مشروعة يجب أن تقتصر النسخ على الأفراد الذين يحتاجون إلى المعرفة لا ينبغي ترك المعلومات دون مراقبة على الطابعة	يجب طباعة المعلومات فقط عندما تكون هناك حاجة مشروعة. يجب أن تقتصر النسخ على الأفراد المصرح لهم بالوصول إلى المعلومات، بعد توقيعهم لاتفاقية سرية يجب عدم ترك المعلومات دون مراقبة على الطابعة. يجب تصنيف النسخ بأنها "سرية"
أمن الشبكة	قد تكون موجودة على شبكة عامة	مطلوب الحماية بجدار حماية الشبكة	مطلوب حماية بجدار حماية للشبكة باستخدام مجموعة

ضوابط الأمن السيبراني
لموردي ومقاولي الخدمات المدارة

	يوصي بتوفير حماية بجدران حماية يوصي بتوفير حماية IDS / IPS الحماية فقط مع الموجه ACLs مقبولة	مطلوب حماية IDS / IPS حماية مع موجه ACLs اختيارية لا ينبغي أن تكون الخوادم التي تستضيف البيانات مرئية للإنترنت بالكامل قد تكون في شبكة فرعية لخادم شبكة مشترك مع مجموعة قواعد جدار حماية مشتركة لمجموعة الخوادم	قواعد "الرفض الافتراضي" مطلوب حماية IDS / IPS حماية مع موجه ACLs اختيارية لا ينبغي أن تكون الخوادم التي تستضيف البيانات مرئية للإنترنت بالكامل، ولا للشبكات الفرعية غير المحمية مثل قاعات الإقامة وشبكات الضيف اللاسلكية للنظام يجب مراجعة مجموعة قواعد جدار الحماية بشكل دوري بواسطة مدقق خارجي
أمن النظام	يجب اتباع الممارسات الرائدة العامة لإدارة النظام والأمن (خطوط أساس الحد الأدنى للأمن المطبقة لدي stc) يوصى باستخدام جدار حماية للبرامج المستندة إلى المضيف	يجب اتباع أفضل الممارسات الخاصة بـ stc ونظام التشغيل لإدارة النظام والأمن مطلوب جدار حماية للبرامج المستندة إلى المضيف يوصى باستخدام برامج IDS / IPS القائمة على المضيف	يجب اتباع أفضل الممارسات الخاصة بـ stc ونظام التشغيل لإدارة النظام والأمن مطلوب جدار حماية للبرامج المستندة إلى المضيف يوصى باستخدام برامج IDS / IPS القائمة على المضيف
البيئات الافتراضية	يمكن استضافتها في بيئة خادم افتراضي تنطبق جميع ضوابط الأمن الأخرى على كل من الأجهزة الافتراضية للمضيف والضيف	يمكن استضافتها في بيئة خادم افتراضي تنطبق جميع ضوابط الأمن الأخرى على كل من الأجهزة الافتراضية للمضيف والضيف. يجب ألا تشارك نفس بيئة المضيف الافتراضية مع الخوادم الافتراضية للضيف من تصنيفات الأمن الأخرى	يمكن استضافتها في بيئة خادم افتراضي تنطبق جميع ضوابط الأمن الأخرى على كل من الأجهزة الافتراضية للمضيف والضيف لا يمكن مشاركة نفس بيئة المضيف الافتراضية مع الخوادم الافتراضية للضيف من تصنيفات الأمن الأخرى
الأمن المادي	يجب قفل النظام أو تسجيل الخروج عند في حالة عدم التواجد يوصى باستخدام جدار حماية للبرامج المستندة إلى المضيف	يجب قفل النظام أو تسجيل الخروج عند في حالة عدم التواجد مطلوب استضافة في مكان آمن؛ يوصى باستخدام مركز بيانات آمن	يجب قفل النظام أو تسجيل الخروج عند في حالة عدم التواجد مطلوب استضافة في مركز بيانات آمن يجب مراقبة الوصول المادي وتسجيله وقصره على الأفراد المصرح لهم على مدار الساعة طوال أيام الأسبوع
الوصول عن بعد للأنظمة التي تستضيف البيانات	لا توجد قيود	الوصول مقيد إلى الشبكة المحلية أو خدمة الشبكة الافتراضية الخاصة لـ stc الوصول عن بعد من قبل طرف خارجي للدعم الفني محدود بالوصول المؤقت والمصادق عبر مودم اتصال مباشر أو بروتوكولات آمنة عبر الإنترنت	مقيد على الشبكة المحلية أو مجموعة الشبكة الافتراضية الخاصة الآمنة لا يُسمح بالوصول عن بُعد غير الخاضع للإشراف من قبل جهة خارجية للدعم فني يوصى بالمصادقة الثنائية
تخزين المعلومات	يوصى بالتخزين على خادم آمن يوصى بالتخزين في مركز	يوصى بالتخزين على خادم آمن يوصي بالتخزين في مركز بيانات آمن	مطلوب التخزين على خادم آمن مطلوب التخزين في مركز

	بيانات آمن	لا يجب التخزين على محطة عمل فردية أو جهاز محمول	بيانات الآمن لا يجب التخزين على محطة عمل فردية أو جهاز محمول (مثل، كمبيوتر محمول)؛ إذا تم التخزين على محطة عمل فردية أو جهاز محمول، فيجب استخدام تشفير القرص بالكامل مطلوب تشفير على وسائط النسخ الاحتياطي مطلوب تشفير AES مع مفتاح 192 بت أو أطول لا يجب ترك الورق/ النسخ الورقية دون رقابة حيث يمكن للآخرين الإطلاع عليها؛ ويجب تخزينها في مكان آمن
النقل	لا توجد قيود	لا توجد متطلبات	التشفير مطلوب (على سبيل المثال، عبر SSL أو بروتوكولات نقل الملفات الآمنة). لا يمكن الإرسال عبر البريد الإلكتروني إلا إذا تم تشفيره وتأمينه باستخدام توقيع رقمي
النسخ الاحتياطي / التعافي من الكوارث	مطلوب عمل نسخ احتياطي يوصى بالنسخ الاحتياطي يومياً	مطلوب عمل نسخ احتياطي يومي. يوصى بالتخزين خارج الموقع	مطلوب عمل نسخ احتياطي يومي. مطلوب تخزين خارج الموقع في مكان آمن
التدرب	يوصى بتدريب عام يتعلق بالتوعية الأمنية. يوصى بتدريب إدارة النظام	مطلوب تدريب عام يتعلق بالتوعية الأمنية مطلوب تدريب على إدارة النظام. مطلوب تدريب على أمن المعلومات	مطلوب تدريب عام يتعلق بالتوعية الأمنية. مطلوب تدريب على إدارة النظام. يجب على مسؤولي النظام المعينين بعد 1 سبتمبر 2008 اجتياز الفحص الجنائي. مطلوب تدريب على أمن المعلومات. مطلوب تدريب على السياسات واللوائح المعمول بها
جدول التدقيق	حسب ما هو مطلوب	حسب ما هو مطلوب	سنوي

21.3
من أجل ضمان تطبيق الضوابط الصحيحة على أصول المعلومات الخاصة بـ stc، يتم استخدام نظام العلامات الوقائية بحيث تكون جميع الأطراف الخارجية، عند الاقتضاء، على دراية بكيفية إدارة هذه المعلومات.

21.4
يتم وضع ضوابط صارمة على استخدام الوسائط القابلة للإزالة مثل الأقراص المضغوطة وأقراص الفيديو الرقمي والأشرطة ومحركات الأقراص الصلبة الخارجية ووحدات تخزين البيانات داخل stc. جب السماح بالاستخدام المشروع لهذه الأجهزة قبل الاستخدام.

ملحق 1
أمن المستخدم النهائي - يجب على الموظفين اتباع متطلبات تأمين سلامة المكتب وإغلاق الشاشة في جميع الأوقات.

ضوابط الأمن السيبراني
لموردي ومقاولي الخدمات المدارة

تأمين سلامة المكتب

تأمين سلامة المكتب (المكتب النظيف - خلو مكتب الموظف من أي معلومات ورقية قد تؤدي الى افصاح البيانات) كما يوحي الاسم مخصص لأمن المعلومات المادية سواء على مكتب الأفراد أو على الطابعة أو أي مكان آخر غير مراقب. توفر النقاط التالية مبادئ توجيهية لتحقيق ذلك:

- يجب قفل المعلومات السرية في حالة عدم استخدامها وعدم تركها بدون رقابة.
- يجب إزالة المعلومات المصنفة من المنطقة المقاربة للطابعات ولا يجب تركها في لوح التجميع بالطابعة.
- من الجيد دائمًا إيقاف تشغيل الطابعات خارج ساعات العمل العادية.
- طريقة سهلة للامتثال لإجراءات تأمين سلامة المكتب هي العمل مع المستندات الإلكترونية كلما أمكن ذلك بطرح سؤال "هل أحتاج إلى طباعة هذا المستند؟"
- إن أخذ النسخ الإلكترونية الممسوحة ضوئيًا بدلاً من النسخ الورقية وحفظها في محرك شبكة آمن مناسب أو عنوان بريد إلكتروني يقلل من خطر وقوع البيانات أو المعلومات غير المراقبة في أيدي غير مصرح لها.
- التأكد من التخلص من المستندات المطبوعة بشكل آمن.
- عدم وضع المستندات التي تحتوي على معلومات شخصية أو حساسة للشركة مطلقا في حاويات النفايات العامة أو تتركها دون رقابة على المكتب.
- عند الاقتضاء، تخزين النسخ الورقية ووسائط الكمبيوتر في حاويات مناسبة عندما لا تكون قيد الاستخدام، حتى أثناء ساعات العمل.
- المواد المصنفة في أماكن مغلقة عند عدم الحاجة إليها، خاصةً عندما يكون المكتب شاغراً.
- استخدام أكياس النفايات السرية أو الصناديق السرية المؤمنة بقفل ومفتاح أو تمزيق المستندات حسب الاقتضاء.
- يجب الاحتفاظ بجميع أجهزة الكمبيوتر وتخزين البيانات المحمولة، مثل وحدات تخزين البيانات والهواتف النقالة وأجهزة الكمبيوتر المحمولة بشكل آمن في نهاية يوم العمل.
- حماية نقاط البريد الواردة والصادرة وأجهزة الفاكس غير المراقبة.
- لا ينبغي ترك بطاقات الهوية التي تتيح الوصول إلى الطباعة دون رقابة ويجب حملها من الموظفين المعنيين في كافة الأوقات.

تأمين الشاشة

- بصفة دائمة قفل / تسجيل الخروج من الأجهزة مثل الأجهزة الطرفية المتصلة بالكمبيوتر أو الطابعات في حالة تركها دون مراقبة.
- في حالة استخدام محطة عمل مشتركة، يجب بتسجيل الخروج بدلاً من قفل المحطة.
- يعد الضغط على CTRL+ALT+DEL أمرًا سهلاً وبسيطًا لقفل الكمبيوتر. ومع ذلك، فإن مجموعة مفاتيح ويندوز أبسط. اضغط على مفتاح windows + L وسيتم قفل جهاز الكمبيوتر الخاص بك تلقائيًا. مفتاح ويندوز في الجزء الأسفل الأيسر من لوحة المفاتيح ويبدو على شكل علم / نافذة.
- كن دائمًا على دراية بموضع الشاشة على محطة العمل الخاصة بك. حيثما كان ذلك ممكنًا، تأكد من أنه لا يمكن رؤيتها من قبل الأشخاص غير المصرح لهم أثناء الاستخدام.
- استخدم شاشة توقف بكلمة مرور، والتي يجب تفعيلها بعد ثلاثة دقائق من عدم النشاط / وقت الخمول.

يجب أيضًا إيقاف تشغيل الشاشات في نهاية يوم العمل.