معايير الأمن السيبرانى
لموردى stc المعتمدين

الغرض

تعتمد **stc** وموردیها المعتمدين على الأداء الموثوق للبنية التحتية الحيوية لضمان استمرارية الأعمال. وتُعد التهديدات الأمنية السيبرانية من أبرز المخاطر التي تستغل التعقيد المتزايد والترابط العالي في أنظمة البنية التحتية الرقمية التي تعرّض أمن **stc** وموردیها المعتمدين، واقتصادهم، وسلامة أصحاب المصلحة للخطر.

ومن الضروري أن يتقيد الموردون المعتمدون بتطبيق معايير الأمن السيبراني الأساسية في **stc** لحماية بيئة أنظمة المعلومات لديهم، ولضمان سرية وسلامة وتوافر الموارد الحيوية.

تشمل الأهداف الرئيسية لتحديد وتطبيق قواعد ومعايير الأمن السيبراني ما يلي:

- حماية سرية وسلامة وتوافر بيانات موردي **stc** من خلال معايير تتعلق بالأفراد والعمليات والتقنيات.
- توفير إطار لتطوير وتنفيذ ومراجعة وصيانة الحد الأدنى من المعايير الأمنية اللازمة لحماية بيانات وأنظمة موردي **stc**.
- حماية موردي stc وموظفيهم وعملائهم من الاستخدام غير المشروع لبيانات وأنظمة الشركة.
- ضمان فعالية المعايير الأمنية على البيانات والأنظمة التي تدعم عمليات موردي **stc**.
- تعزيز الوعي بالأمن السيبراني فيما يتعلق بالمخاطر الحالية والناشئة.
- الالتزام بالمتطلبات القانونية والتنظيمية السارية، بالإضافة إلى حقوق الملكية الفكرية (IPR)

ونظراً لاختلاف المخاطر والأولويات والأنظمة لدى كل مورد من موردي **stc**، فقد تختلف الأدوات والأساليب المستخدمة لتحقيق النتائج الموضحة في المعايير الأساسية.

التعريفات

تنطبق معايير الأمن السيبراني على جميع فرق **stc** التي تتواصل وتدير العلاقات مع موردي **stc** من وكلاء وموزعين وشركات خارجية.
ويقع على عاتق كل فرد معني مسؤولية فهم مدى انطباق هذه الإرشادات، والعمل على توضيح أي استفسارات قد تكون لديه بشأنها.

الخطوات الإجرائية

تصنيف المعايير

الرقم: يتم تخصيص رقم فريد لكل معيار من معايير الأمن السيبراني.
الهدف: يوضح الهدف الأمني السيبراني المطلوب تحقيقه، بغض النظر عن طريقة التنفيذ المستخدمة.
إرشادات التنفيذ: الوسائل المقترحة التي يمكن من خلالها تحقيق هدف المعيار.

تم تضمين أمثلة مناسبة ضمن وثيقة المعايير الأساسية لتسهيل فهم وتطبيق **وثيقة معايير الأمن السيبراني لمزودي الخدمات وموردي stc، بهدف تعزيز حماية الأنظمة والبيانات وضمان الالتزام بأفضل الممارسات الأمنية.**

تصف هذه الوثيقة الأساسية مجموعة من المعايير الأمنية الإلزامية لموردي خدمات **stc**، وهي تُشكّل أساساً أمنياً موحداً لكافة الجهات المعنية، ويجب على جميع موردي **stc** تنفيذها ضمن البنية التحتية المحلية أو البعيدة أو السحابية الخاصة بهم.
وقد اختارت **stc** إعطاء الأولوية لهذه المعايير الإلزامية بهدف تحديد هدف واقعي لتحقيق مكاسب أمنية ملموسة على المدى القريب، والحد من المخاطر بشكل فعّال.

معايير الأمن السيبراني القياسية الإلزامية
الخاصة بموردي stc

معايير إدارة الأصول

نوع المعيار: إلزامي	**المرجع:** ISMS-POL-04 - سياسة إدارة الأصول

الهدف من المعيار:
ضمان تطبيق معايير أمن معلومات كافية على البيانات وأنظمة المعلومات التي تتعامل مع معلومات سرية.

إرشادات التنفيذ:
يجب على موردي الخدمات تطبيق معايير أمن إدارة الأصول التالية:

المعيار 1.1

أ) يجب على مالكي الأصول المعلوماتية والقائمين على حفظها تحديد ما يقع منها تحت مسؤوليتهم، بما في ذلك: المعلومات الإلكترونية، الأصول المادية، المستندات، الأفراد، التطبيقات / البرمجيات، وخدمات معالجة المعلومات. كما يجب الاحتفاظ بجرد رسمي لجميع الأصول تحت عهدتهم.

ب) يجب إبلاغ إدارة **stc** فور فقدان أو سرقة أو سوء استخدام أي من الأصول.

طبيعة الأصل	مثال (لا يقتصر عليه)
بيانات رقمية	قواعد البيانات، ملفات البيانات، وثائق التشغيل والدعم، وغيرها.
أصول مادية	مثل الخوادم، أجهزة الحاسوب المكتبية، جدران الحماية من الاختراق (Firewalls)، الطابعات، الآلات، أجهزة الفاكس، الهواتف، وحدات UPS، أجهزة التبريد، وغيرها.
وثائق/ مستندات ورقية	الأدلة الإرشادية للمستخدم، العقود، الاتفاقيات، إجراءات التشغيل والدعم. تشمل أيضاً الأفراد المطلوبين لدعم وتشغيل الأصول الأخرى.
أفراد	الأشخاص ومؤهلاتهم، مهاراتهم، وخبراتهم.
التطبيقات	البرامج والتطبيقات الرقمية، أنظمة التشغيل.
برمجيات	أدوات التطوير، والبرامج المساعدة.
خدمات	تشمل خدمات الحوسبة والاتصالات، والخدمات العامة.

المعيار 1.2

أ) يتوجب على مالكي المعلومات والقائمين على حفظها التوثيق والصيانة والتحقق من جرد الأصول بشكل دوري.
ومراعاة تسجيل المعلومات التالية لتسهيل التخطيط واستعادة الأصول في حال الانقطاع أو التلف أو الفقدان أو التدمير:

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

المعيار 1.3

يجب إدراج جميع الأصول المعلوماتية في سجل جرد رسمي يتم مراجعته بشكل دوري.

تصنيف الأصول والتعامل معها:
يجب تصنيف الأصول وفقاً لحساسيتها وأهميتها، وتطبيق إجراءات مناسبة للتعامل معها، وتخزينها، ونقلها، والتخلص منها بناءً على هذا التصنيف.

دورة حياة الأصل:
يتحمل مالكو الأصول مسؤولية إدارة الأصول بشكل آمن طوال دورة حياتها، بدءاً من مرحلة الاقتناء وحتى التخلص منها، بما في ذلك محو البيانات أو التخلص منها بشكل آمن.

A

معايير الاستخدام المقبول للأصول

نوع المعيار: إلزامي	**المرجع:** ISMS-POL-04 - سياسة إدارة الأصول

الهدف من المعيار:

ضمان تحديد الاستخدام المقبول وغير المقبول للأجهزة الإلكترونية وموارد الشبكة لدى موردي **stc**، بما يتماشى مع ثقافتهم المؤسسية القائمة على السلوك الأخلاقي والقانوني، والانفتاح، والثقة، والنزاهة.

إرشادات التنفيذ

يجب على موردي **stc**، كحد أدنى، تطبيق المعايير التالية المتعلقة بالاستخدام المقبول للأصول:

المعيار 2.1

يجب وضع قواعد واضحة للاستخدام المقبول للمعلومات والأصول التالية:

- الأصول المعلوماتية
- مرافق معالجة المعلومات
- الموظفون الذين يستخدمون أجهزتهم الشخصية ضمن سياسة "استخدام جهازك الخاص".

المعيار 2.2

- يجب على المستخدمين استخدام الأصول والمصادر المعلوماتية المقدمة فقط لأغراض العمل المشروعة، وحماية سرية معلومات وأعمال **stc**.
- تحتفظ إدارة **stc** بحق الوصول إلى جميع المعلومات المخزنة على أي جهاز تابع لها، ويجب الحصول على تفويض صريح لتعطيل أي خدمات أو أجهزة أو برامج أمنية.
- تحتفظ إدارة **stc** بحق إجراء مراجعات دورية لضمان الالتزام بهذه السياسة، ويجب الإبلاغ عن أي حوادث أو نقاط ضعف مشتبه بها إلى قسم الأمن السيبراني.
- لا يجوز مناقشة نقاط الضعف المشتبه بها مع الزملاء بعد الإبلاغ عنها للجهة المختصة.
- يجب أن يكون استخدام موارد **stc** ضمن الحدود القانونية.
- يجب استخدام أجهزة العمل ووسائل الاتصال وفقاً لسياسة الاستخدام المقبول المحددة.

المعيار 2.3

- تُوفر الموارد التقنية لتسهيل التواصل الإلكتروني الآمن والفعال والأخلاقي في بيئة العمل.
- لا يجوز استخدامها إلا بعد موافقة الإدارة، ولأغراض معتمدة ومن قبل مستخدمين مخولين.
- يقوم فريق تقنية المعلومات بإزالة أي برامج غير مصرح بها من أنظمة المستخدمين.

المعيار 2.4

- يتعين على المستخدمين التنازل لصالح شركة **stc** عن جميع حقوق الملكية الفكرية التي تنشأ أثناء تنفيذهم للمهام الموكلة إليهم بموجب الاتفاقية التعاقدية، بما يشمل كافة حقوق النشر والعلامات التجارية وبراءات الاختراع الحالية والمستقبلية، بالإضافة إلى امتداداتها وتجديداتها، وكافة الحقوق المرتبطة بالمواد الفكرية.
- لا يجوز للمستخدمين أو لأي طرف ثالث يتعامل مع الملكية الفكرية استخدام حقوق الملكية الفكرية أو المواد الفكرية إلا في نطاق تنفيذ المهام المحددة في الاتفاقية، ويحظر عليهم الإفصاح عن أي من هذه المواد لأي جهة أخرى دون الحصول على موافقة خطية مسبقة من إدارة **stc**.
- يجب على المستخدمين تسليم كافة المواد الفكرية والمعدات المملوكة للشركة التي تكون بحوزتهم أو تحت سيطرتهم إلى **stc** فور انتهاء أو إنهاء الاتفاقية التعاقدية لأي سبب، أو عند طلب الشركة ذلك.

ولا يجوز الاحتفاظ بأي نسخ أو سجلات من هذه المواد إلا بموافقة خطية مسبقة من إدارة **stc**.

المعيار 2.5

- يجب استخدام حسابات أنظمة وتطبيقات **stc** (معرّفات الدخول وكلمات المرور) فقط للأغراض المهنية التي تم طلبها والموافقة عليها. ويُمنع مشاركة كلمات المرور تحت أي ظرف.
- يُحظر استخدام حساب المستخدم للمشاركة في أي نشاط مالي شخصي، أو استثمار، أو مسابقة ترويجية، أو ما شابه ذلك.
- يتحمل المستخدمون المسؤولية الكاملة عن حماية أي معلومات يتم استخدامها أو تخزينها أو الوصول إليها من خلال حساباتهم الفردية.
- لا يجوز للمستخدمين الإفصاح عن معلومات **stc** لأي جهة خارج الشركة دون الحصول على تفويض رسمي. وتُعتبر جميع المعلومات المتاحة للمستخدم في إطار عمله معلومات "داخلية"، ما لم يُنص صراحة على خلاف ذلك.
- يُمنع على المستخدمين محاولة الوصول إلى أي بيانات أو برامج موجودة على أي نظام ليس لديهم تفويض أو موافقة خطية صريحة من مالك النظام للوصول إليه.
- تُستخدم وسائل الاتصال الإلكترونية (مثل البريد الإلكتروني وتصفح الإنترنت) فقط للأغراض المهنية المصرح بها. ويُمنع إرسال أو استقبال أو تخزين أي رسائل أو مواد احتيالية أو مسيئة أو فاحشة عبر أنظمة **stc**. وتحظر هذه السياسة بشكل صريح تصفح المواقع أو الرسائل الفاحشة باستخدام مرافق الشركة. وأي انتهاك لذلك سيؤدي إلى اتخاذ إجراءات تأديبية صارمة، قد تشمل إنهاء العقد.
- يُمنع إرسال أي مواد تنتهك قوانين أو أنظمة أو أوامر دولة الكويت.
- لا يجوز للمستخدمين تحميل أي برامج مجانية أو غير مرخصة أو نسخ غير رسمية من البرامج من الإنترنت دون الحصول على تفويض وموافقة مسبقة من قسم الأمن السيبراني في **stc**.

المعيار 2.6 – الأنشطة المحظورة

يُحظر بشكل صارم ممارسة الأنشطة التالية ما لم يُنص عليها صراحة في هذه السياسة:

- تنفيذ اختراقات أمنية أو التسبب في تعطيل الاتصال بالشبكة. وتشمل الاختراقات الأمنية – على سبيل المثال لا الحصر – استخدام أي أدوات أو برامج لتجاوز الضوابط أو السياسات المعتمدة للنظام، تجاوز آليات المصادقة، تعطيل التسجيل، الوصول إلى بيانات لا يُعد المستخدم من المستفيدين المصرّح لهم بها، أو تسجيل الدخول إلى خادم أو حساب دون تفويض صريح، ما لم تكن هذه المهام ضمن نطاق الواجبات الوظيفية المحددة من قبل إدارة المستخدم.
- ويشمل مصطلح "التعطيل" في هذه السياسة – على سبيل المثال لا الحصر – عمليات التنصت على الشبكة، الهجمات المتكررة (Ping Floods)، تزوير الحزم (Packet Spoofing)، هجمات حجب الخدمة (Denial of Service)، وتزوير معلومات التوجيه لأغراض غير قانونية أو أخلاقية.
- يُحظر إجراء فحص المنافذ أو الفحص الأمني بشكل صريح، ما لم يتم إخطار فريق تقنية المعلومات في **stc** مسبقاً والحصول على موافقة رسمية، وذلك في حال كان الفحص جزءاً من تقييم التدقيق السنوي.
- لا يجوز للمستخدمين غير المخولين تنفيذ أي نوع من مراقبة الشبكة التي قد تؤدي إلى اعتراض بيانات غير موجهة إلى جهاز المستخدم.
- يُمنع على المستخدمين نسخ ملفات إعداد النظام لاستخدامهم الشخصي غير المصرح به أو لتقديمها لأشخاص أو مستخدمين آخرين بشكل غير مصرح.
- يُحظر التدخل في أو منع الخدمة عن أي مستخدم، مثل تنفيذ هجمات حجب الخدمة (DoS)

المعيار 2.7

- يُعرّف الاستخدام المهني المقبول بأنه الأنشطة التي تدعم أعمال **stc**.
- يُسمح بالاستخدام الشخصي المحدود أثناء وقت العمل مثل التواصل الشخصي أو الترفيه أو القراءة أو اللعب إذا كان ذلك متاحاً.
- يتم حظر الوصول إلى مواقع معينة أثناء ساعات العمل.
- يُمنع استخدام الأجهزة لتخزين أو نقل مواد غير قانونية أو معلومات ملكية لشركات أخرى أو لمضايقة الآخرين أو للقيام بأنشطة تجارية خارجية.
- يمكن استخدام الأجهزة المحمولة للوصول إلى موارد **stc** مثل البريد الإلكتروني والمستندات.

المعيار 2.8

- يُسمح باستخدام الهواتف الذكية مثل iPhone وAndroid وWindows
- يُسمح باستخدام الأجهزة اللوحية مثل iPad وAndroid.
- يتم دعم مشاكل الاتصال من قبل قسم تقنية المعلومات.

المعيار 2.9

- يجب حماية الأجهزة بكلمة مرور قوية. لمنع أي دخول أو اختراق غير مصرح به.
- سياسة كلمات مرور قوية: 8 أحرف على الأقل، تشمل حروف صغيرة وكبيرة، أرقام، ورموز خاصة. يتم تغييرها كل 45 يوماً، ولا يجوز استخدام أي من آخر 5 كلمات مرور.
- يجب أن يتم قفل الجهاز تلقائياً عند الخمول.
- بعد 5 محاولات دخول فاشلة، يتم قفل الجهاز ويجب التواصل مع فريق تقنية المعلومات.
- يُمنع استخدام الأجهزة المخترقة.
- يُمنع تحميل أو استخدام تطبيقات غير معتمدة.
- يُمنع توصيل الأجهزة غير المعتمدة إلى الشبكة.
- يتم تحديد وصول المستخدمين إلى بيانات **stc** وفقاً لملفات تعريف المستخدم.

المعيار 2.10

- يتخذ فريق تقنية المعلومات كافة الاحتياطات لمنع فقدان بيانات المستخدم الشخصية عند الحاجة إلى مسح الجهاز عن بُعد.
- تحتفظ **stc** بحق فصل الأجهزة أو تعطيل الخدمات دون إشعار مسبق.
- يجب الإبلاغ عن الأجهزة المفقودة أو المسروقة خلال 24 ساعة.
- يجب استخدام الأجهزة بطريقة أخلاقية والالتزام بسياسة الاستخدام المقبول.
- يتحمل المستخدم المسؤولية الكاملة عن أي مخاطر، وتحتفظ **stc** بحق اتخاذ الإجراءات التأديبية المناسبة.

المعيار 2.11

يجب على جميع المستخدمين إعادة أي أصول تابعة للشركة تكون بحوزتهم عند انتهاء الاتفاقية التعاقدية.

معايير تصنيف وحماية المعلومات

نوع المعيار: إلزامي	**المرجع:** ISMS-POL-04 - سياسة إدارة الأصول
الهدف من المعيار: ضمان تصنيف بيانات الشركة بشكل مناسب لتمكين تطبيق مستوى الحماية الملائم لها.	
إرشادات التنفيذ: يجب على موردي **stc** تطبيق معايير تصنيف المعلومات التالية كحد أدنى:	

المعيار 3.1 – تصنيف الأصول المعلوماتية

يجب تصنيف الأصول المعلوماتية لدى **stc** بشكل مناسب ضمن الفئات التالية: **خاص، سري، وعام**، وذلك استناداً إلى المعايير التالية:

- أهمية المعلومات
- المتطلبات القانونية لحمايتها
- القيمة الجوهرية للمعلومات
- درجة الحساسية
- متطلبات السرية، السلامة، والتوافر
- نوع الأصل
- تأثير أي خرق أمني محتمل

المعيار 3.2

- يجب أن تحمل جميع الأصول المعلوماتية (مثل التجهيزات، الملحقات، وسائط البرمجيات، الوثائق الورقية، والمعلومات المخزنة في الأنظمة الحاسوبية) علامات تصنيف واضحة سواء كانت مادية أو إلكترونية، وفقاً لتصنيفها المعتمد.

المعيار 3.3

- يجب التعامل مع الأصول المعلوماتية بطريقة تضمن حمايتها من الإفصاح غير المصرح به أو العرضي، أو التعديل، أو الفقد.
- يجب أن تكون عمليات التعامل، المعالجة، التخزين، والنقل للمعلومات متوافقة مع تصنيفها لضمان الحماية من الوصول غير المصرح به أو سوء الاستخدام.

المعيار 3.4

- يجب استخدام الوسائط المقدمة من **stc** فقط لتخزين أو معالجة أو نقل أو التخلص من البيانات أو المعلومات لأغراض العمل.
- يُمنع استخدام أي وسائط لم يتم توفيرها من قبل **stc**.
- يجب تخزين معلومات **stc** المصنفة على أنها "سرية" على وسائط مشفرة.
- عند توصيل الوسائط بنظام مثل الحاسوب المكتبي أو المحمول، يجب استخدام برامج مكافحة البرمجيات الخبيثة لفحص وإزالة الفيروسات إن وجدت.
- يجب حفظ بيانات **stc** المصرح بها والضرورية فقط على الوسائط.
- يجب اتخاذ إجراءات وقائية لحماية الوسائط والبيانات المخزنة من الفقد أو السرقة أو التلف.
- يجب تقييد الوصول إلى الوسائط لضمان الوصول المصرح فقط.

المعيار 3.5 – التخلص الآمن من البيانات

- يجب محو البيانات من الوسائط قبل إعادة استخدامها أو التخلص منها.
- في حال تلف أجهزة التخزين قبل التخلص منها، وكانت تحتوي على بيانات حساسة، يجب تدميرها مادياً إذا تعذر محوها بشكل آمن.
- يجب كسر أو خدش الوسائط البصرية (مثل الأقراص) عند عدم الحاجة إليها.

المعيار 3.6

- يمكن إرسال الأصول المصنفة على أنها "عامة" عبر البريد المفتوح أو شركات الشحن العادية.
- يجب إرسال الأصول المصنفة على أنها "سرية" أو "خاصة بالشركة" فقط عبر موظفين موثوقين أو من خلال شركات شحن تربطها عقود رسمية مع **stc**.

معايير التحكم في الوصول

نوع المعيار: إلزامي	**المرجع:** ISMS-POL-05 - سياسة إدارة الأصول

هدف المعيار:

السماح بالوصول فقط للمستخدمين المخولين (أو البرمجيات والتطبيقات التي يستخدمونها) بما يتوافق مع المهام الموكلة إليهم، ووفقاً لأهداف المؤسسة ووظائفها التشغيلية.

إرشادات التنفيذ:

يجب على موردي **stc** ، كحد أدنى، تطبيق المعايير التالية المتعلقة بالتحكم في الوصول.

المعيار 4.1 – وصول الموردين إلى أصول المعلومات

تكون مسؤولية طلب الوصول إلى أصول معلومات **stc** من قبل أفراد الطرف الثالث، وكذلك إلغاء هذا الوصول، على عاتق الفريق المعني بالمشروع.

يُمنح الوصول إلى أصول معلومات **stc** للمقاولين أو المستشارين أو أفراد الموردين فقط بناءً على عقد رسمي وتوقيع اتفاقية عدم إفشاء المعلومات (NDA).

ويجب أن تتضمن الاتفاقية ما يلي:

- الشروط والأحكام التي يتم بموجبها منح الوصول
- مسؤوليات المقاولين أو المستشارين أو أفراد الموردين
- التزام المقاولين أو المستشارين أو أفراد الموردين بسياسة stc للأمن السيبراني، بما يشمل المتطلبات الأمنية مثل الحفاظ على سرية المعلومات، وضوابط توزيعها خلال فترة الوصول

المعيار 4.2 – التحكم في الوصول إلى أنظمة المعلومات

يجب تقييد الوصول إلى أنظمة معلومات **stc** للمستخدمين المخولين فقط، وذلك لدعم وتنفيذ متطلبات العمل.
ويتم التحكم في الوصول استناداً إلى ما يلي:

- تصنيف الأصول المعلوماتية من حيث أمن المعلومات.
- الالتزامات القانونية أو التعاقدية التي تفرض قيوداً أو حماية على الوصول إلى الأصول المعلوماتية.
- **معايير الوصول:**
  - **الحاجة إلى المعرفة:** يُمنح الوصول فقط إلى المعلومات اللازمة لأداء الدور الوظيفي، وليس أكثر.
  - **الحاجة إلى الاستخدام:** يُسمح للمستخدمين بالوصول فقط إلى المرافق المادية والمنطقية المطلوبة لأداء مهامهم.
  - **الحماية متعددة الطبقات:** يجب ألا يعتمد الأمن على عنصر حماية واحد، بل على مجموعة من الضوابط المتكاملة.
  - **أقل امتياز:** يجب أن يكون الافتراض الأساسي هو عدم الحاجة إلى الوصول، إلا إذا ثبت خلاف ذلك.

- يجب التحكم في الوصول إلى الأصول المعلوماتية وفي تفعيل حسابات المستخدمين للمقاولين أو المستشارين أو العاملين المؤقتين أو أفراد الموردين المعتمدين، ويكون ذلك فقط أثناء فترة تقديم الخدمة الفعلية لصالح **stc**.
- يُسمح بالوصول عن بُعد إلى شبكة وموارد **stc** فقط بعد التحقق من هوية المستخدمين المخولين، وتقييد صلاحياتهم.
- يجب تقييد الوصول إلى أوامر نظام التشغيل للأشخاص المخولين بأداء وظائف إدارة الأنظمة.
- يجب منح الوصول مع ضمان الفصل بين المهام لتجنب تضارب المصالح.
- يجب ضمان الفصل بين المهام في بيئات التطوير والاختبار والإنتاج.

المعيار 4.3

- يُمنح الوصول إلى خدمات الشبكة حسب الحاجة لدعم متطلبات العمل.
- يجب تقييد الوصول إلى الشبكة للمستخدمين والأنظمة المخولين فقط، وفقاً لمبدأ أقل امتياز.

المعيار 4.4

- يجب على المستخدمين عن بُعد الاتصال بشبكة **stc** فقط من خلال خدمات الوصول عن بُعد المعتمدة والمحددة، وبوابات آمنة، مع ضرورة التحقق من هوية المستخدم وتفويضه.
- توفر **stc** خدمة VPN للمستخدمين بناءً على متطلبات العمل وبعد الحصول على الموافقات اللازمة.

المعيار 4.5 – إدارة أنواع حسابات الوصول
يتم إدارة الوصول إلى الموارد المعلوماتية باستخدام أنواع متعددة من الحسابات، تشمل:

- الحسابات العادية – تُمنح للأفراد لتوفير الحد الأدنى من الموارد المعلوماتية ووظائف النظام اللازمة لأداء مهامهم، دون امتيازات إضافية تتجاوز ما يتطلبه الدور الوظيفي.
- الحسابات ذات الامتياز / حسابات المسؤول – تُمنح للأفراد الذين يؤدون مهام إدارة النظام وصيانة حسابات المستخدمين، أو الذين يديرون موارد معلوماتية مقيدة.

- يجب استخدام الحسابات ذات الامتياز وفقاً للإرشادات التالية:
  - يجب أن يُقتصر تخصيصها على الأفراد الذين تتطلب مهامهم امتيازات إضافية.
  - يجب أن تُخصص الحسابات ذات الامتياز لفرد واحد محدد.
  - يجب ألا يستخدم المسؤول أسماء مثل"Administrator" ، "Admin"، "root"، "superuser" أو مشابهة كمعرّف مستخدم (User-ID) لأداء الأنشطة الإدارية على السيرفرات أو قواعد البيانات أو أجهزة الشبكة.
  - يجب ألا تُسمى معرفات الامتياز بطريقة تُظهر صراحة صلاحيات الحساب، ويُسمح بذلك فقط في الحالات التي تكون فيها استخدامات معرف المستخدم العادي محدودة أو مقيدة أو بسبب ظروف تشغيلية.

المعيار 4.6 – سرية معلومات المصادقة

يجب إلزام المستخدمين بالتوقيع على تعهد بالحفاظ على سرية معلومات المصادقة الشخصية، وكذلك الحفاظ على معلومات المصادقة المشتركة (مثل تلك الخاصة بالمجموعات) ضمن نطاق أعضاء المجموعة فقط. ويمكن تضمين هذا التعهد ضمن الشروط والأحكام الخاصة بالاتفاقية التعاقدية.

- **مراجعة الوصول**
يجب على مالكي الأصول مراجعة صلاحيات الوصول بشكل دوري (على الأقل كل ثلاثة أشهر) لضمان استمرار ملاءمتها، وإلغاء أي امتيازات غير ضرورية.

- **المصادقة متعددة العوامل**
يجب تطبيق المصادقة متعددة العوامل على جميع حالات الوصول عن بُعد، والحسابات ذات الامتياز، والوصول إلى الأنظمة الحساسة.

- **التسجيل والمراقبة**
يجب تسجيل ومراقبة جميع أحداث الوصول والمصادقة، بهدف اكتشاف محاولات الوصول غير المصرح بها والاستجابة لها.

- **الوصول المؤقت**

يمكن منح الوصول المؤقت في حالات استثنائية، بشرط الحصول على موافقة رسمية وتحديد تاريخ انتهاء تلقائي. ويجب مراجعة جميع حالات الوصول المؤقت بعد الاستخدام.

المعيار 4.7 – إلغاء الحسابات وصلاحيات الوصول

يجب تعطيل حسابات المستخدمين وصلاحيات الوصول الخاصة بالأفراد المغادرين قبل انتهاء فترة العقد، وذلك من خلال الإجراءات المناسبة، وبناءً على مدى حساسية نطاق عملهم.

المعيار 4.8 – الوصول إلى شيفرة المصدر

يجب تخزين شيفرة المصدر للبرامج والعناصر المرتبطة بها ضمن مكتبات مخصصة ومنفصلة عن بيئة التشغيل. ويهدف ذلك إلى منع إدخال وظائف غير مصرح بها أو تغييرات غير مقصودة، بالإضافة إلى حماية الملكية الفكرية القيمة.

معايير استخدام التشفير

نوع المعيار: إلزامي	**المرجع:** ISMS-POL-06 - سياسة استخدام التشفير

هدف المعيار:

ضمان الاستخدام السليم والفعّال للتشفير من أجل حماية سرية ومصداقية وسلامة معلومات شركة **stc**، وعملائها، والأطراف الخارجية.

إرشادات التنفيذ:

يجب على موردي stc، كحد أدنى، تطبيق الضوابط التالية فيما يتعلق باستخدام التشفير:

المعيار 5.1

- تعتمد stc المصادقة الثنائية (2FA) لتسجيل الدخول إلى أي خادم/شبكة أو بنية تحتية لتقنية المعلومات تُعد حرجة.
- يجب أن تكون هناك معايير وإجراءات معتمدة لاستخدام ضوابط التشفير في جميع أنظمة تقنية المعلومات والشبكات الحرجة، بهدف حماية معلومات stc الحساسة وعملائها والأطراف الخارجية.
- يتم تطبيق الضوابط اللازمة على الأصول المحددة لضمان قابلية تطبيق التشفير. وبشكل عام، يجب اعتماد تقنيات التشفير المناسبة حسب العملية التجارية أو الحالة ذات الصلة، كما هو موضح في الجدول أدناه:

العملية / الحالة	الحلول / التقنيات المعتمدة
أمن البريد الإلكتروني	حلول البريد الإلكتروني المؤسسي المعتمدة
حماية كلمات المرور على الأنظمة	تطبيقات إدارة كلمات المرور
حماية البيانات المخزنة	تشفير الأجهزة الطرفية
الوصول عن بُعد	الشبكة الخاصة الافتراضية (VPN)
الراوترات	الاتصالات المشفرة
السويتشات	الاتصالات المشفرة
جدران الحماية	الاتصالات المشفرة

المعيار 5.2

- يجب أخذ معايير التشفير بعين الاعتبار، على سبيل المثال لا الحصر، في الحالات التالية:
  - الاتصالات الخارجية.
  - المعلومات السرية المتبادلة عبر الشبكات العامة و/أو المشتركة.
- يجب أن يتوافق استخدام معايير التشفير مع جميع القوانين ذات الصلة وأفضل الممارسات المعتمدة في الصناعة، كما يجب مراجعته بشكل دوري لمواكبة أي تنظيمات جديدة.

معايير الأمن المعنوي والمادي

نوع المعيار: إلزامي	**المرجع:** ISMS-POL-07 - سياسة الأمن المعنوي والمادي

هدف المعيار:

نشر معايير مناسبة للأمن المعنوي والمادي بهدف منع وصول أفراد غير مصرح لهم، أو الاختراق، أو السرقة، أو التلف، أو التدخل في مواقع العمل، ومرافق معالجة المعلومات، ومرافق الاتصالات.

إرشادات التنفيذ:

يجب على موردي **stc** المعتمدين، كحد أدنى، تطبيق المعايير التالية فيما يتعلق بالأمن المعنوي والمادي:

المعيار 6.1

- يجب على الزوار (العملاء، الموردين، البائعين، الزوار الميدانيين، الاستشاريين، والمقاولين) الحصول على إذن مسبق قبل دخول مرافق معالجة المعلومات وغرف الخوادم. ويجب إصدار بطاقات تعريف مؤقتة لزوار أو ضيوف **stc**.
- يتم تقييد الوصول الشخصي إلى المناطق الآمنة لدى **stc** مثل مراكز البيانات أو المناطق التي تُخزن فيها المعلومات الحساسة وتوجد فيها مرافق التحكم التشغيلي، وذلك لمنع أي وصول الأفراد غير الحاصلين على تصريح.
- لا يُسمح باستخدام معدات التصوير أو التسجيل (الفيديو، الصوت، أو أي معدات تسجيل أخرى) في المناطق الآمنة (المناطق المقيدة) دون الحصول على إذن مسبق.

- **تسجيل الدخول:**
يجب استخدام أنظمة التحكم الإلكتروني في الوصول لإدارة وتسجيل الدخول إلى المناطق الآمنة. ويجب الاحتفاظ بسجلات الدخول ومراجعتها بشكل منتظم.

- **الضوابط البيئية:**
يجب تجهيز المناطق الآمنة بأنظمة كشف وإطفاء الحرائق، وضوابط لدرجة الحرارة والرطوبة، ومصادر طاقة احتياطية لحماية المعدات والبيانات

- **إدارة الزوار:**
يجب على الزوار تسجيل الدخول والخروج عند الاستقبال، وارتداء بطاقات تعريف مؤقتة مرئية، وأن يكونوا تحت المرافقة الدائمة أثناء وجودهم في المناطق الآمنة.

المعيار 6.2

- يجب إلغاء حقوق الوصول الشخصي إلى المناطق الآمنة فوراً أو حسب موافقة رئيس القسم عند انتهاء خدمة الموظف أو استقالته، أو عند انتهاء الاتفاقية مع الاستشاري أو البائع.
- يجب تجنب عمل الأطراف الثالثة والبائعين في المناطق الآمنة دون إشراف، وذلك لأسباب تتعلق بالسلامة ولمنع أي أنشطة خبيثة محتملة.
- يجب منح موظفي الدعم أو الخدمات من الأطراف الثالثة وصولاً مقيداً إلى المناطق الآمنة فقط عند الحاجة، ويجب أن يكونوا تحت المرافقة والمراقبة أثناء وجودهم في تلك المناطق. كما يجب تحديد موظفين مناسبين لمرافقة عمال النظافة أثناء عمليات التنظيف الروتينية للمناطق الآمنة.

المعيار 6.3

- يجب صيانة المعدات وفقاً للفترات الزمنية والمواصفات الموصى بها من قبل المورد. ويجب توقيع عقود صيانة سنوية (AMC) أو عقود صيانة وقائية (PM) مع البائعين عند الحاجة
- يجب أن يقوم فقط موظفو الصيانة المعتمدون بإجراء الإصلاحات وصيانة المعدات. ويجب الإشراف على أنشطة الصيانة في الموقع لضمان عدم وصول موظفي الدعم إلى بيانات **stc** دون تصريح.
- يجب الإبلاغ فوراً عن أي خرق أمني شخصي أو نشاط مشبوه، والتحقيق فيه وفقاً لإجراءات إدارة الحوادث.

معايير أمن العمليات

نوع المعيار: إلزامي	**المرجع:** ISMS-POL-08 - سياسة أمن العمليات
هدف المعيار ضمان التشغيل الصحيح والآمن لأنظمة المعلومات، من خلال حماية تلك الأنظمة من البرمجيات الخبيثة وفقدان البيانات، وتسجيل الأحداث ومراقبة الامتثال، والتحكم في برامج أنظمة التشغيل، ومنع استغلال الثغرات التقنية.	
إرشادات التنفيذ: يجب على موردي **stc** المعتمدين، كحد أدنى، تطبيق المعايير التالية فيما يتعلق بأمن العمليات:	

المعيار 7.1

- يجب فصل بيئات التطوير والاختبار والتشغيل لتقليل مخاطر الوصول غير المصرح به أو إجراء تغييرات على بيئة التشغيل.

المعيار 7.2

- يجب تثبيت حلول مكافحة البرمجيات الخبيثة على جميع أنظمة المعلومات لدى **stc**، بما في ذلك الخوادم، وأجهزة الحاسوب المكتبية، والمحمولة. كما يجب نشر حلول وضوابط مكافحة البرمجيات الخبيثة على المستويات التالية:
  - مستوى أجهزة الحاسوب المكتبية
  - مستوى الخوادم
  - نقاط الوصول الحرجة / البوابات المحددة التي تدخل منها المعلومات من المجال العام إلى شبكة stc مثل البريد الإلكتروني وحركة مرور الويب
- يجب على المستخدمين الإبلاغ عن جميع الحوادث المتعلقة بالفيروسات، وأحصنة طروادة، وغيرها من البرمجيات الخبيثة إلى مكتب خدمات تقنية المعلومات في **stc**. ويجب إزالة أجهزة الحاسوب المصابة من الشبكة أو وضعها في منطقة حجر مؤقتة بمجرد تحديدها، إلى أن يتم التحقق من خلوها من الفيروسات.

المعيار 7.3

- يجب تسجيل وتخزين وحماية سجلات الأحداث والاستثناءات والأحداث الأمنية ذات الصلة في أنظمة تقنية المعلومات والشبكات، وفقاً لمتطلبات العمل والتنظيم. كما يجب مراجعة سجلات الأحداث الأمنية، وصيانة معلومات التسجيل، ومراقبة سجلات مسؤولي النظام والمشغلين. ويجب مزامنة الوقت لجميع الأنظمة المتصلة بشبكة **stc** لضمان دقة معلومات السجلات.

  تشمل المعايير ما يلي:
  - تدابير الحماية من الأفراد
  - صلاحيات المسؤولين والمشغلين في حذف أو تعطيل السجلات
  - المصادقة متعددة العوامل للوصول إلى الأصول الحرجة عند الاقتضاء
  - نسخ احتياطي لسجلات التدقيق في مواقع خارجية
  - أرشفة تلقائية للسجلات للحفاظ على سعة التخزين

المعيار 7.4

- يتم إجراء تقييمات دورية للثغرات التقنية بواسطة فريق الأمن السيبراني أو خبراء خارجيين مؤهلين بموجب عقد واضح واتفاقية عدم إفشاء. ويتم تقييم الثغرات التقنية المكتشفة من حيث المخاطر المحتملة ومعالجتها وفقاً لخطة التصحيح.
- يجب تقييم وتطبيق التحديثات والرقع الأمنية في الوقت المناسب للتخفيف من الثغرات المعروفة.

المعيار 7.5

- لا يُسمح للمستخدمين بتثبيت البرامج على أجهزة **stc** ما لم يتم الحصول على إذن خاص بذلك.
- يتحمل الموظفون المعتمدون مسؤولية تثبيت البرامج والتحديثات والرقع الأمنية.

معايير أمن الاتصالات

نوع المعيار: إلزامي	**المرجع:** ISMS-POL-09 - سياسة أمن الاتصالات

هدف المعيار:

ضمان حماية المعلومات ضمن شبكات **stc** والحفاظ على أمن المعلومات المنقولة داخل المنظمة ومع أي جهة خارجية.

إرشادات التنفيذ:

يجب على موردي **stc** المعتمدين، كحد أدنى، تطبيق المعايير التالية فيما يتعلق بأمن الاتصالات:

المعيار 8.1

- يجب تحديد آليات الأمان، ومستويات الخدمة، ومتطلبات الإدارة لجميع خدمات الشبكة، وإدراجها ضمن اتفاقيات خدمات الشبكة. وعند التعامل مع مزودي خدمات خارجيين، يجب تطبيق بروتوكولات الاستعانة بمصادر خارجية كجزء من الاتفاقية.
- يجب أن تكون خدمات المعلومات داخل **stc** مفصولة بشكل مناسب على الشبكة، بما يشمل الفصل بين بيئات الاختبار والتشغيل، وفصل الشبكات الحرجة عن الإنترنت وعن الشبكات الداخلية الأخرى الأقل حساسية باستخدام تقنيات الفصل المناسبة.
- يجب على **stc** ضمان وجود فصل في المهام بين مستخدمي خدمات الشبكة، مع منحهم الحقوق المناسبة وضوابط الوصول الملائمة.

المعيار 8.2

- يجب على **stc** ضمان وجود سياسات وإجراءات للحفاظ على أمن المعلومات المنقولة داخل المنظمة ومع أي جهة خارجية، وتشمل – على سبيل المثال لا الحصر – المجالات التالية:

  - اتفاقيات أمن الشبكات
  - اتفاقيات السرية
  - اتفاقيات عدم الإفشاء

- استخدام الإنترنت
- أمن البريد الإلكتروني
- مرشحات الويب

- يجب أن تتضمن أنظمة البريد الإلكتروني قدرات مكافحة الرسائل المزعجة (Anti-Spam)، ومكافحة التصيد الإلكتروني (Anti-Phishing)، والتشفير، لحماية المستخدمين من التهديدات الشائعة عبر البريد الإلكتروني.
- يجب تأمين الاتصالات مع مزودي الخدمات من الأطراف الثالثة من خلال اتفاقيات تعاقدية وضوابط تقنية لضمان سرية وسلامة المعلومات.
- يجب تشفير جميع البيانات الحساسة المنقولة عبر الشبكات، بما في ذلك رسائل البريد الإلكتروني ونقل الملفات، باستخدام معايير التشفير المعتمدة.
- يجب تحديد الاستخدام المقبول وغير المقبول ضمن شبكة **stc** أو ضمن خدمات المنظمة.

معايير حماية دورة تطوير الأنظمة

نوع المعيار: إلزامي	**المرجع:** ISMS-POL-10 - سياسة حماية دورة تطوير الأنظمة

هدف المعيار

ضمان أن يكون أمن المعلومات جزءاً أساسياً ومتكاملاً في أنظمة المعلومات طوال فترة صلاحيتها، بما في ذلك الخدمات عبر الشبكات العامة، من خلال تطبيق التدابير الأمنية لحماية التطبيقات ومصدر الشيفرة البرمجية أثناء مراحل التصميم والتطوير والصيانة، بالإضافة إلى حماية البيانات خلال مرحلة الاختبار.

إرشادات التنفيذ:

يجب على موردي **stc** المعتمدين، كحد أدنى، تطبيق المعايير التالية فيما يتعلق بحماية دورة تطوير الأنظمة:

المعيار 9.1

يجب أن تخضع عمليات تطوير البرمجيات الخارجية للإشراف والمراقبة من قبل شركة **stc** من خلال اتفاقيات عدم الإفشاء (NDA)، وتقييم المخاطر، والاتفاقيات التعاقدية، واجتماعات مراجعة الإدارة، وذلك حسب ما ينطبق.

يجب تقييد الوصول إلى مستودعات الشيفرة المصدرية وتسجيله، مع استخدام التشفير لحماية الشيفرة أثناء التخزين.

المعيار 9.2

يجب اختبار أي تطبيق تم تطويره ويُخطط لنشره في بيئة الإنتاج بشكل شامل لضمان الامتثال لسياسات stc للأمن السيبراني.

يجب إجراء نمذجة التهديدات وتقييم المخاطر أثناء مرحلة التصميم لتحديد ومعالجة المخاطر الأمنية.

يجب أن تخضع التطبيقات لاختبارات أمنية ثابتة وديناميكية قبل النشر في بيئة الإنتاج، مع معالجة جميع النتائج المكتشفة.

المعيار 9.3

يتطلب الحصول على موافقة من فريق الأمن السيبراني في **stc** قبل أي عملية نشر في بيئة الإنتاج.

عند انتهاء صلاحية التطبيق، يجب التأكد من إزالة جميع الشيفرات المرتبطة بالتطبيق المنتهي من بيئة الإنتاج.

يجب الحفاظ على تفعيل ميزات تتبع التدقيق في أنظمة التطبيقات وقواعد البيانات بشكل دائم.

معايير أمن العلاقة مع الموردين

نوع المعيار: إلزامي	**المرجع:** ISMS-POL-11 - سياسة أمن العلاقة مع الموردين

هدف المعيار

ضمان حماية أصول الشركة التي يمكن للموردين الوصول إليها، والحفاظ على مستوى متفق عليه من أمن المعلومات وجودة تقديم الخدمات بما يتماشى مع الاتفاقيات المبرمة مع الموردين.

إرشادات التنفيذ:

يجب على موردي **stc** المعتمدين، كحد أدنى، تطبيق المعايير التالية فيما يتعلق بأمن العلاقة مع الموردين.

المعيار 10.1

- يجب الاتفاق مع المورد وتوثيق متطلبات أمن المعلومات اللازمة للتخفيف من المخاطر المرتبطة بوصول الموردين إلى أصول معلومات **stc**.
- يجب تنفيذ ضوابط أمنية متوافقة مع المعايير المعتمدة قبل السماح للموردين بالوصول إلى أصول معلومات stc.

وتشمل هذه الضوابط العمليات والإجراءات التي يجب تنفيذها من قبل **stc** وتلك التي يجب تنفيذها من قبل المورد.

- يجب أن تستند الترتيبات مع الموردين التي تتضمن الوصول إلى معلومات **stc** أو معالجتها أو تخزينها أو التواصل بشأنها أو إدارتها، بما في ذلك الأنظمة والمرافق الخاصة بمعالجة المعلومات، إلى اتفاقية رسمية تحتوي على المتطلبات الأمنية اللازمة.

المعيار 10.2

يجب على فريق الأمن السيبراني في **stc**، بالتنسيق مع إدارة علاقات الموردين المعنية، مراقبة ومراجعة البنود والشروط المتعلقة بالأمن السيبراني في الاتفاقيات المبرمة مع الموردين. أما البنود غير المتعلقة بالأمن، فيجب التعامل معها وفقاً لسياسات مشتريات **stc.**

ويجب أن تشمل العمليات ما يلي:

- مراجعة تقارير الخدمة التي يصدرها المورد.
- إلزام الموردين ومقدمي خدمات الإدارة (MS Vendors) بعقد ورش عمل وتوعية بالأمن السيبراني لِفرَقهم بشكل سنوي، وتقديم أدلة تثبت مؤهلاتهم.
- إلزام الموردين بقبول تركيب برامج أو وكلاء أمنية مناسبة على أجهزة فرقهم.
- إلزام الموردين وفِرَقهم بقراءة وفهم جميع سياسات وإجراءات وعمليات الأمن السيبراني.
- التأكد من أن المورد يحتفظ بقدرة خدمية كافية، حيثما ينطبق ذلك.

معايير إدارة الحوادث الأمنية السيبرانية

نوع المعيار: إلزامي	**المرجع:** ▪ **ISMS-POL-12** - سياسة إدارة الحوادث الأمنية السيبرانية ▪ **ISMS-PR01-p03** - إجراء عدم المطابقة والإجراءات التصحيحية ▪ **ISMS-PR10-p01** - إجراء إدارة الحوادث الأمنية السيبرانية

هدف المعيار

ضمان اتباع نهج موحد وفعّال في إدارة الحوادث المتعلقة بأمن المعلومات، بما يشمل التواصل بشأن الأحداث الأمنية ونقاط الضعف.

إرشادات التنفيذ:

يجب على موردي **stc** المعتمدين، كحد أدنى، تطبيق المعايير التالية فيما يتعلق بإدارة الحوادث الأمنية السيبرانية.

المعيار 11.1

- يجب على **stc** اعتماد إطار عمل لإدارة الحوادث الأمنية السيبرانية من خلال وضع إجراء خاص بإدارة حوادث أمن المعلومات، يشمل الجوانب التالية:
  - الإبلاغ الفوري عن الحوادث السيبرانية.
  - تحديد أنواع الحوادث السيبرانية المحتملة والاستجابة لها.
  - تنفيذ الإجراءات التصحيحية المناسبة.
  - إعداد تقرير رسمي للحوادث الحرجة يتضمن وصف الحادث، والإجراءات المتخذة، والتدابير الوقائية الموصى بها.

- يجب أن يؤدي تنفيذ هذه السياسة إلى إنشاء الآليات التالية:
  - رفع مستوى الوعي لدى الموظفين والمقاولين والمستخدمين الآخرين لأنظمة المعلومات
  - توفير قنوات إبلاغ معتمدة لتمكين الأفراد من الإبلاغ عن الحوادث السيبرانية (الانتهاكات الفعلية أو المشتبه بها)
  - توفير الموارد الداخلية أو الخارجية اللازمة لإجراء التحقيقات الجنائية الرقمية عند الحاجة
  - تحديد الإجراءات التصحيحية والوقائية المناسبة للاستجابة للحادث
  - التوصية باتخاذ تدابير استباقية لتجنب تكرار الحوادث المشابهة مستقبلاً، بناءً على الدروس المستفادة

المعيار 11.2

يمكن تحديد حالات عدم المطابقة من أي مصدر، ويشجّع المدير العام للأمن السيبراني في **stc** الموظفين والمستخدمين والعملاء والموردين على اقتراح طرق لمعالجتها.

المعيار 11.3

قد يتم اكتشاف حدث أو حادث أمني سيبراني من قبل أي شخص في **stc**، ويُعد إبلاغ الأشخاص المعنيين في الوقت المناسب أمراً بالغ الأهمية. ولهذا الغرض، يجب توعية جميع الأطراف الخارجية والمستخدمين من الجهات الثالثة، حيثما ينطبق، بآلية الإبلاغ عن مثل هذه الأحداث أو الحوادث، ويجب اتخاذ الإجراءات التالية:

- يجب على الموظف أو الطرف الخارجي أو المستخدم من جهة ثالثة، الذي يلاحظ حدثاً أو حادثاً سيبرانياً أو خللاً وظيفياً، الإبلاغ عنه في أقرب وقت ممكن إلى فريق الأمن السيبراني في **stc** عبر مكتب الخدمة.
- يجب توفير معلومات اتصال شاملة لضمان التواصل الفعّال بين الأشخاص المسؤولين. ويجب تضمين معلومات الاتصال المحدثة مثل خط ساخن خلال ساعات العمل وخط ساخن خارج ساعات العمل، وعنوان البريد الإلكتروني، ورقم الهاتف المحمول عند الحاجة.

المعيار 11.4

قد تكون نقطة الضعف السيبرانية عبارة عن خلل أو ثغرة في نظام المعلومات أو الخدمة، والتي إذا تُركت دون معالجة أو إدارة، قد تؤدي إلى أحداث أو حوادث أمنية سيبرانية. ولهذا الغرض، يجب اتخاذ الإجراءات التالية:

- يجب على الأطراف الخارجية والمستخدمين من الجهات الثالثة الإبلاغ عن أي نقطة ضعف سيبرانية ملحوظة أو مشتبه بها في أنظمة المعلومات أو الخدمات الخاصة بهم إلى فريق الأمن السيبراني في **stc** عبر مكتب الخدمة.
- يجوز لفريق الأمن السيبراني، بالتنسيق مع المدير العام لتقنية المعلومات في **stc**، اتخاذ الإجراءات المناسبة مع مزود الخدمة أو المورد المعني بأسرع وقت ممكن، لمنع وقوع أي حوادث أمنية ناتجة عن تلك الثغرة في النظام أو الخدمة.

معايير ضبط كلمات المرور

نوع المعيار: إلزامي	**المرجع:** ISMS-POL-15 - سياسة كلمات المرور

هدف المعيار

يجب التأكد من استخدام كلمات مرور قوية للوصول إلى المعلومات والأصول المعلوماتية في البيئة.

إرشادات التنفيذ:

يجب أن يكون لدى موردي **stc** المعتمدين، كحد أدنى، إعدادات الضبط التالية المتعلقة بالتحكم في كلمات المرور.

المعيار 13.1

يجب تكوين الأنظمة لضمان تغيير كلمات المرور الأولية والمؤقتة للحسابات الجديدة عند أول تسجيل دخول، كما يجب الاحتفاظ بسجل لآخر خمس كلمات مرور للحساب لمنع إعادة استخدامها.

المعيار 13.2

يجب فرض انتهاء صلاحية كلمات المرور المستخدمة لأول مرة إذا لم يقم المستخدم بالوصول إلى حسابه خلال فترة محددة مسبقاً.

المعيار 13.3

إذا تم تخزين بيانات اعتماد المستخدم في تطبيق أو قاعدة بيانات، فإن مالك البيانات مسؤول عن تنفيذ تدابير الحماية مثل تشفير ملفات بيانات الاعتماد/كلمات المرور. ويجب على القسم المعني التنسيق مع مزود التطبيق لضمان تنفيذ هذا الجانب.

المعيار 13.4

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

المعيار 13.5

يجب أن يتم تكوين جميع التطبيقات والأنظمة بشكل افتراضي بحيث لا يتم عرض كلمات المرور على الشاشة أثناء إدخالها.

المعيار 13.6

يجب على فريق أمن المعلومات في **stc** تقديم تدريب توعوي لجميع المستخدمين (بما في ذلك موظفي الجهات الخارجية والموظفين المتعاقدين) لضمان الالتزام بإجراءات وسياسات كلمات المرور من قبل جميع المستخدمين.

المعيار 13.7

يجب ألا تكون كلمات المرور مستندة إلى اسم الشركة أو موقعها الجغرافي.

المعيار 13.8

يجب على المستخدمين حماية كلمات المرور الخاصة بهم، وهم مسؤولون عن جميع الأنشطة التي تتم من خلال معرف المستخدم الخاص بهم.

المعيار 13.9

يجب عدم مشاركة كلمات المرور.

المعيار 13.10
يجب عدم استخدام كلمة المرور المؤسسية على أي حساب عبر الإنترنت لا يحتوي على تسجيل دخول آمن أو إذا كانت بداية عنوان المتصفح "http://" بدلاً من "https://".

المعيار 13.11
يجب على الجهات الخارجية الالتزام بسياسة stc لكلمات المرور. ويجب أن تتضمن متطلبات قوة كلمة المرور الحد الأدنى من النقاط التالية:

- يجب تحديد الحد الأدنى لعمر كلمة المرور بيوم واحد.
- يجب ألا يقل طول كلمة المرور عن 12 حرفاً.
- يجب الاحتفاظ بسجل لآخر خمس كلمات مرور (تاريخ كلمة المرور) لمنع إعادة استخدامها.
- يجب أن تحتوي كلمة المرور على مزيج من الأحرف وغيرها (أرقام، علامات ترقيم أو رموز خاصة)، أو مزيج من نوعين على الأقل خلافاً للأحرف.
- يجب أن تكون كلمة المرور حساسة لحالة الأحرف، وتحتوي على مزيج من الأحرف الكبيرة والصغيرة مثل (a-z، A-Z).
- يجب تحديد الحد الأقصى لعمر كلمة المرور لحسابات المستخدمين والمسؤولين بأن تكون 90 يوماً.
- يجب أن يكون حد الإغلاق التلقائي للحساب بعد خمس محاولات تسجيل دخول غير صحيحة متتالية.
- يجب تحديد مدة الإغلاق التلقائي للحساب بأن تكون 0 دقيقة، ومدة إعادة التعيين بأن تكون 30 دقيقة.

المعيار 13.12
يجب إبلاغ فريق الأمن السيبراني في **stc** في حال تم التعرف أو الاشتباه أن كلمة مرور أحد المستخدمين قد تم اختراقها.

المعيار 13.13
يجب ألا تستند كلمات المرور إلى ما يلي:

- أشهر السنة، أيام الأسبوع أو أي جانب من جوانب التاريخ (مثل تاريخ الميلاد، تاريخ الانضمام، إلخ).
- أسماء العائلة أو الأحرف الأولى منها.
- أرقام تسجيل المركبات.
- رقم الموظف / معرف الموظف أو المسميات الوظيفية.
- مصطلحات وأسماء الحاسوب، الأوامر، المواقع، الشركات، الأجهزة، البرمجيات.
- أسماء المشاريع أو الأقسام أو الإشارات إليها.
- أسماء الشركات أو معرفاتها أو الإشارات إليها أو كلمات المرور المعروفة علناً مثل: (123456، **stc**، stc1234، admin، password، viva@1234، إلخ).
- أرقام الهواتف أو مجموعات رقمية مشابهة.
- معرف المستخدم، اسم المستخدم، معرف المجموعة أو أي معرف نظام آخر.
- مجموعات رقمية بالكامل أو أبجدية بالكامل.

المعيار 13.14
يجب على مطوري التطبيقات التأكد من أن برامجهم تحتوي على الاحتياطات التالية لأمان كلمات المرور:

- يجب أن تدعم التحقق من هوية المستخدمين الأفراد وليس المجموعات.
- يجب ألا يتم تخزين كلمات المرور بصيغة نصية واضحة أو بطريقة يسهل استرجاعها.
- يجب أن توفر نوعاً من إدارة الأدوار، بحيث يمكن لمستخدم أن يتولى مهام مستخدم آخر دون الحاجة إلى معرفة كلمة مروره.
- يجب أن تدعم بروتوكولات مثل TACACS+، وخدمة المصادقة عن بُعد (RADIUS)، واسترجاع خدمات Active Directory حيثما أمكن.

المعيار 13.15
يجب حفظ كلمات المرور في الذاكرة وعدم كتابتها أو تسجيلها مع معلومات الحساب أو أسماء المستخدمين المرتبطة بها.

معايير ضبط الوثائق

نوع المعيار: إلزامي	**المرجع:** ISMS-PR02-p02 - سياسة ضبط الوثائق
هدف المعيار: ضمان وجود الضوابط والعمليات اللازمة أثناء إنشاء، الوصول إلى، تعديل، تخزين، والتخلص من مخرجات نظام إدارة أمن المعلومات (ISMS).	
إرشادات التنفيذ: يجب على موردي **stc** المعتمدين، كحد أدنى، تطبيق المعايير التالية فيما يتعلق بسياسة ضبط الوثائق.	

المعيار 14.1

- يجب أن يكون جميع المتعاقدين والموردين من الجهات الخارجية على دراية بمسؤولياتهم عند كتابة أو تطوير أو اعتماد أي وثيقة لصالح **stc**.
- توضح هذه الإرشادات متطلبات التوثيق وتؤكد على مدى التزام **stc** بإجراءات التوثيق والتحكم في الإصدارات للوثائق التي يتم كتابتها أو تطويرها أو اعتمادها.
- يُتوقع من المستخدمين الالتزام بالترتيبات الموضحة في هذه الإرشادات والإجراءات، والإبلاغ عن أي ظروف يعتقدون أنها تمثل خرقاً في التحكم أو استخدام الوثائق بالشكل المناسب.
- قد يؤدي انتهاك المتطلبات القانونية للاحتفاظ بالبيانات/السجلات إلى اتخاذ إجراءات تأديبية ضد الفرد، بالإضافة إلى تحمله المسؤولية الشخصية عن العقوبات المدنية و/أو الجنائية من قبل المحاكم أو الجهات القانونية.

المعيار 14.2

- يجب اعتبار جميع الوثائق التي يتم إعدادها في البداية على أنها مسودّات.
- عند مراجعة الوثيقة المسودة، يجب إصدار نسخة منها وتحديثها تدريجياً مع كل مراجعة حتى يتم اعتمادها.
- تصبح الوثيقة المسودة وثيقة معتمدة إذا تم اعتمادها من قبل الجهة المختصة.
- يجب اعتبار أي تغيير جوهري في الوثيقة تغييراً في الإصدار، أما التغييرات البسيطة فيجب اعتبارها مراجعة.
- عند إجراء تغيير في الإصدار أو المراجعة، يجب وضع علامة "تم استبدالها" على الوثيقة السابقة.
- يجب التخلص من النسخ الخاضعة للتحكم عند استبدالها بإصدار/مراجعة جديدة.
- يجب إدراج التغييرات في النسخة الإلكترونية من الوثيقة، ويجب نسخ الوثيقة بالكامل إلى المواقع التي تحتفظ بالنسخ الخاضعة للتحكم.

معايير إدارة استمرارية الأعمال في الأمن السيبراني

نوع المعيار: إلزامي	المرجع: ISMS-PR05-p01 - سياسة إدارة استمرارية الأعمال في الأمن السيبراني

هدف المعيار:

وضع خطط وإجراءات تُستخدم في حالة حدوث انقطاع، وتشمل خطط الطوارئ، وخطط وإجراءات استعادة الكوارث، وخطة استمرارية الأعمال.

إرشادات التنفيذ:

يجب على موردي **stc** المعتمدين، كحد أدنى، تطبيق المعايير التالية فيما يتعلق بسياسة إدارة استمرارية الأعمال في الأمن السيبراني

المعيار 15.1 – إدارة استمرارية الأعمال

- يجب أن تتضمن إدارة استمرارية الأعمال ضوابط لتحديد وتقليل المخاطر التي تؤثر على توفر الخدمات الحيوية، بالإضافة إلى عملية التقييم العام للمخاطر، والحد من تبعات الحوادث الضارة، وضمان توفر المعلومات اللازمة للعمليات التجارية بشكل فوري.
- يجب على مالكي العمليات التجارية تحديد الأحداث الرئيسية التي قد تتسبب في تعطيل عملياتهم، وتوثيق التأثيرات السلبية المحتملة، مثل فئات التأثير التالية:
  - التأثير المالي
  - التأثير على الصحة والسلامة وجودة البيئة
  - التأثير على السمعة
  - التأثير التنظيمي/الامتثال
- يجب أن يكون مالك خطة استمرارية الأعمال مسؤولاً عن تنسيق تحديثات الخطة، بما في ذلك تحديثات الوثائق والإجراءات. ويشمل ذلك، على سبيل المثال لا الحصر:
  - الموقع الحالي ومعلومات الاتصال للأطراف ذات الصلة بالخطة
  - الإجراءات أو العمليات اللازمة لتنفيذ الخطة
  - الاتفاقيات مع الأطراف الخارجية، حسب الاقتضاء
  - قوائم الأصول أو المتطلبات المتعلقة بالخطة
  - مواد التدريب والتوعية والتعليم للمشاركين
  - الوثائق المتعلقة بالأمن السيبراني

معايير إدارة التغيير

نوع المعيار: إلزامي	**المرجع:** ISMS-PR06-p01 - سياسة إدارة التغيير

هدف المعيار: إنشاء نظام فعّال لإدارة التغيير والمحافظة عليه، للتحكم في جميع التغييرات، بما في ذلك أعمال الصيانة الطارئة، والتوثيق، والتحديثات الأمنية، المتعلقة بالبنية التحتية والتطبيقات ضمن بيئة الإنتاج، وتقليل احتمالية حدوث اضطرابات ناتجة عن أخطاء أو تغييرات غير مصرح بها.

إرشادات التنفيذ: يجب على موردي **stc** المعتمدين، كحد أدنى، تطبيق المعايير التالية فيما يتعلق بإجراءات إدارة عمليات التغيير.

المعيار 16.1

- يجب أن تكون وثائق طلب التغيير مصحوبة بمتطلبات تغيير مفصلة وإجراءات تنفيذ مناسبة. كما ينبغي أن تتضمن إجراءات/خطط تفصيلية للتراجع عن التغيير، بالإضافة إلى تقييم الأثر في حال فشل التغيير أو عدم تحقيق النتيجة المرجوة.
- يجب أن تُمكّن عملية إدارة التغيير من التواصل والإبلاغ بجميع التغييرات إلى أصحاب المصلحة الداخليين والخارجيين المتأثرين داخل شركة **stc**.
- يجب المحافظة على منهجية مناسبة للفصل بين المهام لضمان عدم إمكانية تنفيذ التغييرات على أنظمة الإنتاج بشكل فردي.
- يجب اختبار التغييرات في بيئة معزولة ومضبوطة وتمثيلية (عندما تكون مثل هذه البيئة ممكنة) قبل التنفيذ، وذلك لتقليل التأثير على العمليات/الأنشطة التجارية ذات الصلة.
- يجب إجراء اختبار قبول المستخدم لضمان أن التغييرات المنفذة قد حققت الأهداف المتوقعة والمحددة في طلب التغيير.

معايير إدارة التحديثات

نوع المعيار: إلزامي	**المرجع:** ISMS-PR07-p01 - سياسة إدارة التحديثات
هدف المعيار: تقديم المشورة بشأن تحديث الأنظمة بهدف تعزيز حمايتها من الهجمات، وإجراء تقييمات الثغرات الأمنية المتعلقة بشبكة **stc**.	
إرشادات التنفيذ: يجب على موردي **stc** المعتمدين، كحد أدنى، تطبيق المعايير التالية فيما يتعلق بإجراءات إدارة التحديثات.	

المعيار 17.1

- يجب على شركة **stc** إنشاء عملية لتحديد الثغرات الأمنية المكتشفة حديثاً من خلال الوسائل التالية:
  - الاشتراك في قوائم التنبيهات والإشعارات التي تُبلغ عن أي تحديثات أو ترقيات أو تصحيحات جديدة للبرمجيات.
  - الإشعارات المباشرة من البائعين ومزودي البرمجيات.
  - تقارير تقييم الثغرات الصادرة عن فريق الأمن السيبراني.
- يجب أن تحتوي جميع أنظمة تقنية المعلومات والشبكات على أحدث التحديثات / التصحيحات / الحزم الخدمية / الإصلاحات العاجلة، وفقاً للجداول الزمنية المخطط لها.
- يجب وجود آلية لاختبار التحديثات / التصحيحات / الحزم الخدمية / الإصلاحات العاجلة لجميع الأنظمة والتطبيقات الحيوية للأعمال في بيئة اختبارية قبل تطبيقها على الأنظمة الحية.
- لضمان تنفيذ التصحيحات بشكل منتظم وتحت رقابة متوقعة، يجب إنشاء جدول زمني مخصص للتصحيحات.
- يجب تنفيذ نشر التصحيحات من خلال عملية إدارة التغيير حسب ما هو معمول به.
- يجب تقدير فترة التوقف المحتملة، إن وجدت، أثناء نشر التصحيحات في بيئات الإنتاج، مع اتخاذ الترتيبات اللازمة لإبلاغ المستخدمين مسبقاً أو جدولة التوقف خارج ساعات العمل.
- يجب أن تكون هناك آليات للتراجع في حال حدوث مشكلات غير متوقعة، بحيث يمكن إعادة النظام إلى حالته السابقة.
- يجب نشر التصحيحات الخاصة بمعالجة الثغرات من نوع "Zero-Day" فور إصدارها من قبل البائع، ووفقاً للجداول الزمنية المحددة.
- في حال عدم توفر التصحيحات، يجب على البائعين تنفيذ ضوابط تعويضية / حلول بديلة لتخفيف المخاطر ضمن اتفاقية مستوى الخدمة (SLA) المتفق عليها.

معايير نقل المعلومات

نوع المعيار: إلزامي	**المرجع:** ISMS-PR08-p01 - سياسة نقل المعلومات
هدف المعيار: حماية المعلومات بشكل كاف لأسباب قانونية مثل السرية أو حماية البيانات، وللحفاظ على ثقة مستخدمي الخدمة وشركائنا.	
إرشادات التنفيذ: يجب على موردي **stc** المعتمدين، كحد أدنى، تطبيق المعايير التالية فيما يتعلق بإجراءات نقل المعلومات.	

المعيار 18.1 – استخدام نظام البريد الإلكتروني وإدارته

- يُعد نظام البريد الإلكتروني ملكاً لشركة **stc**، وتُعتبر جميع الرسائل التي يتم إنشاؤها أو إرسالها أو استلامها أو تخزينها ضمن النظام ملكاً لشركة **stc**
- تحتفظ **stc** بحقها، بعد الحصول على موافقة اللجنة الإدارية، في مراجعة وتدقيق واعتراض والوصول إلى ومراقبة وحذف وكشف جميع الرسائل التي يتم إنشاؤها أو إرسالها أو استلامها أو تخزينها ضمن نظام البريد الإلكتروني.
- توفر **stc** أنظمة المعلومات والاتصالات الإلكترونية بهدف دعم احتياجاتها ومصالحها التجارية.
- يُقتصر الوصول إلى الرسائل الإلكترونية على الموظفين المخولين فقط.
- لا يجوز استخدام موارد معلومات **stc** في إرسال أو استقبال أي محتوى يحتوي على مواد مسيئة أو تشهيرية أو تهديدية للآخرين.

- يجب أن تتضمن أي رسالة بريد إلكتروني قد تُفهم على أنها تمثل **stc** التنويه التالي:
  - ❖ *قد تحتوي هذه الرسالة على معلومات تتعلق بشركة* **stc** *، وذلك بسبب العلاقة التعاقدية الشخصية للمرسل مع* **stc.**
- لا تتحمل **stc** أي مسؤولية عن محتوى هذه الرسالة أو عن أي تصرفات يتم اتخاذها بناءً على المعلومات الواردة فيها، ما لم يتم تأكيد تلك المعلومات لاحقاً بشكل رسمي ومكتوب من قبل **stc.**
- يجب تعطيل أو إزالة حسابات البريد الإلكتروني التي تم إنشاؤها للموظفين الخارجيين أو مقدمي الخدمات أو الأطراف الثالثة عند انتهاء التعاقد أو الاتفاق مع **stc**.
- يجب على كل مستخدم اتخاذ التدابير اللازمة لمنع الاستخدام غير المصرح به لحسابات البريد الإلكتروني، ويُعد المستخدم مسؤولاً شخصياً عن جميع الرسائل الصادرة من حسابه. يُمنع تماماً تزوير معلومات رأس الرسالة (بما في ذلك عنوان المصدر، عنوان الوجهة، والطوابع الزمنية).
- لا يجوز استخدام أنظمة **stc** في إرسال أو استقبال الأسرار التجارية أو المواد المحمية بحقوق النشر أو المعلومات الملكية أو السرية.
- تُعد المعلومات السرية، بما في ذلك الاتفاقيات القانونية أو التعاقدية والمعلومات الفنية المتعلقة بعمليات **stc** أو أمنها، غير قابلة للإرسال عبر البريد الإلكتروني دون اتخاذ التدابير الكافية لحمايتها من الوصول غير المصرح به.
- تحتفظ **stc** بحقها في مراقبة أو تقييد الوصول إلى البريد الإلكتروني عبر الإنترنت. ويتحمل المستخدمون مسؤولية عدم الوصول إلى بريد **stc** الإلكتروني من الأنظمة العامة مثل أجهزة الإنترنت في المقاهي. وفي حال الضرورة القصوى لاستخدام جهاز عام، يجب على المستخدم التأكد من حذف جميع النسخ المؤقتة أو المحلية للرسائل والمرفقات، وعدم حفظ بيانات الدخول على الجهاز.

المعيار 18.2 – حجم صندوق البريد الإلكتروني وتصفية المحتوى

- الحجم الافتراضي لصندوق البريد الإلكتروني لموظفي **stc** هو **1.1GB**، وللمتعاقدين هو **110MB.** ومع ذلك، يمكن للمستخدمين طلب زيادة في حجم صندوق البريد بشرط وجود سبب تجاري مبرر وموافقة مناسبة.
- يجب تكوين حلول تصفية المحتوى لحظر الرسائل المشبوهة في البريد الإلكتروني.

المعيار 18.3 – استخدام الإنترنت

- يُمنح استخدام الإنترنت فقط لغرض دعم الأنشطة التجارية اللازمة لأداء المهام الوظيفية.
- لا يجوز للموظفين أو المتعاقدين أو العملاء أو الموردين أو الاستشاريين استخدام أي نوع آخر من الاتصالات عند اتصال النظام أو الجهاز بشبكة **stc** الداخلية.

المعيار 18.4 – حماية المحتوى من الإنترنت

- يجب فحص جميع المحتويات التي يتم تنزيلها من الإنترنت عند بوابة الشبكة وعند أجهزة المستخدمين لضمان خلوها من أي رموز ضارة مثل الفيروسات أو أحصنة طروادة أو الديدان الإلكترونية.
- لا يُسمح للمستخدمين بتنزيل أو تحميل أي برامج من/إلى الإنترنت دون الحصول على موافقة مسبقة.
- يجب استخدام خدمة الإنترنت لتعزيز مساهمة المستخدمين المهنية في الشركة. كما يجب على جميع المستخدمين التأكد من استخدامهم لخدمات الإنترنت بطريقة أخلاقية وقانونية لتجنب أي مسؤولية قانونية على **stc.**

المعيار 18.5 – الاستخدام غير المقبول لخدمات الإنترنت

- يجب أن يكون المستخدمون على علم بأن **stc** لا تتحمل أي مسؤولية عن تعرضهم لمحتوى مسيء قد يتم الوصول إليه عبر الإنترنت.
- لا يجوز للمستخدمين الوصول إلى المواقع المحجوبة من قبل الجهات الحكومية، كما يُمنع زيارة المواقع غير الرسمية أو المشبوهة.
- فيما يلي أمثلة توضيحية عن الاستخدام غير المقبول لخدمات الإنترنت:
  - إرسال أي محتوى مسيء أو تحرشي أو احتيالي، أو ينتهك القانون أو يسيء إلى سمعة الشركة أو الجهات الرسمية.
  - ممارسة الأعمال الشخصية باستخدام موارد الشركة.
  - تنزيل برامج غير مرخصة.
  - إرسال رسائل أو ملفات تحتوي على تهديدات.
  - إرسال رسائل أو ملفات ذات طابع تحرشي جنسي أو عنصري.
  - إرسال ملفات تحتوي على فيروسات أو رموز خبيثة أخرى.
  - محاولة الوصول إلى الأنظمة دون الحصول على التصريحات اللازمة.
  - إرسال أو نشر معلومات سرية لأشخاص غير مخولين.
  - نشر معلومات التكوين أو تفاصيل الثغرات المحتملة في البنية التحتية لتقنية المعلومات الخاصة بشركة **stc** على النطاقات العامة.
  - الوصول إلى أو تنزيل المواقع أو الصور أو الأغاني أو النكات أو الرسوم المتحركة أو الأفلام أو أي مواد أخرى تحمل طابع إباحي أو عنصري أو غير قانوني.
  - استخدام الإنترنت للوصول إلى مواقع تروّج للمقامرة أو لتحقيق مكاسب تجارية شخصية أو لغسل الأموال.
  - إنشاء اتصالات عبر الإنترنت أو شبكات خارجية قد تتيح لمستخدمين غير تابعين لشركة **stc** الوصول إلى أنظمة وتطبيقات الشركة.
  - التدخل المتعمد في التشغيل الطبيعي لبوابة الإنترنت.
  - لا يُسمح باتصالات خدمة المحطّة الطرفية (Terminal Service) غير المؤمنة الواردة أو الصادرة عبر الإنترنت.
  - يُحظر استخدام خدمات المحادثة الداخلية (IRC) وخدمات مشاركة الملفات من نظير إلى نظير (P2P).

نوع المعيار: إلزامي	**المرجع:** ISMS-PR09-p01 – إجراءات حوكمة موردي الأمن السيبراني
هدف المعيار: وضع القواعد الأساسية لإدارة أمن الطرف الثالث (مثل الموردين والبائعين وغيرهم) الذين يمتلكون وصولاً مباشراً أو غير مباشر إلى أنظمة وبيانات **stc.**	
إرشادات التنفيذ: يجب على موردي **stc** المعتمدين، كحد أدنى، تطبيق المعايير التالية فيما يتعلق بإجراءات حوكمة موردي الأمن السيبراني.	

المعيار 19.1

يجب على موردي خدمات الإدارة (MS Vendors) استخدام الضوابط الأساسية المعتمدة من **stc** وقائمة التقييم لتطوير خطة فعالة لتقييم الأمن، بهدف جمع وتحليل المعلومات اللازمة لتحديد مدى كفاءة الضوابط الأمنية المطبقة في نظام المعلومات. عند إعداد خطة التقييم، ينبغي أخذ المعلومات المتوفرة مسبقاً حول الضوابط الأمنية بعين الاعتبار.

المعيار 19.2

يمكن استخدام المعلومات الناتجة عن تقييم الضوابط الأمنية من قبل موردي خدمات الإدارة في الأمور التالية:

- تحديد نقاط الضعف والقصور في نظام المعلومات.
- التأكد من معالجة النقاط الضعيفة والمشكلات التي تم تحديدها.
- دعم قرارات الميزانية والاستثمار في البنية التحتية.

المعيار 19.3

يلتزم موردي خدمات الإدارة تعاقدياً وتشغيلياً بالامتثال للمتطلبات التجارية والأمنية والتنظيمية الخاصة بشركة **stc**. ويجب تضمين المتطلبات التالية في الاتفاقيات مع الأطراف الخارجية:

- توقيع اتفاقية عدم إفشاء تنص صراحة على منع أي شخص لديه وصول إلى منشآت stc أو معلوماتها الخاصة من مشاركة أي معلومات دون إذن كتابي من **stc**.
- التزام الطرف الثالث بإبلاغ **stc** في حال وقوع حادث أمني لديه قد يؤثر على **stc** (مثل انتشار فيروس أو اختراق ناجح لشبكته).
- التزام الطرف الثالث بالحفاظ على سرية وسلامة وتوافر معلومات **stc.**
- إمكانية إعادة التفاوض أو إنهاء العقد في حال عدم الالتزام بالشروط، مثل عدم الإفصاح عن حادث أمني أو عدم تحقيق مستويات الخدمة المتفق عليها.
- معالجة قضايا التعاقد من الباطن في حال استعانة الطرف الثالث بموردين آخرين لتقديم الخدمات، ويجب أن يلتزم هؤلاء الموردون بمعايير **stc** للأمن والامتثال التنظيمي.
- وجود ضوابط لضمان أمان الاتصالات عن بُعد بين الطرفين، ويجب على الطرف الثالث استخدام البنية التحتية الأمنية الخاصة بشركة **stc** وتحمل مسؤولية صيانتها.
- تحديد ملكية التراخيص والملكية الفكرية، بما في ذلك اتفاقيات الحفظ الاحتياطي (escrow).
- إدراج بند "الحق في التدقيق" يسمح للإدارة أو ممثل مفوض بتقييم بيئة الضوابط لدى الطرف الثالث بشكل مادي أو منطقي.
- تحديد نوع وحجم وتكرار الملفات أو التقارير التي سيتم تبادلها بين الطرفين.
- وضع ترتيبات لاستمرارية الأعمال والتعافي من الكوارث لضمان استئناف خدمات الطرف الثالث في حال انقطاع الخدمة أو فقدان/تلف البيانات.

معايير النسخ الاحتياطي للمعلومات

نوع المعيار: إلزامي	**المرجع:** ISMS-PR12-p01 – إجراءات النسخ الاحتياطي
هدف المعيار: التأكد من إجراء نسخ احتياطي منتظم لبيانات المستخدمين، والمعلومات المؤسسية (مثل رسائل البريد الإلكتروني، والمعاملات، وسجلات العملاء، وخطط الأعمال)، بالإضافة إلى بيانات الأنظمة المخزنة في أنظمة المعلومات الخاصة بشركة **stc**.	
إرشادات التنفيذ: يجب على موردي **stc** المعتمدين، كحد أدنى، تطبيق المعايير التالية فيما يتعلق بإجراءات النسخ الاحتياطية للمعلومات.	

المعيار 20.1

يجب تحديد وتوثيق وإجراء نسخ احتياطي للبيانات الحيوية الخاصة بالمؤسسة، بما في ذلك على سبيل المثال لا الحصر:

- بيانات المستخدمين: مثل مستخدمي الأنظمة والتطبيقات، ومعلومات الموظفين.
- بيانات الأنظمة: مثل أنظمة التشغيل، وبرمجيات التطبيقات، والتراخيص.
- البيانات التجارية: مثل بيانات العملاء، وخطط الأعمال، ورسائل البريد الإلكتروني، ومعلومات المنتجات وغيرها.

المعيار 20.2

يجب تحديد وتوثيق استراتيجية النسخ الاحتياطي، بحيث تشمل ما يلي:

- أنواع البيانات التي يجب نسخها احتياطياً، مثل البيانات المؤسسية، وبيانات المستخدمين، وبيانات الأنظمة.
- أنواع طرق النسخ الاحتياطي التي سيتم استخدامها، مثل النسخ الكامل الأسبوعي والشهري، والنسخ التفاضلي والنسخ التزايدي خلال أيام الأسبوع، مع الرجوع إلى الجدول أدناه لتحديد الطريقة المناسبة حسب احتياجات العمل المختلفة.

الشروع بالنسخ الاحتياطي المجدول	الحاجة
طلب نسخ احتياطي	إذا كانت هناك حاجة عمل لنسخ أي معلومات احتياطياً، فيجب تقديم طلب، وسيتم تفعيل هذا الإجراء.
طلب نسخ احتياطي طارئ / استجابة طارئة	في حالة حدوث تغيير عاجل أو كارثة، يتم تقديم طلب نسخ احتياطي طارئ، وسيتم تفعيل هذا الإجراء.
طلب نسخ احتياطي مشروط (طلب تغيير / تنفيذ تصحيح)	التأكد من تنفيذ إجراءات النسخ الاحتياطي والاستعادة بشكل صحيح.
خطة نسخ احتياطي دورية	في حال وجود طلب نسخ احتياطي دوري، سيتم تفعيل هذا الإجراء.
إدارة توفر النسخ الاحتياطية	في حال وقوع كارثة، سيتم تفعيل توفر النسخ الاحتياطي للطوارئ، وسيتم تفعيل هذا الإجراء.

- فترة الاحتفاظ بالبيانات المنسوخة احتياطياً:
  يجب تحديد فترة الاحتفاظ بالنسخ الاحتياطية وفقاً لسياسة **stc** المعتمدة، كما هو موضح في الجدول أدناه، لضمان توفر البيانات عند الحاجة والتوافق مع المتطلبات التنظيمية والتشغيلية.

خارج الموقع	في الموقع	عدد النسخ	فترة الحفظ	المالك	التكرار	نوع النسخ الاحتياطي	النظام
نعم	نعم	2	شهر واحد	مدير التطبيق	النسخ اليومي	قاعدة البيانات	كل النظم
نعم	نعم	2	3 أشهر	مدير التطبيق	نسخة كاملة اسبوعياً		
نعم	نعم	1	6 أشهر	مدير التطبيق	نسخة كاملة شهرياً	نظام الملفات	
نعم	نعم	1	شهر واحد	مدير التطبيق	النسخ اليومي		
نعم	نعم	2	لا تتلف	مدير التطبيق	النسخ اليومي	التسجيلات الصوتية	
نعم	نعم	2	لا تتلف	مدير التطبيق	النسخ اليومي	تسجيلات المحادثات	
نعم	نعم	2	3 أشهر	مدير التطبيق	النسخ اليومي	التبادل	
نعم	نعم	2	لا تتلف	مدير التطبيق	نسخة كاملة شهرياً		

- أمن البيانات المنسوخة احتياطياً:
  يجب تأمين النسخ الاحتياطية باستخدام وسائل مثل التشفير، والتخزين في مواقع خارجية (offsite)، وإجراء اختبارات استرجاع دورية لضمان سلامة البيانات وقابليتها للاسترجاع.
- متطلبات النسخ الاحتياطي على وسائط التخزين: يجب تحديد نوع وسائط النسخ الاحتياطي المستخدمة، سواء كانت أشرطة (tapes)، أقراص (disks)، أو مزيجاً من الاثنين، بناءً على حجم البيانات، وتكرار النسخ، ومتطلبات الاسترجاع.

- **المعيار 20.3:** تنفيذ النسخ الاحتياطي وفقاً للاستراتيجية المحددة.
- **المعيار 20.4:** تخزين النسخ الاحتياطية في مواقع آمنة داخلية، مثل خزائن مقاومة للحريق في حال استخدام الأشرطة.
- **المعيار 20.5:** حفظ نسخة ثانية من النسخ الاحتياطية في موقع بعيد، إما إلكترونياً أو عبر شحن الوسائط فعلياً.
- **المعيار 20.6:** استخدام التواقيع الرقمية والتجزئة التشفيرية لضمان سلامة النسخ الاحتياطية.
- **المعيار 20.7:** ضمان توفر النسخ الاحتياطية لاستمرارية الأعمال من خلال اختبار الاسترجاع باستخدام أسلوب العينات.

معايير تصنيف المعلومات

نوع المعيار: إلزامي	**المرجع:** ISMS-PR12-p03 – إجراءات تصنيف المعلومات
هدف المعيار: وضع آلية لتصنيف بيانات/معلومات شركة **stc** بناءً على مستوى حساسيتها، قيمتها، وأهميتها الحيوية للشركة.	
إرشادات التنفيذ: يجب على موردي **stc** المعتمدين، كحد أدنى، تطبيق المعايير التالية فيما يتعلق بتصنيف المعلومات.	

المعيار 21.1

يعتمد تصنيف المعلومات في **stc** على مدى سريتها، وسلامتها، وتوافرها. يوضح الجدول أدناه مستويات تصنيف المعلومات:

المستوى	الوصف
متاح للعموم	ينطبق هذا التصنيف على المعلومات المتاحة للجمهور العام والمخصصة للتوزيع خارج الشركة. يمكن نشر هذه المعلومات بحرية دون أن يترتب على ذلك أي ضرر محتمل. وعلى الرغم من عدم وجود قيود على الإفصاح لحماية البيانات العامة (نظراً لأن المعلومات متاحة للعرض العام)، يجب تطبيق حماية كافية لمنع التعديل غير المصرح به لهذه المعلومات. ينطبق هذا التصنيف على المعلومات التي يُقصد نشرها وتوزيعها.
مخصص للاستخدام الداخلي فقط	ضمن نطاق الشركة، لا يُتوقع أن يؤدي الكشف أو التعديل أو الإتلاف غير المصرح به لهذه البيانات إلى تأثير خطير أو سلبي على **stc** أو موظفيها أو أصحاب المصلحة. ينطبق هذا التصنيف على المعلومات التي تُعتبر خاصة، أي التي يمكن الوصول إليها فقط من قبل عدد محدود من الموظفين.
سري	ينطبق هذا التصنيف على المعلومات التي تُعتبر خاصة، والتي يقتصر الوصول إليها على عدد محدود من الموظفين فقط. قد يؤدي الكشف غير المصرح به إلى تأثير سلبي على المنظمة وموظفيها وأصحاب المصلحة. تشمل هذه الفئة الأصول المعلوماتية التي تخضع لمتطلبات قانونية تمنع الكشف غير المصرح به أو تفرض عقوبات مالية في حال حدوثه. وتشمل معلومات يحظر كشفها وفقاً للقوانين والأنظمة المحلية المرعية الإجراء، مثل سجلات المخاطر، وتقارير التدقيق، والمعلومات المالية.
سري للغاية	ينطبق هذا التصنيف على المعلومات عالية الحساسية التي قد يؤدي الكشف عنها إلى إلحاق أضرار جسيمة بعمليات stc أو سمعتها أو موقعها التنافسي، أو قد يترتب عليه تبعات قانونية أو تنظيمية خطيرة. ويُقصر الوصول إلى هذه المعلومات بشكل صارم على الأفراد المخوّلين صراحةً، ووفق مبدأ الحاجة إلى المعرفة فقط. وتشمل الأمثلة على ذلك الخطط الاستراتيجية التنفيذية، وبنية الأمن السيبراني، وبيانات الاعتماد للأنظمة الحيوية، والمفاتيح الخاصة، والاتفاقيات أو البيانات ذات الطابع الوطني.

المعيار 21.2

يوضّح الجدول التالي معايير أمن المعلومات والضوابط المطلوبة لحماية المعلومات استناداً إلى تصنيفها. إضافةً إلى معايير أمن المعلومات التالية، يجب أن تلتزم أي معلومات تخضع للقوانين أو اللوائح الحكومية أو الاتفاقيات التعاقدية بمتطلبات الأمان المحددة في تلك القوانين أو اللوائح أو العقود.

الفئة	معلومات سرية	معلومات مقيدة للشركة	معلومات عامة
فئة التحكم الأمني	تتطلب المصادقة والتفويض للوصول. يجب توقيع اتفاقية سرية	التفويض من مالك المعلومات أو من ينوب عنه، بالإضافة إلى موافقة المشرف	لا توجد قيود على العرض
الطباعة/النسخ	يجب أن تكون النسخ محدودة للأفراد المخولين والموقعين على اتفاقية سرية. يجب عدم ترك المعلومات على الطابعة دون مراقبة	يجب أن تكون النسخ محدودة للأفراد الذين لديهم حاجة معرفية. يجب عدم ترك المعلومات على الطابعة دون مراقبة	لا توجد قيود
أمن الشبكة	يجب أن تكون الخوادم غير مرئية للإنترنت بالكامل أو للشبكات غير المحمية. يجب مراجعة قواعد الجدار الناري دورياً	الحماية بجدار ناري باستخدام قواعد «الرفض الافتراضي» مطلوبة. يجب أن تكون الخوادم غير مرئية للإنترنت	يمكن أن تكون على شبكة عامة. يُوصى بالحماية بجدار ناري
أمن النظام	يجب اتباع أفضل الممارسات الخاصة بشركة stc ونظام التشغيل. جدار ناري وبرمجيات IDS/IPS مطلوبة	يجب اتباع أفضل الممارسات الخاصة بشركة stc ونظام التشغيل. جدار ناري مطلوب، IDS/IPS موصى بها	يجب اتباع الممارسات العامة. يُوصى بجدار ناري
البيئات الافتراضية	لا يمكن مشاركة نفس البيئة الافتراضية مع خوادم أخرى ذات تصنيفات مختلفة	يُفضل عدم مشاركة البيئة الافتراضية مع خوادم أخرى ذات تصنيفات مختلفة	يمكن الاستضافة في بيئة افتراضية، وتطبق نفس الضوابط
الأمن الفيزيائي	يجب أن يكون النظام في مركز بيانات آمن. يجب مراقبة وتسجيل الوصول الفيزيائي	يجب أن يكون النظام في موقع آمن. يُوصى بمركز بيانات آمن	يجب قفل أو تسجيل الخروج من النظام عند تركه دون مراقبة
الوصول عن بُعد	الوصول مقيد بشبكة محلية أو VPN آمن. لا يُسمح بالدعم الفني غير المراقب	الوصول مقيد بشبكة محلية أو VPN عام. يُسمح بالدعم الفني المؤقت عبر بروتوكولات آمنة	لا توجد قيود
تخزين المعلومات	التخزين على خادم آمن ومركز بيانات مطلوب. يجب استخدام تشفير كامل للقرص	التخزين على خادم آمن ومركز بيانات موصى به. لا يُفضل التخزين على أجهزة شخصية	يُوصى بالتخزين على خادم آمن
النقل	التشفير مطلوب (مثل SSL أو بروتوكولات نقل آمنة). لا يمكن الإرسال عبر البريد الإلكتروني إلا إذا كان مشفراً وموقعاً رقمياً	لا توجد متطلبات	لا توجد قيود
النسخ الاحتياطي/التعافي	نسخ احتياطي يومي مطلوب. التخزين الخارجي في موقع آمن مطلوب	نسخ احتياطي يومي مطلوب. يُوصى بالتخزين الخارجي	يُوصى بالنسخ الاحتياطي اليومي

الفئة	معلومات سرية	معلومات مقيدة للشركة	معلومات عامة
التدريب	تدريب على أمن المعلومات مطلوب. تدريب على السياسات واللوائح مطلوب	تدريب على أمن المعلومات مطلوب. تدريب على إدارة النظام مطلوب	يُوصى بالتدريب العام على الأمن. يُوصى بتدريب إدارة النظام
جدول التدقيق	سنوي	حسب الحاجة	حسب الحاجة

المعيار 21.3

لضمان تطبيق معايير العقود المناسبة على الأصول المعلوماتية لشركة **stc**، سيتم استخدام نظام للوسم الوقائي بحيث يكون جميع الأطراف الخارجية، عند الاقتضاء، على دراية بكيفية إدارة تلك المعلومات.

المعيار 21.4

تُفرض معايير صارمة على استخدام الوسائط القابلة للإزالة مثل الأقراص المدمجة **(CDs)**، وأقراص الفيديو الرقمية **(DVDs)**، والأشرطة، والأقراص الصلبة الخارجية، وفلاشات **USB** داخل شركة **stc** حيث يتوجب الحصول على تفويض مسبق قبل الاستخدام المشروع لهذه الأجهزة.

ملحق - 1

أمن المستخدم – يجب على الموظفين الالتزام بمتطلبات المكتب النظيف والشاشة النظيفة في جميع الأوقات.

المكتب النظيف (Clear Desk)

يشير مفهوم المكتب النظيف إلى حماية المعلومات المادية الموجودة على مكتب الموظف أو على الطابعة أو في أي موقع غير مراقب. وفيما يلي إرشادات لتحقيق ذلك:

- يجب حفظ المعلومات السرية في مكان آمن عند عدم استخدامها، وعدم تركها دون رقابة.
- يجب إزالة المعلومات المصنفة من محيط الطابعات وعدم تركها في سلة التجميع الخاصة بالطابعة.
- يُفضل دائماً إيقاف تشغيل الطابعات خارج ساعات العمل الرسمية.
- من الطرق السهلة للامتثال لإجراء المكتب النظيف هو العمل على المستندات الإلكترونية قدر الإمكان، وطرح سؤال: "هل أحتاج إلى طباعة هذا؟"
- التقاط نسخ إلكترونية ممسوحة ضوئياً بدلاً من النسخ الورقية وحفظها في موقع آمن على الشبكة أو إرسالها إلى بريد إلكتروني مناسب يقلل من خطر وصول البيانات إلى جهات غير مصرح لها.
- التأكد من التخلص الآمن من المستندات الورقية.
- عدم وضع المستندات التي تحتوي على معلومات شخصية أو حساسة في سلال المهملات العامة أو تركها دون رقابة على المكتب.
- عند الاقتضاء، يجب تخزين الأوراق ووسائط الحاسوب في حاويات مناسبة عند عدم استخدامها، حتى خلال ساعات العمل.
- يجب حفظ المواد المصنفة في مكان آمن عند عدم الحاجة إليها، خاصة عند خلو المكتب.
- استخدام أكياس النفايات السرية أو الصناديق المؤمنة بالقفل والمفتاح، أو تمزيق المستندات حسب الحاجة.
- يجب حفظ جميع أجهزة الحوسبة المحمولة ووسائط تخزين البيانات (مثل وحدات USB، الهواتف المحمولة، وأجهزة الكمبيوتر المحمولة) بشكل آمن في نهاية يوم العمل.
- حماية نقاط البريد الوارد والصادر والفاكسات غير المراقبة.
- يجب عدم ترك بطاقات التعريف التي تتيح الوصول إلى الطباعة دون رقابة، ويجب أن يحملها الموظفون في جميع الأوقات.

الشاشة النظيفة (Clear Screen)

- يجب دائماً قفل أو تسجيل الخروج من الأجهزة مثل الحواسيب أو الطابعات عند تركها دون رقابة.
- عند استخدام محطة عمل مشتركة، يُفضل تسجيل الخروج بدلاً من القفل.
- الضغط على CTRL+ALT+DEL هو طريقة بسيطة لقفل الجهاز، ولكن استخدام مفتاح Windows + L أكثر سهولة. يوجد مفتاح Windows عادة في الزاوية السفلية اليسرى من لوحة المفاتيح ويشبه نافذة أو علماً.
- يجب الانتباه إلى موقع الشاشة على محطة العمل، والتأكد قدر الإمكان من عدم إمكانية رؤيتها من قبل أشخاص غير مصرح لهم أثناء الاستخدام.
- استخدام شاشة توقف محمية بكلمة مرور يتم تفعيلها بعد 3 دقائق من عدم النشاط.
- يجب أيضاً إيقاف تشغيل الشاشات في نهاية يوم العمل.