الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

# الدليل الإرشادي لتطبيق ضوابط الأمن السيبراني للعمل عن بعد

Guide to Telework Cybersecurity Controls Implementation

(GTCC– 1 : 2023)

| |
|---|
| إشارة المشاركة: أبيض |
| تصنيف الوثيقة: عام |

**إخلاء مسؤولية:** طُور هذا الدليل الإرشادي عن طريق الهيئة الوطنية للأمن السيبراني لتمكين الجهات من تطبيق ضوابط الأمن السيبراني للعمل عن بعد، كما تخلي الهيئة الوطنية للأمن السيبراني مسؤوليتها من الاعتماد على هذه الوثيقة فقط؛ وتؤكد على ضرورة الأخذ بعين الاعتبار المتطلبات الخاصة بالجهة وبيئتها؛ وتؤكد الهيئة الوطنية للأمن السيبراني بأن هذه الوثيقة ماهي إلا دليل إرشادي يمكن استخدامه كمثال ولا تعني بالضرورة أن تكون الطريقة الوحيدة لتطبيق الضوابط على ألا تتعارض الطرق الأخرى مع متطلبات الهيئة الوطنية للأمن السيبراني. تحتوي هذه الوثيقة على بعض الأمثلة للمخرجات ذات العلاقة بتطبيق الضوابط، ويحق للمقيم أو المدقق أن يطلب أدلة أخرى حسب ما يراه المقيم أو المدقق لضمان التأكد من تطبيق جميع الضوابط.

بسم الله الرحمن الرحيم

# بروتوكول الإشارة الضوئية (TLP):

تم إنشاء نظام بروتوكول الإشارة الضوئية لمشاركة أكبر قدر من المعلومات الحساسة ويستخدم على نطاق واسع في العالم وهناك أربعة ألوان (إشارات ضوئية):

### أحمر – شخصي وسري للمستلم فقط

المستلم لا يحق له مشاركة المصنف بالإشارة الحمراء مع أي فرد سواء من داخل او خارج المنشأة خارج النطاق المحدد للإستلام.

### برتقالي – مشاركة محدودة

المستلم بالإشارة البرتقالية يمكنه مشاركة المعلومات في نفس المنشأة مع الأشخاص المعنين فقط، ومن يتطلب الأمر منه اتخاذ إجراء يخص المعلومة.

### أخضر – مشاركة في نفس المجتمع

حيث يمكنك مشاركتها مع آخرين من منشأتك أو منشأة أخرى على علاقة معكم أو بنفس القطاع، ولا يسمح بتبادلها أو نشرها من خلال القنوات العامة.

### أبيض – غير محدود

# قائمة المحتويات



# قائمة الأشكال

# مقدمة

طورت الهيئة الوطنية للأمن السيبراني (ويشار لها في هذه الوثيقة بـ "الهيئة") الدليل الإرشادي لتطبيق ضوابط الأمن السيبراني المنصوص عليها في ضوابط الأمن السيبراني للعمل عن بعد (TCC - 1: 2021) (ويشار لها في هذه الوثيقة بـ "الضوابط")، وذلك للمساهمة في تمكين الجهات الوطنية من تطبيق متطلبات الالتزام بضوابط الأمن السيبراني للعمل عن بعد. حيث تم بناء هذا الدليل الإرشادي بالاعتماد على المعلومات والخبرات التي قامت الهيئة بجمعها وتحليلها منذ نشر الضوابط ومواءمة هذا الدليل الإرشادي مع أفضل الممارسات الرائدة في الأمن السيبراني لتسهيل تطبيق الضوابط في الجهات الوطنية.

# الهدف

الهدف الرئيسي من هذا الدليل الإرشادي هو المساهمة في تمكين الجهات الوطنية لتحقيق متطلبات الالتزام بتطبيق ضوابط الأمن السيبراني للعمل عن بعد في الجهة، وذلك بهدف رفع وتعزيز مستوى الأمن السيبراني لديها، وتقليل مخاطر الأمن السيبراني التي تنشأ من التهديدات السيبرانية الداخلية والخارجية.

# نطاق العمل

نطاق العمل لهذا الدليل كما هو مذكور في ضوابط الأمن السيبراني للعمل عن بعد (TCC -1:2021) وهو:

- الجهات الحكومية في المملكة العربية السعودية (وتشمل الـوزارات والهيئات والمؤسسات وغيرها) والجهات والشركات التابعة لها، وجهات القطاع الخاص التي تمتلك بنى تحتية وطنية حساسة ( Critical National Infrastructure "CNIs" ) أو تقوم بتشغيلها أو استضافتها، (ويشار لها جميعاً في هذا الوثيقة بـ "الجهة").
- تشجع الهيئة الجهات الأخرى في المملكة وبشدة على الاستفادة من هذه الضوابط لتطبيق أفضل الممارسات في ما يتعلق بتحسن الأمن السيبراني وتطويره داخل الجهة.

# مكونات وهيكلية ضوابط الأمن السيبراني للعمل عن بعد

يوضح الشكل رقم (١) أدناه المكونات الأساسية والفرعية لضوابط الأمن السيبراني للعمل عن بعد.

| | | | | | |
|---|---|---|---|---|---|
| ١ | حوكمة الأمن السيبراني<br>Cybersecurity Governance | ١-١ | سياسات وإجراءات الأمن السيبراني<br>Cybersecurity Policies and Procedures | ١-٢ | إدارة مخاطر الأمن السيبراني<br>Cybersecurity Risk Management |
| | | ١-٣ | برنامج التوعية والتدريب بالأمن السيبراني<br>Cybersecurity Awareness and Training Program | | |
| ٢ | تعزيز الأمن السيبراني<br>Cybersecurity Defense | ٢-١ | إدارة الأصول<br>Asset Management | ٢-٢ | إدارة هويات الدخول والصلاحيات<br>Identity and Access Management |
| | | ٢-٣ | حماية الأنظمة وأجهزة معالجة المعلومات<br>Information System and Processing Facilities Protection | ٢-٤ | إدارة أمن الشبكات<br>Networks Security Management |
| | | ٢-٥ | أمن الأجهزة المحمولة<br>Mobile Devices Security | ٢-٦ | حماية البيانات والمعلومات<br>Data and Information Protection |
| | | ٢-٧ | التشفير<br>Cryptography | ٢-٨ | إدارة النسخ الاحتياطية<br>Backup and Recovery Management |
| | | ٢-٩ | إدارة الثغرات<br>Vulnerability Management | ٢-١٠ | اختبار الاختراق<br>Penetration Testing |
| | | ٢-١١ | إدارة سجلات الأحداث ومراقبة الأمن السيبراني<br>Cybersecurity Event Logs and Monitoring Management | ٢-١٢ | إدارة حوادث وتهديدات الأمن السيبراني<br>Cybersecurity Incident and Threat management |
| ٣ | الأمن السيبراني المتعلق بالأطراف الخارجية والحوسبة السحابية<br>Third-Party and Cloud Computing Cybersecurity | ٣-١ | الأمن السيبراني المتعلق بالحوسبة السحابية والاستضافة<br>Cloud Computing and Hosting Cybersecurity | | |

شكل ١: المكونات الأساسية والفرعية لضوابط الأمن السيبراني للعمل عن بعد

# هيكلية الدليل الإرشادي

يوضح الشكل رقم (٢) أدناه هيكلية الدليل الإرشادي لضوابط الأمن السيبراني للعمل عن بعد.

| | |
|---|---|
|  | اسم المكون الأساسي |
| الرقم المرجعي للمكون الأساسي | |
| الرقم المرجعي للمكون الفرعي | اسم المكون الفرعي |
| الهدف | |
| **الضوابط** | |
| الرقم المرجعي للضابط | بنود الضابط |
| **أدوات الأمن السيبراني ذات العلاقة:**<br>**إرشادات تطبيق الضوابط:** | |
| **المخرجات المتوقعة:** | |

شكل ٢: هيكلية الدليل الإرشادي لضوابط الأمن السيبراني للعمل عن بعد

# إرشادات عامة لتطبيق ضوابط الأمن السيبراني للعمل عن بعد

| إرشادات عامة |
| --- |
| • حصر جميع الخدمات والأنظمة التي يتم الوصول لها عن بعد، ومراجعتها بشكل دوري.<br>• حصرجميع حسابات المستخدمين ذوي الصلاحيات الهامة والحساسة (Privileged Accounts) والذين لديهم القدرة على الإدارة و الوصول لأنظمة العمل عن بعد، ومراجعتها بشكل دوري.<br>• تحديد وتوثيق متطلبات الأمن السيبراني للعمل عن بعد للجهة والأدوار والمسؤوليات المتعلقة بها، واعتمادها من قبل صاحب الصلاحية ومراجعتها بشكل دوري.<br>• مراجعة الدليل الإرشادي لتطبيق الضوابط الأساسية للأمن السيبراني والعمل على تطبيق الضوابط ذات العلاقة بضوابط الأمن السيبراني للعمل عن بعد.<br>• وضع خطة لتطبيق ضوابط الأمن السيبراني للعمل عن بعد، ومتابعتها بشكل مستمر. |

# إرشادات تطبيق ضوابط الأمن السيبراني للعمل عن بعد

## ١ حوكمة الأمن السيبراني (Cybersecurity Governance)

| ١-١ | سياسات وإجراءات الأمن السيبراني (Cybersecurity Policies and Procedures) | |
|---|---|---|
| الهدف | ضمان توثيق وإعتماد ونشر متطلبات الأمن السيبراني والتزام الجهة بها، وذلك وفقاً لمتطلبات الأعمال التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية ذات العلاقة. | |
| **الضوابط** | | |
| ١-١-١ | رجوعا للضابط ١ - ٣- ١ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي سياسات وإجراءات الأمن السيبراني بحد أدنى، مايلي: | |
| | ١-١-١-١ | تحديد وتوثيق متطلبات وضوابط الأمن السيبراني للعمل عن بعد ضمن سياسات الأمن السيبراني للجهة. |
| | **أدوات الأمن السيبراني ذات العلاقة:**<br>• إجراء تطوير وثائق الأمن السيبراني<br>**إرشادات تطبيق الضوابط:**<br>• العمل على تطوير وتوثيق سياسة الأمن السيبراني للعمل عن بعد وقد تحتوي على سبيل المثال لا الحصر:<br>○ تقييم مخاطر الأمن السيبراني لأنظمة العمل عن بعد، مرة واحدة سنوياً، على الأقل.<br>○ تقييم مخاطر الأمن السيبراني عند التخطيط وقبل السماح بالعمل عن بعد لأي خدمة أو نظام.<br>○ تضمين مخاطر الأمن السيبراني الخاصة بأنظمة العمل عن بعد والخدمات والأنظمة المسموح لها بالعمل عن بعد في سجل مخاطر الأمن السيبراني الخاص بالجهة، ومتابعته مرة واحدة سنويا، على الأقل.<br>○ الاستخدام الآمن للأجهزة المخصصة للعمل عن بعد والمحافظة عليها وحمايتها.<br>○ التعامل الآمن مع هويات الدخول وكلمات المرور.<br>○ حماية البيانات التي يتم حفظها على الأجهزة المستخدمة للعمل عن بعد والتعامل معها حسب تصنيفها وإجراءات وسياسات الجهة.<br>○ التعامل الآمن مع التطبيقات والحلول المستخدمة للعمل عن بعد كالاجتماعات الافتراضية، والتعاون ومشاركة الملفات. | |

| | |
|---|---|
| | ○ التعامل الآمن مع الشبكات المنزلية والتأكد من إعدادت الحماية الخاصة بها.<br>○ تجنب العمل عن بعد باستخدام أجهزة أو شبكات عامة غير موثوقة أو أثناء التواجد في أماكن عامة.<br>○ الوصول المادي غير المصرح به والفقدان والسرقة والتخريب للأصول التقنية وأنظمة العمل عن بعد.<br>○ التواصل مباشرة مع الإدارة المعنية بالأمن السيبراني في الجهة حال الاشتباه بتهديد أمن سيبراني.<br>○ تدريب العاملين على المهارات التقنية اللازمة لضمان تطبيق متطلبات وممارسات الأمن السيبراني عند التعامل مع أنظمة العمل عن بعد.<br>● العمل على أن تكون المتطلبات في الجهة مدعومة من قبل الإدارة التنفيذية. وذلك من خلال اعتماد وموافقة رئيس الجهة أو من ينيبه. |
| | **المخرجات المتوقعة:**<br>● وثيقة توضح متطلبات الأمن السيبراني للعمل عن بعد المعتمدة من قبل الجهة بما يتماشى مع الضوابط الأساسية للأمن السيبراني. (مثال: نسخة إلكترونية أو نسخة ورقية رسمية).<br>● موافقة رسمية من قبل رئيس الجهة أو من ينيبه على المتطلبات (مثال: عن طريق البريد الإلكتروني الرسمي للجهة، أو التوقيع الورقي أو الإلكتروني). |
| ٢-١ | **إدارة مخاطر الأمن السيبراني (Cybersecurity Risk Management)** |
| الهدف | ضمان إدارة مخاطر الأمن السيبراني على نحو ممنهج يهدف إلى حماية الأصول المعلوماتية والتقنية للجهة، وذلك وفقاً للسياسات والإجراءات التنظيمية للجهة والمتطلبات التشريعية والتنظيمية ذات العلاقة. |
| **الضوابط** | |
| ١-٢-١ | بالإضافة للضوابط ضمن المكون الفرعي ١ - ٥ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي منهجية إدارة مخاطر الأمن السيبراني بحد أدنى ما يلي: |
| ١-٢-١-١ | تقييم مخاطر الأمن السيبراني لأنظمة العمل عن بعد، مرة واحدة سنوياً، على الأقل. |
| | **أدوات الأمن السيبراني ذات العلاقة:**<br>● سياسة إدارة مخاطر الأمن السيبراني<br>● إجراء إدارة مخاطر الأمن السيبراني<br>● سجل مخاطر الأمن السيبراني<br>**إرشادات تطبيق الضوابط:**<br>● العمل على إجراء تقييم مخاطر الأمن السيبراني على أنظمة العمل عن بعد وذلك لتحديد جميع التهديدات المحتملة والتي من الممكن أن تؤثر على سلامة تلك الأنظمة أو تعرض المعلومات التي تعالجها لأي مخاطر سيبرانية أو ثغرات محتملة، مع الأخذ بالاعتبار طبيعة تلك الأنظمة. |

- العمل على تقييم مخاطر الأمن السيبراني لكل نظام دورياً ، بحيث يتم مرة واحدة سنوياً على الأقل.
- العمل على إنشاء تقارير بعمليات تقييم مخاطر الأمن السيبراني لكل نظام، على ان يتم توثيق بها ما يلي:
  - المخاطر السيبرانية والثغرات المحتملة.
  - احتمالية حدوث الخطر.
  - نسبة التأثير.
  - مستوى الخطر.
  - المسؤول عن الخطر المحتمل.
  - وصف خطة المعالجة للخطر.
  - الأصول المتأثرة.
- العمل على تطوير خطة معالجة لقائمة مخاطر الأمن السيبراني لكل نظام.

**المخرجات المتوقعة:**

- تقارير تقييم مخاطر الأمن السيبراني الدورية على نطاق أنظمة العمل عن بعد في الجهة.
- خطط المعالجة لمخاطر الأمن السيبراني لكل أنظمة العمل عن بعد.
- متابعة خطط المعالجة والتحقق من تنفيذها.

| | |
|---|---|
| ١-٢-١-٢ | تقييم مخاطر الأمن السيبراني عند التخطيط وقبل السماح بالعمل عن بعد لأي خدمة أو نظام. |

**أدوات الأمن السيبراني ذات العلاقة:**

- سياسة إدارة مخاطر الأمن السيبراني
- إجراء إدارة مخاطر الأمن السيبراني
- سجل مخاطر الأمن السيبراني

**إرشادات تطبيق الضوابط:**

- العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية.
- العمل على تضمين متطلبات الأمن السيبراني ضمن دورة إدارة التغيرات التقنية في الجهة (IT Change Management).
- العمل على تنفيذ إجراءات تقييم مخاطر الأمن السيبراني عند التخطيط وقبل السماح بالعمل عن بعد لأي خدمة أو نظام.
- العمل على معالجة جميع مخاطر الأمن السيبراني المحددة حسب منهجية إدارة مخاطر الأمن السيبراني.
- العمل على تطوير خطة معالجة لقائمة مخاطر الامن السيبراني لكل نظام مع متابعة خطة المعالجة دوريا.

**المخرجات المتوقعة:**

- وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية).
- تقرير يوضح تحديد وتقييم ومعالجة مخاطر الأمن السيبراني المتعلقة بالتخطيط وقبل السماح بالعمل عن بعد لأي خدمة أو نظام.
- سجل مخاطر الأمن السيبراني للعمل عن بعد يتضمن (أثناء التخطيط, وعند التنفيذ وقبل الإستخدام).

| | |
|---|---|
| ١-٢-١-٣ | تضمين مخاطر الأمن السيبراني الخاصة بأنظمة العمل عن بعد والخدمات والأنظمة المسموح لها بالعمل عن بعد في سجل مخاطر الأمن السيبراني الخاص بالجهة، ومتابعته مرة واحدة سنويا، على الأقل. |

**أدوات الأمن السيبراني ذات العلاقة:**

- سياسة إدارة مخاطر الأمن السيبراني
- إجراء إدارة مخاطر الأمن السيبراني
- سجل مخاطر الأمن السيبراني

**إرشادات تطبيق الضوابط:**

- العمل على إنشاء سجل مخاطر الأمن السيبراني خاص بأنظمة العمل عن بعد والخدمات والأنظمة المسموح لها بالعمل عن بعد أو تضمين المخاطر المتعلقة بها بشكل واضح ضمن سجل مخاطر الأمن السيبراني العام بالجهة، بحيث يحتوي على التالي:
  - المخاطر السيبرانية والثغرات المحتملة.
  - احتمالية حدوث الخطر.
  - نسبة التأثير.
  - مستوى الخطر.
  - المسؤول عن الخطر المحتمل.
  - وصف خطة المعالجة للخطر.
  - الأصول المتأثرة.
- العمل على تضمين مخاطر الأمن السيبراني الخاصة بأنظمة العمل عن بعد والخدمات والأنظمة المسموح لها بالعمل عن بعد التي تم تحديدها وتقييمها خلال عملية التقييم، وإسنادها لأصحاب المصلحة.
- متابعة سجل مخاطر الأمن السيبراني الخاص بأنظمة العمل عن بعد والخدمات والأنظمة المسموح لها بالعمل عن بعد دورياً، مرة واحدة سنويا على الأقل، بحيث يتم متابعة خطط المعالجة والتحقق من تنفيذها وإضافة أي مخاطر جديدة وتوثيق التغييرات في السجل.

**المخرجات المتوقعة:**

- سجل مخاطر الأمن السيبراني الخاص بأنظمة العمل عن بعد والخدمات والأنظمة المسموح لها بالعمل عن بعد.

| | |
|---|---|
| | • سجل التغييرات الخاصة بسجل مخاطر الأمن السيبراني الخاص بأنظمة العمل عن بعد والخدمات والأنظمة المسموح لها بالعمل عن بعد<br>• متابعة خطط المعالجة والتحقق من تنفيذها.<br>• المراجعة دوريا لمخاطر الامن السيبراني الخاصة بأنظمة العمل عن بعد. |
| ٣-١ | برنامج التوعية والتدريب بالأمن السيبراني (Cybersecurity Awareness and Training Program) |
| الهدف | ضمان التأكد من أن العاملين بالجهة لديهم التوعية الأمنية اللازمة وعلى دراية بمسؤولياتهم في مجال الأمن السيبراني. والتأكد من تزويد العاملين بالجهة بالمهارات والمؤهلات والدورات التدريبية المطلوبة في مجال الأمن السيبراني لحماية الأصول المعلوماتية والتقنية للجهة والقيام بمسؤولياتهم تجاه الأمن السيبراني. |
| **الضوابط** | |
| ١-٣-١ | بالإضافة للضوابط الفرعية ضمن الضابط ١ - ١٠ - ٣ في الضوابط الأساسية للأمن السيبراني، فإنه يجب أن يغطي برنامج التوعية بالأمن السيبراني المخاطر والتهديدات السيبرانية للعمل عن بعد والاستخدام الآمن للحد من هذه المخاطر والتهديدات، بما في ذلك: |
| ١-٣-١-١ | الاستخدام الآمن للأجهزة المخصصة للعمل عن بعد والمحافظة عليها وحمايتها. |
| | **أدوات الأمن السيبراني ذات العلاقة:**<br>• برنامج التوعية بالأمن السيبراني<br>**إرشادات تطبيق الضوابط:**<br>• العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية.<br>• العمل على تقديم برامج توعوية في الأمن السيبراني تغطي الإستخدام الآمن لأجهزة العمل عن بعد وكيفية حمايتها. |
| | **المخرجات المتوقعة:**<br>• وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية).<br>• خطة عمل لتنفيذ برنامج التوعية بالأمن السيبراني المعتمد الذي يغطي الاستخدام الآمن لأجهزة العمل عن بعد وكيفية حمايتها.<br>• إثبات على تقديم محتوى توعوي للإستخدام الآمن لأجهزة العمل عن بعد وكيفية حمايتها. |
| ١-٣-١-٢ | التعامل الآمن مع هويات الدخول وكلمات المرور. |

| | |
|---|---|
| **أدوات الأمن السيبراني ذات العلاقة:**<br>• برنامج التوعية بالأمن السيبراني<br>**إرشادات تطبيق الضوابط:**<br>• العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية.<br>• العمل على تقديم برامج توعوية في الأمن السيبراني تغطي التعامل الآمن مع هويات الدخول وكلمات المرور.<br>**المخرجات المتوقعة:**<br>• وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية).<br>• خطة عمل لتنفيذ برنامج التوعية بالأمن السيبراني الذي يغطي التعامل الآمن مع هويات الدخول وكلمات المرور.<br>• إثبات على تقديم محتوى توعوي للتعامل الآمن مع هويات الدخول وكلمات المرور. | ١-٣-١-٣ حماية البيانات التي يتم حفظها على الأجهزة المستخدمة للعمل عن بعد والتعامل معها حسب تصنيفها وإجراءات وسياسات الجهة. |
| **أدوات الأمن السيبراني ذات العلاقة:**<br>• برنامج التوعية بالأمن السيبراني<br>**إرشادات تطبيق الضوابط:**<br>• العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية.<br>• العمل على تقديم برامج توعوية في الأمن السيبراني تغطي حماية البيانات التي يتم حفظها على الأجهزة المستخدمة للعمل عن بعد والتعامل معها حسب تصنيفها وإجراءات وسياسات الجهة.<br>**المخرجات المتوقعة:**<br>• وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية).<br>• خطة عمل لتنفيذ برنامج التوعية بالأمن السيبراني الذي يغطي حماية البيانات التي يتم حفظها على الأجهزة المستخدمة للعمل عن بعد والتعامل معها حسب تصنيفها وإجراءات وسياسات الجهة.<br>• إثبات على تقديم محتوى توعوي حماية البيانات التي يتم حفظها على الأجهزة المستخدمة للعمل عن بعد والتعامل معها حسب تصنيفها وإجراءات وسياسات الجهة. | ١-٣-١-٤ التعامل الآمن مع التطبيقات والحلول المستخدمة للعمل عن بعد كالاجتماعات الافتراضية، والتعاون ومشاركة الملفات. |

**أدوات الأمن السيبراني ذات العلاقة:**

- برنامج التوعية بالأمن السيبراني

**إرشادات تطبيق الضوابط:**

- العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية.
- العمل على تقديم برامج توعوية في الأمن السيبراني تغطي التعامل الآمن مع التطبيقات والحلول المستخدمة للعمل عن بعد كالاجتماعات الافتراضية، والتعاون ومشاركة الملفات.

**المخرجات المتوقعة:**

- وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية).
- خطة عمل لتنفيذ برنامج التوعية بالأمن السيبراني الذي يغطي التعامل الآمن مع التطبيقات والحلول المستخدمة للعمل عن بعد كالاجتماعات الافتراضية، والتعاون ومشاركة الملفات.
- إثبات على تقديم محتوى توعوي التعامل الآمن مع التطبيقات والحلول المستخدمة للعمل عن بعد كالاجتماعات الافتراضية، والتعاون ومشاركة الملفات.

| | |
|---|---|
| ١-٣-١-٥ | التعامل الآمن مع الشبكات المنزلية والتأكد من إعدادت الحماية الخاصة بها. |

**أدوات الأمن السيبراني ذات العلاقة:**

- برنامج التوعية بالأمن السيبراني

**إرشادات تطبيق الضوابط:**

- العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية.
- العمل على تقديم برامج توعوية في الأمن السيبراني تغطي التعامل الآمن مع الشبكات المنزلية والتأكد من إعدادت الحماية الخاصة بها.

**المخرجات المتوقعة:**

- وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية).
- خطة عمل لتنفيذ برنامج التوعية بالأمن السيبراني الذي يغطي التعامل الآمن مع الشبكات المنزلية والتأكد من إعدادت الحماية الخاصة بها.
- إثبات على تقديم محتوى توعوي التعامل الآمن مع الشبكات المنزلية والتأكد من إعدادت الحماية الخاصة بها.

| | | |
|---|---|---|
| | ١-٣-١-٦ | تجنب العمل عن بعد باستخدام أجهزة أو شبكات عامة غير موثوقة أو أثناء التواجد في أماكن عامة. |
| | **أدوات الأمن السيبراني ذات العلاقة:**<br>• برنامج التوعية بالأمن السيبراني<br>**إرشادات تطبيق الضوابط:**<br>• العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية.<br>• العمل على تقديم برامج توعوية في الأمن السيبراني تغطي تجنب العمل عن بعد باستخدام أجهزة أو شبكات عامة غير موثوقة أو أثناء التواجد في أماكن عامة. | |
| | **المخرجات المتوقعة:**<br>• وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية).<br>• خطة عمل لتنفيذ برنامج التوعية بالأمن السيبراني الذي يغطي تجنب العمل عن بعد باستخدام أجهزة أو شبكات عامة غير موثوقة أو أثناء التواجد في أماكن عامة.<br>• إثبات على تقديم محتوى توعوي تجنب العمل عن بعد باستخدام أجهزة أو شبكات عامة غير موثوقة أو أثناء التواجد في أماكن عامة. | |
| | ١-٣-١-٧ | الوصول المادي غير المصرح به والفقدان والسرقة والتخريب للأصول التقنية وأنظمة العمل عن بعد. |
| | **أدوات الأمن السيبراني ذات العلاقة:**<br>• برنامج التوعية بالأمن السيبراني<br>**إرشادات تطبيق الضوابط:**<br>• العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية.<br>• العمل على تقديم برامج توعوية في الأمن السيبراني تغطي الوصول المادي غير المصرح به والفقدان والسرقة والتخريب للأصول التقنية وأنظمة العمل عن بعد. | |

| | | |
|---|---|---|
| | **المخرجات المتوقعة:**<br>• وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية).<br>• خطة عمل لتنفيذ برنامج التوعية بالأمن السيبراني الذي يغطي الوصول المادي غير المصرح به والفقدان والسرقة والتخريب للأصول التقنية وأنظمة العمل عن بعد.<br>• إثبات على تقديم محتوى توعوي الوصول المادي غير المصرح به والفقدان والسرقة والتخريب للأصول التقنية وأنظمة العمل عن بعد. | |
| | ٨-١-٣-١ | التواصل مباشرة مع الإدارة المعنية بالأمن السيبراني في الجهة حال الاشتباه بتهديد أمن سيبراني. |
| | **أدوات الأمن السيبراني ذات العلاقة:**<br>• برنامج التوعية بالأمن السيبراني<br>**إرشادات تطبيق الضوابط:**<br>• العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية.<br>• العمل على تقديم برامج توعوية في الأمن السيبراني تغطي التواصل مباشرة مع الإدارة المعنية بالأمن السيبراني في الجهة حال الاشتباه بتهديد أمن سيبراني. | |
| | **المخرجات المتوقعة:**<br>• وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية).<br>• خطة عمل لتنفيذ برنامج التوعية بالأمن السيبراني الذي يغطي التواصل مباشرة مع الإدارة المعنية بالأمن السيبراني في الجهة حال الاشتباه بتهديد أمن سيبراني.<br>• إثبات على تقديم محتوى توعوي التواصل مباشرة مع الإدارة المعنية بالأمن السيبراني في الجهة حال الاشتباه بتهديد أمن سيبراني. | |
| ٢-٣-١ | بالإضافة للضوابط الفرعية ضمن الضابط ١ - ١٠ - ٤ في الضوابط الأساسية للأمن السيبراني، فإنه يجب تدريب العاملين على المهارات التقنية اللازمة لضمان تطبيق متطلبات وممارسات الأمن السيبراني عند التعامل مع أنظمة العمل عن بعد. | |
| | **أدوات الأمن السيبراني ذات العلاقة:**<br>• برنامج التوعية بالأمن السيبراني<br>**إرشادات تطبيق الضوابط:** | |

| | |
|---|---|
| | • العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية.<br>• تطوير وتنفيذ برنامج تدريبي للموظفين العاملين في فريق الأمن السيبراني أو أعضاء الفريق الآخرين حيثما لزم الأمر ، لضمان تزويد الفريق بالمهارات التقنية المطلوبة لتنفيذ متطلبات الأمن السيبراني لأنظمة العمل عن بعد.<br>• العمل على تقديم برامج توعوية دورية لضمان التعامل الآمن مع حوادث الأمن السيبراني ومتطلبات التنفيذ / الخدمات. |
| | **المخرجات المتوقعة:**<br>• وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية).<br>• برنامج تدريبي موثق مع الخطة التنفيذية له بشكل دوري للتعامل مع خدمات الأمن السيبراني ودعم متطلبات العمل عن بعد.<br>• شهادات تدريبية للعاملين على المهارات التقنية اللازمة لضمان تطبيق متطلبات وممارسات الأمن السيبراني عند التعامل مع أنظمة العمل عن بعد. |

## ٢ تعزيز الأمن السيبراني (Cybersecurity Defense)

| ٢-١ | إدارة الأصول (Asset Management) |
|---|---|
| الهدف | للتأكد من أن الجهة لديها قائمة جرد دقيقة وحديثة للأصول تشمل التفاصيل ذات العلاقة لجميع الأصول المعلوماتية والتقنية المتاحة للجهة، من أجل دعم العمليات التشغيلية للجهة ومتطلبات الأمن السيبراني، لتحقيق سرية وسلامة الأصول المعلوماتية والتقنية للجهة ودقتها وتوافرها. |
| **الضوابط** | |
| ٢-١-١ | بالإضافة للضوابط ضمن المكون الفرعي ٢- ١ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني لإدارة الأصول المعلوماتية والتقنية، بحد أدنى، مايلي: |
| ٢-١-١-١ | تحديد وحصر الأصول المعلوماتية والتقنية لأنظمة العمل عن بعد، وتحديثها مرة واحدة، كل سنة؛ على الأقل. |
| | **أدوات الأمن السيبراني ذات العلاقة:**<br>• سياسة إدارة الأصول<br>• نموذج معيار تصنيف الأصول<br>**إرشادات تطبيق الضوابط:**<br>• العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني ، واعتمادها من قبل صاحب الصلاحية.<br>• العمل على تطوير قائمة جرد الأصول المعلوماتية والتقنية لأنظمة العمل عن بعد بصيغة إلكترونية مع تحديد تاريخ الجرد. ويمكن تطبيق عدة طرق لتخزين واستخدام قائمة جرد وحصر الأصول ، على سبيل المثال لا الحصر:<br>○ قاعدة بيانات إدارة الإعدادات (CMDB).<br>○ برامج إدارة الأصول.<br>○ أداة متخصصة في إدارة الأصول.<br>○ جداول البيانات (Spreadsheets).<br>○ قاعدة البيانات.<br>• تحديد جميع أنواع الأصول المعلوماتية والتقنية (الأجهزة والبرامج) المستخدمة في أنظمة العمل عن بعد وتوثيقها. |

| | |
|---|---|
| | • العمل على أن تكون قائمة الجرد مركزية بين الإدارة المعنية بالأمن السيبراني وتقنية المعلومات والإدارات المعنية الأخرى، وعلى أن يتم تحديثها والتأكد من دقتها على الأقل مرة واحدة سنوياً.<br>**المخرجات المتوقعة:**<br>• وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية).<br>• سجل مفصل لجميع الأصول المعلوماتية والتقنية لأنظمة العمل عن بعد.<br>• تقارير المراجعة السنوية لتحديث سجل الأصول المعلوماتية والتقنية لأنظمة العمل عن بعد. |
| ٢-٢ | إدارة هويات الدخول والصلاحيات (Identity and Access Management) |
| الهدف | ضمان حماية الأمن السيبراني للوصول المنطقي (Logical Access) إلى الأصول المعلوماتية والتقنية للجهة من أجل منع الوصول غير المصرح به وتقييد الوصول إلى ما هو مطلوب لإنجاز الأعمال المتعلقة بالجهة. |
| **الضوابط** | |
| ٢-٢-١ | بالإضافة للضوابط الفرعية ضمن الضابط ٢- ٢- ٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني المتعلقة بإدارة هويات الدخول، والصلاحيات للأنظمة المستخدمة في العمل عن بعد في الجهة، بحد أدنى، مايلي: |
| ٢-٢-١-١ | إدارة صلاحيات المستخدمين للعمل عن بعد بناءً على احتياجات العمل، مع مراعاة حساسية الأنظمة ومستوى الصلاحيات، ونوعية الأجهزة المستخدمة من قبل الموظفين للعمل عن بعد. |
| | **أدوات الأمن السيبراني ذات العلاقة:**<br>• سياسة إدارة هويات الدخول والصلاحيات<br>**إرشادات تطبيق الضوابط:**<br>• العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني ، واعتمادها من قبل صاحب الصلاحية.<br>• العمل على تطوير إجراءات إدارة صلاحيات المستخدمين للعمل عن بعد من قبل الجهة ، مع مراعاة ما يلي:<br>○ حساسية النظام.<br>○ مستوى حق الوصول.<br>○ نوع الأجهزة التي يستخدمها الموظفون للعمل عن بعد. |

| | |
|---|---|
| | ○ مدة الصلاحية.<br>● تطبيق الضوابط التقنية المطلوبة لتوفير وإدارة الهويات ومنح الصلاحيات للمستخدمين للعمل عن بعد. |
| | **المخرجات المتوقعة:**<br>● وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية).<br>● قائمة لجميع الصلاحيات المستخدمة للعمل عن بعد.<br>● طلبات منح الصلاحيات للمستخدمين للعمل عن بعد والموافقات المطلوبة.<br>● تقارير مراجعة أنشطة الحسابات ذات الصلاحيات. |
| ٢-٢-١-٢ | تقييد إمكانية الوصول عن بعد لنفس المستخدم من أجهزة حاسبات متعددة في نفس الوقت (Concurrent Logins). |
| | **أدوات الأمن السيبراني ذات العلاقة:**<br>● سياسة إدارة هويات الدخول والصلاحيات<br>**إرشادات تطبيق الضوابط:**<br>● العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني ، واعتمادها من قبل صاحب الصلاحية.<br>● تطبيق إدارة الجلسة الآمنة عن طريق تعيين الحد الأقصى لعدد الجلسات التي يسمح بها للمستخدم.<br>● عند الحاجة للاستثناء من هذا المتطلب ، تحدد الإجراءات للحصول على الموافقة اللازمة من الإدارة المعنية والإدارة المعنية بالأمن السيبراني. |
| | **المخرجات المتوقعة:**<br>● وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية).<br>● لقطة شاشة لتقييد إمكانية الوصول عن بعد لنفس المستخدم من أجهزة حاسبات متعددة في نفس الوقت حيث تتضمن الحد الأقصى لعدد الجلسات التي يسمح بها للمستخدم.<br>● الإجراءات المعتمدة للاستثناء من هذا المتطلب.<br>● موافقة رسمية على أي استثناء. |
| ٢-٢-١-٣ | استخدام معايير آمنة لإدارة الهويات وكلمات المرور المستخدمة في أنظمة العمل عن بعد. |
| | **أدوات الأمن السيبراني ذات العلاقة:** |

- سياسة إدارة هويات الدخول والصلاحيات
- معيار إدارة هويات الدخول والصلاحيات

**إرشادات تطبيق الضوابط:**

- العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني ، واعتمادها من قبل صاحب الصلاحية.
- العمل على إعداد معايير كلمة المرور أخذًا بالاعتبار أفضل الممارسات، على سبيل المثال لا الحصر:
  - أن يكون أقل عدد لرموز كلمة المرور للصلاحيات الهامة والحساسة هو ١٠ وباقي الصلاحيات هو ٨
  - مدة صلاحية كلمة المرور (Expiration Period) على الأقل ٣٠ يومًا للصلاحيات الهامة والحساسة وباقي الصلاحيات ٩٠ يومًا على الأقل
  - تعقيد كلمة المرور (Complexity)
  - تأمين كلمة المرور (Lockout)
  - تفعيل كلمة المرور (Activation)
  - سجل كلمة المرور (History)
  - أن يكون عدد المحاولات المسموحة هي 3 محاولات
  - أن لا يتم تكرار كلمات المرور التي أستخدمت خلال المرات الـ 12 الأخيرة
  - أن لا يتم استخدام كلمات المرور بناءً على البيانات الشخصية للمستخدم ذي الصلاحيات والامتيازات، مثل تاريخ الميلاد
  - أن تكون كلمة المرور معقدة وتتضمن على الأقل ٤ رموز من التالي:
    - أحرف كبيرة (Upper case letters)
    - أحرف صغيرة (Lower case letters)
    - أرقام (١٢٣٤)
    - رموز خاصة (@#%*)
- العمل على تفعيل التحقق متعدد العناصر لأنظمة العمل عن بعد بجانب اسم المستخدم وكلمة المرور وقد يكون مثلًا:
  - كلمة المرور الصالحة لمرة واحدة (One Time Password) في رسالة نصية ترسل لرقم الجوال المسجل للمستفيد.
  - كلمة المرور الصالحة لمرة واحدة (One Time Password) تعرض في برنامج أو جهاز توليد أرقام عشوائية (hard token) للتحقق من الهوية متعدد العناصر.
  - التحقق من الهوية باستخدام بصمات حيوية (مثال: بصمة الإصبع).
- إستخدام تقنيات الدخول عن بعد الآمنة (VPN) لتشفير الإتصال بين المستخدم والنظام.

| | |
|---|---|
| | **المخرجات المتوقعة:**<br>• وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية).<br>• إثبات يوضح تطبيق إستخدام المعايير الآمنة لإدارة الهويات ولكمات المرور في أنظمة العمل عن بعد على سبيل المثال لا الحصر: لقطة شاشة لتطبيق سياسة كلمة المرور ولقطة شاشة لتطبيق التحقق من الهوية متعدد العناصر (MFA). |
| ٢-٢-٢ | رجوعاً للضابط الفرعي٢-٢-٣-٥ في الضوابط الأساسية للأمن السيبراني، يجب مراجعة هويات الدخول والصلاحيات المستخدمة للعمل عن بعد، بحد أدنى مرة واحدة كل سنة. |
| | **أدوات الأمن السيبراني ذات العلاقة:**<br>• سياسة إدارة هويات الدخول والصلاحيات<br>**إرشادات تطبيق الضوابط:**<br>• العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني ، واعتمادها من قبل صاحب الصلاحية.<br>• العمل على مراجعة هويات الدخول والصلاحيات المستخدمة للعمل عن بعد في الجهة من خلال إجراء تقييم دوري (وذلك حسب خطة موثقة ومعتمدة للمراجعة، وبناء على فترة زمنية محددة بحد أدنى مرة واحدة سنوياً).<br>• العمل على مراجعة جميع هويات الدخول والصلاحيات المستخدمة للعمل عن بعد من جميع النواحي على سبيل المثال لا الحصر:<br>○ مبدأ الحد الأدنى من الصلاحيات والامتيازات<br>○ مبدأ فصل المهام ومبدأ الحاجة إلى المعرفة والاستخدام بالتعاون مع الإدارات ذات العلاقة (كالإدارة المعنية بتقنية المعلومات).<br>○ مدة الصلاحية الممنوحة.<br>○ حالة المخوّل له بالصلاحيات الممنوحة على سبيل المثال لا الحصر: إن كان لا يزال موجود في الإدارة أو تم نقله إلى فريق آخر أو تمت استقالته من الجهة أو لا يتطلب عمل المستخدم حاجة للوصول إلى العمل عن بعد و إتخاذ مايلزم حسب حالة المخول له بصلاحية العمل عن بعد.<br>• العمل على توثيق جميع المراجعات والتغييرات التي تتم على هويات الدخول والصلاحيات المستخدمة للعمل عن بعد في الجهة على سبيل المثال لا الحصر:<br>○ المراجعات الدورية للصلاحيات الممنوحة.<br>○ التغييرات التي حصلت من آخر مراجعة تمت.<br>○ التغييرات أو التعديلات المتطلب تغييرها للصلاحيات الممنوحة. |
| | **المخرجات المتوقعة:** |

| | |
|---|---|
| | • وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية).<br>• نتائج مراجعة هويات الدخول والصلاحيات للأنظمة الحساسة في الجهة.<br>• خطة دورية موثقة لمراجعة هويات مستخدمي العمل عن بعد وحقوق الوصول الخاصة بهم.<br>• إثبات تطبيق متطلبات المراجعة الدورية للهوية وصلاحيات الوصول ، على سبيل المثال ، وثيقة رسمية ومعتمدة توضح المراجعة الدورية للهويات وصلاحيات الوصول لمستخدمي خاصية الوصول عن بعد. |
| ٢-٣ | حماية الأنظمة وأجهزة معالجة المعلومات (Information System and Processing Facilities Protection) |
| الهدف | ضمان حماية الأنظمة وأجهزة معالجة المعلومات بما في ذلك أجهزة المستخدمين والبنى التحتية للجهة من المخاطر السيبرانية. |
| **الضوابط** | |
| ٢-٣-١ | بالإضافة للضوابط الفرعية ضمن الضابط ٢- ٣- ٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني لحماية أنظمة العمل عن بعد، وأجهزة المعلومات الخاصة بها، بحد أدنى، مايلي: |
| ٢-٣-١-١ | تطبيق حزم التحديثات، والإصلاحات الأمنية لأنظمة العمل عن بعد، مرة واحدة شهريا على الأقل. |
| | **أدوات الأمن السيبراني ذات العلاقة:**<br>• سياسة إدارة حزم التحديثات والإصلاحات<br>• معيار الإعدادات والتحصين الآمن<br>• معيار إدارة التحديثات والإصلاحات<br>**إرشادات تطبيق الضوابط:**<br>• العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني ، واعتمادها من قبل صاحب الصلاحية.<br>• تحديد إجراءات إدارة تطبيق حزم التحديثات والإصلاحات للأنظمة والأجهزة والتطبيقات الخاصة بالعمل عن بعدلعمل عن بعد ، والتي تشمل:<br>○ تحديد نطاق أنظمة العمل عن بعد التي يتم تطبيق حزم التحديثات والإصلاحات فيها لتشمل:<br>▪ أجهزة المستخدمين.<br>▪ أنظمة التشغيل. |

- أجهزة الشبكات.
- قواعد البيانات.
- التطبيقات.

- أن تكون الفترة الزمنية المطلوبة لتطبيق حزم التحديثات والإصلاحات للأنظمة والأجهزة والتطبيقات الخاصة بالعمل عن بعد مرة واحدة شهرياً على الأقل.
- تضمين إجراءات حزم التحديثات والإصلاحات لأنظمة العمل عن بعد في منهجية إدارة التغيير أو تضمين إدارة التغيير في سياسة إدارة حزم التحديثات والإصلاحات.
- تضمين موافقة إدارة التغيير من ضمن الموافقات في نموذج إجراء حزم التحديثات والإصلاحات على جميع نطاق أنظمة العمل عن بعد والأجهزة والتطبيقات، على سبيل المثال لا الحصر: طلب الموافقات عن طريق البريد الإلكتروني أو ورقياً أو عن طريق نظام داخلي.
- تطبيق حزم التحديثات والإصلاحات على النطاق المحدد بعد الحصول على الموافقة اللازمة.
- مراجعة تطبيق حزم التحديثات والإصلاحات باستمرار للتأكد من أن جميع التحديثات اللازمة تم تطبيقها على جميع نطاق الأجهزة والأنظمة والتطبيقات الخاصة بالعمل عن بعد.

**المخرجات المتوقعة:**

- وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية).
- إجراءات موثقة ومعتمدة تشير إلى أن موافقة إدارة التغيير مطلوبة لحزم التحديثات والإصلاحات.
- تقارير تفيد بأن نطاق حزم التحديثات يغطي جميع أجهزة وتطبيقات أنظمة العمل عن بعد.
- تقارير تفيد بأن حزم التحديثات يتم إجراؤها وفقًا للمدة المحددة في الإجراءات (بما في ذلك على سبيل المثال لا الحصر: لقطة شاشة أو مثال مباشر يعرض تاريخ ونطاق عدة عينات من تطبيق حزم التحديثات المعتمدة عن طريق البريد الإلكتروني أو النظام الداخلي أو ورقي التي تم إجراؤها مسبقًا لتشمل الأجهزة والأنظمة والتطبيقات بشكل دوري).

| | |
|---|---|
| ٢-١-٣-٢ | مراجعة إعدادات الحماية لأنظمة العمل عن بعد والتحصين ( Secure Configuration and Hardening), مرة واحدة كل سنة على الأقل. |

**أدوات الأمن السيبراني ذات العلاقة:**

- سياسة الإعدادات والتحصين
- معيار الإعدادات والتحصين الآمن

**إرشادات تطبيق الضوابط:**

- العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة
- متطلبات الأمن السيبراني ، واعتمادها من قبل صاحب الصلاحية.

| | |
|---|---|
| • تحديد معيار تقني لمراجعة إعدادت والتحصين لأنظمة العمل عن بعد من مصادر موثوقة على سبيل المثال لا الحصر: معيار تقني لمورد نظام العمل عن بعد.<br>• تحديد إجراءات لمراجعة الإعدادات والتحصين لنظام العمل عن بعد.<br>• مراجعة الإعدادات والتحصين لنظام العمل عن بعد على أساس المعيار المعتمد مرة واحدة كل سنة على الأقل ، وهذا يشمل على سبيل المثال لا الحصر: إدارة الوصول والتشفير وإعدادات الحماية. | |
| **المخرجات المتوقعة:**<br>• وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية).<br>• معيار معتمد لمراجعة الإعدادات والتحصين لنظام العمل عن بعد (على سبيل المثال: نسخة معتمدة ورقية أو إلكترونية).<br>• التقارير التي تفيد بأن إعدادات وتحصين أنظمة العمل عن بعد تتم مراجعتها كل عام على الأقل. | |
| ٢-٣-١-٣ | مراجعة وتحصين الإعدادت المصنعية (Default Configuration) للأصول التقنية لأنظمة العمل عن بعد، ومنها وجود كلمات مرور ثابتة، وخلفية افتراضية. |
| **أدوات الأمن السيبراني ذات العلاقة:**<br>• سياسة الإعدادات والتحصين<br>• معيار الإعدادات والتحصين الآمن<br>**إرشادات تطبيق الضوابط:**<br>• العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني ، واعتمادها من قبل صاحب الصلاحية.<br>• مراجعة الإعدادات المصنعية لأنظمة العمل عن بعد من خلال التأكد من عدم وجود كلمات مرور ثابتة أو خلفية افتراضية على أنظمة العمل عن بُعد بناءً على المعايير المعتمدة وتوثيق النتائج. | |
| **المخرجات المتوقعة:**<br>• وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية).<br>• تقارير لمراجعة الإعدادات والتحصين الافتراضية وتغييرها ، وضمان إزالة كلمات المرور الثابتة و / أو الخلفية و / أو الافتراضية. | |
| ٢-٣-١-٤ | الإدارة الآمنة للجلسات (Secure Session Management)، ويشمل موثوقية الجلسات (Authenticity)، وإقفالها (Lockout)، وإنهاء مهلتها (Session Timeout). |

**إرشادات تطبيق الضوابط:**

- العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني ، واعتمادها من قبل صاحب الصلاحية.
- تطبيق عملية إدارة آمنة للجلسات (Secure Session Management) حيث تشمل على:
  - موثوقية الجلسات (Authenticity).
  - الدخول المصرح (Authorization).
  - الدخول (Access).
  - التحكم (Control).
  - الإقفال (Lockout).
  - إنهاء مهلتها (Timeout).
- تحديد مدة الجلسة من خلال ضمان عدم وجود تأثير على توافر الخدمات والمعلومات أثناء العمل عن بعد.
- توثيق المدة الزمنية التي سيتم تعيينها في أنظمة العمل عن بعد لإغلاق الجلسة ومهلة الجلسة والحصول على الموافقة من أصحاب المصلحة في الجهة بناء عليها.

**المخرجات المتوقعة:**

- وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية).
- العمل على تحديد عملية إدارة جلسة محددة ، ومدة إقفال الجلسة وإنهاء مهلتها في سياسة العمل عن بعد الموثقة والمعتمدة.
- لقطة شاشة لإدارة الجلسة التي تشمل:
  - موثوقية الجلسة.
  - إقفال الجلسة.
  - إنهاء مهلة الجلسة.

| | |
|---|---|
| ٢-٣-١-٥ | تقييد تفعيل الخصائص والخدمات في أنظمة العمل عن بعد حسب الحاجة، على أن يتم تحليل المخاطر السيبرانية المحتملة في حال الحاجة لتفعيلها. |

**إرشادات تطبيق الضوابط:**

- العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني ، واعتمادها من قبل صاحب الصلاحية.
- توثيق وتحديد القيود في أنظمة العمل عن بعد، وذلك بعد توضيح وقبول المخاطر لضمان التنشيط الآمن عبر الإنترنت لتفعيل الخصائص والخدمات التقنية بناءً على حاجة المستخدم مع تحديد مدة التفعيل.

| | |
|---|---|
| | • تطوير وتوثيق الإجراءات للموافقة المناسبة على طلب المستخدم لتفعيل خصائص أو خدمات محددة مطلوبة لعمليات تشغيلية محددة مع تحديد مدة التفعيل.<br>• إجراء تحليل للمخاطر السيبرانية المحتملة قبل الموافقة على طلب مستخدم محدد وتنشيطه لتفعيل خصائص أو خدمات تقنية معينة في أنظمة العمل عن بُعد مع تحديد مدة التفعيل. |
| | **المخرجات المتوقعة:**<br>• وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية).<br>• وثيقة إجراءات معتمدة لتقييد تفعيل الخصائص والخدمات في أنظمة العمل عن بعد حسب الحاجة.<br>• تقارير تحليل المخاطر السيبرانية المحتملة قبل تفعيلها. |
| ٢-٤ | إدارة أمن الشبكات (Networks Security Management) |
| الهدف | ضمان حماية شبكات الجهة من المخاطر السيبرانية. |
| **الضوابط** | |
| ٢-٤-١ | بالإضافة للضوابط الفرعية ضمن الضابط ٢- ٥- ٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني لإدارة أمن شبكات الجهة للعمل عن بعد، بحد أدنى، مايلي: |
| ٢-٤-١-١ | تقييد منافذ وبروتوكولات وخدمات الشبكة المستخدمة لعمليات الدخول عن بعد، وخصوصاً على الأنظمة الداخلية، وفتحها حسب الحاجة. |
| | **أدوات الأمن السيبراني ذات العلاقة:**<br>• سياسة امن الشبكات<br>• معيار امن الشبكات<br>**إرشادات تطبيق الضوابط:**<br>• العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني ، واعتمادها من قبل صاحب الصلاحية.<br>• تنفيذ متطلبات التقييد على خدمات الشبكة والبروتوكولات والمنافذ المستخدمة للوصول عن بُعد باستخدام التقنيات المناسبة والمتقدمة على سبيل المثال لا الحصر: التقييد بواسطة أنظمة جدار الحماية. |

| | |
|---|---|
| | • إنشاء إجراءات موافقة لتحديث قواعد جدار الحماية لضمان عدم إجراء أي تحديث أو تغيير دون موافقة أصحاب الصلاحية. |
| | **المخرجات المتوقعة:**<br>• وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية).<br>• عينة توضح تنفيذ المتطلبات المتعلقة بخدمات الشبكة والبروتوكولات وتقييد المنافذ ، على سبيل المثال لا الحصر:<br>o نموذج يوضح تنفيذ متطلبات خدمات الشبكة والبروتوكولات وتقييد المنافذ (على سبيل المثال: لقطة شاشة توضح دليل الاشتراك واستخدام التقنيات الحديثة والمتقدمة لتطبيق تقييد خدمات الشبكة والبروتوكولات والمنافذ من خلال نظام جدار الحماية).<br>• نموذج يوضح إجراءات الموافقة لتحديث قواعد جدار الحماية. بالإضافة إلى ذلك ، نموذج يوضح ما تم تحديثه في قواعد جدار الحماية. |
| ٢-١-٤-٢ | مراجعة إعدادات وقوائم جدار الحماية (Firewall Rules) ذات العلاقة بأنظمة العمل عن بعد؛ مرة واحدة كل سنة على الأقل. |
| | **أدوات الأمن السيبراني ذات العلاقة:**<br>• سياسة امن الشبكات<br>• معيار امن الشبكات<br>**إرشادات تطبيق الضوابط:**<br>• العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني ، واعتمادها من قبل صاحب الصلاحية.<br>• العمل على مراجعة إعدادات وقوائم جدار الحماية (Firewall Rules) ذات العلاقة بأنظمة العمل عن بعد؛ مرة واحدة كل سنة على الأقل على سبيل المثال لا الحصر:<br>o مراجعة القوائم الغير مستخدمة/مفعلة خلال آخر ٩٠ يوم ليتم حذفها وتعطيلها.<br>o تحديث الإعدادات حسب إصدارات المورد الحديثة.<br>o ترتيب القوائم حسب الفعالية والأداء.<br>o مراجعة وتحليل قوائم VPN.<br>• توثيق نتائج المراجعة بحيث يشمل على سبيل المثال لا الحصر:<br>o التغييرات بعد المراجعة.<br>o تاريخ المراجعة.<br>o الاعتماد. |

**المخرجات المتوقعة:**

- وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية).
- تقرير مراجعة إعدادات جدار الحماية للأنظمة الحساسة في الجهة (جدول تقييم).
- وثيقة للمراجعة الدورية لقواعد وإعدادات التحصين لجدار الحماية.

| | |
|---|---|
| ٢-٤-١-٣ | الحماية من هجمات تعطيل الشبكات (Distributed Denial of Service (DDoS)) على أنظمة العمل عن بعد للحد من المخاطر الناتجة عن هجمات تعطيل الشبكات. |

**أدوات الأمن السيبراني ذات العلاقة:**

- سياسة امن الشبكات
- معيار امن الشبكات
- معيار الحماية من هجمات حجب الخدمة الموزعة(DDoS Attacks)

**إرشادات تطبيق الضوابط:**

- العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني ، واعتمادها من قبل صاحب الصلاحية.
- العمل على توفير أنظمة الحماية من هجمات تعطيل الشبكات ( Distributed Denial of Service Attack "DDoS") على أنظمة العمل عن بعد للحد من المخاطر الناتجة عن هجمات تعطيل الشبكات وتحديثها بشكل مستمر.
- ضبط إعدادات جدار الحماية (Firewall) للحماية من هجمات تعطيل الشبكات والخدمات ( Distributed Denial of Service Attack "DDoS").
- العمل على تطبيق مبدأ التوافر المتعدد (High Availability) على أنظمة العمل عن بعد للجهة على سبيل المثال لا الحصر: أنظمة جدار الحماية, أنظمة الويب (Web Proxy).
- العمل على عقد اتفاقية مع مقدم الخدمات أو مزود خدمات الإنترنت من تطبيق آليات وضمان الحماية ضد هجمات تعطيل الشبكات (Distributed Denial of Service Attack "DDoS").

**المخرجات المتوقعة:**

- وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية).
- أنظمة وتقنيات الحماية من هجمات تعطيل الشبكات على أنظمة العمل عن بعد.
- قائمة إعدادات وضوابط الحماية من هجمات تعطيل الشبكات ( Distributed Denial of Service Attack "DDoS").

| | | |
|---|---|---|
| | ٢-٤-١-٤ | الحماية من التهديدات المتقدمة المستمرة على مستوى الشبكة لأنظمة العمل عن بعد (Network APT). |
| | **أدوات الأمن السيبراني ذات العلاقة:**<br>• سياسة امن الشبكات<br>• معيار امن الشبكات<br>• معيار معيار الحماية من التهديدات المستمرة المتقدمة(APT)<br>**إرشادات تطبيق الضوابط:**<br>• العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني ، واعتمادها من قبل صاحب الصلاحية.<br>• العمل على توفير أنظمة الحماية من التهديدات المتقدمة المستمرة على مستوى الشبكة لأنظمة العمل عن بعد (Network APT) وتحديثها بشكل مستمر على سبيل المثال لا الحصر:<br>○ العمل على توفير أنظمة الحماية المتقدمة لاكتشاف ومنع الاختراقات مثل: (Intrusion Prevention/Detection Systems (IDS/IPS,HIDS/HIPS على جميع أجزاء الشبكة وتحديثها بشكل مستمر.<br>○ العمل على تحديث اجراءات المراقبة المستمرة على مستوى الشبكة للحماية من التهديدات. | |
| | **المخرجات المتوقعة:**<br>• وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية).<br>• قائمة لجميع الأنظمة المتوفرة للحماية من التهديدات المتقدمة المستمرة لأنظمة العمل عن بعد.<br>• إجراءات موثقة للمراقبة المستمرة وتطبيق أدوات الحماية من التهديدات المتقدمة المستمرة. | |
| ٢-٥ | **أمن الأجهزة المحمولة (Mobile Devices Security)** | |
| الهدف | ضمان حماية أجهزة الجهة المحمولة (بما في ذلك أجهزة الحاسب المحمول والهواتف الذكية والأجهزة الذكية اللوحية) من المخاطر السيبرانية. وضمان التعامل بشكل آمن مع المعلومات الحساسة والمعلومات الخاصة بأعمال الجهة وحمايتها أثناء النقل والتخزين عند استخدام الأجهزة الشخصية للعاملين في الجهة (مبدأ «BYOD»). | |
| **الضوابط** | | |

| | | |
|---|---|---|
| ٢-٥-١ | بالإضافة للضوابط الفرعية ضمن الضابط ٢- ٦- ٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني الخاصة بأمن الأجهزة المحمولة للعمل عن بعد في الجهة، بحد أدنى، مايلي: | |
| | ٢-٥-١-١ | إدارة الأجهزة المحمولة وأجهزة (BYOD) مركزياً باستخدام نظام إدارة الأجهزة المحمولة (Mobile Device Management (MDM)) |
| | **أدوات الأمن السيبراني ذات العلاقة:**<br>• نموذج سياسة امن أجهزة المستخدمين والأجهزة المحمولة والأجهزة الشخصية<br>• معيار امن الأجهزة المحمولة<br>**إرشادات تطبيق الضوابط:**<br>• العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني ، واعتمادها من قبل صاحب الصلاحية.<br>• ضمان إدارة الأجهزة المحمولة وأجهزة (BYOD) مركزياً باستخدام نظام إدارة الأجهزة المحمولة ( Mobile) Device Management للحفاظ على السرية والسلامة وتوافر معلومات الجهة.<br>**المخرجات المتوقعة:**<br>• وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية).<br>• وثيقة إجراءات محددة لتطبيق نظام إدارة الأجهزة المحمولة على جميع أجهزة BYOD بإستخدام MDM المقدم من الجهة.<br>• عينة من تطبيق نظام إدارة الأجهزة المحمولة (Mobile Device Management). | |
| | ٢-٥-١-٢ | تطبيق حزم التحديثات، والإصلاحات الأمنية للأجهزة المحمولة، مرة واحدة شهريا، على الأقل. |
| | **أدوات الأمن السيبراني ذات العلاقة:**<br>• نموذج سياسة امن أجهزة المستخدمين والأجهزة المحمولة والأجهزة الشخصية<br>• معيار امن الأجهزة المحمولة<br>**إرشادات تطبيق الضوابط:**<br>• العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني ، واعتمادها من قبل صاحب الصلاحية. | |

| | |
|---|---|
| | • التأكد من أن موافقة إدارة التغيير في الجهة جزء من الموافقات المطلوبة لتطبيق حزم التحديثات والإصلاحات الأمنية بأمن الأجهزة المحمولة للعمل عن بعد في الجهة.<br>• تحديد خطة دورية موثقة لتطبيق التحديثات والإصلاحات الأمنية للأجهزة المحمولة وحلول إدارة الأجهزة المحمولة (MDM) الخاصة بأمن الأجهزة المحمولة للعمل عن بعد مرة واحدة شهرياً على الأقل.<br>• متابعة تطبيق حزم التحديثات والإصلاحات الأمنية الخاصة بأمن الأجهزة المحمولة للعمل عن بعد في الجهة بشكل مستمر من خلال استخدام أدوات وتقنيات إدارة حزم التحديثات وإدارة الثغرات. |
| | **المخرجات المتوقعة:**<br>• وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية).<br>• وثيقة لعملية تطبيق التحديثات والإصلاحات الأمنية على الأجهزة المحمولة.<br>• تقارير تفيد بأن التحديثات والإصلاحات الأمنية تتم حسب الفترة المحددة في الإجراءات. |
| ٢-٦ | **حماية البيانات والمعلومات (Data and Information Protection)** |
| الهدف | ضمان حماية السرية وسلامة بيانات ومعلومات الجهة ودقتها وتوافرها، وذلك وفقاً للسياسات والإجراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية ذات العلاقة. |
| **الضوابط** | |
| ٢-٦-١ | بالإضافة للضوابط الفرعية ضمن الضابط ٢- ٧- ٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني لحماية البيانات والمعلومات للعمل عن بعد في الجهة، بحد أدنى، مايلي: |
| ٢-٦-١-١ | تحديد البيانات المصنفة، حسب التشريعات ذات العلاقة، التي يمكن استخدامها أو الوصول إليها أو التعامل معها من خلال أنظمة العمل عن بعد. |
| | **أدوات الأمن السيبراني ذات العلاقة:**<br>• معيار الحماية من فقدان البيانات<br>**إرشادات تطبيق الضوابط:**<br>• العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني ، واعتمادها من قبل صاحب الصلاحية.<br>• تحديد البيانات في حالة التخزين والبيانات أثناء النقل في أنظمة العمل عن بعد الخاصة وفقًا لسياسات بيانات الجهة و ضوابط الأمن السيبراني للبيانات (DCC) الصادرة من الهيئة الوطنية للأمن السيبراني. |

- تحديد تصنيف البيانات في كل مرحلة حسب ضوابط الأمن السيبراني للبيانات (DCC).
- التأكد من أنه تم تصنيف جميع البيانات التي يمكن استخدامها أو الوصول إليها أو التعامل معها من خلال أنظمة العمل عن بعد ا عتماداً على المتطلبات التشريعية والتنظيمية ذات العلاقة.
- العمل على تحديد آليات وطرق التعامل مع البيانات بناءً على تصنيفها.

**المخرجات المتوقعة:**

- وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية).
- وثيقة معتمدة لأنواع البيانات وتصنيف البيانات في أنظمة العمل عن بعد.
- دليل لتطبيق الأنظمة التقنية في الأمن السيبراني لتصنيف البيانات ضمن أنظمة العمل عن بعد.

| | |
|---|---|
| ٢-١-٦-٢ | حماية البيانات المصنفة، التي تم تحديدها في الضابط ٢- ٦- ١- ١، باستخدام ضوابط مثل منع استخدام نوع من البيانات المصنفة أو تقنيات مثل منع تسريب البيانات ( Data Leakage Prevention) ويمكن تحديد هذه الضوابط والتقنيات عن طريق تحليل المخاطر السيبرانية للجهة. |

**أدوات الأمن السيبراني ذات العلاقة:**

- معيار الحماية من فقدان البيانات

**إرشادات تطبيق الضوابط:**

- العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني ، واعتمادها من قبل صاحب الصلاحية.
- العمل على تحديد وتصنيف بيانات أنظمة العمل عن بعد اعتماداً على المتطلبات التشريعية والتنظيمية ذات العلاقة.
- العمل على إجراء تحليل مخاطر الأمن السيبراني على البيانات المصنفة (التي تم حصرها ضمن مخرجات ضابط رقم ٢-٦-١-١) وذلك لتحديد جميع التهديدات المحتملة والتي من الممكن أن تؤثر على سلامة تلك البيانات أو تعرضها لأي مخاطر سيبرانية أو ثغرات محتملة، مع الأخذ بالاعتبار طبيعة تلك البيانات.
- بناءً على نتائج تقارير تحليل المخاطر السيبرانية، يتم العمل على تحديد ضوابط أو تقنيات تساهم في منع استخدام نوع من البيانات المصنفة أو منع تسريب البيانات في الجهة.
- مراجعة واعتماد وتنفيذ الضوابط اللازمة لمنع فقدان البيانات ، باستخدام أدوات منع تسرب البيانات وغيرها ، والتي تحدد على أساس حالات الاستخدام وعوامل الخطر المحددة.
- يمكن التحكم في حالات استخدام منع البيانات على مستويات مختلفة ، على سبيل المثال لا الحصر: البريد الإلكتروني ، وارسال وثائق مع طرف خارجي ، ونقل البيانات عبر الأجهزة المادية مثل: (USB ، والقرص الصلب ، وما إلى

| | |
|---|---|
| | ذلك) ، ومشاركة البيانات عبر محركات أقراص الشبكة ، النقل عبر اتصال Bluetooth ، والوصول غير المرغوب فيه إلى خادم قاعدة البيانات الداخلي لمستخدمي العمل عن بُعد ، واستخدام تطبيقات المشاركة عن بُعد. |
| | **المخرجات المتوقعة:**<br>• وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية).<br>• وثيقة معتمدة مع دليل لتنفيذ الضوابط لحماية البيانات (منع تسرب البيانات).<br>• دليل لتطبيق ضوابط وتقنيات الأمن السيبراني لمنع الوصول إلى المعلومات المقيدة واستخدامها ونقلها إلى مستخدم داخلي أو خارجي. |
| ٢-٧ | التشفير (Cryptography) |
| الهدف | ضمان الاستخدام السليم والفعال للتشفير لحماية الأصول المعلوماتية الإلكترونية للجهة، وذلك وفقاً للسياسات والإجراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية ذات العلاقة. |
| **الضوابط** | |
| ١-٧-٢ | بالإضافة للضوابط الفرعية ضمن الضابط ٢- ٨- ٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني الخاصة بالتشفير لدى المشتركين، بحد أدنى مايلي: |
| ١-١-٧-٢ | إستخدام طرق وخوارزميات محدثة وآمنة للتشفير على كامل الاتصال الشبكي المستخدم للعمل عن بعد وفقاً للمستوى المتقدم (Advanced) ضمن المعايير الوطنية للتشفير (NCS 1 :2020). |
| | **أدوات الأمن السيبراني ذات العلاقة:**<br>• سياسة التشفير<br>• معيار التشفير<br>• معيار إدارة مفاتيح التشفير<br>**إرشادات تطبيق الضوابط:**<br>• العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني ، واعتمادها من قبل صاحب الصلاحية.<br>• العمل على تحديد خوارزميات ومفاتيح وأجهزة تشفير آمنة عبر الالتزام بمعايير التطبيق الصحيح ومحدثة عبر مراجعتها سنويا والتأكد من أنها تتماشى وفقًا لما تصدره هيئة الأمن السيبراني من معايير تشفير. |

| | |
|---|---|
| | • استخدام المستوى المتقدم (Advanced) عبر الشبكة بالكامل المستخدمة للعمل عن بُعد من طرق وخوارزميات التشفير بناءً على المعايير الوطنية للتشفير(NCS 1 :2020).<br>• مراجعة فعالية التقنيات المستخدمة للإدارة الآمنة للخوارزميات ومفاتيح وأجهزة التشفير.<br>• إستخدام خوارزميات وأدوات التشفير حيثما كان ذلك ممكناً، على سبيل المثال لا الحصر: تشفير كلمة مرور جهاز العمل عن بُعد ، وتشفير ملفات البيانات أثناء النقل لطرف خارجي ، وتشفير المعلومات السرية المخزنة في أنظمة العمل عن بُعد. |
| | **المخرجات المتوقعة:**<br>• وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية).<br>• إجراءات الأمن السيبراني التي تغطي الإدارة الآمنه لخوارزميات ومفاتيح وأجهزة التشفير في الجهة (مثال: نسخة إلكترونية أو نسخة ورقية رسمية).<br>• وثيقة تحدد دورة مراجعة فعالية التقنيات المستخدمة؛ للإدارة الآمنة للخوارزميات ومفاتيح وأجهزة التشفير خلال عمليات دورة حياتها في الجهة.<br>• قائمة البروتوكولات والتقنيات المستخدمة للتشفير على كامل الاتصال الشبكي المستخدم للعمل عن بعد. |
| ٢-٨ | **إدارة النسخ الاحتياطية (Backup and Recovery Management)** |
| الهدف | ضمان حماية بيانات ومعلومات الجهة والإعدادات التقنية للأنظمة والتطبيقات الخاصة بالجهة من الاضرار الناتجة من فقدان البيانات (بشكل عام)، وذلك وفقاً للسياسات والإجراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية ذات العلاقة. |
| **الضوابط** | |
| ١-٨-٢ | بالإضافة للضوابط الفرعية ضمن الضابط ٢- ٩- ٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني لإدارة النسخ الاحتياطية لأنظمة العمل عن بعد في الجهة، بحد أدنى، مايلي: |
| ١-١-٨-٢ | عمل النسخ الاحتياطي على فترات زمنية مخطط لها؛ بناء على تقييم المخاطر للجهة، لأنظمة العمل عن بعد. وتوصي الهيئة بأن يتم عمل النسخ الاحتياطية، لأنظمة العمل عن بعد مرة واحدة كل أسبوع. |
| | **أدوات الأمن السيبراني ذات العلاقة:** |

| | |
|---|---|
| | • **سياسة النسخ الاحتياطية**<br>• **معيار النسخ الاحتياطية**<br>**إرشادات تطبيق الضوابط:**<br>• العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني ، واعتمادها من قبل صاحب الصلاحية.<br>• بما يتماشى مع سياسة تقييم مخاطر للجهة، تحديد خطة النسخ الاحتياطي الدوري للبيانات وإعدادات أنظمة العمل عن بعد.<br>• مراجعة تطبيق إجراءات النسخ الاحتياطي ضمن الخطط الداخلية للجهة.<br>• ضمان استمرارية الأعمال من خلال النسخ الإحتياطية لأنظمة العمل عن بعد.<br>**المخرجات المتوقعة:**<br>• وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية).<br>• خطة موثقة ومعتمدة لعمل النسخ الاحتياطية لأنظمة العمل عن بعد.<br>• دليل لتنفيذ الضوابط التقنية المطلوبة لإجراء النسخ الاحتياطي المخطط له لأنظمة العمل عن بعد وضمان استمرارية الأعمال. |
| ٢-٨-٢ | رجوعاً للضابط ٢- ٩- ٣- ٣ في الضوابط الأساسية للأمن السيبراني، يجب إجراء فحص دوري؛ كل ستة أشهر على الأقل، لتحديد مدى فعالية استعادة النسخ الاحتياطية، الخاصة بأنظمة العمل عن بعد. |
| | **أدوات الأمن السيبراني ذات العلاقة:**<br>• **سياسة النسخ الاحتياطية**<br>• **معيار النسخ الاحتياطية**<br>**إرشادات تطبيق الضوابط:**<br>• العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني ، واعتمادها من قبل صاحب الصلاحية.<br>• استناداً إلى الخطة الدورية للنسخ الاحتياطي المحددة وخطة استمرارية الأعمال ، يتم تحديد واعتماد خطة الاختبار الدورية لأنظمة النسخ الاحتياطي للعمل عن بُعد مرة واحدة على الأقل كل ستة أشهر.<br>• العمل على التأكد من فعالية إجراءات الاستعادة من خلال اجراء اختبار لاستعادة النسخ الاحتياطية بشكل دوري بحيث يضمن قدرة استعادة البيانات وأنظمة العمل عن بعد حسب المدة المحددة في الاجراءات وحسب المدة التي تم حسابها لاكتمال استعادة النسخ الاحتياطية. |

| | |
|---|---|
| | **المخرجات المتوقعة:**<br>• وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية).<br>• وثيقة خطة وإجراءات عمل لتطبيق متطلبات الأمن السيبراني لإدارة النسخ الاحتياطية.<br>• تقارير اختبارات فحص فعالية النسخ الاحتياطية لأنظمة العمل عن بعد ، بحيث يوضح الفرق بين المدة المتوقعة ومدة الاختبار لاستعادة جميع النسخ الاحتياطية. |
| ٢-٩ | إدارة الثغرات (Vulnerabilities Management) |
| الهدف | ضمان اكتشاف الثغرات التقنية في الوقت المناسب ومعالجتها بشكل فعال، وذلك لمنع أو تقليل احتمالية استغلال هذه الثغرات من قبل الهجمات السيبرانية وتقليل الاثار المترتبة على أعمال الجهة. |
| **الضوابط** | |
| ٢-٩-١ | بالإضافة للضوابط الفرعية ضمن الضابط ٢- ١٠ - ٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني لإدارة الثغرات للأصول التقنية وأنظمة العمل عن بعد، بحد أدنى، مايلي: |
| ٢-٩-١-١ | فحص الثغرات واكتشافها على أنظمة العمل عن بعد وتصنيفها حسب خطورتها، مرة واحدة كل ثلاثة أشهر على الأقل. |
| | **أدوات الأمن السيبراني ذات العلاقة:**<br>• سياسة إدارة الثغرات<br>• معيار إدارة الثغرات<br>• إجراء تقييم الثغرات الأمنية<br>• سجل الثغرات<br>**إرشادات تطبيق الضوابط:**<br>• العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني ، واعتمادها من قبل صاحب الصلاحية.<br>• تثبيت وربط تقنيات وأدوات فحص واكتشاف الثغرات مع الأصول المعلوماتية والتقنية لأنظمة العمل عن بعد في الجهة. |

- العمل على تطوير خطة دورية (مرة واحدة كل ثلاثة أشهر على الأقل) وإجراءات لفحص واكتشاف الثغرات على الأصول المعلوماتية والتقنية لأنظمة العمل عن بعد في الجهة.

**المخرجات المتوقعة:**

- وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية).
- إجراءات معتمدة لإدارة الثغرات وخطة دورية (مرة واحدة كل ثلاثة أشهر على الأقل) لفحص واكتشاف الثغرات في أنظمة العمل عن بعد.
- تقارير دورية لفحص واكتشاف الثغرات في أنظمة العمل عن بعد.

| | |
|---|---|
| ٢-٩-١-٢ | معالجة الثغرات على أنظمة العمل عن بعد، مرة واحدة كل ثلاثة أشهر على الأقل. |

**أدوات الأمن السيبراني ذات العلاقة:**

- سياسة إدارة الثغرات
- معيار إدارة الثغرات
- إجراء تقييم الثغرات الأمنية
- سجل الثغرات

**إرشادات تطبيق الضوابط:**

- العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني ، واعتمادها من قبل صاحب الصلاحية.
- مشاركة تقارير فحص واكتشاف الثغرات على الأصول المعلوماتية والتقنية لأنظمة العمل عن بعد في الجهة مع الإدارات المعنية والتي تشمل على سبيل المثال لا الحصر:
  - الإدارة المعنية بإدارة التطبيقات
  - الإدارة المعنية بأجهزة المستخدمين
  - الإدارة المعنية بالبنية التحتية
  - الإدارة المعنية بإدارة قواعد البيانات
  - الإدارة المعنية بالشبكات
- التأكد من ان تقارير الثغرات لأنظمة العمل عن بعد التي تم مشاركتها تحتوي على:
  - وصف للثغرات
  - اسم الأصول المعنية التي تم فحص واكتشاف الثغرات فيها
  - تصنيف للثغرات

| | |
|---|---|
| | • العمل مع الإدارات المعنية لتحديد مدة زمنية وخطة لمعالجة الثغرات، مع الأخذ بعين الاعتبار تصنيف الثغرات وتصنيف الأصول المعنية<br>• وضع آلية للتأكد من معالجة الثغرات بناءً على الخطة. |
| | **المخرجات المتوقعة:**<br>• وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية).<br>• إجراءات إدارة الثغرات.<br>• إجراءات إدارة حزم التحديثات والإصلاحات الأمنية لأنظمة العمل عن بعد.<br>• تقارير فحص واكتشاف الثغرات لأنظمة العمل عن بعد (قبل وبعد المعالجة). |
| ٢-١٠ | اختبار الاختراق (Penetration Testing) |
| الهدف | تقييم مدى فعالية قدرات تعزيز الأمن السيبراني واختباره في الجهة؛ وذلك من خلال عمل محاكاة لتقنيات الهجوم السيبراني الفعلية وأساليبه، وكذلك اكتشاف نقاط الضعف الأمنية غير المعروفة التي قد تؤدي إلى الاختراق السيبراني للجهة؛ وذلك وفقاً للمتطلبات التشريعية والتنظيمية ذات العلاقة. |
| **الضوابط** | |
| ٢-١٠-١ | بالإضافة للضوابط الفرعية ضمن الضابط ٢- ١١- ٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني لاختبار الاختراق لأنظمة العمل عن بعد، بحد أدنى، ما يلي: |
| ٢-١٠-١-١ | نطاق عمل اختبار الاختراق، ليشمل جميع المكونات التقنية لأنظمة العمل عن بعد. |
| | **أدوات الأمن السيبراني ذات العلاقة:**<br>• سياسة اختبار الاختراق<br>• معيار اختبار الاختراق<br>**إرشادات تطبيق الضوابط:**<br>• العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني ، واعتمادها من قبل صاحب الصلاحية.<br>• تحديد جميع المكونات التقنية التي تدعم أنظمة العمل عن بعد. |

| | |
|---|---|
| | • تحديد المتطلبات المسبقة المناسبة والموافقة من أصحاب المصلحة المطلوبة قبل إجراء اختبار الاختراق في أنظمة العمل عن بعد ومكوناته التقنية.<br>• توثيق نطاق اختبار الاختراق والمستوى المسموح به لمختبري الإختراق من قبل الجهة لضمان عدم وجود تأثير على العمليات التشغيلية. |
| | **المخرجات المتوقعة:**<br>• وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية).<br>• وثيقة معتمدة تحدد نطاق اختبار الاختراق لجميع أنظمة العمل عن بعد والمكونات التقنية. |
| ٢-١٠-٢ | رجوعاً للضابط ٢- ١١- ٣- ٢ في الضوابط الأساسية للأمن السيبراني، يجب عمل اختبار الاختراق على أنظمة العمل عن بعد مرة واحدة كل سنة على الأقل. |
| | **أدوات الأمن السيبراني ذات العلاقة:**<br>• سياسة اختبار الاختراق<br>• معيار اختبار الاختراق<br>**إرشادات تطبيق الضوابط:**<br>• العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني ، واعتمادها من قبل صاحب الصلاحية.<br>• استناداً إلى نطاق الاختراق ، يتم القيام بتوثيق المتطلبات المسبقة وموافقات أصحاب المصلحة المطلوبة قبل إجراء اختبار الاختراق على أنظمة العمل عن بُعد والمكونات التقنية التابعة لها.<br>• إعداد الموافقة على الخطة لإجراء اختبار الاختراق وإبلاغ أصحاب المصلحة ذوي الصلة قبل الاختبار لضمان عدم وجود تأثير على العمليات التشغيلية.<br>• تأكد من إجراء اختبار الاختراق المخطط له مرة واحدة على الأقل كل عام على أنظمة العمل عن بعد والمكونات التقنية.<br>• إعداد تقرير اختبار الاختراق لغرض المراجعة والامتثال والمعالجة.<br>• اعداد خطة لمعالجة الثغرات المكتشفة في أنظمة العمل عن بعد و متابعتها بشكل دوري. |
| | **المخرجات المتوقعة:**<br>• وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية). |

| | |
|---|---|
| | • خطة موثقة ومعتمدة لإجراء اختبار الاختراق الدوري لأنظمة العمل عن بعد والمكونات التقنية بحيث تكون مرة واحدة على الأقل كل عام.<br>• تقرير مفصل لاختبار الاختراق لأنظمة العمل عن بعد.<br>• خطة محدثة و موثقة لمعالجة الثغرات المكتشفه في انظمة العمل عن بعد و متابعتها بشكل دوري. |
| ٢-١١ | **إدارة سجلات الأحداث ومراقبة الأمن السيبراني**<br>**(Cybersecurity Event Logs and Monitoring Management)** |
| الهدف | ضمان تجميع سجلات الأمن السيبراني وتحليلها ومراقبتها في الوقت المناسب؛ من أجل الاكتشاف الاستباقي للهجمات السيبرانية، وإدارة مخاطرها بفعالية؛ لمنع الآثار المترتبة على أعمال الجهة أو تقليلها. |
| **الضوابط** | |
| ٢-١١-١ | بالإضافة للضوابط الفرعية ضمن الضابط ٢- ١٢ - ٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات إدارة سجلات الأحداث، ومراقبة الأمن السيبراني للأصول التقنية وأنظمة العمل عن بعد، بحد أدنى، مايلي: |
| ٢-١١-١-١ | تفعيل سجلات الأحداث (Event Logs) الخاصة بالأمن السيبراني على الأصول التقنية وأنظمة العمل عن بعد. |
| | **أدوات الأمن السيبراني ذات العلاقة:**<br>• سياسة إدارة سجلات الأحداث ومراقبة الأمن السيبراني<br>• معيار إدارة سجلات الأحداث ومراقبة الأمن السيبراني<br>**إرشادات تطبيق الضوابط:**<br>• العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني ، واعتمادها من قبل صاحب الصلاحية.<br>• استناداً إلى سياسات الأمن السيبراني للجهة والضوابط الأساسية للأمن السيبراني (ECC) ، يتم تحديد نطاقًا لسجلات الأحداث وإدارة المراقبة لأنظمة العمل عن بُعد ومكوناته التقنية.<br>• تفعيل ومراجعة تسجيل جميع أحداث الأمن السيبراني لأنظمة العمل عن بعد. |
| | **المخرجات المتوقعة:** |

| | |
|---|---|
| • وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية).<br>• صورة شاشة أو مثال مباشر يوضح تفعيل السجلات من خلال نظام مراقبة الأحداث (SIEM). | |
| ٢-١-١١-٢ | مراقبة سلوك مستخدمي أنظمة العمل عن بعد( User Behavior Analytics (UBA) وتحليله. |
| **أدوات الأمن السيبراني ذات العلاقة:**<br>• سياسة إدارة سجلات الأحداث ومراقبة الأمن السيبراني<br>• معيار إدارة سجلات الأحداث ومراقبة الأمن السيبراني<br>**إرشادات تطبيق الضوابط:**<br>• العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني ، واعتمادها من قبل صاحب الصلاحية.<br>• العمل على توفير أنظمة متخصصة لمراقبة سلوك المستخدم وتحليله.<br>• العمل مع الإدارات المعنية في الجهة لتحديد السلوك المقبول للمستخدم على أنظمة العمل عن بعد ليتم تحديد السلوك المشتبه به.<br>• العمل على تطوير إجراءات أمنية (Incedint response playbook) يتم اتخاذها للحالات التي تم دراستها وتحديدها مع الإدارات المعنية تحت إطار السلوك المشتبه به. | |
| **المخرجات المتوقعة:**<br>• وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية).<br>• قائمة بجميع الأنظمة والإعدادات لمراقبة سلوك المستخدم لضمان التحليل المستمر.<br>• قائمة بجميع الحالات التي تمت دراستها وتحليلها (Use cases).<br>• الإجراءات الأمنية (Incedint response playbook). | |
| ٢-١-١١-٣ | مراقبة سجلات الأحداث، الخاصة بالأصول التقنية وأنظمة العمل عن بعد على مدار الساعة. |
| **أدوات الأمن السيبراني ذات العلاقة:**<br>• سياسة إدارة سجلات الأحداث ومراقبة الأمن السيبراني<br>• معيار إدارة سجلات الأحداث ومراقبة الأمن السيبراني | |

**إرشادات تطبيق الضوابط:**

- العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني ، واعتمادها من قبل صاحب الصلاحية.
- العمل على مراقبة جميع أحداث الأمن السيبراني لأنظمة العمل عن بعد على مدار الساعة (365/٣٦٥/٧/٢٤) عن طريق فرق متخصصة.

**المخرجات المتوقعة:**

- وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية).
- مراقبة سجلات الأحداث الخاصة بالأصول التقنية وأنظمة العمل عن بعد على مدار الساعة، على سبيل المثال لا الحصر: جدول يوضح أوقات الفرق المتخصصة للمراقبة على مدار الساعة.
- عقد يوضح فيه نموذج المراقبة المتبع في حال كان مركز العمليات الأمنية أو المراقبة من قبل مقدم خدمة.

| | |
|---|---|
| ٢-١١-١-٤ | تحديث إجراءات مراقبة الأمن السيبراني على مدار الساعة وتطبيقها، بحيث تشمل مراقبة عمليات الدخول عن بعد، ولاسيما عمليات الدخول عن بعد من خارج المملكة والتحقق من صحتها. |

**أدوات الأمن السيبراني ذات العلاقة:**

- سياسة إدارة سجلات الأحداث ومراقبة الأمن السيبراني
- معيار إدارة سجلات الأحداث ومراقبة الأمن السيبراني

**إرشادات تطبيق الضوابط:**

- العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني ، واعتمادها من قبل صاحب الصلاحية.
- مراجعة إجراءات مراقبة الأمن السيبراني والتحقق منها وتحديثها وتنفيذ الضوابط للمراقبة على مدار الساعة.
- قد تشمل مراقبة وتحليل سجلات الأحداث، على سبيل المثال لا الحصر: عمليات الوصول عن بعد داخل المملكة أو من خارج المملكة العربية السعودية بعد التحقق من صحتها ، وسجلات أحداث التطبيق ، وسجلات أحداث النظام ، وسجلات أحداث التخزين ، وسجلات أحداث مكافحة الفيروسات ، وسجلات الحوادث وغيرها.
- العمل على حفظ جميع الأنشطة والسجلات لعمليات الدخول عن بعد والتأكد من إرسالها لمركز العمليات والمراقبة لضمان مراقبتها باستمرار من قبل الفرق المتخصصة عن طريق ربط سجلات الدخول مع أنظمة المراقبة مثال: نظام (SEIM).

| | |
|---|---|
| | **المخرجات المتوقعة:**<br>• وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية).<br>• وثيقة إجراءات مراقبة الأمن السيبراني بحيث تشمل مراقبة عمليات الدخول عن بعد، ولاسيما عمليات الدخول عن بعد من خارج المملكة والتحقق من صحتها.<br>• دليل يوضح مراقبة أحداث الدخول عن بعد على مدار الساعة عن طريق مركز العمليات الأمنية الخاص بالجهة. |
| ٢-١١-٢ | رجوعاً للضابط ٢- ١٢ - ٣- ٥ في الضوابط الأساسية للأمن السيبراني، يجب ألا تقل مدة الاحتفاظ بسجلات الأحداث الخاصة بالأمن السيبراني لأنظمة العمل عن بعد عن ١٢ شهراً؛ حسب المتطلبات التشريعية والتنظيمية ذات العلاقة. |
| | **إرشادات تطبيق الضوابط:**<br>• العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني ، واعتمادها من قبل صاحب الصلاحية.<br>• تحديد وتطوير آلية لتخزين جميع سجلات أحداث الأمن السيبراني لأنظمة العمل عن بعد والمكونات التقنية لمدة احتفاظ لا تقل عن ١٢ شهرًا أو أكثر ، وفقًا للمتطلبات التشريعية والتنظيمية ذات الصلة.<br>• تحديد وتوثيق واعتماد الضوابط الآمنة لأرشفة أو مسح السجلات المخزنة وفقًا لسياسة الاحتفاظ والأمن السيبراني للجهة المحددة لأنظمة العمل عن بُعد. |
| | **المخرجات المتوقعة:**<br>• وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية).<br>• لقطة شاشة أو دليل مباشر من نظام SIEM يعرض مدة حفظ السجلات لمدة ١٢ شهرًا على الأقل.<br>• عينة من السجلات المخزنة المستخرجة من نظام SIEM يبين أنها تم الاحتفاظ بالسجلات لمدة ١٢ شهرًا على الأقل. |
| **٢-١٢** | **إدارة حوادث وتهديدات الأمن السيبراني (Cybersecurity Incident and Threat Management)** |
| الهدف | ضمان تحديد واكتشاف حوادث الأمن السيبراني في الوقت المناسب وإدارتها بشكل فعال والتعامل مع تهديدات الأمن السيبراني استباقياً من أجل منع أو تقليل الآثار المترتبة على أعمال الجهة. مع مراعاة ما ورد في الامر السامي الكريم رقم ٣٧١٤٠ تاريخ ١٤٣٨/٨/١٤هـ |

| | |
|---|---|
| ٢-١٢-١ | بالإضافة للضوابط الفرعية ضمن الضابط ٢- ١٣ - ٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات إدارة حوادث وتهديدات الأمن السيبراني في الجهة، بحد أدنى، مايلي: |
| ٢-١٢-١-١ | تحديث خطط الاستجابة لحوادث الأمن السيبراني ومعلومات التواصل داخل الجهة بما يتوافق مع حالة العمل عن بعد، وبما يضمن القدرة على التواصل وجاهزية فرق الاستجابة للحوادث. |
| **أدوات الأمن السيبراني ذات العلاقة:**<br>• سياسة إدارة حوادث وتهديدات الأمن السيبراني<br>• معيار إدارة حوادث وتهديدات الأمن السيبراني<br>• نماذج الخطط التفصيلية للاستجابة لحوادث الأمن السيبراني<br>**إرشادات تطبيق الضوابط:**<br>• العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني ، واعتمادها من قبل صاحب الصلاحية.<br>• استناداً إلى سياسات إدارة التهديدات وحوادث الأمن السيبراني للجهة ، يتم تحديد خطط الاستجابة والمعلومات ذات الصلة وأنظمة العمل عن بُعد والقيام بتحديثها.<br>• الإعداد والتخطيط لتشغيل الحملات المناسبة للإبلاغ عن الحوادث السيبرانية وسياسات إدارة التهديدات ، لمنع الإجراءات المضللة من قبل مستخدمي العمل عن بعد.<br>• إبلاغ المستخدمين حول كيفية رفع الحوادث السيبرانية في حالة الاشتباه في وجود نشاط أو حدث فعلي وإظهار استعداد فريق الاستجابة للحوادث بالجهة. | |
| **المخرجات المتوقعة:**<br>• وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية).<br>• خطط استجابة محدثة لأنظمة العمل عن بعد.<br>• خطة موثقة ومعتمدة لعمل حملات لنشر سياسات إدارة الحوادث والتهديدات السيبرانية.<br>• عينة لتقرير إبلاغ من مستخدمي العمل عن بعد عن حادثة سيبرانية. | |
| ٢-١٢-١-٢ | الحصول على المعلومات الاستباقية (Threat Intelligence) ذات العلاقة بأنظمة العمل عن بعد بشكل دوري والتعامل معها. |
| **أدوات الأمن السيبراني ذات العلاقة:** | |

- سياسة إدارة حوادث وتهديدات الأمن السيبراني
- معيار إدارة حوادث وتهديدات الأمن السيبراني
- نماذج الخطط التفصيلية للاستجابة لحوادث الأمن السيبراني

**إرشادات تطبيق الضوابط:**

- العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني ، واعتمادها من قبل صاحب الصلاحية.
- العمل على الاشتراك مع المنصات المسؤولة عن ارسال المعلومات الاستباقية (Threat Intelligence) عن طريق البريد الإلكتروني أو المنصات التقنية الأخرى، ومن هذه المنصات:
  - المركز الوطني الإرشادي للأمن السيبراني (Saudi CERT).
  - منصة مشاركة المعلومات الخاصة بحصين.
  - النشرة البريدية الخاصة بهيئة الاتصالات وتقنية المعلومات.
  - النشرات المقدمة من قبل الشركات المختصة بالأمن السيبراني.
  - النشرات المقدمة من قبل مقدمي الخدمات الأمنية والتقنية التي تم التعاقد معها مسبقاً من قبل الجهة.
- العمل على التعامل مع التنبيهات المرسلة من قبل هذه المنصات من خلال:
  - ارسالها للفريق المعني للتعامل معها (على سبيل المثال لا الحصر: إدارة تقنية المعلومات، مركز العمليات الأمنية، الإدارة الخاصة بالتحديثات والاصلاحات).
  - تحديد مدة للتعامل مع هذه التنبيهات حسب مستوى الخطورة.
  - المتابعة المستمرة للتأكد من انه تم التعامل مع التنبيهات المرسلة للفريق المعني بشكل أمن (على سبيل المثال لا الحصر: التأكد من تطبيق التحديث الخاص بالثغرات المرسلة).

**المخرجات المتوقعة:**

- وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية).
- لقطة شاشة أو دليل مباشر توضح اشتراك الجهة مع أحد المنصات.
- لقطة شاشة أو دليل حي لمثال من التنبيهات على أنظمة العمل عن بعد التي تم التعامل معها مسبقاً حسب الاجراءات اللازمة.

| | |
|---|---|
| ٢-١٢-١-٣ | تنفيذ وتطبيق التوصيات والتنبيهات الخاصة بحوادث وتهديدات الأمن السيبراني الصادرة من مشرف القطاع أو الهيئة الوطنية للأمن السيبراني. |

**أدوات الأمن السيبراني ذات العلاقة:**

- سياسة إدارة حوادث وتهديدات الأمن السيبراني

- معيار إدارة حوادث وتهديدات الأمن السيبراني
- نماذج الخطط التفصيلية للاستجابة لحوادث الأمن السيبراني

**إرشادات تطبيق الضوابط:**

- العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني ، واعتمادها من قبل صاحب الصلاحية.
- تطوير آلية لتلقي المعلومات باستمرار من منصات معلومات الإستباقية والمعلومات الصادرة عن الهيئة الوطنية.
- تطوير واعتماد وتطبيق آلية لمعالجة التوصيات الواردة للتنبيهات / الحوادث / التهديدات السيبرانية.
- التواصل بالمخاطر / التهديدات / الحوادث السيبرانية المحددة مع فريق الأمن السيبراني ولجنة المخاطر لضمان اتخاذ قرار استباقي لتقليل التأثير على العمليات التشغيلية.

**المخرجات المتوقعة:**

- وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية).
- وثيقة معتمدة لمعالجة التوصيات المتعلقة بحوادث وتهديدات من قبل مشرف القطاع أو الهيئة الوطنية للأمن السيبراني.
- وثيقة لعملية إبلاغ الحوادث / التهديدات السيبرانية لفريق الأمن السيبراني بالجهة والتعامل معها.

## ٣ الأمن السيبراني المتعلق بالأطراف الخارجية والحوسبة السحابية (Third-Party and Cloud Computing Cybersecurity)

| ١-٣ | الأمن السيبراني المتعلق بالحوسبة السحابية والاستضافة (Cloud Computing and Hossting Cybersecurity) |
|---|---|
| الهدف | ضمان معالجة المخاطر السيبرانية، وتنفيذ متطلبات الأمن السيبراني للحوسبة السحابية،والاستضافة بشكل ملائم وفعّال؛ وذلك وفقاً للسياسات والإجراءات التنظيمية للجهة، والمتطلبات التشريعية، والتنظيمية، والأوامر، والقرارات ذات العلاقة. وضمان حماية الأصول المعلوماتية والتقنية للجهة، على خدمات الحوسبة السحابية؛ التي تتم استضافتها، أو معالجتها، أو إدارتها بواسطة أطراف خارجية. |
| **الضوابط** | |
| ١-١-٣ | بالإضافة للضوابط الفرعية ضمن الضابط ٤ - ٢- ٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني الخاصة باستخدام خدمات الحوسبة السحابية والاستضافة، بحد أدنى، ما يلي: |
| ١-١-١-٣ | موقع استضافة أنظمة العمل عن بعد يجب أن يكون داخل المملكة. |
| | **أدوات الأمن السيبراني ذات العلاقة:**<br>• سياسة الأمن السيبراني المتعلق بالحوسبة السحابية والاستضافة<br>**إرشادات تطبيق الضوابط:**<br>• العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني ، واعتمادها من قبل صاحب الصلاحية.<br>• التأكد من استضافة أنظمة العمل عن بعد الخاصة بالجهة، أو أي جزء من مكوناتها التقنية في مكان موثوق وآمن داخل المملكة العربية السعودية.<br>**المخرجات المتوقعة:**<br>• وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية). |

| | |
|---|---|
| | • وثيقة رسمية تُثبت أن استضافة أنظمة العمل عن بعد الخاصة بالجهة، أو أي جزء من مكوناتها التقنية في مكان موثوق وآمن داخل المملكة العربية السعودية. |