



الهيئة الوطنية للأمن السيبراني  
National Cybersecurity Authority

# الضوابط الأساسية للأمن السيبراني

Essential Cybersecurity Controls

(ECC - 1 : 2018)

إشارة المشاركة: أبيض  
تصنيف الوثيقة: غير مصنف



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 أربعةألوان (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 للتسليم.

### برتقالي - مشاركة محدودة

المستلم بالإشارة البرترقالية يمكنه مشاركة المعلومات في نفس المنشأة مع الأشخاص المعنيين 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

|    |   |
|----|---|
| ١  | الملخص التنفيذي   |
| ٧  | المقدمة   |
| ٨  | الأهداف   |
| ٩  | نطاق العمل وقابلية التطبيق  |
| ٩  | نطاق عمل الضوابط  |
| ٩  | قابلية التطبيق داخل الجهة (ECC Statement of Applicability)  |
| ١٠ | التنفيذ والالتزام   |
| ١٠ | أداة التقييم وقياس الالتزام   |
| ١٠ | التحديث والمراجعة   |
| ١١ | مكونات وهيكلية الضوابط الأساسية للأمن السيبراني   |
| ١١ | المكونات الأساسية   |
| ١٢ | المكونات الفرعية  |
| ١٣ | الهيكلية  |
| ١٤ | الضوابط الأساسية للأمن السيبراني  |
| ١٤ | ١- حوكمة الأمان السيبراني (Cybersecurity Governance)  |
| ١٩ | ٢- تعزيز الأمان السيبراني (Cybersecurity Defense)   |
| ٢٦ | ٣- صمود الأمان السيبراني (Cybersecurity Resilience)   |
|    | ٤- الأمان السيبراني المتعلق بالأطراف الخارجية والحوسبة السحابية (Third-Party and Cloud Computing Cybersecurity) |
| ٢٩ | ٥- الأمان السيبراني لأنظمة التحكم الصناعي (Industrial Control Systems Cybersecurity)                            |
|    | ملحق  |
| ٣٠ | ملحق (أ): مصطلحات وتعريفات  |
| ٣٨ | ملحق (ب): قائمة الاختصارات  |
|    | قائمة الجداول   |
| ٣٣ | جدول ١: هيكلية الضوابط  |
| ٣٠ | جدول ٢: مصطلحات وتعريفات  |
| ٣٨ | جدول ٣: قائمة الاختصارات  |
|    | قائمة الأشكال والرسوم التوضيحية   |
| ١١ | شكل ١: المكونات الأساسية للضوابط  |
| ١٢ | شكل ٢: المكونات الفرعية للضوابط   |
| ١٣ | شكل ٣: معنى رموز الضوابط  |
| ١٣ | شكل ٤: هيكلية الضوابط   |

## الملخص التنفيذي

كما جاءت ملبياً لجوانب التحديث ومتابعة الالتزام من قبل الجهات الحكومية وغير الحكومية بما يعزز دور الأمن السيبراني وأهميته وال الحاجة الملحة التي ازدادت مع ازدياد التهديدات والمخاطر الأمنية في الفضاء السيبراني أكثر من أي وقت مضى.

وقد نص التنظيم المشار إليه أن مسؤولية هذه الهيئة لا يُخلي أي جهة عامة أو خاصة أو غيرها من مسؤوليتها تجاه أمنها السيبراني، وهو ما أكدته الأمر السامي الكريم رقم ٥٧٣١ وتاريخ ١٤٣٩/١١/١٠هـ بأن «على جميع الجهات الحكومية رفع مستوى أمنها السيبراني لحماية شبكاتها وأنظمتها وبياناتها الإلكترونية، والالتزام بما تصدره الهيئة الوطنية للأمن السيبراني من سياسات وأطر ومعايير وضوابط وإرشادات بهذا الشأن».

ومن هذا المنطلق، قامت الهيئة الوطنية للأمن السيبراني بتطوير الضوابط الأساسية للأمن السيبراني (ECC) لوضع الحد الأدنى من متطلبات الأمان السيبراني في الجهات الوطنية التي تندرج تحت نطاق عمل هذه الضوابط. وتوضح هذه الوثيقة تفاصيل هذه الضوابط، وأهدافها، ونطاق العمل وقابلية التطبيق، وآلية الالتزام ومتابعته.

وعلى مختلف الجهات الوطنية تنفيذ ما يحقق الالتزام الدائم والمستمر بهذه الضوابط، تحقيقاً لما ورد في الفقرة الثالثة من المادة العاشرة في تنظيم الهيئة الوطنية للأمن السيبراني وكذلك ما ورد في الأمر السامي الكريم رقم ٥٧٣١ وتاريخ ١٤٣٩/١١/١٠هـ

استهدفت رؤية المملكة العربية السعودية ٢٠٣٠ التطوير الشامل للوطن وأمنه واقتصاده ورفاهية مواطنيه وعيشهم الكريم، ولقد كان من الطبيعي أن يكون أحد مستهدفاتها التحول نحو العالم الرقمي وتنمية البنية التحتية الرقمية؛ بما يعبر عن مواكبة التقدم العالمي المتتسارع في الخدمات الرقمية وفي الشبكات العالمية المتعددة، وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية، ويتماشى مع تنامي قدرات المعالجة الحاسوبية وقدرات التخزين الهائلة للبيانات وتراسلها، وبما يهيئ للتعامل مع معطيات الذكاء الاصطناعي وتحولات الثورة الصناعية الرابعة.

إن هذا التحول يتطلب انسيابية المعلومات وأمانها وتكامل أنظمتها، ويستوجب المحافظة على الأمن السيبراني للمملكة العربية السعودية، وتعزيزه، حماية للمصالح الحيوية للدولة وأمنها الوطني والبني التحتية الحساسة والقطاعات ذات الأولوية والخدمات والأنشطة الحكومية؛ لذلك أتى تأسيس الهيئة الوطنية للأمن السيبراني والموافقة على تنظيمها بموجب الأمر الملكي الكريم رقم ٦٨٠١ وتاريخ ١٤٣٩/٢/١١هـ، وجعلها الجهة المختصة في المملكة بالأمن السيبراني، والمراجع الوطني في شؤونه.

لقد جاءت مهامات هذه الهيئة واحتياصاتها ملبياً لجوانب الاستراتيجية، ولجوانب وضع السياسات وآليات الحكومة والأطر ومعايير والضوابط والإرشادات المتعلقة بالأمن السيبراني وتعديدها على الجهات.

## المقدمة

قامت الهيئة الوطنية للأمن السيبراني (ويشار لها في هذه الوثيقة بـ "الهيئة") بتطوير الضوابط الأساسية للأمن السيبراني (ECC : 1 - 2018) بعد دراسة عدة معايير وأطر وضوابط للأمن السيبراني قامت بإعدادها سابقاً عدة جهات ومنظمات (محليه ودولية)، ودراسة متطلبات التشريعات والتنظيمات والقرارات الوطنية ذات العلاقة، وبعد الاطلاع على أفضل الممارسات والتجارب في مجال الأمن السيبراني والاستفادة منها، وتحليل ما تم رصده من حوادث وهجمات سيبرانية على مستوى الجهات الحكومية وغيرها من الجهات الحساسة، وبعد استطلاع آراء العديد من الجهات الوطنية وأخذ مئياتها.

ت تكون هذه الضوابط من:

- ٠ مكونات أساسية (Main Domains) لضوابط الأمان السيبراني
- ٢٩ مكوناً فرعياً (Subdomains) لضوابط الأمان السيبراني
- ١١٤ ضابطاً أساسياً (Controls) للأمن السيبراني

كما أن هذه الضوابط مرتبطة مع المتطلبات التشريعية والتنظيمية الوطنية والدولية ذات العلاقة.

## الأهداف

تهدف هذه الضوابط إلى توفير الحد الأدنى من المتطلبات الأساسية للأمن السيبراني المبنية على أفضل الممارسات والمعايير لتقليل المخاطر السيبرانية على الأصول المعلوماتية والتقنية للجهات من التهديدات (Threats) الداخلية والخارجية. وتنطلب حماية الأصول المعلوماتية والتقنية للجهة التركيز على الأهداف الأساسية للحماية، وهي:

- سرية المعلومة (Confidentiality)
- سلامة المعلومة (Integrity)
- توافر المعلومة (Availability)

وتأخذ هذه الضوابط بالاعتبار المحاور الأربع الأساسية التي يرتكز عليها الأمان السيبراني، وهي:

- الإستراتيجية (Strategy)
- الأشخاص (People)
- الإجراء (Process)
- التقنية (Technology)

نطاق العمل وقابلية التطبيق

نطاق عمل الضوابط

تُطبّق هذه الضوابط على الجهات الحكومية في المملكة العربية السعودية (وتشمل الوزارات والهيئات والمؤسسات وغيرها) والجهات والشركات التابعة لها، وجهات القطاع الخاص التي تمتلك بني تحتية وطنية حساسة ("CNIs") (Critical National Infrastructures) أو تقوم بتشغيلها أو استضافتها، (ويشار لها جمِيعاً في هذا الوثيقة بـ "الجهة"). كما تُشجع الهيئة الجهات الأخرى في المملكة وبشدة على الاستفادة من هذه الضوابط لتطبيق أفضل الممارسات فيما يتعلق بتحسين الأمن السيبراني وتطويره داخل الجهة.

## **(ECC Statement of Applicability) المهمة ذات الصلة (ECC Statement of Applicability)**

تم إعداد هذه الضوابط بحيث تكون ملائمة لاحتياجات الأمن السيبراني لجميع الجهات والقطاعات في المملكة العربية السعودية بتنوع طبيعة أعمالها، ويجب على كل جهة الالتزام بجميع الضوابط القائلة للتطبيق، عليها.

من الأمثلة على الضوابط التي تتفاوت فيها قابلية التطبيق من جهة إلى أخرى حسب طبيعة أعمال الجهة واستخدامها للتقنيات المذكورة:

- الضوابط ضمن المكون الفرعي رقم (٤-٢) المتعلقة بالأمن السيبراني للحوسبة السحابية والاستضافة (Cloud Computing and Hosting Cybersecurity) تكون قابلة التطبيق وملزمة على الجهة التي تستخدم حالياً خدمات الحوسبة السحابية والاستضافة أو تخطط لاستخدامها.
  - الضوابط ضمن المكون الرئيسي رقم (٥) المتعلقة بالأمن السيبراني لأنظمة التحكم الصناعي (Industrial Control Systems Cybersecurity) تكون قابلة التطبيق وملزمة على الجهة التي تستخدم حالياً أنظمة التحكم الصناعي أو تخطط لاستخدامها.

## التنفيذ والالتزام

تحقيقاً لما ورد في الفقرة الثالثة من المادة العاشرة في تنظيم الهيئة الوطنية للأمن السيبراني وكذلك ما ورد في الأمر السامي الكريم رقم ٥٧٣١ وتاريخ ١٤٣٩/١١/٠ هـ، يجب على جميع الجهات ضمن نطاق عمل هذه الضوابط تنفيذ ما يحقق الالتزام الدائم والمستمر بهذه الضوابط.

تقوم الهيئة بتقييم التزام الجهات بما ورد في هذه الضوابط بطرق متعددة، منها: التقييم الذاتي للجهات، التقارير الدورية لأدابة الالتزام و/أو الزيارات الميدانية للتدقيق، وفق الآلية التي تراها الهيئة مناسبة لذلك.

### أداة التقييم وقياس الالتزام

سوف تقوم الهيئة بإصدار أداة (ECC – 1 : 2018 Assessment and Compliance Tool) لتنظيم عملية تقييم وقياس مدى التزام الجهات بتطبيق الضوابط الأساسية للأمن السيبراني.

## التحديث والمراجعة

تتولى الهيئة التحديث والمراجعة الدورية للضوابط الأساسية للأمن السيبراني حسب متطلبات الأمن السيبراني والمستجدات ذات العلاقة. كما تتولى الهيئة إعلان الإصدار المحدث من الضوابط لتطبيقه والالتزام به.

## مكونات وهيكلية الضوابط الأساسية للأمن السيبراني

### المكونات الأساسية

يوضح الشكل ١ أدناه المكونات الأساسية للضوابط.



شكل ١: المكونات الأساسية للضوابط

## المكونات الفرعية

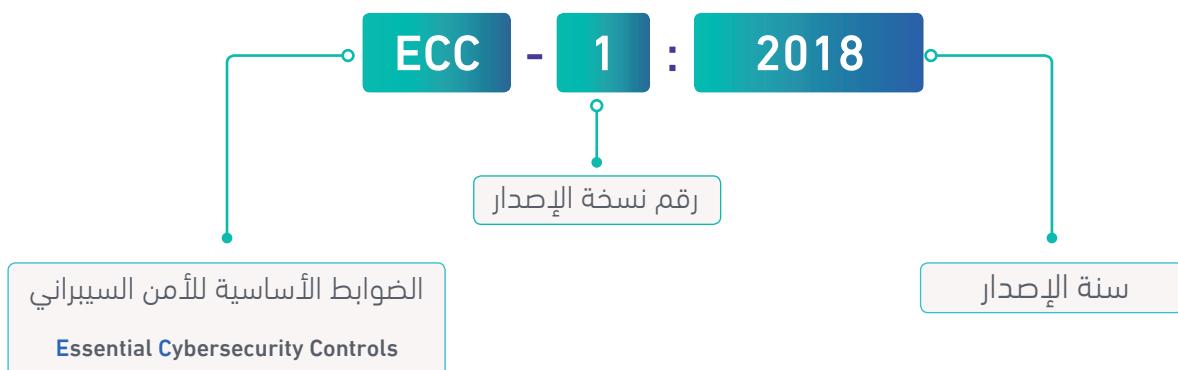
يوضح الشكل ٢ أدناه المكونات الفرعية للضوابط.

|  |        |  |        |  |
|--|--------|--|--------|--|
| إدارة الأمان السيبراني<br>Cybersecurity Management   | ٢-١    | إستراتيجية الأمان السيبراني<br>Cybersecurity Strategy  | ١-١    | ١ - حوكمة الأمان السيبراني<br><br><b>Cybersecurity Governance</b>  |
| أدوار ومسؤوليات الأمان السيبراني<br>Cybersecurity Roles and Responsibilities   | ٤-١    | سياسات وإجراءات الأمان السيبراني<br>Cybersecurity Policies and Procedures                        | ٣-١    |  |
| الأمن السيبراني ضمن إدارة المشاريع المعلوماتية<br>والتقنية<br>Cybersecurity in Information Technology Projects                     | ٦-١    | إدارة مخاطر الأمان السيبراني<br>Cybersecurity Risk Management                                    | ٥-١    |  |
| المراجعة والتدقيق الدوري للأمن السيبراني<br>Cybersecurity Periodical Assessment and Audit  | ٨-١    | الالتزام بتشريعات وتنظيمات ومعايير الأمان<br>السيبراني<br>Cybersecurity Regulatory Compliance    | ٧-١    |  |
| برنامج التوعية والتدريب بالأمان السيبراني<br>Cybersecurity Awareness and Training Program  | ١٠-١   | الأمن السيبراني المتعلق بالموارد البشرية<br>Cybersecurity in Human Resources                     | ٩-١    |  |
| إدارة هويات الدخول والصلحيات<br>Identity and Access Management   | ٢ - ٢  | إدارة الأصول<br>Asset Management   | ١ - ٢  | ٢ - تعزيز الأمان السيبراني<br><br><b>Cybersecurity Defense</b>   |
| حماية البريد الإلكتروني<br>Email Protection  | ٤ - ٢  | حماية الأنظمة وأجهزة معالجة المعلومات<br>Information System and Processing Facilities Protection | ٣ - ٢  |  |
| أمن الأجهزة المحمولة<br>Mobile Devices Security  | ٦ - ٢  | إدارة أن الشبكات<br>Networks Security Management   | ٥ - ٢  |  |
| التشفير<br>Cryptography  | ٨ - ٢  | حماية البيانات والمعلومات<br>Data and Information Protection                                     | ٧ - ٢  |  |
| إدارة الثغرات<br>Vulnerabilities Management  | ١٠ - ٢ | إدارة النسخ الاحتياطية<br>Backup and Recovery Management   | ٩ - ٢  |  |
| إدارة سجلات الأحداث ومراقبة الأمان السيبراني<br>Cybersecurity Event Logs and Monitoring Management                                 | ١٢ - ٢ | اختبار الاختراق<br>Penetration Testing   | ١١ - ٢ | ٣ - صمود الأمان السيبراني<br><br><b>Cybersecurity Resilience</b>   |
| الأمن المادي<br>Physical Security  | ١٤ - ٢ | إدارة حوادث وتهديدات الأمان السيبراني<br>Cybersecurity Incident and Threat Management            | ١٣ - ٢ |  |
| حماية تطبيقات الويب<br>Web Application Security  |        |  | ١٠ - ٢ |  |
| جوانب صمود الأمان السيبراني في إدارة استمرارية الأعمال<br>Cybersecurity Resilience aspects of Business Continuity Management (BCM) |        |  | ١ - ٣  |  |
| الأمن السيبراني المتعلق بالحوسبة السحابية<br>والاستضافة<br>Cloud Computing and Hosting Cybersecurity                               | ٢ - ٤  | الأمن السيبراني المتعلق بالأطراف الخارجية<br>Third-Party Cybersecurity                           | ١ - ٤  |  |
| حماية أجهزة وأنظمة التحكم الصناعي<br>Industrial Control Systems (ICS) Protection   |        |  | ١ - ٠  | ٤ - الأمان السيبراني المتعلق<br>بالأطراف الخارجية والمحسبة<br>السحابية<br><br><b>Third-Party and Cloud Computing Cybersecurity</b> |
|  |        |  |        | ٥ - الأمان السيبراني لأنظمة<br>التحكم الصناعي<br><br><b>ICS Cybersecurity</b>  |

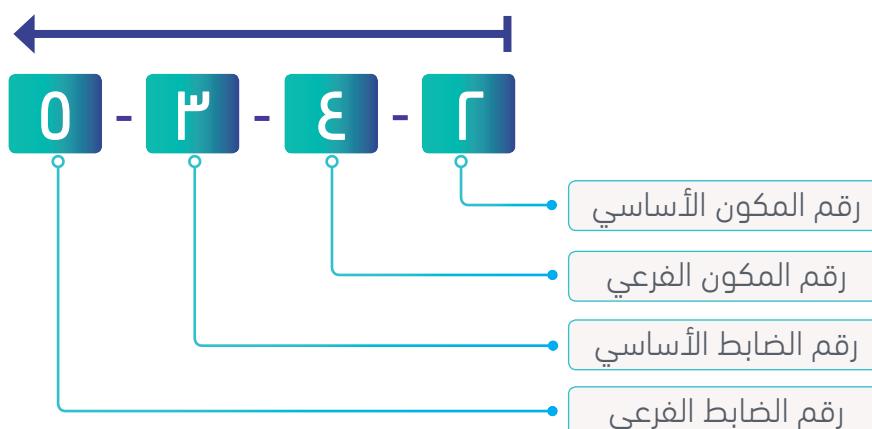
شكل ٢: المكونات الفرعية للضوابط

**الهيكلية**

يوضح الشكلان ٣ و٤ أدناه معنى رموز الضوابط.



شكل ٣: معنى رموز الضوابط



شكل ٤: هيكلية الضوابط

يوضح الجدول (١) أدناه طريقة هيكلية الضوابط

جدول ١: هيكلية الضوابط

|                          |                         |
|--------------------------|-------------------------|
| اسم المكون الأساسي       | ١                       |
| رقم مرجعي للمكون الأساسي |                         |
| اسم المكون الفرعي        | رقم مرجعي للمكون الفرعي |
|                          | الهدف                   |
|                          | الضوابط                 |
| بنود الضابط              | رقم مرجعي للضابط        |

## الضوابط الأساسية للأمن السيبراني

### تفاصيل الضوابط الأساسية للأمن السيبراني

#### **حكومة الأمن السيبراني (Cybersecurity Governance)**



##### **استراتيجية الأمن السيبراني**

١-١

ضمان إسهام خطط العمل للأمن السيبراني والأهداف والمبادرات والمشاريع داخل الجهة في تحقيق المتطلبات التشريعية والتنظيمية ذات العلاقة.

الهدف

##### **الضوابط**

يجب تحديد وتوثيق واعتماد إستراتيجية الأمن السيبراني للجهة ودعمها من قبل رئيس الجهة أو من ينفيه (ويشار له في هذه الضوابط باسم «صاحب الصلاحية»)، وأن تتماشى الأهداف الإستراتيجية للأمن السيبراني للجهة مع المتطلبات التشريعية والتنظيمية ذات العلاقة.

١-١-١

يجب العمل على تنفيذ خطة عمل لتطبيق إستراتيجية الأمن السيبراني من قبل الجهة.

١-١-٢

يجب مراجعة إستراتيجية الأمن السيبراني على فترات زمنية مخططة لها (أو في حالة حدوث تغييرات في المتطلبات التشريعية والتنظيمية ذات العلاقة).

١-١-٣

##### **إدارة الأمن السيبراني**

٢-١

ضمان التزام ودعم صاحب الصلاحية للجهة فيما يتعلق بإدارة وتطبيق برامج الأمن السيبراني في تلك الجهة وفقاً للمتطلبات التشريعية والتنظيمية ذات العلاقة.

الهدف

##### **الضوابط**

يجب إنشاء إدارة معنية بالأمن السيبراني في الجهة مستقلة عن إدارة تقنية المعلومات والاتصالات (ICT / IT) (وفقاً للأمر السامي الكريم رقم ٣٧٤٠ وتاريخ ١٤٣٨ / ٨ / ١٤ هـ). ويفضل ارتباطها مباشرة برئيس الجهة أو من ينفيه، مع الأخذ بالاعتبار عدم تعارض المصالح.

١-٢-١

يجب أن يشغل رئاسة الإدارة المعنية بالأمن السيبراني والوظائف الإشرافية والحساسة بها مواطنون متفرغون ذو كفاءة عالية في مجال الأمن السيبراني.

٢-٢-١

يجب إنشاء لجنة إشرافية للأمن السيبراني بتوجيه من صاحب الصلاحية للجهة لضمان التزام ودعم ومتابعة تطبيق برامج وتشريعات الأمن السيبراني، ويتم تحديد وتوثيق واعتماد أعضاء اللجنة ومسؤولياتها وإطار حوكمة أعمالها على أن يكون رئيس الإدارة المعنية بالأمن السيبراني أحد أعضائها. ويفضل ارتباطها مباشرة برئيس الجهة أو من ينفيه، مع الأخذ بالاعتبار عدم تعارض المصالح.

٣-٢-١

##### **سياسات وإجراءات الأمن السيبراني**

٣-١

ضمان توثيق ونشر متطلبات الأمن السيبراني والتزام الجهة بها، وذلك وفقاً لمتطلبات الأعمال التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

الهدف

| الضوابط  |       |
|--|-------|
| يجب على الإدارة المعنية بالأمن السيبراني في الجهة تحديد سياسات وإجراءات الأمان السيبراني وما تشمله من ضوابط ومتطلبات الأمان السيبراني، وتوثيقها واعتمادها من قبل صاحب الصلاحية في الجهة، كما يجب نشرها إلى ذوي العلاقة من العاملين في الجهة والأطراف المعنية بها.                              | ١-٣-١ |
| يجب على الإدارة المعنية بالأمن السيبراني ضمن تطبيق سياسات وإجراءات الأمان السيبراني في الجهة وما تشمله من ضوابط ومتطلبات.  | ٢-٣-١ |
| يجب أن تكون سياسات وإجراءات الأمان السيبراني مدعومة بمعايير تقنية أمنية (على سبيل المثال: المعايير التقنية للأمنية لجدار الحماية وقواعد البيانات، وأنظمة التشغيل، إلخ).  | ٣-٣-١ |
| يجب مراجعة سياسات وإجراءات ومعايير الأمان السيبراني وتحديثها على فترات زمنية مخططة لها (أو في حالة حدوث تغييرات في المتطلبات التشريعية والتنظيمية والمعايير ذات العلاقة)، كما يجب توثيق التغييرات واعتمادها.   | ٤-٣-١ |
| ٤- أدوار ومسؤوليات الأمان السيبراني  |       |
| ضمان تحديد أدوار ومسؤوليات واضحة لجميع الأطراف المشاركة في تطبيق ضوابط الأمان السيبراني في الجهة.  | الهدف |
| الضوابط  |       |
| يجب على صاحب الصلاحية تحديد وتوثيق واعتماد الهيكل التنظيمي للحكومة والأدوار والمسؤوليات الخاصة بالأمن السيبراني للجهة، وتكييف الأشخاص المعنيين بها، كما يجب تقديم الدعم اللازم لإنفاذ ذلك، مع الأخذ بالاعتبار عدم تعارض المصالح.   | ١-٤-١ |
| يجب مراجعة أدوار ومسؤوليات الأمان السيبراني في الجهة وتحديثها على فترات زمنية مخططة لها (أو في حالة حدوث تغييرات في المتطلبات التشريعية والتنظيمية ذات العلاقة).   | ٢-٤-١ |
| ٥- إدارة مخاطر الأمان السيبراني  |       |
| ضمان إدارة مخاطر الأمان السيبراني على نحو ممنهج يهدف إلى حماية الأصول المعلوماتية والتقنية للجهة، وذلك وفقاً للسياسات والإجراءات التنظيمية للجهة والمتطلبات التشريعية والتنظيمية ذات العلاقة.  | الهدف |
| الضوابط  |       |
| يجب على الإدارة المعنية بالأمن السيبراني في الجهة تحديد وتوثيق واعتماد منهجية وإجراءات إدارة مخاطر الأمان السيبراني في الجهة، وذلك وفقاً لاعتبارات السرية وتوافر وسلامة الأصول المعلوماتية والتقنية.   | ١-٥-١ |
| يجب على الإدارة المعنية بالأمن السيبراني تطبيق منهجية وإجراءات إدارة مخاطر الأمان السيبراني في الجهة.  | ٢-٥-١ |
| يجب تنفيذ إجراءات تقييم مخاطر الأمان السيبراني بحد أدنى في الحالات التالية:<br>١-٣-٠-١ في مرحلة مبكرة من المشاريع التقنية.<br>١-٣-٠-٢ قبل إجراء تغيير جوهري في البنية التقنية.<br>١-٣-٠-٣ عند التخطيط للحصول على خدمات طرف خارجي.<br>١-٣-٠-٤ عند التخطيط وقبل إطلاق منتجات وخدمات تقنية جديدة. | ٣-٥-١ |

|  |       |
|--|-------|
| يجب مراجعة منهجية وإجراءات إدارة مخاطر الأمن السيبراني وتحديثها على فترات زمنية مخططة لها (أو في حالة حدوث تغييرات في المتطلبات التشريعية والتنظيمية والمعايير ذات العلاقة)، كما يجب توثيق التغييرات واعتمادها.  | ٤-٠-٤ |
| <b>الأمن السيبراني ضمن إدارة المشاريع المعلوماتية والتقنية</b>   | ١-١   |
| <b>الضوابط</b>   |       |
| التأكد من أن متطلبات الأمان السيبراني مضمنة في منهجية وإجراءات إدارة مشاريع الجهة لحماية السرية وسلامة الأصول المعلوماتية والتقنية للجهة ودققتها وتوافرها، وذلك وفقاً للسياسات والإجراءات التنظيمية للجهة والمتطلبات التشريعية والتنظيمية ذات العلاقة.   | الهدف |
| يجب تضمين متطلبات الأمان السيبراني في منهجية وإجراءات إدارة المشاريع وفي إدارة التغيير على الأصول المعلوماتية والتقنية في الجهة لضمان تحديد مخاطر الأمان السيبراني ومعالجتها كجزء من دورة حياة المشروع التقني، وأن تكون متطلبات الأمان السيبراني جزء أساسى من متطلبات المشاريع التقنية.  | ١-٦-١ |
| يجب أن تغطي متطلبات الأمان السيبراني لإدارة المشاريع والتغييرات على الأصول المعلوماتية والتقنية للجهة بحد أدنى ما يلي:<br>١-٦-١-١ تقييم الثغرات ومعالجتها.<br>١-٦-٢-١ اجراء مراجعة للإعدادات والتحصين (Secure Configuration and Hardening) وحزم التحديثات قبل إطلاق وتدشين المشاريع والتغييرات.  | ٢-٦-١ |
| يجب أن تغطي متطلبات الأمان السيبراني لمشاريع تطوير التطبيقات والبرمجيات الخاصة للجهة بحد أدنى ما يلي:<br>١-٦-٣-١ استخدام معايير التطوير الآمن للتطبيقات (Secure Coding Standards).<br>١-٦-٣-٢ استخدام مصادر مرخصة وموثوقة لأدوات تطوير التطبيقات والمكتبات الخاصة بها (Libraries).<br>١-٦-٣-٣ اجراء اختبار للتحقق من مدى استيفاء التطبيقات للمتطلبات الأمانية السيبرانية للجهة.<br>١-٦-٣-٤ أمن التكامل (Integration) بين التطبيقات.<br>١-٦-٣-٥ اجراء مراجعة للإعدادات والتحصين (Secure Configuration and Hardening) وحزم التحديثات قبل إطلاق وتدشين التطبيقات. | ٣-٦-١ |
| يجب مراجعة متطلبات الأمان السيبراني في إدارة المشاريع في الجهة دورياً.   | ٤-٦-١ |
| <b>الالتزام بتشريعات وتنظيمات ومعايير الأمان السيبراني</b>   | ١-٧   |
| <b>الضوابط</b>   |       |
| ضمان التأكد من أن برنامج الأمان السيبراني لدى الجهة يتوافق مع المتطلبات التشريعية والتنظيمية ذات العلاقة.  | الهدف |
| يجب على الجهة الالتزام بالمتطلبات التشريعية والتنظيمية الوطنية المتعلقة بالأمان السيبراني.   | ١-٧-١ |
| في حال وجود اتفاقيات أو إلتزامات دولية معتمدة محلياً تتضمن متطلبات خاصة بالأمان السيبراني، فيجب على الجهة الالتزام بتلك المتطلبات.   | ٢-٧-١ |

| <b>المراجعة والتدقيق الدوري للأمن السيبراني</b>   |       | <b>١-٨</b>   |
|---|-------|--|
| <b>الضوابط</b>  |       |  |
| يجب على الإدارة المعنية بالأمن السيبراني في الجهة مراجعة تطبيق ضوابط الأمان السيبراني دورياً.   | ١-٨-١ | ضمان التأكد من أن ضوابط الأمان السيبراني لدى الجهة مطبقة وتعمل وفقاً للسياسات والإجراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية الوطنية ذات العلاقة، والمتطلبات الدولية المقروءة تنظيمياً على الجهة. |
| يجب مراجعة وتدقيق تطبيق ضوابط الأمان السيبراني في الجهة، من قبل أطراف مستقلة عن الإدارة المعنية بالأمن السيبراني (مثل الإدارة المعنية بالمراجعة في الجهة). على أن تتم المراجعة والتدقيق بشكل مستقل يراعى فيه مبدأ عدم تعارض المصالح، وذلك وفقاً للمعايير العامة المقبولة للمراجعة والتدقيق والمتطلبات التشريعية والتنظيمية ذات العلاقة. | ٢-٨-١ |  |
| يجب توثيق نتائج مراجعة وتدقيق الأمان السيبراني، وعرضها على اللجنة الإشرافية للأمن السيبراني وصاحب الصلاحية. كما يجب أن تشمل النتائج على نطاق المراجعة والتدقيق، واللاحظات المكتشفة، والتوصيات والإجراءات التصحيحية، وخطة معالجة الملاحظات.  | ٣-٨-١ |  |
| <b>الأمن السيبراني المتعلق بالموارد البشرية</b>   |       | <b>٩-١</b>   |
| <b>الضوابط</b>  |       |  |
| يجب تحديد وتوثيق واعتماد متطلبات الأمان السيبراني المتعلقة بالعاملين (موظفين ومتعاقدين) في الجهة تعالج بفعالية قبل وأثناء وعند انتهاء/ إنهاء عملهم، وذلك وفقاً للسياسات والإجراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية ذات العلاقة.  | ١-٩-١ | ضمان التأكد من أن مخاطر ومتطلبات الأمان السيبراني المتعلقة بالعاملين (موظفين ومتعاقدين) في   |
| يجب تطبيق متطلبات الأمان السيبراني المتعلقة بالعاملين في الجهة.   | ٢-٩-١ | الجهة تعالج بفعالية قبل وأثناء وعند انتهاء/ إنهاء عملهم في الجهة.  |
| يجب أن تغطي متطلبات الأمان السيبراني قبل بدء علاقة العاملين المهنية بالجهة بحد أدنى ما يلي:<br>١-٣-٩-١ تضمين مسؤوليات الأمان السيبراني وبنود المحافظة على سرية المعلومات في عقود العاملين في الجهة (Non-Disclosure Clauses) التي تشمل خلل وبعد انتهاء/ إنهاء العلاقة الوظيفية مع الجهة.   | ٣-٩-١ |  |
| ١-٣-٩-٢ إجراء المسح الأمني (Screening or Vetting) للعاملين في وظائف الأمان السيبراني والوظائف التقنية ذات الصلاحيات الهامة والحساسة.  | ٤-٩-١ |  |
| يجب أن تغطي متطلبات الأمان السيبراني خلال علاقة العاملين المهنية بالجهة بحد أدنى ما يلي:<br>١-٤-٩-١ التوعية بالأمن السيبراني (عند بداية المهنة الوظيفية وخلالها).<br>١-٤-٩-٢ تطبيق متطلبات الأمان السيبراني والالتزام بها وفقاً لسياسات وإجراءات وعمليات الأمان السيبراني للجهة.  | ٥-٩-١ |  |
| يجب مراجعة وإلغاء الصلاحيات للعاملين مباشرة بعد انتهاء/ إنهاء الخدمة المهنية لهم بالجهة.  | ٦-٩-١ |  |
| يجب مراجعة متطلبات الأمان السيبراني المتعلقة بالعاملين في الجهة دورياً.   | ٧-٩-١ |  |



| برنامج التوعية والتدريب بالأمن السيبراني  | ١٠-١ |
|---|------|
| الهدف   |      |
| الضوابط   |      |
| ضمان التأكيد من أن العاملين بالجهة لديهم التوعية الأمنية الضرورية وعلى دراية بمسؤولياتهم في مجال الأمن السيبراني، والتأكد من تزويدهم العاملين بالجهة بالمهارات والمؤهلات والدورات التدريبية المطلوبة في مجال الأمن السيبراني لحماية الأصول المعلوماتية والتقنية للجهة والقيام بمسؤولياتهم تجاه الأمان السيبراني.  | ١-١  |
| يجب تطوير واعتماد برنامج للتوعية بالأمن السيبراني في الجهة من خلال قنوات متعددة دوريًا، وذلك لتعزيز الوعي بالأمن السيبراني وتهدياته ومخاطره، وبناء ثقافة إيجابية للأمن السيبراني.   | ٢-١  |
| يجب تطبيق البرنامج المعتمد للتوعية بالأمن السيبراني في الجهة.   | ٣-١  |
| يجب أن يغطي برنامج التوعية بالأمن السيبراني كيفية حماية الجهة من أهم المخاطر والتهديدات السيبرانية وما يستجد منها، بما في ذلك: <ul style="list-style-type: none"> <li>١-١-٣-١ التعامل الآمن مع خدمات البريد الإلكتروني خصوصاً مع رسائل التصيد الإلكتروني.</li> <li>١-١-٣-٢ التعامل الآمن مع الأجهزة المحمولة ووسائل التخزين.</li> <li>١-١-٣-٣ التعامل الآمن مع خدمات تصفح الإنترنت.</li> <li>١-١-٣-٤ التعامل الآمن مع وسائل التواصل الاجتماعي.</li> </ul>                           | ٤-١  |
| يجب توفير المهارات المتخصصة والتدريب اللازم للعاملين في المجالات الوظيفية ذات العلاقة المباشرة بالأمن السيبراني في الجهة، وتصنيفها بما يتناسب مع مسؤولياتهم الوظيفية فيما يتعلق بالأمن السيبراني، بما في ذلك: <ul style="list-style-type: none"> <li>١-١-٤-١ موظفو الإداراة المعنية بالأمن السيبراني.</li> <li>١-١-٤-٢ الموظفون العاملون في تطوير البرامج والتطبيقات والموظفو المشغلون للأصول المعلوماتية والتقنية للجهة.</li> <li>١-١-٤-٣ الوظائف الإشرافية والتنفيذية.</li> </ul> | ٥-١  |
| يجب مراجعة تطبيق برنامج التوعية بالأمن السيبراني في الجهة دوريًا.   | ٦-١  |

## تعزيز الأمان السيبراني (Cybersecurity Defense)



| إدارة الأصول (Asset Management) <span style="float: right;">١-٢</span>  |       |
|---|-------|
| 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 الأمان السيبراني، لتحقيق سرية وسلامة الأصول المعلوماتية والتقنية للجهة ودققتها وتوافرها.           | الهدف |
| الضوابط   |       |
| يجب تحديد وتوثيق واعتماد متطلبات الأمان السيبراني لإدارة الأصول المعلوماتية والتقنية للجهة.   | ١-١-٢ |
| يجب تطبيق متطلبات الأمان السيبراني لإدارة الأصول المعلوماتية والتقنية للجهة.  | ٢-١-٢ |
| يجب تحديد وتوثيق واعتماد ونشر سياسة الاستخدام المقبول للأصول المعلوماتية والتقنية للجهة.  | ٣-١-٢ |
| يجب تطبيق سياسة الاستخدام المقبول للأصول المعلوماتية والتقنية للجهة.  | ٤-١-٢ |
| يجب تصنيف الأصول المعلوماتية والتقنية للجهة وترميزها (Labeling) والتعامل معها وفقاً للمتطلبات التشريعية والتنظيمية ذات العلاقة.   | ٥-١-٢ |
| يجب مراجعة متطلبات الأمان السيبراني لإدارة الأصول المعلوماتية والتقنية للجهة دوريآ.   | ٦-١-٢ |
| إدارة هويات الدخول والصلاحيات (Identity and Access Management) <span style="float: right;">٢-٢</span>   |       |
| ضمان حماية الأمان السيبراني للوصول المنطقي (Logical Access) إلى الأصول المعلوماتية والتقنية للجهة من أجل منع الوصول غير المصرح به وتقيد الوصول إلى ما هو مطلوب لإنجاز الأعمال المتعلقة بالجهة.  | الهدف |
| الضوابط   |       |
| يجب تحديد وتوثيق واعتماد متطلبات الأمان السيبراني لإدارة هويات الدخول والصلاحيات في الجهة.  | ١-٢-٢ |
| يجب تطبيق متطلبات الأمان السيبراني لإدارة هويات الدخول والصلاحيات في الجهة.   | ٢-٢-٢ |
| يجب أن تغطي متطلبات الأمان السيبراني المتعلقة بإدارة هويات الدخول والصلاحيات في الجهة بحد أدنى ما يلي:  |       |
| ٢-٣-١ التحقق من هوية المستخدم (User Authentication) بناء على إدارة تسجيل المستخدم، وإدارة كلمة المرور.  |       |
| ٢-٣-٢ التتحقق من الهوية متعدد العناصر (Multi-Factor Authentication) لعمليات الدخول عن بعد.  |       |
| ٢-٣-٣ إدارة تصاريح وصلاحيات المستخدمين (Authorization) بناء على مبادئ التحكم بالدخول، والصلاحيات (مبدأ الحاجة إلى المعرفة والاستخدام "Need-to-know and Need-to-use" ، ومبدأ الحد الأدنى من الصلاحيات والامتيازات "Least Privilege" ، ومبدأ فصل المهام ("Segregation of Duties") . | ٣-٢-٢ |
| ٢-٣-٤ إدارة الصلاحيات الهامة والحساسة (Privileged Access Management).   |       |
| ٢-٣-٥ المراجعة الدورية لهويات الدخول والصلاحيات.  |       |
| يجب مراجعة تطبيق متطلبات الأمان السيبراني لإدارة هويات الدخول والصلاحيات في الجهة دوريآ.  | ٤-٢-٢ |

| حماية الأنظمة وأجهزة معالجة المعلومات<br>(Information System and Processing Facilities Protection)  | ٣-٢   |
|---|-------|
| الهدف   |       |
| ضمان حماية الأنظمة وأجهزة معالجة المعلومات بما في ذلك أجهزة المستخدمين والبني التحتية للجهة من المخاطر السيبرانية.  |       |
| الضوابط   |       |
| يجب تحديد وتوثيق واعتماد متطلبات الأمان السيبراني لحماية الأنظمة وأجهزة معالجة المعلومات للجهة.   | ١-٣-٢ |
| يجب تطبيق متطلبات الأمان السيبراني لحماية الأنظمة وأجهزة معالجة المعلومات للجهة.  | ٢-٣-٢ |
| يجب أن تغطي متطلبات الأمان السيبراني لحماية الأنظمة وأجهزة معالجة المعلومات للجهة بحد أدنى ما يلي:  |       |
| ١-٣-٣-٢ الحماية من الفيروسات والبرامج والأنشطة المشبوهة والبرمجيات الضارة (Malware) على أجهزة المستخدمين والخوادم باستخدام تقنيات وآليات الحماية الحديثة والمتقدمة، وإدارتها بشكل آمن.                        | ٣-٣-٢ |
| ٢-٣-٣-٢ التقييد الحازم لاستخدام أجهزة وسائط التخزين الخارجية والأمن المتعلقة بها.   |       |
| ٣-٣-٣-٢ إدارة حزم التحديثات والإصلاحات لأنظمة التطبيقات والأجهزة (Patch Management).  |       |
| ٤-٣-٣-٢ مزامنة التوقيت (Clock Synchronization) مركزاً ومن مصدر دقيق وموثوق، ومن هذه المصادر ما توفره الهيئة السعودية للمواصفات والمقاييس وجودة.   |       |
| يجب مراجعة متطلبات الأمان السيبراني لحماية الأنظمة وأجهزة معالجة المعلومات للجهة دوريأً.  | ٤-٣-٢ |
| حماية البريد الإلكتروني (Email Protection)  | ٤-٢   |
| الهدف   |       |
| ضمان حماية البريد الإلكتروني للجهة من المخاطر السيبرانية.   |       |
| الضوابط   |       |
| يجب تحديد وتوثيق واعتماد متطلبات الأمان السيبراني لحماية البريد الإلكتروني للجهة.   | ١-٤-٢ |
| يجب تطبيق متطلبات الأمان السيبراني لحماية البريد الإلكتروني للجهة.  | ٢-٤-٢ |
| يجب أن تغطي متطلبات الأمان السيبراني لحماية البريد الإلكتروني للجهة بحد أدنى ما يلي:  |       |
| ١-٣-٤-٢ تحليل وتصفية رسائل البريد الإلكتروني (Filtering) (وخصوصاً رسائل التصيد الإلكتروني «Spam Emails» ورسائل ال欺詐性的郵件 «Phishing Emails») باستخدام تقنيات وآليات الحماية الحديثة والمقدمة للبريد الإلكتروني. |       |
| ٢-٣-٤-٢ التحقق من الهوية متعدد العناصر (Multi-Factor Authentication) للدخول عن بعد والدخول عن طريق صفحة موقع البريد الإلكتروني (Webmail).   | ٣-٤-٢ |
| ٣-٣-٤-٢ النسخ الاحتياطي والأرشفة للبريد الإلكتروني.   |       |
| ٤-٣-٤-٢ الحماية من التهديدات المتقدمة المستمرة (APT Protection)، التي تستخدم عادة الفيروسات والبرمجيات الضارة غير المعروفة مسبقاً (Zero-Day Malware). وإدارتها بشكل آمن.                                      |       |
| ٥-٣-٤-٢ توثيق مجال البريد الإلكتروني للجهة بالطرق التقنية، مثل طريقة إطار سياسة المرسل (Sender Policy Framework).   |       |
| يجب مراجعة تطبيق متطلبات الأمان السيبراني الخاصة بحماية البريد الإلكتروني للجهة دوريأً.   | ٤-٤-٢ |

| <b> إدارة أمن الشبكات (Networks Security Management)</b>  |  | <b> ٥-٢</b> |
|---|--|-------------|
| ضمان حماية شبكات الجهة من المخاطر السيبرانية.   |  | الهدف       |
| <b> الضوابط</b>   |  |             |
|   | يجب تحديد وتوثيق واعتماد متطلبات الأمان السيبراني لإدارة أمن شبكات الجهة.  | ١-٥-٢       |
|   | يجب تطبيق متطلبات الأمان السيبراني لإدارة أمن شبكات الجهة.   | ٢-٥-٢       |
|   | <p> يجب أن تغطي متطلبات الأمان السيبراني لإدارة أمن شبكات الجهة بحد أدنى ما يلي:</p> <p> ٢-٣-٠-٢ العزل والتقطيع المادي أو المنقطعي لأجزاء الشبكات بشكل آمن، واللازم للسيطرة على مخاطر الأمان السيبراني ذات العلاقة، باستخدام جدار الحماية (Firewall) ومبدأ الدفاع الأمني متعدد المراحل (Defense-in-Depth).</p> <p> ٢-٣-٠-٢ عزل شبكة بيئة الإنتاج عن شبكات بيئات التطوير والاختبار.</p> <p> ٢-٣-٠-٢ أمن التصفح والاتصال بالإنترنت، ويشمل ذلك التقييد اللازم للمواقع الإلكترونية المشبوهة، ومواقع مشاركة وتخزين الملفات، ومواقع الدخول عن بعد.</p> <p> ٢-٣-٠-٢ أمن الشبكات اللاسلكية وحمايتها باستخدام وسائل آمنة للتحقق من الهوية والتشفير، وعدم ربط الشبكات اللاسلكية بشبكة الجهة الداخلية إلا بناءً على دراسة متكاملة للمخاطر المتربعة على ذلك والتعامل معها بما يضمن حماية الأصول التقنية للجهة.</p> <p> ٠-٣-٠-٢ قيود وإدارة منافذ بروتوكولات وخدمات الشبكة.</p> <p> ٠-٣-٠-٢ أنظمة الحماية المتقدمة للكشف ومنع الاختراقات (Intrusion Prevention Systems).</p> <p> ٧-٣-٠-٢ أمن نظام أسماء النطاقات (DNS).</p> <p> ٨-٣-٠-٢ حماية قناة تصفح الإنترنت من التهديدات المتقدمة المستمرة (APT Protection)، التي تستخدم عادة الفيروسات والبرمجيات الضارة غير المعروفة مسبقاً (Zero-Day Malware)، وإدارتها بشكل آمن.</p> | ٣-٥-٢       |
|   | يجب مراجعة تطبيق متطلبات الأمان السيبراني لإدارة أمن شبكات الجهة دوريًا.   | ٤-٥-٢       |
| <b> أمن الأجهزة المحمولة (Mobile Devices Security)</b>  |  | <b> ٦-٢</b> |
| ضمان حماية أجهزة الجهة المحمولة (بما في ذلك أجهزة الكمبيوتر 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»). |  | الهدف       |
| <b> الضوابط</b>   |  |             |
|   | يجب تحديد وتوثيق واعتماد متطلبات الأمان السيبراني الخاصة بأمن الأجهزة المحمولة والأجهزة الشخصية للعاملين (BYOD) عند ارتباطها بشبكة الجهة.  | ١-٦-٢       |
|   | يجب تطبيق متطلبات الأمان السيبراني الخاصة بأمن الأجهزة المحمولة وأجهزة (BYOD) للجهة.   | ٢-٦-٢       |

|  |       |
|--|-------|
| يجب أن تغطي متطلبات الأمان السيبراني الخاصة بأمن الأجهزة المحمولة وأجهزة (BYOD) للجهة بحد أدنى ما يلي:   |       |
| ٢-٣-٦-٢ فصل وتشفير البيانات والمعلومات (الخاصة بالجهة) المخزنة على الأجهزة المحمولة وأجهزة (BYOD).   | ٣-٦-٢ |
| ٢-٣-٦-٢ الاستخدام المحدد والمقييد بناءً على ما تتطلبه مصلحة أعمال الجهة.   |       |
| ٢-٣-٦-٢ حذف البيانات والمعلومات (الخاصة بالجهة) المخزنة على الأجهزة المحمولة وأجهزة (BYOD) عند فقدان الأجهزة أو بعد انتهاء/ إنهاء العلاقة الوظيفية مع الجهة. |       |
| ٢-٣-٦-٢ التوعية الأمنية للمستخدمين.  |       |

|  |       |
|--|-------|
| يجب مراجعة تطبيق متطلبات الأمان السيبراني الخاصة لأمن الأجهزة المحمولة وأجهزة (BYOD) للجهة دورياً. | ٤-٦-٢ |
|--|-------|

## حماية البيانات والمعلومات (Data and Information Protection)

٧-٢

|  |       |
|--|-------|
| ضمان حماية السرية وسلامة بيانات ومعلومات الجهة ودققتها وتوافرها، وذلك وفقاً لسياسات وإجراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية ذات العلاقة. | الهدف |
|--|-------|

## الضوابط

|   |       |
|---|-------|
| يجب تحديد وتوثيق واعتماد متطلبات الأمان السيبراني لحماية بيانات ومعلومات الجهة، والتعامل معها وفقاً للمتطلبات التشريعية والتنظيمية ذات العلاقة. | ١-٧-٢ |
|---|-------|

|  |       |
|--|-------|
| يجب تطبيق متطلبات الأمان السيبراني لحماية بيانات ومعلومات الجهة. | ٢-٧-٢ |
|--|-------|

|  |       |
|--|-------|
| يجب أن تغطي متطلبات الأمان السيبراني لحماية البيانات والمعلومات بحد أدنى ما يلي: |       |
| ٢-٣-٧-٢ ملكية البيانات والمعلومات.   | ٣-٧-٢ |

|  |  |
|--|--|
| ٢-٣-٧-٢ تصنیف البيانات والمعلومات وآلية تمیزها (Classification and Labeling Mechanisms). |  |
| ٢-٣-٧-٢ خصوصية البيانات والمعلومات.  |  |

|  |       |
|--|-------|
| يجب مراجعة تطبيق متطلبات الأمان السيبراني لحماية بيانات ومعلومات الجهة دورياً. | ٤-٧-٢ |
|--|-------|

## (Cryptography) التشفير

٨-٢

|   |       |
|---|-------|
| ضمان الاستخدام السليم والفعال للتشفيـر لـحماية الأصول المعلوماتية الإلكترونية للجهة، وذلك وفقاً للسياسات وإجراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية ذات العلاقة. | الهدف |
|---|-------|

## الضوابط

|  |       |
|--|-------|
| يجب تحديد وتوثيق واعتماد متطلبات الأمان السيبراني للتشفيـر في الجهة. | ١-٨-٢ |
|--|-------|

|   |       |
|---|-------|
| يجب تطبيق متطلبات الأمان السيبراني للتشفيـر في الجهة. | ٢-٨-٢ |
|---|-------|

|  |  |
|--|--|
| يجب أن تغطي متطلبات الأمان السيبراني للتشفيـر بحد أدنى ما يلي: |  |
|--|--|

|  |       |
|--|-------|
| ٢-٣-٨-٢ معايير حلول التشفير المعتمدة والقيود المطبقة عليها (تقنياً وتنظيمياً). |       |
| ٢-٣-٨-٢ الإدارة الآمنة لمفاتيح التشفير خلال عمليات دورتها حياتها.              | ٣-٨-٢ |

|  |  |
|--|--|
| ٢-٣-٨-٢ تشفير البيانات أثناء النقل والتخزين بناءً على تصنيفها وحسب المتطلبات التشريعية والتنظيمية ذات العلاقة. |  |
|--|--|

|   |       |
|---|-------|
| يجب مراجعة تطبيق متطلبات الأمان السيبراني للتشفيـر في الجهة دورياً. | ٤-٨-٢ |
|---|-------|

| <b>إدارة النسخ الاحتياطية (Backup and Recovery Management)</b>  |         | ٩-٢  |
|---|---------|------|
| ضمان حماية بيانات ومعلومات الجهة والإعدادات التقنية للأنظمة والتطبيقات الخاصة بالجهة من الأضرار الناجمة عن المخاطر السيبرانية، وذلك وفقاً للسياسات والإجراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية ذات العلاقة.   | الهدف   |      |
| <b>الضوابط</b>  |         |      |
| يجب تحديد وتوثيق واعتماد متطلبات الأمان السيبراني لإدارة النسخ الاحتياطية للجهة.  | ١-٩-٢   |      |
| يجب تطبيق متطلبات الأمان السيبراني لإدارة النسخ الاحتياطية للجهة.   | ٢-٩-٢   |      |
| يجب أن تغطي متطلبات الأمان السيبراني لإدارة النسخ الاحتياطية بحد أدنى ما يلي:<br>١-٣-٩-١ نطاق النسخ الاحتياطية وشموليتها للأصول المعلوماتية والتقنية الحساسة.<br>٢-٣-٩-٢ القدرة السريعة على استعادة البيانات والأنظمة بعد التعرض لحوادث الأمان السيبراني.<br>٣-٣-٩-٢ إجراء فحص دوري لمدى فعالية استعادة النسخ الاحتياطية. | ٣-٩-٢   |      |
| يجب مراجعة تطبيق متطلبات الأمان السيبراني لإدارة النسخ الاحتياطية للجهة.  | ٤-٩-٢   |      |
| <b>إدارة الثغرات (Vulnerabilities Management)</b>   |         | ١٠-١ |
| ضمان اكتشاف الثغرات التقنية في الوقت المناسب ومعالجتها بشكل فعال، وذلك لمنع أو تقليل احتمالية استغلال هذه الثغرات من قبل الهجمات السيبرانية وتقليل الآثار المترتبة على أعمال الجهة.   | الهدف   |      |
| <b>الضوابط</b>  |         |      |
| يجب تحديد وتوثيق واعتماد متطلبات الأمان السيبراني لإدارة الثغرات التقنية للجهة.   | ١-١٠-٢  |      |
| يجب تطبيق متطلبات الأمان السيبراني لإدارة الثغرات التقنية للجهة.  | ٢-١٠-٢  |      |
| يجب أن تغطي متطلبات الأمان السيبراني لإدارة الثغرات بحد أدنى ما يلي:<br>١-٣-١-٢ فحص واكتشاف الثغرات دورياً.<br>٢-٣-١-٢ تصنيف الثغرات حسب خطورتها.<br>٣-١-٣-٢ معالجة الثغرات بناءً على تصنيفها والمخاطر السيبرانية المترتبة عليها.<br>٤-١-٣-٢ إدارة حزم التحديثات والإصلاحات الأمنية لمعالجة الثغرات.                      | ٣-١-٠-٢ |      |
| ٥-١-٣-٢ التواصل والاشتراك مع مصادر موثوقة فيما يتعلق بالتنبيهات المتعلقة بالثغرات الجديدة والمحدثة.   |         |      |
| يجب مراجعة تطبيق متطلبات الأمان السيبراني لإدارة الثغرات التقنية للجهة دورياً.  | ٤-١-٠-٢ |      |
| <b>اختبار الاختراق (Penetration Testing)</b>  |         | ١١-٢ |
| تقييم واختبار مدى قدرات تعزيز الأمان السيبراني في الجهة، وذلك من خلال عمل محاكاة لتقنيات وأساليب الهجوم السيبراني الفعلية، ولاكتشاف نقاط الضعف الأمنية غير المعروفة والتي قد تؤدي إلى الاختراق السيبراني للجهة. وذلك وفقاً للمتطلبات التشريعية والتنظيمية ذات العلاقة.  | الهدف   |      |
| <b>الضوابط</b>  |         |      |
| يجب تحديد وتوثيق واعتماد متطلبات الأمان السيبراني لعمليات اختبار الاختراق في الجهة.   | ١-١١-٢  |      |
| يجب تنفيذ عمليات اختبار الاختراق في الجهة.  | ٢-١١-٢  |      |

|  |                  |
|--|------------------|
| <p>يجب أن تغطي متطلبات الأمان السيبراني لاختبار الاختراق بحد أدنى ما يلي:</p> <p>٢-١١-٣-١-١-٢ نطاق عمل اختبار الاختراق، ليشمل جميع الخدمات المقدمة خارجياً (عن طريق الإنترنت) ومكوناتها التقنية، ومنها: البنية التحتية، المواقع الإلكترونية، تطبيقات الويب، تطبيقات الهواتف الذكية واللوحية، البريد الإلكتروني والدخول عن بعد.</p> <p>٢-١١-٣-٢ عمل اختبار الاختراق دوريًا.</p> | ٣-١١-٣           |
| <p>يجب مراجعة تطبيق متطلبات الأمان السيبراني لعمليات اختبار الاختراق في الجهة دوريًا.</p>  | ٤-١١-٣           |
| <b>إدارة سجلات الأحداث ومراقبة الأمان السيبراني<br/>(Cybersecurity Event Logs and Monitoring Management)</b>   | ١٢-٣             |
| <p>ضمان تجميع وتحليل ومراقبة سجلات أحداث الأمان السيبراني في الوقت المناسب من أجل الاكتشاف الاستباقي للهجمات السيبرانية وإدارة مخاطرها بفعالية لمنع أو تقليل الآثار المترتبة على أعمال الجهة.</p>  | الهدف            |
| <b>الضوابط</b>   |                  |
| <p>يجب تحديد وتوثيق واعتماد متطلبات إدارة سجلات الأحداث ومراقبة الأمان السيبراني للجهة.</p> <p>يجب تطبيق متطلبات إدارة سجلات الأحداث ومراقبة الأمان السيبراني للجهة.</p>   | ١-١٢-٣<br>٢-١٢-٣ |
| <p>يجب أن تغطي متطلبات إدارة سجلات الأحداث ومراقبة الأمان السيبراني بحد أدنى ما يلي:</p> <p>١-١٢-٣-١ تفعيل سجلات الأحداث (Event logs) الخاصة بالأمن السيبراني على الأصول المعلوماتية الحساسة لدى الجهة.</p>  |                  |
| <p>١-١٢-٣-٢ تفعيل سجلات الأحداث الخاصة بالحسابات ذات الصلاحيات الهامة والحساسة على الأصول المعلوماتية وأحداث عمليات الدخول عن بعد لدى الجهة.</p>   | ٣-١٢-٣           |
| <p>١-١٢-٣-٣ تحديد التقنيات اللازمة (SIEM) لجمع سجلات الأحداث الخاصة بالأمن السيبراني.</p> <p>٤-١٢-٣-١ المراقبة المستمرة لسجلات الأحداث الخاصة بالأمن السيبراني.</p> <p>٤-١٢-٣-٢ مدة الاحتفاظ بسجلات الأحداث الخاصة بالأمن السيبراني (على ألا تقل عن ١٢ شهر).</p>   |                  |
| <p>يجب مراجعة تطبيق متطلبات إدارة سجلات الأحداث ومراقبة الأمان السيبراني في الجهة دوريًا.</p>  | ٤-١٢-٣           |
| <b>إدارة حوادث وتهديدات الأمان السيبراني<br/>(Cybersecurity Incident and Threat Management)</b>  | ١٣-٣             |
| <p>ضمان تحديد واكتشاف حوادث الأمان السيبراني في الوقت المناسب وإدارتها بشكل فعال والتعامل مع تهديدات الأمان السيبراني استباقياً من أجل منع أو تقليل الآثار المترتبة على أعمال الجهة. مع مراعاة ما ورد في الأمر السامي الكريم رقم ٣٧١٤٠ وتاريخ ١٤ / ٨ / ١٤٣٨هـ</p>  | الهدف            |
| <b>الضوابط</b>   |                  |
| <p>يجب تحديد وتوثيق واعتماد متطلبات إدارة حوادث وتهديدات الأمان السيبراني في الجهة.</p> <p>يجب تطبيق متطلبات إدارة حوادث وتهديدات الأمان السيبراني في الجهة.</p>   | ١-١٣-٣<br>٢-١٣-٣ |
| <p>يجب أن تغطي متطلبات إدارة حوادث وتهديدات الأمان السيبراني بحد أدنى ما يلي:</p> <p>١-١٣-٣-١ وضع خطط الاستجابة للحوادث الأمنية وآليات التصعيد.</p> <p>٢-١٣-٣-٢ تصنيف حوادث الأمان السيبراني.</p> <p>٣-١٣-٣-٢ تبليغ الهيئة عند حدوث حادثة أمن سيبراني.</p>   |                  |
| <p>٤-١٣-٣-١ مشاركة التنبيهات والمعلومات الاستباقية ومؤشرات الاختراق وتقارير حوادث الأمان السيبراني مع الهيئة.</p> <p>٤-١٣-٣-٢ الحصول على المعلومات الاستباقية (Threat Intelligence) والتعامل معها.</p>   |                  |
| <p>يجب مراجعة تطبيق متطلبات إدارة حوادث وتهديدات الأمان السيبراني في الجهة دوريًا.</p>   | ٤-١٣-٣           |

| <b>(Physical Security)</b>  |        | <b>الأمن المادي (Physical Security)</b>               | <b>١٤-٢</b> |
|---|--------|---|-------------|
| ضمان حماية الأصول المعلوماتية والتقنية للجهة من الوصول المادي غير المصرح به والفقدان والسرقة والتخريب.  | الهدف  |   |             |
| <b>الضوابط</b>  |        |   |             |
| يجب تحديد وتوثيق واعتماد متطلبات الأمان السيبراني لحماية الأصول المعلوماتية والتقنية للجهة من الوصول المادي غير المصرح به والفقدان والسرقة والتخريب.  | ١-١٤-٢ |   |             |
| يجب تطبيق متطلبات الأمان السيبراني لحماية الأصول المعلوماتية والتقنية للجهة من الوصول المادي غير المصرح به والفقدان والسرقة والتخريب.   | ٢-١٤-٢ |   |             |
| يجب أن تغطي متطلبات الأمان السيبراني لحماية الأصول المعلوماتية والتقنية للجهة من الوصول المادي غير المصرح به والفقدان والسرقة والتخريب بحد أدنى ما يلي:<br>١-٣-١٤-٢ الدخول المصرح به للأماكن الحساسة في الجهة (مثل: مركز بيانات الجهة، مركز التعافي من الكوارث، أماكن معالجة المعلومات الحساسة، مركز المراقبة الأمنية، غرف اتصالات الشبكة، مناطق الإمداد الخاصة بالأجهزة والعتاد التقنية، وغيرها).<br>٢-٣-١٤-٢ سجلات الدخول والمراقبة (CCTV).<br>٣-٣-١٤-٢ حماية معلومات سجلات الدخول والمراقبة.<br>٤-٣-١٤-٢ أمن إتلاف وإعادة استخدام الأصول المادية التي تحتوي على معلومات مصنفة (وتشمل: الوثائق الورقية ووسائل الحفظ والتزيين).<br>٥-٣-١٤-٢ أمن الأجهزة والمعدات داخل مباني الجهة وخارجها. | ٣-١٤-٢ |   |             |
| يجب مراجعة متطلبات الأمان السيبراني لحماية الأصول المعلوماتية والتقنية للجهة من الوصول المادي غير المصرح به والفقدان والسرقة والتخريب دورياً.   | ٤-١٤-٢ |   |             |
| <b>(Web Application Security)</b>   |        | <b>حماية تطبيقات الويب (Web Application Security)</b> | <b>١٥-٢</b> |
| ضمان حماية تطبيقات الويب الخارجية للجهة من المخاطر السيبرانية.  | الهدف  |   |             |
| <b>الضوابط</b>  |        |   |             |
| يجب تحديد وتوثيق واعتماد متطلبات الأمان السيبراني لحماية تطبيقات الويب الخارجية للجهة من المخاطر السيبرانية.  | ١-١٥-٢ |   |             |
| يجب تطبيق متطلبات الأمان السيبراني لحماية تطبيقات الويب الخارجية للجهة.   | ٢-١٥-٢ |   |             |
| يجب أن تغطي متطلبات الأمان السيبراني لحماية تطبيقات الويب الخارجية للجهة من المخاطر السيبرانية لجهة:<br>١-٣-١٥-٢ استخدام جدار الحماية لتطبيقات الويب (Web Application Firewall).<br>٢-٣-١٥-٢ استخدام مبدأ المعمارية متعددة المستويات (Multi-tier Architecture).<br>٣-٣-١٥-٢ استخدام بروتوكولات آمنة (مثل بروتوكول HTTPS).<br>٤-٣-١٥-٢ توضيح سياسة الاستخدام الآمن للمستخدمين.<br>٥-٣-١٥-٢ التحقق من الهوية متعدد العناصر (Multi-Factor Authentication) لعمليات دخول المستخدمين.   | ٣-١٥-٢ |   |             |
| يجب مراجعة متطلبات الأمان السيبراني لحماية تطبيقات الويب للجهة من المخاطر السيبرانية دورياً.  | ٤-١٥-٢ |   |             |

## صمود الأمان السيبراني (Cybersecurity Resilience)



| جوانب صمود الأمان السيبراني في إدارة استمرارية الأعمال<br>(Cybersecurity Resilience aspects of Business Continuity Management "BCM")   | ١-٣   |
|--|-------|
| الضوابط  |       |
| ضمان توافر متطلبات صمود الأمان السيبراني في إدارة استمرارية أعمال الجهة. وضمان معالجة وتقليل الآثار المترتبة على الأضرار في الخدمات الإلكترونية الحرجية للجهة وأنظمة وأجهزة معالجة معلوماتها جراء الكوارث الناتجة عن المخاطر السيبرانية.   | الهدف |
| يجب تحديد وتوثيق واعتماد متطلبات الأمان السيبراني ضمن إدارة استمرارية أعمال الجهة.   | ١-١-٣ |
| يجب تطبيق متطلبات الأمان السيبراني ضمن إدارة استمرارية أعمال الجهة.  | ٢-١-٣ |
| يجب أن تغطي إدارة استمرارية الأعمال في الجهة بحد أدنى ما يلي:<br>١-٣-١-٣ التأكد من استمرارية الأنظمة والإجراءات المتعلقة بالأمان السيبراني.<br>٢-٣-١-٣ وضع خطط الاستجابة لحوادث الأمان السيبراني التي قد تؤثر على استمرارية أعمال الجهة.<br>٣-٣-١-٣ وضع خطط التعافي من الكوارث (Disaster Recovery Plan). | ٣-١-٣ |
| يجب مراجعة متطلبات الأمان السيبراني ضمن إدارة استمرارية أعمال الجهة دوريًا.  | ٤-١-٣ |



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

| الأمن السيبراني المتعلق بالأطراف الخارجية   |       | ٤-١   |
|---|-------|-------|
| ضمان حماية أصول الجهة من مخاطر الأمن السيبراني المتعلقة بالأطراف الخارجية (بما في ذلك خدمات الإسناد لتقنية المعلومات "Outsourcing" والخدمات المدارة "Managed Services"). وفقاً للسياسات والإجراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية ذات العلاقة.  |       | الهدف |
| الضوابط   |       |       |
| يجب تحديد وتوثيق واعتماد متطلبات الأمان السيبراني ضمن العقود والاتفاقيات مع الأطراف الخارجية للجهة.   | ٤-١-٤ |       |
| <p> يجب أن تغطي متطلبات الأمان السيبراني ضمن العقود والاتفاقيات (مثل اتفاقية مستوى الخدمة SLA) مع الأطراف الخارجية التي قد تتأثر بإصابتها بيانات الجهة أو الخدمات المقدمة لها بحد أدنى ما يلي:</p> <p>٤-٢-١-٤ بنود المحافظة على سرية المعلومات (Non-Disclosure Clauses) و الحذف الآمن من قبل الطرف الخارجي لبيانات الجهة عند انتهاء الخدمة.</p> <p>٤-٢-١-٤ إجراءات التواصل في حال حدوث حادثة أمن سيبراني.</p> <p>٤-٢-١-٤ إلزام الطرف الخارجي بتطبيق متطلبات وسياسات الأمان السيبراني للجهة والمتطلبات التشريعية والتنظيمية ذات العلاقة.</p> | ٤-١-٤ |       |
| <p> يجب أن تغطي متطلبات الأمان السيبراني مع الأطراف الخارجية التي تقدم خدمات إسناد لتقنية المعلومات، أو خدمات مدارة بحد أدنى ما يلي:</p> <p>٤-٣-١-٤ إجراء تقييم لمخاطر الأمان السيبراني، والتأكد من وجود ما يضمن السيطرة على تلك المخاطر، قبل توقيع العقود والاتفاقيات أو عند تغيير المتطلبات التشريعية والتنظيمية ذات العلاقة.</p> <p>٤-٣-١-٤ أن تكون مراكز عمليات خدمات الأمان السيبراني المدارة للتشغيل والمراقبة، والتي تستخدم طريقة الوصول عن بعد، موجودة بالكامل داخل المملكة.</p>  | ٣-١-٤ |       |
| يجب مراجعة متطلبات الأمان السيبراني مع الأطراف الخارجية دوريًا.   | ٤-١-٤ |       |
| الأمن السيبراني المتعلق بالحوسبة السحابية والاستضافة  |       | ٤-٢   |
| ضمان معالجة المخاطر السيبرانية وتنفيذ متطلبات الأمان السيبراني للحوسبة السحابية والاستضافة بشكل ملائم وفعال، وذلك وفقاً للسياسات والإجراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية والأوامر والقرارات ذات العلاقة. وضمان حماية الأصول المعلوماتية والتقنية للجهة على خدمات الحوسبة السحابية التي تم استضافتها أو معالجتها أو إدارتها بواسطة أطراف خارجية.   | الهدف |       |
| يجب تحديد وتوثيق واعتماد متطلبات الأمان السيبراني الخاصة باستخدام خدمات الحوسبة السحابية والاستضافة.  | ٤-٢-٤ |       |
| يجب تطبيق متطلبات الأمان السيبراني الخاصة بخدمات الحوسبة السحابية والاستضافة للجهة.   | ٤-٢-٤ |       |

|   |       |
|---|-------|
| <p>بما يتوافق مع المتطلبات التشريعية والتنظيمية ذات العلاقة، وبالإضافة إلى ما ينطبق من الضوابط ضمن المكونات الرئيسية رقم (١) و (٢) و (٣) والمكون الفرعي رقم (٤-١) الضرورية لحماية بيانات الجهة أو الخدمات المقدمة لها، يجب أن تغطي متطلبات الأمن السيبراني الخاصة باستخدام خدمات الحوسبة السحابية والاستضافة بحد أدنى ما يلي:</p> <ul style="list-style-type: none"> <li>١-٣-٢-٤ تصنيف البيانات قبل استضافتها لدى مقدمي خدمات الحوسبة السحابية والاستضافة، وإعادتها للجهة (بصيغة قابلة للاستخدام) عند إنتهاء الخدمة.</li> <li>٢-٣-٢-٤ فصل البيئة الخاصة بالجهة (وخصوصاً الخوادم الافتراضية) عن غيرها من البيئات التابعة لجهات أخرى في خدمات الحوسبة السحابية.</li> <li>٣-٢-٣-٤ موقع استضافة وتخزين معلومات الجهة يجب أن يكون داخل المملكة.</li> </ul> <p>يجب مراجعة متطلبات الأمن السيبراني الخاصة بخدمات الحوسبة السحابية والاستضافة دوريًا.</p> | ٣-٢-٤ |
|---|-------|

## الأمن السيبراني لأنظمة التحكم الصناعي (Industrial Control Systems Cybersecurity)



| الهدف   | 1-0 حماية أجهزة وأنظمة التحكم الصناعي |
|---|---------------------------------------|
| ضمان إدارة الأمان السيبراني بشكل سليم وفعال لحماية توافر وسلامة وسرية أصول الجهة المتعلقة بأجهزة وأنظمة التحكم الصناعي (OT/ICS) ضد الهجوم السيبراني (مثلاً الوصول غير المصرح به والتخييب والتجسس والتلاعب) بما يتماشى مع إستراتيجية الأمان السيبراني للجهة، وإدارة مخاطر الأمان السيبراني، والمتطلبات التشريعية والتنظيمية ذات العلاقة، وكذلك المتطلبات الدولية المقروءة تنظيمياً على الجهة المتعلقة بالأمان السيبراني. |                                       |
| الضوابط   |                                       |
| يجب تحديد وتوثيق واعتماد متطلبات الأمان السيبراني لحماية أجهزة وأنظمة التحكم الصناعي (OT/ICS) للجهة.  | 1-1-0                                 |
| يجب تطبيق متطلبات الأمان السيبراني لحماية أجهزة وأنظمة التحكم الصناعي (OT/ICS) للجهة.   | 2-1-0                                 |
| بالإضافة إلى ما يمكن تطبيقه من الضوابط ضمن المكونات الرئيسية رقم (١) و (٢) و (٣) و (٤) الضرورية لحماية بيانات الجهة وخدماتها، فإن متطلبات الأمان السيبراني لحماية أجهزة وأنظمة التحكم الصناعي (OT/ICS) يجب أن تغطي بحد أدنى ما يلي:   |                                       |
| ١-٣-١-٠ التقيد الحازم والتقسيم المادي والمنطقي عند ربط شبكات الإنتاج الصناعية مع الشبكات الأخرى التابعة للجهة، مثل: شبكة الأعمال الداخلية للجهة "Corporate Network".  | 3-1-0                                 |
| ١-٣-٢-٠ التقيد الحازم والتقسيم المادي والمنطقي عند ربط الأنظمة أو الشبكات الصناعية مع شبكات خارجية، مثل: الإنترنت أو الدخول عن بعد أو الاتصال اللاسلكي.   | 3-1-0                                 |
| ١-٣-٣-٠ تفعيل سجلات الأحداث (Event logs) الخاصة بالأمان السيبراني للشبكة الصناعية والاتصالات المرتبطة بها ما أمكن ذلك، والمراقبة المستمرة لها.  | 3-1-0                                 |
| ١-٣-٤-٠ عزل أنظمة معدات السلامة (Safety Instrumented System "SIS").   | 3-1-0                                 |
| ٢-٣-١-٠ التقيد الحازم لاستخدام وسائل التخزين الخارجية.  | 2-1-0                                 |
| ٢-٣-٢-٠ التقيد الحازم لتوصيل الأجهزة محمولة على شبكة الإنتاج الصناعية.  | 2-1-0                                 |
| ٢-٣-٣-٠ مراجعة إعدادات وتحصين الأنظمة الصناعية، وأنظمة الدعم والأجهزة الآلية الصناعية Secure Configuration and Hardening دورياً.  | 2-1-0                                 |
| ٢-٣-٤-٠ إدارة ثغرات الأنظمة الصناعية (OT/ICS Vulnerability Management).   | 2-1-0                                 |
| ٢-٣-٥-٠ إدارة حزم التحديثات والإصلاحات الأمنية لأنظمة الصناعية (OT/ICS Patch Management).   | 2-1-0                                 |
| ٢-٣-٦-٠ إدارة البرامج الخاصة بالأمان السيبراني الصناعي لحماية من الفيروسات والبرمجيات المشبوهة والضارة.   | 2-1-0                                 |
| يجب مراجعة متطلبات الأمان السيبراني لحماية أجهزة وأنظمة التحكم الصناعي (OT/ICS) للجهة دورياً.   | 4-1-0                                 |

## ملحق

### ملحق (أ): مصطلحات وتعريفات

يوضح الجدول ٢ أدناه بعض المصطلحات وتعريفاتها التي ورد ذكرها في هذه الضوابط.

#### جدول ٢: مصطلحات وتعريفات

| المصطلح   | التعريف  |
|---|--|
| الحماية من التهديدات المتقدمة التي تستخدم أساليب خفية تهدف إلى الدخول غير المشروع على الأنظمة والشبكات التقنية ومحاولة البقاء فيها لأطول فترة ممكنة عن طريق تفادي أنظمة الكشف والحماية. وهذه الأساليب تستخدم عادة الفيروسات والبرمجيات الضارة غير المعروفة مسبقاً (Zero-Day Malware) لتحقيق هدفها.                  | الحماية من التهديدات المتقدمة المستمرة Advanced Persistent Threat (APT) Protection |
| أي شيء ملموس أو غير ملموس له قيمة بالنسبة للجهة. هناك أنواع كثيرة من الأصول؛ بعض هذه الأصول تتضمن أشياء واضحة، مثل: الأشخاص، والآلات، والمراقب، وبراءات الاختراع، والبرمجيات والخدمات. ويمكن أن يشمل المصطلح أيضاً أشياء أقلوضواحاً، مثل: المعلومات والخصائص (مثل: سمعة الجهة وصورتها العامة، أو المهارة والمعرفة). | الأصل Asset  |
| أي نوع من الأنشطة الخبيثة التي تحاول الوصول بشكل غير مشروع أو جمع موارد النظم المعلوماتية أو المعلومات نفسها أو تعطيلها أو منعها أو تحطيمها أو تدميرها.   | هجوم Attack  |
| المراجعة المستقلة ودراسة السجلات والأنشطة لتقدير مدى فعالية ضوابط الأمان السيبراني ولضمان الالتزام بالسياسات، والإجراءات التشغيلية، والمعايير والمتطلبات التشريعية والتنظيمية ذات العلاقة.  | تدقيق Audit  |
| التأكد من هوية المستخدم أو العملية أو الجهاز، وغالباً ما يكون هذا الأمر شرطاً أساسياً للسماح بالوصول إلى الموارد في النظام.   | التحقق Authentication  |
| خاصية تحديد والتأكد من حقوق/تراخيص المستخدم للوصول إلى الموارد والأصول المعلوماتية والتقنية للجهة والسماح له وفقاً لما حدد مسبقاً في حقوق/تراخيص المستخدم.  | صلاحية المستخدم Authorization  |
| ضمان الوصول إلى المعلومات والبيانات والأنظمة والتطبيقات واستخدامها في الوقت المناسب.  | توافر Availability   |
| الملفات والأجهزة والبيانات والإجراءات المتاحة للستخدام في حالة الأعطال أو فقدان، أو إذا حذف الأصل منها أو توقف عن الخدمة.   | النسخ الاحتياطية Backup  |

| المصطلح   | التعريف  |
|---|--|
| أحضر الجهاز الخاص بك<br>Bring Your Own Device (BYOD)  | يشير هذا المصطلح إلى سياسة جهة تسمح (سواء بشكل جزئي أو كلي) للعاملين فيها بجلب الأجهزة الشخصية الخاصة بهم (أجهزة الكمبيوتر المحمولة والأجهزة اللوحية والهواتف الذكية) إلى أماكن العمل في الجهة، واستخدام هذه الأجهزة للوصول إلى الشبكات والمعلومات والتطبيقات والأنظمة التابعة للجهة المقيدة بصلاحيات دخول.  |
| الدائرة التلفزيونية المغلقة<br>(CCTV)   | يستخدم التليفزيون ذو الدائرة المغلقة، المعروف أيضاً باسم المراقبة بالفيديو، كاميرات الفيديو لإرسال إشارة إلى مكان محدد على مجموعة محدودة من الشاشات. وغالباً ما يطلق هذا المصطلح على تلك التقنية المستخدمة للمراقبة في المناطق التي قد تحتاج إلى مراقبة حيث يشكل الأمن المادي مطلبآ هاماً فيها.  |
| إدارة التغيير<br>Change Management  | وهو نظام لإدارة الخدمة حيث يضمن منهجاً نظامياً واستباقياً باستخدام أساليب وإجراءات معيارية فعالة (على سبيل المثال: التغيير في البنية التحتية للجهة وشبكاتها، إلخ). تساعد إدارة التغيير جميع الأطراف المعنيين، بما في ذلك الأفراد والفرق على حد سواء، على الانتقال من حالتهم الحالية إلى الحالة المرغوبة التالية، كما تساعد إدارة التغيير أيضاً على تقليل تأثير الحوادث ذات العلاقة على الخدمة.   |
| الحوسبة السحابية<br>Cloud Computing   | نموذج لتمكين الوصول عند الطلب إلى مجموعة مشتركة من موارد تقنية المعلومات (مثل: الشبكات والخوادم والتخزين والتطبيقات والخدمات) التي يمكن توفيرها بسرعة وإطلاقها بالحد الأدنى من الجهد الإداري التشغيلي والتدخل/ التفاعل لإعداد الخدمة من مزود الخدمة. تسمح الحوسبة السحابية للمستخدمين بالوصول إلى الخدمات القائمة على التقنية من خلال شبكة الحوسبة السحابية دون الحاجة لوجود معرفة لديهم أو تحكم في البنية التحتية التقنية التي تدعمهم. يتالف نموذج الحوسبة السحابية من خمس خصائص أساسية: خدمة ذاتية حسب الطلب، ووصول إلى الشبكة بشكل واسع، ومجمع الموارد، ومرنة سريعة، والخدمة المقاسة. |
| وهناك ثلاثة نماذج لتقديم خدمات الحوسبة السحابية وهي: البرمجيات السحابية كخدمة "Software-as-Service" Saas، والنظام أو المنصة السحابية كخدمة Platform-as-Service "PaaS" ، والبنية التحتية السحابية كخدمة Infrastructure-as-Service "IaaS" . كما أن هناك أربعة نماذج للحوسبة السحابية حسب طبيعة الدخول: الحوسبة السحابية العامة، والحوسبة السحابية المجتمعية، والحوسبة السحابية الخاصة، والحوسبة السطحية الهجين. |  |
| انتهاك أمني<br>Compromise   | الإفصاح عن أو الحصول على معلومات لأشخاص غير مصرح تسريبيها أو الحصول عليها، أو انتهاك السياسة الأمنية السيبرانية للجهة بالإفصاح عن أو تغيير أو تخريب أو فقد شيء سواء بقصد أو بغیر بقصد. ويقصد بالانتهاك الأمني الإفصاح عن أو الحصول على بيانات حساسة أو تسريبيها أو تغييرها أو تبديلها أو استخدامها بدون تصريح (بما في ذلك مفاتيح تشفير النصوص وغيرها من المعايير الأمنية السيبرانية الحرجية).  |
| السرية<br>Confidentiality   | الاحتفاظ بقيود مصرح بها على الوصول إلى المعلومات والإفصاح عنها بما في ذلك وسائل حماية معلومات الخصوصية والملكية الشخصية.   |

| التعريف  | المصطلح  |
|--|--|
| <p>هي المعلومات (أو البيانات) التي تعتبر غاية في الحساسية والأهمية، حسب تصنيف الجهة، والمعدة للاستخدام من قبل جهة أو جهات محددة. وأحد الطرق التي يمكن استخدامها في تصنيف هذا النوع من المعلومات هو قياس مدى الضرر عند الإفصاح عنها أو الاطلاع عليها بشكل غير مصحح به أو فقدانها أو تخريبها، حيث قد يؤدي ذلك إلى أضرار مادية أو معنوية على الجهة أو المتعاملين معها، أو التأثير على حياة الأشخاص ذو العلاقة بتلك المعلومات، أو التأثير والضرر بأمن الدولة أو اقتصادها الوطني أو مقدراتها الوطنية.</p> <p>وتشمل المعلومات الحساسة كل المعلومات التي يتربّع على الإفصاح عنها بشكل غير مصحح به أو فقدانها أو تخريبها مساعدةً أو عقوبات نظامية.</p> | <p>المعلومات (أو البيانات)<br/>الحساسة<br/>Confidential Data/<br/>Information</p>  |
| <p>تلك العناصر الأساسية للبنية التحتية (أي الأصول، والمرافق، والنظم، والشبكات، والعمليات، والعاملون الأساسيون الذين يقومون بتشغيلها ومعالجتها)، والتي قد يُؤدي فقدانها أو تعرّضها لانتهاكات أمنية إلى:</p> <ul style="list-style-type: none"> <li>أثر سلبي كبير على توافر الخدمات الأساسية أو تكاملها أو تسليمها - بما في ذلك الخدمات التي يمكن أن تؤدي في حال تعرضها للخطر إلى خسائر كبيرة في الممتلكات و/أو الأرواح و/أو الإصابات - مع مراعاة الآثار الاقتصادية و/أو الاجتماعية الكبيرة.</li> <li>تأثير كبير على الأمن القومي و/أو الدفاع الوطني و/أو اقتصاد الدولة أو مقدراتها الوطنية.</li> </ul>  | <p>البنية التحتية الوطنية<br/>الحساسة<br/>Critical National<br/>Infrastructure</p> |
| <p>(ويسمى أيضًا علم التشغیر) وهي القواعد التي تشتمل مبادئ ووسائل وطرق تخزين ونقل البيانات أو المعلومات في شكل معين وذلك من أجل إخفاء محتواها الدلالي، ومنع الاستخدام غير المصحح به أو منع التعديل غير المكتشف، بحيث لا يمكن لغير الأشخاص المعنيين قراءتها ومعالجتها.</p>   | <p>التشغیر<br/>Cryptography</p>  |
| <p>الاستغلال المتعمّد لأنظمة الحاسوب الآلي والشبكات والجهات التي يعتمد عملها على تقنية المعلومات والاتصالات الرقمية بهدف إحداث أضرار.</p>  | <p>الهجوم السيبراني<br/>Cyber-Attack</p>   |
| <p>المخاطر التي تمس عمليات أعمال الجهة (بما في ذلك رؤية الجهة أو رسالتها أو إدارتها أو صورتها أو سمعتها) أو أصول الجهة أو الأفراد أو الجهات الأخرى أو الدولة، بسبب إمكانية الوصول غير المصحح به أو الاستخدام أو الإفصاح أو التعطيل أو التعديل أو تدمير المعلومات و/أو نظم المعلومات.</p>   | <p>المخاطر السيبرانية<br/>Cyber Risks</p>  |
| <p>القدرة الشاملة للجهة على الصمود أمام الأحداث السيبرانية، ومبنيات الضرر، والتعافي منها.</p>  | <p>الصمود الأمني السيبراني<br/>Cybersecurity Resilience</p>                        |
| <p>حسب ما نص عليه تنظيم الهيئة الصادر بالأمر الملكي رقم (٦٨٠١) وتاريخ (١١/٢/١٤٣٩هـ)، فإن الأمان السيبراني هو حماية الشبكات وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية، ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات، وما تحتويه من بيانات، من أي اختراق أو تعطيل أو تعديل أو دخول أو استخدام أو استغلال غير مشروع. ويشمل مفهوم الأمان السيبراني أمن المعلومات والأمن الإلكتروني والأمن الرقمي ونحو ذلك.</p>   | <p>الأمن السيبراني<br/>Cybersecurity</p>   |

| المصطلح  | التعريف   |
|--|---|
| الفضاء السيبراني<br>Cyberspace   | الشبكة المترابطة من البنية التحتية لتقنية المعلومات، والتي تشمل الإنترن特 وشبكات الاتصالات وأنظمة الحاسوب الآلي والأجهزة المتصلة بالإنترن特، إلى جانب المعالجات وأجهزة التحكم المرتبطة بها. كما يمكن أن يشير المصطلح إلى عالم أو نطاق افتراضي كظاهرة مجربة أو مفهوم مجرد.   |
| تصنيف البيانات والمعلومات<br>Data and Information Classification               | تعيين مستوى الحساسية للبيانات والمعلومات التي ينتج عنها ضوابط أمنية لكل مستوى من مستويات التصنيف. يتم تعيين مستويات حساسية البيانات والمعلومات وفقاً لفئات محددة مسبقاً حيث يتم إنشاء البيانات والمعلومات أو تعديلها أو تحسينها أو تخزينها أو نقلها. مستوى التصنيف هو مؤشر على قيمة أو أهمية البيانات والمعلومات للجهة. |
| أرشيف البيانات<br>Data Archiving   | عملية نقل البيانات التي لم تعد مستخدمة بشكل فعال في جهاز تخزين منفصل للحفظ طويل الأجل. تكون بيانات الأرشيف من بيانات قديمة لا تزال مهمة للجهة وقد تكون مطلوبة للرجوع إليها في المستقبل، وبيانات يجب الاحتفاظ بها للالتزام بالتشريعات والتنظيمات ذات العلاقة.  |
| الدفاع الأمني متعدد المراحل<br>Defense-in-Depth                                | هو مفهوم لتأكيد المعلومات (Information Assurance) حيث يتم وضع مستويات متعددة من الضوابط الأمنية (كدفاع) في نظام تقنية المعلومات (IT) أو تقنية التشغيل (OT).   |
| التعافي من الكوارث<br>Disaster Recovery  | الأنشطة والبرامج والخطط المصممة لإرجاع وظائف وخدمات الأعمال الحيوية للجهة إلى حالة مقبولة، بعد التعرض إلى هجمات سيبرانية أو تعطل لهذه الخدمات والوظائف.   |
| نظام أسماء النطاقات<br>Domain Name System                                      | نظام تقني يستخدم قاعدة بيانات يتم توزيعها عبر الشبكة وأو الإنترنوت تسهم بتحويل أسماء النطاقات إلى عناوين الشبكة (IP Addresses)، والعكس، لتحديد عناوين الخدمات مثل خوادم المواقع الإلكترونية والبريد الإلكتروني.   |
| فعالية<br>Effectiveness  | تشير الفعالية إلى الدرجة التي يتم بها تحقيق تأثير مخطط له. وتعتبر الأنشطة المخططة فعالة إذا تم تنفيذ هذه الأنشطة بالفعل، وتعتبر النتائج المخطط لها فعالة إذا تم تحقيق هذه النتائج بالفعل. يمكن استخدام مؤشرات قياس الأداء Key Performance Indicators "KPIs" لقياس وتقييم مستوى الفعالية.                                |
| كفاءة<br>Efficiency  | العلاقة بين النتائج المحققة (المخرجات) والموارد المستخدمة (المدخلات). يمكن تعزيز كفاءة العملية أو النظام من خلال تحقيق نتائج أكثر باستخدام نفس الموارد (المدخلات) أو أقل.   |
| حدث<br>Event   | شيء يحدث في مكان محدد (مثل الشبكة والأنظمة والتطبيقات وغيرها) وفي وقت محدد.   |
| بروتوكول نقل النص التشعبي الآمن<br>Hyper Text Transfer Protocol Secure (HTTPS) | بروتوكول يستخدم التشفير لتأمين صفحات وبيانات الويب عند انتقالها عبر الشبكة. وهو عبارة عن نسخة آمنة من نظام بروتوكول نقل النص التشعبي (HTTP).  |

| التعريف  | المصطلح   |
|--|---|
| وسيلة التدقيق من هوية المستخدم أو العملية أو الجهاز، وهي عادة شرط أساسى لمنح حق الوصول إلى الموارد في النظام.  | هوية<br>Identification  |
| انتهاك أمني بمخالفة سياسات الأمان السيبراني أو سياسات الاستخدام المقبول أو ممارسات أو ضوابط أو متطلبات الأمان السيبراني.   | حادثة<br>Incident   |
| الحماية ضد تعديل أو تخريب المعلومات بشكل غير مصرح به، وتتضمن خمان عدم الإنكار للمعلومات (Non-Repudiation) والموثوقية.  | سلامة المعلومة<br>Integrity   |
| المتطلبات الوطنية هي متطلبات طورتها جهة تشريعية في المملكة العربية السعودية للاستخدام بشكل تنظيمي (مثل: الضوابط الأساسية للأمن السيبراني ECC-1:2018).<br>المتطلبات الدولية هي متطلبات طورتها جهة أو منظمة دولية عالمية للاستخدام بشكل تنظيمي في جميع أنحاء العالم (مثل: PCI, SWIFT, وغيرها).   | المتطلبات الوطنية والدولية<br>(Inter)National Requirements                            |
| نظام لديه قدرات كشف الاختراقات، بالإضافة إلى القدرة على منع وإيقاف محاولات الأنشطة والحوادث المشبوهة أو المحتملة.  | نظام الحماية المتقدمة<br>لاكتشاف ومنع الاختراقات<br>Intrusion Prevention System (IPS) |
| نوع من أدوات قياس مستوى الأداء يقيّم مدى نجاح نشاط ما أو جهة تجاه تحقيق أهداف محددة.   | مؤشر قياس الأداء<br>Key Performance Indicator (KPI)                                   |
| عرض معلومات (بتنسيق وترميز محدد وقياسي) توضح على أصول الجهة (مثل: الأجهزة والتطبيقات والمستندات وغيرها) لبسطها إلى لإشارة إلى بعض المعلومات المتعلقة بتصنيف الأصل وملكيته ونوعه وغيرها من المعلومات المتعلقة بإدارة الأصول.  | ترميز أو علامة<br>Labeling  |
| مبدأً أساسى في الأمان السيبراني يهدف إلى منح المستخدمين صلاحيات الوصول التي يحتاجونها لتنفيذ مسؤولياتهم الرسمية فقط.   | الحد الأدنى من الصلاحيات<br>Least Privilege   |
| برنامج يُصيب الأنظمة بطريقة خفية (في الغالب) لانتهاك سرية أو سلامة ودقة أو توافر البيانات أو التطبيقات أو نظم التشغيل.   | البرمجيات الخارة<br>Malware   |
| نظام أمني يتحقق من هوية المستخدم، يتطلب استخدام عدة عناصر مستقلة من آليات التحقق من الهوية. تتضمن آليات التحقق عدة عناصر: <ul style="list-style-type: none"><li>• المعرفة (شيء يعرّفه المستخدم فقط مثل كلمة المرور).</li><li>• الحياة (شيء يملكه المستخدم فقط مثل برنامج أو جهاز توليد أرقام عشوائية أو الرسائل القصيرة المؤقتة لتسجيل الدخول، ويطلق عليها "One-Time-Password").</li><li>• الملزمة (صفة أو سمة حيوية متعلقة بالمستخدم نفسه فقط مثل بصمة الإصبع).</li></ul> | التحقق من الهوية متعدد العناصر<br>Multi-Factor Authentication (MFA)                   |

| المصطلح   | التعريف   |
|---|---|
| المعمارية متعددة المستويات<br>Multi-tier Architecture                         | معمارية أو بنية تُطبق أسلوب عميل-خادم الذي يتم فيه تطوير وصيانة منطق العملية الوظيفية، والوصول إلى البيانات، وت تخزين البيانات وواجهة المستخدم كوحدات مستقلة على منصات منفصلة.  |
| النecessity إلى المعرفة والحاجة إلى الاستخدام<br>Need-to-know and Need-to-use | القيود المفروضة على البيانات، والتي تعتبر حساسة ما لم يكن لدى الشخص حاجة محددة للطلع على البيانات لغرض ما متعلق بأعمال ومهام رسمية.   |
| النسخ الاحتياطي غير المتصل أو خارج الموقع<br>Offline/Offsite Backup           | نسخة احتياطية لقاعدة البيانات وإعدادات الأنظمة والتطبيقات والأجهزة عندما تكون النسخة غير متصلة وغير قابلة للتحديث. عادةً ما تستخدم أشرطة (Tapes) في حالة النسخة الاحتياطية خارج الموقع.   |
| النسخ الاحتياطي المتصل<br>Online Backup                                       | طريقة للتخلص فيها النسخ الاحتياطي بانتظام عبر شبكة على خادم بعيد، (إما داخل شبكة الجهة أو بالاستضافة لدى مزود خدمة).  |
| العاملون في الجهة<br>Organization Staff                                       | الأشخاص الذين يعملون في الجهة (بما في ذلك الموظفون الرسميون والموظفو المؤقتون والمعاقدون).  |
| الاسناد الخارجي<br>Outsourcing  | الحصول على (السلع أو الخدمات) عن طريق التعاقد مع مورد أو مزود خدمة.   |
| حزم التحديثات والإصلاحات<br>Patch   | حزم بيانات داعمة لتحديث أو إصلاح أو تحسين نظام التشغيل للحاسوب الآلي أو لتطبيقاته أو برامجها. وهذا يشمل إصلاح الثغرات الأمنية وغيرها من الأخطاء، حيث تسمى هذه الحزم عادةً إصلاحات أو إصلاح الأخطاء وتحسين إمكانية الاستخدام أو الأداء.  |
| اختبار الاختراق<br>Penetration Testing  | ممارسة اختبار على نظام حاسوب آلي أو شبكة أو تطبيق موقع إلكتروني أو تطبيق هوافر ذكية للبحث عن ثغرات يمكن أن يستغلها المهاجم.   |
| رسائل التصيد الإلكتروني<br>Phishing Emails                                    | محاولة الحصول على معلومات حساسة مثل أسماء المستخدمين وكلمات المرور أو تفاصيل بطاقة الائتمان، غالباً لأسباب نوايا ضارة وخبيثة، وذلك بالتركيز على هيئة جهة جديرة بالثقة في رسائل بريد إلكترونية.  |
| الأمن المادي<br>Physical Security   | يصف الأمان المادي التدابير الأمنية التي تم تصميمها لمنع الوصول غير المصرح به إلى المرافق والمعدات والموارد التابعة للجهة، وحماية الأفراد والممتلكات من التلف أو الضرر (مثل التجسس أو السرقة، أو الهجمات الإرهابية). ينطوي الأمان المادي على استخدام طبقات متعددة من نظم مترابطة، تشمل الدوائر التلفزيونية المغلقة (CCTV)، وحراس الأمان، وحدود أمنية، والأقفال، وأنظمة التحكم في الوصول، والعديد من التقنيات الأخرى. |

| المصطلح   | التعريف  |
|---|--|
| سياسة   | وثيقة تحدد بنودها التزاماً عاماً أو توجيهآً أو نية ما كما تم التعبير عن ذلك رسمياً من قبل صاحب الصلاحية للجهة.   |
| Policy  | سياسة الأمان السيبراني هي وثيقة تعبر بنودها عن الالتزام الرسمي للإدارة العليا للجهة بتنفيذ وتحسين برنامج الأمان السيبراني في الجهة، وتشتمل السياسة على أهداف الجهة فيما يتعلق ببرنامج الأمان السيبراني وظواهاته ومتطلباته آلية تحسينه وتطويره. |
| الخصوصية  | الحرية من التدخل غير المصرح به أو الكشف عن معلومات شخصية حول فرد.  |
| Privacy   | عملية إدارة الصلاحيات ذات الخطورة العالية على أنظمة الجهة والتي تحتاج في الغالب إلى تعامل خاص لتقليل المخاطر التي قد تنشأ من سوء استخدامها.  |
| إدارة الصلاحيات الهامة والحساسة                   | عملية إدراة الصلاحيات ذات الخطورة العالية على أنظمة الجهة والتي تحتاج في الغالب إلى تعامل خاص لتقليل المخاطر التي قد تنشأ من سوء استخدامها.  |
| Privileged Access Management                      | وثيقة تحتوي على وصف تفصيلي للخطوات الضرورية لأداء عمليات أو أنشطة محددة في التوافق مع المعايير والسياسات ذات العلاقة. وتعرف الإجراءات على أنها جزء من العمليات.  |
| إجراءات   | مجموعة من الأنشطة المتراكبة أو التفاعلية تحول المدخلات إلى مخرجات. وهذه الأنشطة متأثرة بسياسات الجهة.  |
| Procedure   | عملية  |
| الاستعادة   | إجراء أو عملية لاستعادة أو التحكم في شيء منقطع أو تالف أو مسروق أو ضائع.   |
| Recovery  | مدة الاحتفاظ   |
| Retention   | هي المدة الزمنية التي يجب فيها الاحتفاظ بالمعلومات أو البيانات أو سجلات الأحداث أو النسخ الاحتياطية، بغض النظر عن الشكل (ورقي أو إلكتروني أو غير ذلك).   |
| Retention   | المعايير الأمنية لشفرة البرامج والتطبيقات  |
| Secure Coding Standards                           | ممارسة تطوير برمجيات وتطبيقات الحاسوب الآلي بطريقة تحمي من التعرض غير المقصود لثغرات الأمان السيبراني المتعلقة بالبرمجيات والتطبيقات.  |
| Secure Coding Standards                           | المعايير الأمنية لشفرة البرامج والتطبيقات  |
| مراجعة الإعدادات والتحصين                         | حماية وتحصين وضبط إعدادات جهاز الحاسوب الآلي، والنظام، والتطبيق، وجهاز الشبكة، والجهاز الأمني لمقاومة الهجمات السيبرانية. مثل: إيقاف أو تغيير الحسابات المصنوعية والافتراضية، إيقاف الخدمات غير المستخدمة، إيقاف منافذ الشبكة غير المستخدمة.   |
| Secure Configuration and Hardening                | مراجعة الإعدادات والتحصين  |
| نظام إدارة سجلات الأحداث ومراقبة الأمان السيبراني | نظام يقوم بإدارة وتحليل بيانات سجلات الأحداث الأمنية في الوقت الفعلي لتوفير مراقبة للتهديدات، وتحليل نتائج القواعد المتربطة لسجلات الأحداث، والتقارير حول بيانات السجلات، والاستجابة للحوادث.  |
| Security Information and Event Management (SIEM)  | نظام إدارة سجلات الأحداث ومراقبة الأمان السيبراني  |

| المصطلح  | التعريف   |
|--|---|
| الاختبار الأمني<br>Security Testing                      | عملية تهدف إلى التأكد من أن النظام أو التطبيق المعدل أو الجديد يتضمن ضوابط وحماية مناسبة ولا يحتوي على أي ثغرات أمنية قد تضر بالنظام أو التطبيقات الأخرى، أو تؤدي إلى سوء استخدام النظام أو التطبيق أو معلوماته، وكذلك للحفاظ على وظيفة النظام أو التطبيق على النحو المنشود.  |
| الأمن من خلال التصميم<br>Security-by-Design              | منهجية لتطوير الأنظمة والتطبيقات وتصميم الشبكات التي تسعى إلى جعلها خالية من نقاط الضعف والثغرات الأمنية السيبرانية، والمقدمة على صد الهجوم السيبراني قدر الإمكان من خلال عدة تدابير على سبيل المثال: الاختبار المستمر، وحماية المصادقة والتمسك بأفضل ممارسات البرمجة والتصميم، وغيرها.   |
| فصل المهام<br>Segregation of Duties                      | مبدأ أساسى في الأمان السيبراني يهدف إلى تقليل الأخطاء والاحتيال خلال مراحل تنفيذ عملية محددة عن طريق التأكد من ضرورة وجود أكثر من شخص لإكمال هذه المراحل وبصلاحيات مختلفة.  |
| إطار سياسة المرسل<br>Sender Policy Framework             | طريقة للتحقق من أن خادم البريد الإلكتروني المستخدم في إرسال رسائل البريد الإلكتروني يتبع المجال الخاص بالجهة المرسلة.   |
| طرف خارجي<br>Third-Party                                 | أى جهة تعمل كطرف في علاقة تعاقدية لتقديم السلع أو الخدمات (وهذا يشمل موادي ومزودي الخدمات).   |
| تهديد<br>Threat  | أى ظرف أو حدث من المحتمل أن يؤثر سلباً على أعمال الجهة (بما في ذلك مهمتها أو وظائفها أو مصداقيتها أو سمعتها) أو أصولها أو منسوبيها مستعيناً أحد أنظمة المعلومات عن طريق الوصول غير المصرح به إلى المعلومات أو تدميرها أو كشفها أو تغييرها أو حجب الخدمة. وأيضاً قدرة مصدر التهديد على النجاح في استغلال أحد نقاط الضعف الخاصة بنظام معلومات معين. وهذا التعريف يشمل التهديدات السيبرانية. |
| المعلومات الاستباقية<br>Threat Intelligence              | يوفر معلومات منتظمة وتحليلها حول الهجمات الأخيرة واللحالية والمحتملة التي يمكن أن تشكل تهديداً سيبرانياً للجهة.   |
| الثغرة<br>Vulnerability                                  | أى نوع من نقاط الضعف في نظام الحاسوب الآلي، أو برمجه أو تطبيقاته، أو في مجموعة من الإجراءات، أو في أى شيء يجعل الأمان السيبراني عرضة للتهديد.   |
| جدار الحماية لتطبيقات الويب<br>Web Application Firewall  | نظام حماية يوضع قبل تطبيقات الويب لتقليل المخاطر الناجمة من محاولات الهجوم الموجهة على تطبيقات الويب.   |
| البرمجيات الضارة غير المعروفة مسبقاً<br>Zero-Day Malware | عبارة عن برامجيات ضارة (Malware) غير معروفة مسبقاً، تم إنتاجها أو نشرها حديثاً. ويصعب في العادة اكتشافها بواسطة وسائل الحماية التي تعتمد على المعرفة المسبقة للبرمجيات الضارة (Signature-based Protection).   |

**ملحق (ب): قائمة الاختصارات**

يوضح الجدول ٣ أدناه معنى الاختصارات التي ورد ذكرها في هذه الضوابط.

**جدول ٣ : قائمة الاختصارات**

| معناه   | الاختصار |
|---|----------|
| التهديدات المتقدمة المستمرة Advanced Persistent Threat                                      | APT      |
| إدارة استمرارية الأعمال Business Continuity Management                                      | BCM      |
| سياسة أحضر الجهاز الخاص بك Bring Your Own Device  | BYOD     |
| الدائرة التلفزيونية المغلقة Closed-circuit television                                       | CCTV     |
| البنية التحتية الحساسة Critical National Infrastructure                                     | CNI      |
| نظام أسماء النطاقات Domain Name System  | DNS      |
| الضوابط الأساسية للأمن السيبراني Essential Cybersecurity Controls                           | ECC      |
| بروتوكول نقل النص التشعبي الآمن Hyper Text Transfer Protocol Secure                         | HTTPS    |
| نظام التحكم الصناعي Industrial Control System   | ICS      |
| تقنية المعلومات والاتصالات Information and Communication Technology                         | ICT      |
| تقنية المعلومات Information Technology  | IT       |
| التحقق من الهوية متعدد العناصر Multi-Factor Authentication                                  | MFA      |
| التقنية التشغيلية Operational Technology  | OT       |
| نظام إدارة سجلات الأحداث ومراقبة الأمان السيبراني Security Information and Event Management | SIEM     |
| نظام معدات السلامة Safety Instrumented System   | SIS      |
| اتفاقية مستوى الخدمة Service Level Agreement  | SLA      |





الم الهيئة الوطنية للمن امن السيبراني  
National Cybersecurity Authority

