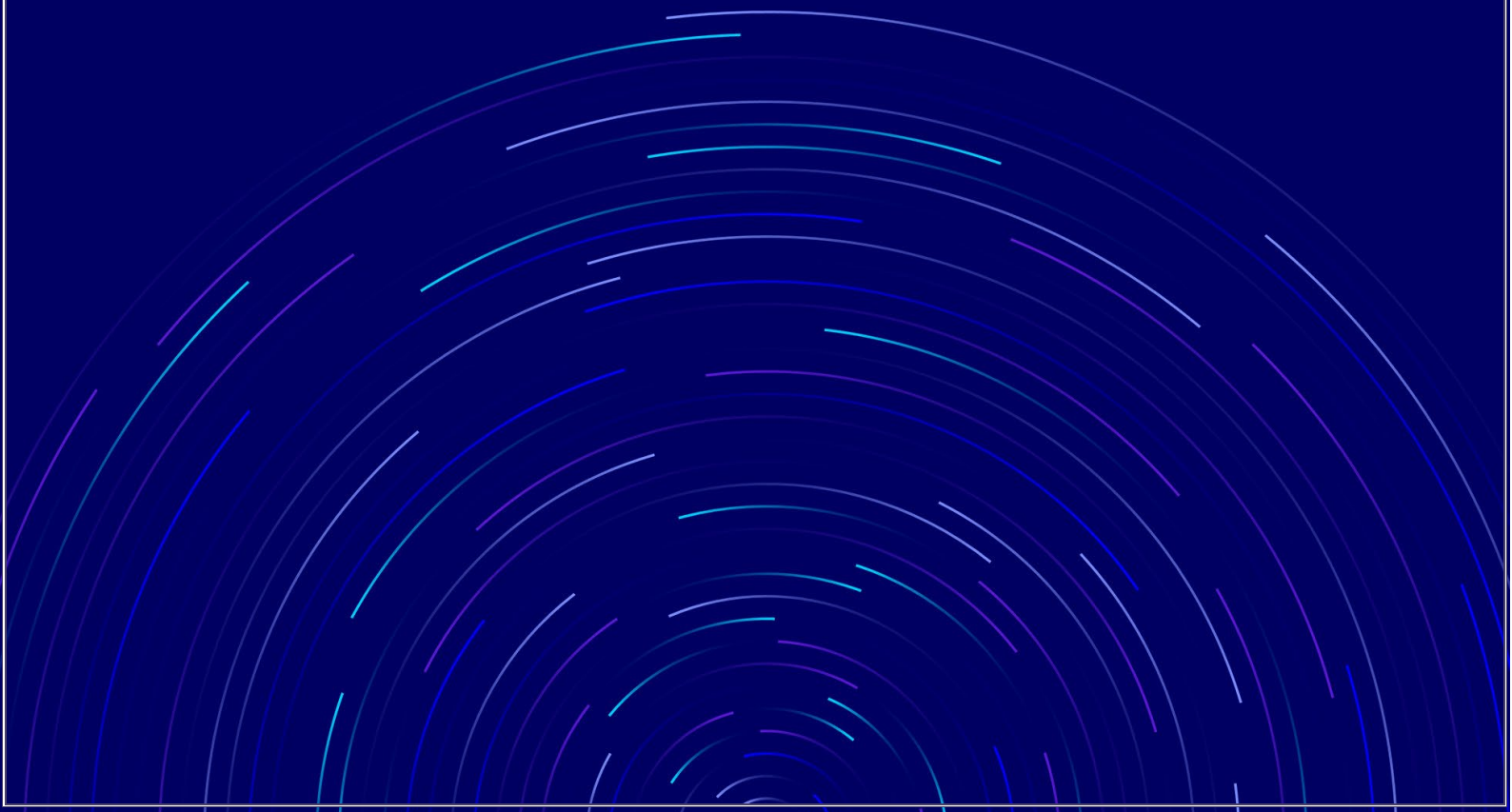
هيئة الاتصالات والفضاء والتقنية
Communications, Space & Technology Commission

الإطار التنظيمي للأمن السيبراني لمقدمي الخدمة في قطاع الاتصالات وتقنية المعلومات

الإصدار: 1.0

التاريخ: يونيو 2020م



المحتويات

1. مقدمة

وفقًا لنظام الاتصالات (النظام) ولائحته التنفيذية (اللائحة) وتنظيم هيئة الاتصالات وتقنية المعلومات وما تضمنه من صلاحيات للهيئة ومن ذلك تلك المتعلقة بحماية المصلحة العامة ومصالح المستخدمين والمحافظة على سرية الاتصالات وأمن المعلومات، وتماشياً مع رؤية المملكة 2030، أعدت هيئة الاتصالات والفضاء والتقنية (الهيئة) إطاراً تنظيمياً شاملاً للأمن السيبراني (الإطار التنظيمي) بهدف زيادة مستوى نضج الأمن السيبراني في قطاع الاتصالات وتقنية المعلومات ويعنى بشكل رئيس بالجهات المرخصة أو المسجلة من الهيئة وتلك الخاضعة لها بصفتها الجهة المنظمة لقطاع الاتصالات وتقنية المعلومات في المملكة العربية السعودية.

يعد قطاع الاتصالات وتقنية المعلومات أحد الركائز الرئيسية للنمو الاقتصادي الذي يوفر القدرة التنافسية الأساسية للاقتصاد الوطني من خلال النطاق العريض عالي السرعة، والخدمات الإلكترونية، والأصول المعلوماتية، ومع تزايد التوقعات نحو استمرار توافر الخدمات وشفافية تجربة المستخدمين، وكذلك فاعلية حماية الأنظمة والبيانات الحساسة، أصبح تعزيز الأمن السيبراني في المملكة العربية السعودية أمراً في غاية الأهمية لزيادة ثقة الوطن الرقمي في سلامة وصمود البنية التحتية لقطاع الاتصالات وتقنية المعلومات وخدماته.

2. الغرض

يوفر الإطار التنظيمي متطلبات لتحسين إدارة مخاطر الأمن السيبراني من خلال نهج متسق مع أفضل الممارسات العالمية وأُطر الأمن السيبراني المحلية. يهدف الإطار التنظيمي للأمن السيبراني إلى:

- تنظيم وتمكين ممارسات الأمن السيبراني لدى مقدمي الخدمة في قطاع الاتصالات وتقنية المعلومات.
- زيادة مستوى نضج الأمن السيبراني في قطاع الاتصالات وتقنية المعلومات.
- تبني منهجية إدارة المخاطر لتحقيق متطلبات الأمن السيبراني.
- تشجيع مقدمي الخدمة في قطاع الاتصالات وتقنية المعلومات على تطبيق أفضل الممارسات لوضع تدابير الأمن السيبراني المناسبة.
- ضمان سرية الخدمات المقدمة للعملاء، وسلامتها، وتوافرها.

3. النطاق

يوفر هذا الإطار مجموعة شاملة من متطلبات الحد الأدنى لضوابط الأمن السيبراني الواجب تطبيقها لمقدمي خدمات الاتصالات وتقنية المعلومات في قطاع الاتصالات وتقنية المعلومات (مقدم الخدمة). مع عدم الإخلال بالأحكام الواردة في أنظمة الهيئة ويقصد بها نظام الاتصالات ولائحته التنفيذية وتنظيم هيئة الاتصالات وتقنية المعلومات والأطر التنظيمية والسياسات والإرشادات وغير ذلك بما فيها القرارات التي تصدرها الهيئة والتوجيهات والأنظمة ذات الصلة، تطبق أحكام هذا الإطار على مقدمي الخدمة في قطاع الاتصالات وتقنية المعلومات الخاضعين للهيئة بصفتها المنظم للقطاع، وبشكل أخص على مقدمي الخدمة المرخصين أو المسجلين بتقديم الخدمات. وتجدر الإشارة إلى أن هذا الإطار لا يهدف إلى استبدال الأطر التنظيمية الصادرة، ولا ينبغي اعتباره بديلًا لأي منها. قد تحدد الهيئة وفق تقديرها المطلق

نطاق التطبيق لهذا الإطار على كافة الجهات من مقدمي خدمات الاتصالات وتقنية المعلومات، وقد يكون ذلك في شكل تطبيق إلزامي على الجميع أو إلزامي وإرشادي أو تطبيق إلزامي بشكل جزئي.

4. مقدمي الخدمة في قطاع الاتصالات وتقنية المعلومات المصنفين كبنى تحتية وطنية حساسة

على جميع مقدمي الخدمة في قطاع الاتصالات وتقنية المعلومات الذين يتم تصنيفهم كبنية تحتية وطنية حساسة بالتوافق بين الهيئة والهيئة الوطنية للأمن السيبراني الالتزام بالتالي:

وثيقة الضوابط الأساسية للأمن السيبراني الصادرة من الهيئة الوطنية للأمن السيبراني (المنشورة في موقع الهيئة الوطنية للأمن السيبراني).

الأدوار والمسؤوليات

1. مقدم الخدمة المصنف كبنى تحتية وطنية حساسة هو المسؤول عن أمنه السيبراني.
2. تقوم الهيئة الوطنية للأمن السيبراني بمتابعة الالتزام بوثيقة الضوابط الأساسية للأمن السيبراني الصادرة من الهيئة الوطنية للأمن السيبراني (المنشورة في موقع الهيئة الوطنية للأمن السيبراني).
3. يقوم مقدمي الخدمة المصنفين كبنى تحتية وطنية حساسة بتطبيق وتنفيذ الضوابط في هذا القسم وفقاً لمتطلبات الالتزام المحددة.
4. يقوم مقدمي الخدمة المصنفين كبنى تحتية وطنية حساسة بتزويد الهيئة بنسخة من تقارير الالتزام المرفوعة للهيئة الوطنية للأمن السيبراني.
5. يقوم مقدمي الخدمة المصنفين كبنى تحتية وطنية حساسة بمشاركة الهيئة أهم مخاطر الأمن السيبراني.
6. عند حدوث حادثة أمن سيبراني يلتزم مقدم الخدمة المصنف كبنى تحتية وطنية حساسة بالإبلاغ الفوري للهيئة الوطنية للأمن السيبراني وإشعار الهيئة بتلك الحادثة.
7. يقوم مقدمي الخدمة المصنفين كبنى تحتية وطنية حساسة بمشاركة التنبيهات والمعلومات الاستباقية ومؤشرات الاختراق وتقارير حوادث الأمن السيبراني مع الهيئة.
8. للهيئة الحق في إضافة ضوابط إضافية متى دعت الحاجة لذلك، وتقوم الهيئة بتحديد ومتابعة مستهدفات الالتزام بتلك الضوابط من خلال طرق مختلفة -على سبيل المثال ودون حصر- الالتزام الذاتي، وعمليات التفتيش الميدانية، وورش عمل الالتزام، وعمليات التدقيق الاستباقي أو الناتج عن البلاغات.

5. مقدمي الخدمة في قطاع الاتصالات وتقنية المعلومات غير المصنفين كبنى تحتية وطنية حساسة

على جميع مقدمي الخدمة غير المصنفين كبنى تحتية وطنية حساسة الالتزام بالمتطلبات والضوابط التالية:

6. المتطلبات

1. الحوكمة

1.1. تحديد استراتيجية الأمن السيبراني ووضع خارطة التنفيذ لتحقيق الأهداف الاستراتيجية المحددة.

1.2. تحديد وتطبيق الهيكل التنظيمي المناسب الذي سيتولى مسؤولية أنشطة الأمن السيبراني داخل الجهة.

1.3. تحقيق الالتزام بالمتطلبات التنظيمية الداخلية والخارجية (المحلية والعالمية) ذات الصلة.

1.4. إجراء عمليات تدقيق مستقلة للأمن السيبراني بصفة دورية تغطي متطلبات الالتزام الداخلية والخارجية لقياس مستوى امتثال الجهة.

1.5. عقد حملات توعوية ودورات تدريبية للأمن السيبراني بصفة دورية للموظفين لضمان حصولهم على المؤهلات والمهارات اللازمة للقيام بمسؤولياتهم.

1.6. تزويد عملائهم بمعلومات الأمن السيبراني ذات الصلة بالخدمات المقدمة لتحسين الوعي بالأمن السيبراني.

1.7. ضمان إدراج المتطلبات التنظيمية للأمن السيبراني في منهجية إدارة المشاريع المطبقة.

1.8. ضمان تلبية متطلبات الأمن السيبراني المتعلقة بالموارد البشرية في حالة حدوث أي تغييرات في الحالة الوظيفية.

2. إدارة الأصول

2.1. الاحتفاظ بقائمة جرد محدثة ودقيقة لجميع الأصول المعلوماتية التي تتضمن جميع التفاصيل ذات الصلة لتسهيل الحماية الفعّالة للأصول المعلوماتية.

2.2. تصنيف الأصول المعلوماتية لضمان الحماية القائمة على المخاطر للأصول المعلوماتية.

2.3. إدارة استخدام أجهزة الموظفين الشخصية لأغراض العمل لحماية الجهة من مخاطر الأمن السيبراني الناجمة عن استخدامها.

2.4. تحديد وتطبيق سياسة الاستخدام المقبول لحماية الجهة من المخاطر الناجمة عن الاستخدام غير المناسب للأصول المعلوماتية.

2.5. الحفاظ على الأصول المعلوماتية لضمان استمرار توافرها وسلامتها.

2.6. ضمان التخلص الآمن من الأصول المعلوماتية من أجل منع الاطلاع غير المصرح به أو تعديل المعلومات المخزنة عليها.

3. إدارة المخاطر للأمن السيبراني

3.1. إعداد وتنفيذ منهجية مناسبة لتحديد مخاطر الأمن السيبراني وتحليلها وتقييمها لحماية الأصول المعلوماتية.

3.2. إعداد وتنفيذ منهجية مناسبة لمراقبة مخاطر الأمن السيبراني ومعالجة المخاطر التي تم

تحديدها ومراقبة خطط المعالجة.

4. الأمن المنطقي

4.1. ضمان الاستخدام الفعال والمناسب للتشفير من أجل حماية سرية وموثوقية وسلامة المعلومات أثناء النقل والتخزين والاستخدام.

4.2. إدارة التغييرات التي تُجرى على الأصول المعلوماتية للتحكم في نتائج تلك التغييرات.

4.3. تحديد الثغرات الأمنية في الأصول المعلوماتية وترتيب أولويات إجراءات المعالجة الموصى بها.

4.4. التأكد من تطبيق حزم التحديثات والإصلاحات الأمنية على الأصول المعلوماتية ضمن إطار زمني مناسب لإصلاح المشكلات التي تم اكتشافها وتعزيز صمود تلك الأصول.

4.5. حماية الشبكات التي يديرها مقدم الخدمة من الأنشطة الخبيثة وضمان صمود الشبكات ضد تهديدات الأمن السيبراني.

4.6. مراقبة وحماية سجلات الأحداث الخاصة بالأصول المعلوماتية والإبلاغ عن أي أنشطة مشبوهة للمسؤولين.

4.7. إدارة صلاحيات الوصول وتطبيق آليات تحقق مناسبة لمنع الوصول غير المصرح به إلى الأصول المعلوماتية.

4.8. إنشاء وتطبيق قائمة بتطبيقات البرمجيات المسموح بتثبيتها واستخدامها داخل الجهة.

4.9. الكشف عن حوادث الأمن السيبراني والاستجابة لها لاحتوائها والحد من أثرها.

4.10. الكشف عن البرمجيات الضارة ومنع انتشارها في الجهة.

4.11. تصنيف معلومات الجهة لضمان حمايتها بشكل ملائم.

4.12. اتخاذ التدابير اللازمة بما في ذلك النسخ الاحتياطي لضمان استعادة الأصول المعلوماتية بعد وقوع أي حادثة.

4.13. تطبيق الإعدادات الأساسية للأنظمة بهدف زيادة صمود الأصول المعلوماتية.

4.14. تنفيذ منهجية دورة حياة تطوير البرمجيات بطريقة آمنة.

4.15. حماية البريد الإلكتروني ومتصفحات الويب من تهديدات الأمن السيبراني.

4.16. إجراء اختبارات الاختراق لتقييم القدرات الدفاعية للجهة وكشف الثغرات.

5. الأمن المادي

5.1. حماية الأصول المعلوماتية من الأضرار المادية والتهديدات.

5.2. إدارة الوصول المادي إلى المرافق التي تحتوي الأصول المعلوماتية لمنع الوصول غير المصرح به والتهديدات التي قد تنتج عنه.

6. الأمن المتعلق بالأطراف الخارجية

6.1. تضمين متطلبات الأمن السيبراني في العقود وإلزام مقدم الخدمة السحابية المتعاقد معه بتطبيقها.

6.2. تضمين متطلبات الأمن السيبراني في العقود وإلزام الأطراف الخارجية التي تقدم الإسناد الخارجي للأصول المعلوماتية للجهة بتطبيقها.

7. الضوابط

1. الحوكمة

1.1	استراتيجية الأمن السيبراني	
الضوابط		
1.1.1	المستوى الأول	تحديد وتوثيق متطلبات [استراتيجية الأمن السيبراني] مع مراعاة ما يلي: • الرسالة العامة للجهة وأهدافها وأنشطتها فيما يتعلق بالأمن السيبراني. • متطلبات الالتزام التشريعية والتنظيمية ذات الصلة. • إنشاء برنامج الأمن السيبراني. • التزام الإدارة العليا تجاه الأمن السيبراني.
1.1.2	المستوى الأول	ضمان اعتماد [استراتيجية الأمن السيبراني] من قبل الإدارة العليا.
1.1.3	المستوى الأول	ضمان أن [خطة العمل] الخاصة بتنفيذ استراتيجية الأمن السيبراني، تراعي ما يلي: • الأنشطة. • الميزانية. • الجدول الزمني. • الموارد (على سبيل المثال: القدرات، الموظفين).
1.1.4	المستوى الثالث	مراجعة وتحديث [استراتيجية الأمن السيبراني] [وخطة العمل] الخاصة بها بشكل مستمر أو عند الحاجة، ولا سيما في حالة حدوث تغييرات في المتطلبات التشريعية والتنظيمية ذات الصلة، أو التغييرات التنظيمية الرئيسية أو بناءً على الدروس المستفادة من تنفيذ خطط العمل السابقة.
المراجع	NIST CSWP - ID.BE NIST.sp.800-53-r4 - PM-1 NCA ECC - 1-1-1 NCA ECC - 1-1-2 NCA ECC - 1-1-3 NCA CSCC -1-1-1 NCA CSCC -1-1-2 NCA CSCC -1-1-3	

1.2	إدارة الأمن السيبراني	
الضوابط		
1.2.1	المستوى الأول	تحديد وتوثيق متطلبات [الهيكل التنظيمي للأمن السيبراني] مع مراعاة ما يلي: • لجنة الأمن السيبراني وتحديد أعضاء يمثلون تخصصات مختلفة داخل الجهة. • مهام/مسؤوليات إدارات الأمن السيبراني اللازمة لتنفيذ [خطة العمل]. • تقديم تقارير مباشرة إلى الإدارة العليا لتجنب تعارض المصالح. • تحديد الأدوار والمسؤوليات بما يكفل الفصل الواضح بين الواجبات والمسؤوليات المتعارضة.
1.2.2	المستوى الأول	تنفيذ [الهيكل التنظيمي للأمن السيبراني] المحدد.
1.2.3	المستوى الأول	تنفيذ [خطة العمل] من خلال [الهيكل التنظيمي للأمن السيبراني].
1.2.4	المستوى الأول	الإشراف على تنفيذ [خطة العمل] من قبل لجنة الأمن السيبراني التي تتولى مراقبة التنفيذ وحل الخلافات وفرض التدابير اللازمة للتحسين.
1.2.5	المستوى الثالث	قياس ومراجعة وتحسين متطلبات [الهيكل التنظيمي للأمن السيبراني] باستمرار لضمان وجود هيكل تنظيمي فعال للأمن السيبراني.
المراجع	ISO 27001 - 5 ISO 27002 - 6.1.1 ISO 27002 - 6.1.2 NCA ECC - 1-2-1 NCA ECC - 1-2-2 NCA ECC - 1-2-3	
1.3	الالتزام بالأمن السيبراني	
الضوابط		
1.3.1	المستوى الأول	تحديد وتوثيق [متطلبات الالتزام بالأمن السيبراني] مع مراعاة ما يلي: • المتطلبات التشريعية والتنظيمية الوطنية ذات الصلة المتعلقة بالأمن السيبراني • المتطلبات الدولية/الخارجية المعتمدة محلياً (على سبيل المثال المدرجة في الاتفاقيات أو الالتزامات الدولية) • المتطلبات الداخلية للجهة
1.3.2	المستوى الأول	تحديد وتنفيذ {عملية الالتزام} لضمان تحديد متطلبات الالتزام بصفة دورية وتوثيقها والرفع بها (على سبيل المثال، يجب تحديث

		متطلبات الأمن السيبراني للجهة إذا أصبحت متطلبات تنظيمية جديدة سارية ونافذة).
1.3.3	المستوى الأول	ضمان إدراج ومراعاة متطلبات الالتزام في جميع أعمال الجهة.
1.3.4	المستوى الثالث	قياس ومراجعة وتحسين [متطلبات الالتزام بالأمن السيبراني] وكذلك فاعلية الإجراءات بشكل مستمر وذلك لضمان تحقيق الالتزام.
المراجع		ISO 27002 - 18.1 NCA ECC - 1-7-1 NCA ECC - 1-7-2
1.4	تدقيق الأمن السيبراني	
الضوابط		
1.4.1	المستوى الثاني	تحديد وتوثيق [متطلبات تدقيق الأمن السيبراني] مع مراعاة ما يلي: • إجراء عمليات تدقيق دورية مستقلة (على سبيل المثال: إجراء عمليات تدقيق مرة واحدة على الأقل في السنة للأنظمة الحساسة). • حماية [سجلات التدقيق] والاحتفاظ بها. • رفع التقارير إلى الإدارة العليا.
1.4.2	المستوى الثاني	تحديد [عملية التدقيق الداخلي] وتنفيذها للتحقق من الالتزام بـ[متطلبات الالتزام بالأمن السيبراني].
1.4.3	المستوى الثاني	إجراء عمليات تدقيق مستقلة على فترات مخطط لها (أو عند حدوث تغييرات كبيرة) لمراجعة تنفيذ [متطلبات الالتزام بالأمن السيبراني].
1.4.4	المستوى الثاني	توثيق النتائج والتوصيات وتقديمها إلى الإدارة العليا.
1.4.5	المستوى الثاني	حماية [سجلات التدقيق] من الوصول غير المصرح به، أو تعديلها، أو إتلافها.
1.4.6	المستوى الثاني	ضمان الاحتفاظ بـ [سجلات التدقيق] كدليل، على سبيل المثال، على الالتزام بالمتطلبات التشريعية والتنظيمية.
1.4.7	المستوى الثالث	قياس ومراجعة وتحسين [متطلبات تدقيق الأمن السيبراني] وكذلك فاعلية إجراءات التدقيق وأنشطة المراجعة بشكل مستمر.
المراجع		ISO 27002 - 18.2 ISO 27002 - 18.1.3 NIST.sp.800-53r4 - AU-6 NIST.sp.800-53r4 - AU-9 NIST.sp.800-53r4 - AU-11 NCA ECC - 1-8 NCA CSCC - 1-4

1.5	التدريب والتوعية بالأمن السيبراني	
الضوابط		
1.5.1	المستوى الأول	تحديد وتوثيق [متطلبات التدريب والتوعية المتعلقة بالأمن السيبراني] مع مراعاة ما يلي: • الأهداف والنطاق • عدد الدورات التدريبية ومعدل تكرارها في العام • الموارد المخصصة
1.5.2	المستوى الأول	تحديد وتنفيذ [برنامج التدريب والتوعية المتعلق بالأمن السيبراني] (على سبيل المثال تحديد الأهداف، والنطاق، والشريحة المستهدفة، ومعايير التحقق) على أن يشمل البرنامج موضوعات الأمن السيبراني المختلفة مع مراعاة ما يلي: • أدوار ومسؤوليات الأمن السيبراني للشريحة المستهدفة. • أحداث وتهديدات الأمن السيبراني الشائعة (على سبيل المثال هجمات الهندسة الاجتماعية على سبيل المثال: الحيل الهاتفية ومكالمات انتحال الشخصية). • توعية العاملين بعدم محاولة القيام بأنشطة غير مصرح بها (على سبيل المثال: إدخال أو استخدام معدات أو برمجيات غير مصرح بها على نظام ما، ونقل المعدات دون صلاحية استخدام مناسبة). • التعامل الآمن مع الأجهزة المحمولة ووسائط التخزين، وخدمات البريد الإلكتروني (خاصة الرسائل الاقتحامية ورسائل التصيّد الإلكتروني)، وخدمات تصفح الإنترنت ووسائل التواصل الاجتماعي. • سياسة المكتب النظيف والشاشة الخالية (على سبيل المثال: تأمين المعلومات الحساسة المخزنة على الأوراق في مكان آمن، وإغلاق شاشات أجهزة الكمبيوتر والوحدات الطرفية في حالة عدم الاستخدام أو عدم المراقبة).
1.5.3	المستوى الثاني	تحسين وتنفيذ [متطلبات التدريب والتوعية المتعلقة بالأمن السيبراني] لتشمل إجراء اختبارات تحقق دورية لتقييم فاعلية [برنامج التدريب والتوعية المتعلق بالأمن السيبراني] وتسجيل نتائج التقييم (على سبيل المثال: التحقق مما إذا كان الموظفون سينقرون على رابط مشبوه يتم إرساله عبر رسائل البريد الإلكتروني).
1.5.4	المستوى الثاني	تحسين وتنفيذ [متطلبات التدريب والتوعية المتعلقة بالأمن السيبراني] لتحديد الحالات التي يتوجب فيها تقديم [برنامج التدريب والتوعية المتعلق بالأمن السيبراني] (على سبيل المثال: التدريبات الأولية على الأمن السيبراني للمستخدمين الجدد، والتدريب عند حدوث تغييرات في أنظمة المعلومات أو في الأدوار الوظيفية).
1.5.5	المستوى	تصميم [برنامج التدريب والتوعية المتعلق بالأمن السيبراني]

	الثاني	بحيث يشمل المهارات المتخصصة أو المتعلقة بالأمن وكذلك تدريب فئات محددة من العاملين، على سبيل المثال: • الإدارة المعنية بالأمن السيبراني • العاملين في تقنية المعلومات • العاملين في تطوير البرمجيات • المعنيين بتقييم مخاطر الأمن السيبراني • العاملين الذين يتمتعون بصلاحيات الدخول إلى الأصول المعلوماتية الحساسة • الموظفين التنفيذيين
1.5.6	المستوى الثالث	قياس ومراجعة وتحسين [متطلبات التدريب والتوعية المتعلقة بالأمن السيبراني]
المراجع		ISO 27002 - 7.2.2 SANS v6.1 - 17.4 NIST.sp.800-53r4 - AT-2 NCA ECC - 1-9-4 NCA ECC - 1-10-1 NCA ECC - 1-10-2 NCA ECC - 1-10-3 NCA ECC - 1-10-4 NCA ECC - 1-10-5
1.6	التوعية بالأمن السيبراني للعملاء	
الضوابط		
1.6.1	المستوى الأول	تحديد وتوثيق [متطلبات التوعية بالأمن السيبراني للعملاء] مع مراعاة ما يلي: • الأهداف والنطاق. • عدد الدورات التدريبية ومعدل تكرارها في العام. • الموارد المخصصة.
1.6.2	المستوى الأول	تحديد وتنفيذ [برنامج التوعية بالأمن السيبراني للعملاء] من خلال - على سبيل المثال- تحديد الأهداف، والنطاق، وشريحة العملاء المستهدفة، وقنوات الاتصال المستخدمة التي يجب أن تأخذ في الاعتبار ما يلي: • المعلومات المتعلقة بأحداث وتهديدات الأمن السيبراني المستجدة ذات الصلة (على سبيل المثال هجمات الهندسة الاجتماعية على سبيل المثال: الحيل الهاتفية ومكالمات انتحال الشخصية). • توصيات محددة متعلقة بالخدمة المقدمة (على سبيل المثال: كيف تكون آمناً أثناء استخدام الإنترنت، رسائل التصيد النصية والإلكترونية، وحماية جهازك المحمول).
1.6.3	المستوى	تحسين وتنفيذ [متطلبات التوعية بالأمن السيبراني للعملاء]

	الثاني	لتنفيذ [برنامج التوعية بالأمن السيبراني للعملاء] بشكل دوري.
1.6.4	المستوى الثالث	قياس ومراجعة وتحسين [متطلبات التوعية بالأمن السيبراني للعملاء] بشكل مستمر.
المراجع		ISO 27002 - 7.2.2
1.7	الأمن السيبراني في إدارة المشاريع	
الضوابط		
1.7.1	المستوى الأول	تحديد وتوثيق [متطلبات الأمن السيبراني في إدارة المشاريع] مع مراعاة ما يلي: • تضمين متطلبات الأمن السيبراني في إدارة المشاريع (على سبيل المثال أن يكون موظفي الأمن السيبراني جزء من فريق المشروع). • تحديد أهداف المشروع بحيث تتضمن اعتبارات الأمن السيبراني خلال جميع مراحل المشروع.
1.7.2	المستوى الأول	إجراء تقييم للمخاطر في بداية وأثناء كل مشروع وفقاً لـ [تقييم مخاطر الأمن السيبراني] لتحديد مخاطر الأمن السيبراني إن وجدت وتحديد خطط المعالجة.
1.7.3	المستوى الثاني	مراقبة مخاطر الأمن السيبراني المحددة وخطط معالجتها أثناء المشروع. [معالجة ومراقبة مخاطر الأمن السيبراني].
1.7.4	المستوى الثالث	قياس ومراجعة وتحسين [متطلبات الأمن السيبراني في إدارة المشاريع] بشكل مستمر.
المراجع		ISO 27002 - 6-1-5 NCA ECC - 1-6-1 NCA ECC - 1-6-2 NCA ECC - 1-6-3 NCA ECC - 1-6-4
1.8	الأمن السيبراني المتعلق بالموارد البشرية	
الضوابط		
1.8.1	المستوى الأول	تحديد وتوثيق [متطلبات الأمن السيبراني المتعلق بالموارد البشرية] مع مراعاة ما يلي: • تحديد متطلبات الأمن السيبراني المتعلقة بالعاملين (الموظفين والمتعاقدين) في الجهة قبل توظيفهم وأثناء عملهم وعند انتهاء/إنهاء عملهم. • إجراء المسح الأمني على جميع المرشحين للتوظيف. • توظيف عاملين على درجة عالية من الاحترافية في الوظائف المتعلقة بالأنظمة الحساسة. • ضمان تغطية البنود والاتفاقيات المتعلقة بالتوظيف لمدونة قواعد السلوك الوظيفي (على سبيل المثال: اتفاقيات عدم الإفصاح، ومسؤوليات الأمن السيبراني)، وإدراجها أثناء وبعد

		إنتهاء/إنهاء العمل لدى الجهة. • ضمان توقيع جميع العاملين على مدونة قواعد السلوك الوظيفي. • إنفاذ سياسة [الاستخدام المقبول للأصول المعلوماتية].
1.8.2	المستوى الأول	ضمان تنفيذ الإجراءات اللازمة (على سبيل المثال: تعديل تصاريح وصلاحيات الوصول وفقاً للدور الوظيفي الجديد) عند إعادة تعيين العاملين أو نقلهم إلى وظائف أخرى داخل الجهة.
1.8.3	المستوى الأول	ضمان التحقيق في جميع المخالفات المتعلقة بمتطلبات الأمن السيبراني وخضوع العاملين المسؤولين عنها إلى تحقيق شامل واتخاذ الإجراءات التأديبية اللازمة.
1.8.4	المستوى الأول	ضمان تنفيذ الإجراءات اللازمة (على سبيل المثال، إلغاء حقوق وصلاحيات الوصول التي يتمتع بها العاملين، واسترداد الأصول المعلوماتية المخصصة، واستعادة صلاحيات الوصول إلى الأصول المعلوماتية التي كانت تقع سابقاً تحت إشراف العامل الذي تم إنهاء عمله) عند انتهاء/إنهاء الخدمة للعاملين في الجهة.
1.8.5	المستوى الثالث	قياس ومراجعة وتحسين [متطلبات الأمن السيبراني المتعلقة بالموارد البشرية] وكذلك فاعلية الإجراءات ذات الصلة بشكل مستمر.
المراجع		ISO 27002 - 7.1.1 ISO 27002 - 7.1.2 ISO 27002 - 7.2.3 ISO 27002 - 7.3.1 ISO 27002 - 8.1.4 NIST.sp.800-53r4 - PS-4 NIST.sp.800-53r4 - PS-5 NCA ECC - 1-9-1 NCA ECC - 1-9-2 NCA ECC - 1-9-3 NCA ECC 1-9-4 NCA ECC - 1-9-5 NCA ECC - 1-9-6 NCA CSCC -1-9-3 NCA CSCC - 1-5-1

2. إدارة الأصول

2.1	اكتشاف الأصول	
الضوابط		
2.1.1	المستوى الأول	تحديد وتوثيق [متطلبات اكتشاف الأصول] مع مراعاة ما يلي: • تحديد قائمة جرد الأصول المعلوماتية [قائمة جرد الأصول] (على سبيل المثال: البرمجيات، والأجهزة، والمعلومات، والأصول المعلوماتية الحساسة، والمعدات، وقواعد البيانات). • تحديد معدل تحديث [قائمة جرد الأصول]. • ملكية الأصول المعلوماتية.
2.1.2	المستوى الأول	تحديد وتنفيذ {عملية اكتشاف الأصول} لتحديد جميع الأصول المعلوماتية التي تملكها الجهة (على سبيل المثال: باستخدام أداة اكتشاف الأصول) وتحديث [قائمة جرد الأصول]، وتعيين مالك لكل أصل من الأصول المعلوماتية.
2.1.3	المستوى الأول	مراجعة وتحديث [قائمة جرد الأصول] بناءً على معدل التحديث المحدد في المتطلبات أو في حالة وجود تعديلات على الأصول المعلوماتية (على سبيل المثال: أي إضافة أو حذف للأصول المعلوماتية).
2.1.4	المستوى الثاني	استخدام أدوات مخصصة ومؤتمتة لاكتشاف الأصول المعلوماتية، وربط الأصول المعلوماتية ببعضها وتتبعها من خلال نظام مركزي.
2.1.5	المستوى الثالث	قياس ومراجعة وتحسين [متطلبات اكتشاف الأصول] وكذلك فاعلية الإجراءات ذات الصلة بشكل مستمر.
المراجع	ISO 27002 - 8.1 ISO 27002 - 8.2 ISO 27002 - 8.3.2 SANS v7.0 - 1.1 SANS v7.0 - 1.2 SANS v7.0 - 2.3 SANS v7.0 - 2.5 NCA ECC - 2-1-1 NCA ECC - 2-1-2 NCA ECC - 2-1-6 NCA CSCC -2-1-1 NCA CSCC -2-1-2 NCA CSCC -2-1-6 NCA CSCC - 2-1-1	

2.2	تصنيف الأصول	
الضوابط		
2.2.1	المستوى الأول	تحديد وتوثيق [متطلبات تصنيف الأصول] مع مراعاة ما يلي: • تصنيف وترميز الأصول المعلوماتية وكذلك التدابير الوقائية المتعلقة بتحديد الأصول المعلوماتية ومعالجتها ونقلها وتخزينها واستعادتها وحذفها والتخلص منها.
2.2.2	المستوى الأول	تحديد وتنفيذ {عملية تصنيف الأصول} لتصنيف وترميز الأصول المعلوماتية الموجودة في [قائمة جرد الأصول] وفقًا لمعايير محددة (على سبيل المثال: الأهمية، والقيمة التجارية، والمتطلبات القانونية، والسرية، والسلامة، والتوافر) و [متطلبات حماية المعلومات].
2.2.3	المستوى الثالث	قياس ومراجعة وتحسين [متطلبات تصنيف الأصول] وكذلك فاعلية الإجراءات ذات الصلة بشكل مستمر.
المراجع		ISO 27002 - 8.1.2 ISO 27002 - 8.2.1 ISO 27002 - 8.2.3 NIST CSWP - ID.AM - 5 NCA ECC - 2-1-5
2.3	أحضر الجهاز الخاص بك	
الضوابط		
2.3.1	المستوى الأول	تحديد وتوثيق [متطلبات الأمن السيبراني لسياسة أحضر الجهاز الخاص بك] داخل الجهة مع مراعاة ما يلي: • فصل المعلومات الشخصية عن المعلومات المتعلقة بالعمل. • القيود المفروضة على استخدام الأجهزة حسب توجهات الجهة. • القيود المفروضة للوصول إلى الأنظمة الحساسة. • تأمين حذف معلومات الجهة.
2.3.2	المستوى الأول	إنفاذ [متطلبات الأمن السيبراني لسياسة أحضر الجهاز الخاص بك] المحددة داخل الجهة.
2.3.3	المستوى الأول	تأمين حذف معلومات الجهة من الأجهزة بعد الانتهاء من المهمة وعندما تكون المعلومات غير ضرورية.
2.3.4	المستوى الثاني	ضمان تشفير معلومات الجهة المُخزنة على الأجهزة.
2.3.5	المستوى الثالث	قياس ومراجعة وتحسين [متطلبات الأمن السيبراني لسياسة أحضر الجهاز الخاص بك] داخل الجهة بشكل مستمر.
المراجع		SANS v6.1 - 15.9 NCA ECC - 2-6-1 NCA ECC - 2-6-2 NCA ECC - 2-6-3 NCA CSCC -2-6-3

	NCA CSCC - 2-5-1	
2.4	الاستخدام المقبول للأصول المعلوماتية	
الضوابط		
2.4.1	المستوى الأول	تحديد وتوثيق [متطلبات الاستخدام المقبول للأصول المعلوماتية] مع مراعاة ما يلي: • الاستخدام المقبول للأصول المعلوماتية.
2.4.2	المستوى الأول	ضمان تنفيذ [متطلبات الاستخدام المقبول للأصول المعلوماتية] (على سبيل المثال: حظر تثبيت البرمجيات غير المرغوب بها، والتحكم بالوصول إلى صفحات الويب والسماح باستخدام أجهزة تخزين الوسائط القابلة للإزالة بناء على احتياجات العمل فقط).
2.4.3	المستوى الثالث	قياس ومراجعة وتحسين [متطلبات الاستخدام المقبول للأصول المعلوماتية] بشكل مستمر.
المراجع	ISO 27002 - 8.1.3 NCA ECC - 2-1-3 NCA ECC - 2-1-4	
2.5	صيانة الأصول	
الضوابط		
2.5.1	المستوى الثاني	تحديد وتوثيق [متطلبات صيانة الأصول] مع مراعاة ما يلي: • صيانة الأصول. • التتبع والمراقبة. • خطة الاستعادة.
2.5.2	المستوى الثاني	تحديد وتنفيذ {عملية صيانة الأصول} لصيانة الأصول المعلوماتية للجهة وإصلاحها (بما في ذلك الأصول خارج الموقع) والاحتفاظ بسجلات لهذه الأنشطة.
2.5.3	المستوى الثاني	وفقاً لخطة الاستعادة التي حددتها الجهة، يتم تنفيذ استعادة الأصول أثناء أو بعد وقوع حادثة أمنية متعلقة بالأمن السيبراني.
2.5.4	المستوى الثاني	إجراء المراقبة والتتبع عن بُعد (على سبيل المثال: استخدام تقنيات تتبع المواقع) للأصول المعلوماتية والتأكد من الاحتفاظ بها داخل المناطق التي تقع تحت إشراف الجهة ومراقبتها بشكل مناسب، بناءً على [تصنيف الأصول].
2.5.5	المستوى الثالث	قياس ومراجعة وتحسين [متطلبات صيانة الأصول] وكذلك فاعلية الإجراءات ذات الصلة بشكل مستمر.
المراجع	NIST CSWP - PR.MA-1 NIST CSWP - PR.MA-2 NIST CSWP - RC.RP-1 NIST.sp.800-53r4 – PE - 20 ISO 27002 - 11.2.4	

2.6	التخلص الآمن من الأصول	
الضوابط		
2.6.1	المستوى الأول	تحديد وتوثيق [متطلبات التخلص الآمن من الأصول] مع مراعاة ما يلي: • وضع قواعد للتخلص من الأصول المعلوماتية بناءً على تصنيف وترميز الأصول المعلوماتية المحددة في [قائمة جرد الأصول].
2.6.2	المستوى الأول	تحديد وتنفيذ {عملية التخلص الآمن من الأصول} للتعامل مع التخلص الآمن من الأصول المعلوماتية بناءً على [متطلبات التخلص الآمن من الأصول] باستخدام التقنيات المناسبة (على سبيل المثال: المحو الآمن والإتلاف المادي) من أجل منع الاطلاع غير المصرح به أو تعديل المعلومات المخزنة على تلك الأصول.
2.6.3	المستوى الثالث	قياس ومراجعة وتحسين [متطلبات التخلص الآمن من الأصول] وكذلك فاعلية الإجراءات ذات الصلة بشكل مستمر.
المراجع	ISO 27002 - 8.3.2 SANS v7.0 - 1.6 SANS v7.0 - 2.6 NCA ECC 2-14-3-4	

3. إدارة المخاطر للأمن السيبراني

3.1	تقييم مخاطر الأمن السيبراني	
الضوابط		
3.1.1	المستوى الأول	تحديد وتوثيق [متطلبات تقييم مخاطر الأمن السيبراني] مع مراعاة ما يلي: • أهداف ونطاق تقييم مخاطر الأمن السيبراني في الجهة. • الحالات التي ينبغي بموجبها إجراء تقييم لمخاطر الأمن السيبراني في الجهة ومعدل تكرار إجراء التقييم. • ضمان تغطية [متطلبات تقييم مخاطر الأمن السيبراني] لمخاطر الأصول المعلوماتية للجهة، والأفراد، والجهات الأخرى.
3.1.2	المستوى الأول	تحديد وتنفيذ {عملية تقييم المخاطر} التي تتكون من: • تحديد المخاطر: تحديد وتوثيق المخاطر الداخلية والخارجية بناءً على الأصول المعلوماتية في الجهة [اكتشاف الأصول] وتسجيل المخاطر التي تم تحديدها في [سجل المخاطر]. • تحليل المخاطر: تحليل وتوثيق المخاطر المحددة من حيث الاحتمالية والأثر. • تقييم المخاطر: تحديد أي مخاطر ينبغي معالجتها أو قبولها وتحديد أولوياتها وتوثيقها بناءً على مستوى تحمل الجهة للمخاطر (يجب اعتماد نتائج تقييم المخاطر رسمياً من قبل الإدارة العليا). • يتم الإبلاغ عن أهم مخاطر الأمن السيبراني الواردة في [سجل

		المخاطر] وخطط المعالجة إلى الهيئة.
3.1.3	المستوى الثاني	إدراج {عملية تقييم المخاطر} ضمن الإطار العام لإدارة المخاطر بالجهة والتأكد من تطبيقها في الحالات التالية كحد أدنى: • في المراحل الأولية للمشاريع التقنية الكبرى أو عند إجراء تغييرات جوهرية في البنية التنظيمية أو التقنية. • قبل إطلاق منتجات وخدمات جديدة.
3.1.4	المستوى الثالث	قياس ومراجعة وتحسين [متطلبات تقييم مخاطر الأمن السيبراني] وكذلك فاعلية الإجراءات ذات الصلة بشكل مستمر.
المراجع		ISO 27005 - 7.2 NIST.sp.800-53r4 - RA-1 NIST.sp.800-53r4 - RA-3 NIST.sp.800-53r4 - PM-9 NIST.sp.800-53r4 - PM-10 NIST CSWP - ID.RA NIST CSWP - ID.SC NCA ECC - 1.5.1 NCA ECC - 1.5.2 NCA ECC - 1.5.3 NCA ECC - 1.5.4 NCA CSCC -1-5-1 NCA CSCC -1-5-2 NCA CSCC -1-5-3 NCA CSCC -1-5-4
3.2	معالجة ومراقبة مخاطر الأمن السيبراني	
الضوابط		
3.2.1	المستوى الأول	تحديد وتوثيق [متطلبات معالجة ومراقبة مخاطر الأمن السيبراني] مع مراعاة ما يلي: • خطة معالجة المخاطر. • خطة مراقبة المخاطر.
3.2.2	المستوى الأول	تحديد وتنفيذ {عملية معالجة المخاطر} التي توضح كيفية معالجة المخاطر التي تم تقييمها وما ينتج عنها من [خطة معالجة المخاطر].
3.2.3	المستوى الأول	تحديد وتنفيذ {عملية مراقبة المخاطر} التي تراقب وتستعرض المخاطر المحددة، وتراقب تنفيذ خطة معالجة المخاطر، بالإضافة إلى مراقبة المخاطر المتبقية، وحالة المخاطر المقبولة.
3.2.4	المستوى الثالث	قياس ومراجعة وتحسين [متطلبات معالجة ومراقبة مخاطر الأمن السيبراني] وكذلك فاعلية الإجراءات ذات الصلة بشكل مستمر.
المراجع		ISO 27005 - 9.3 NIST.sp.800-53r4 - PM-9

	NIST CSWP - ID.RA NIST CSWP - ID.SC NCA ECC - 1.5.1 NCA ECC - 1.5.2 NCA ECC - 1.5.4 NCA CSCC -1-5-1 NCA CSCC -1-5-2 NCA CSCC -1-5-4

4. الأمن المنطقي

4.1	التشفير	
الضوابط		
4.1.1	المستوى الأول	تحديد وتوثيق [متطلبات التشفير] مع مراعاة ما يلي: • تحديد بروتوكولات وتقنيات التشفير الأساسية (على سبيل المثال: AES 256، وRSA 2048، وPKI) بالإضافة إلى القيود ذات الصلة (على سبيل المثال: الشهادات الموقعة ذاتياً، MD5). • الحالات التي ينبغي بموجبها تطبيق بروتوكولات التشفير المعتمدة (أثناء نقل وتخزين واستخدام البيانات) مع مراعاة [متطلبات التشفير].
4.1.2	المستوى الأول	إعداد قائمة [حلول التشفير] (على سبيل المثال: المنتجات والخوارزميات والبروتوكولات) وفقاً للقيود ذات الصلة (على سبيل المثال: القيود القانونية والتقنية والوطنية) والتأكد من اعتمادها من قبل المسؤولين.
4.1.3	المستوى الأول	استخدام [حلول التشفير] بناءً على الحالات المحددة، من أجل حماية المعلومات طوال دورة حياتها الكاملة (أثناء النقل، والتخزين، والاستخدام) ووفقاً لتصنيفها [متطلبات حماية المعلومات].
4.1.4	المستوى الثاني	تحديد وتنفيذ عملية [إدارة دورة حياة مفاتيح التشفير] للتعامل مع إنشاء مفاتيح التشفير، وحمايتها، وأرشفتها، واستعادتها، وإتلافها.
4.1.5	المستوى الثالث	قياس ومراجعة وتحسين [متطلبات التشفير] وكذلك فاعلية الإجراءات ذات الصلة بشكل مستمر.
المراجع	ISO 27002 - 10.1.1 ISO 27002 - 10.1.2 SANS v7.0 - 16.4 SANS v7.0 - 18.5 NIST.sp.800-53r4 - SC-12 NIST.sp.800-53r4 - SC-13 NCA ECC - 2-8-1	

		NCA ECC - 2-8-2 NCA ECC - 2-8-3 NCA ECC - 2-8-4 NCA CSCC -2-8-3
4.2	إدارة التغيير	
الضوابط		
4.2.1	المستوى الأول	تحديد وتوثيق [متطلبات إدارة التغيير] مع مراعاة ما يلي: • تحديد التغييرات على الأصول المعلوماتية التي تؤثر على الأمن السيبراني وتصنيفها وتحديد أولوياتها.
4.2.2	المستوى الأول	تحديد وتنفيذ {عملية إدارة التغيير} للتصريح بالتغييرات ذات الصلة بالأمن السيبراني (على سبيل المثال: تطبيق حزم التحديثات والإصلاحات، أو تغييرات الإعدادات كجزء من المعالجة، أو ترقية الأنظمة، أو استخدام معدات جديدة).
4.2.3	المستوى الأول	التخطيط للتغييرات المحددة واختبارها وتقييم الأثر المحتمل [تقييم مخاطر الأمن السيبراني] للتغييرات على الأمن السيبراني، والإبلاغ عن التغييرات، والحصول على موافقة المسؤولين (العاملين/اللجنة).
4.2.4	المستوى الثاني	تحسين وتنفيذ [متطلبات إدارة التغيير] لمراعاة الإجراءات الخاصة بالتغيير في حالات الطوارئ.
4.2.5	المستوى الثالث	قياس ومراجعة وتحسين [متطلبات إدارة التغيير] وكذلك فاعلية الإجراءات ذات الصلة بشكل مستمر.
المراجع		ISO 27002 - 12.1.2 NCA ECC - 1-6-2 NCA CSCC -1-6-2
4.3	إدارة الثغرات	
الضوابط		
4.3.1	المستوى الأول	تحديد وتوثيق [متطلبات إدارة الثغرات] مع مراعاة ما يلي: • النطاق، والأدوات، والتقنية، ورفع التقارير. • معدل تكرار عمليات الفحص. • الأطر الزمنية لعلاج الثغرات بناءً على مستوى خطورتها.
4.3.2	المستوى الأول	تحديد وتنفيذ {عملية إدارة الثغرات} التي تتكون من: • الفحص: إجراء عمليات فحص واكتشاف الثغرات في الأصول المعلوماتية [قائمة جرد الأصول] باستخدام الأدوات الملائمة وفقاً لمعدل التكرار المحدد في المتطلبات (على سبيل المثال: الفحص شهرياً للأنظمة الحساسة). • التحليل: تحليل أثر وجود ثغرات على الأصول المعلوماتية الحساسة وتحديد مستوى خطورتها وتحديد وتعيين الأطر الزمنية (اعتماداً على

		مستوى خطورتها) التي يجب في غضونها معالجة الثغرات. • رفع التقارير: رفع تقارير بالثغرات [تقرير الثغرات] بالإضافة إلى مستوى حساسية الأصول إلى الإدارات المعنية وتحديد الإجراء الموصى به. [إدارة حزم التحديثات والإصلاحات].
4.3.3	المستوى الثاني	إجراء عمليات فحص واكتشاف الثغرات الناجمة عن أحداث محددة (على سبيل المثال: إصدار منتج، وتغيير تقني جوهري، وإضافة معدات جديدة إلى الشبكات).
4.3.4	المستوى الثاني	استخدام أدوات الفحص المتخصصة والمؤتمتة (على سبيل المثال: الأدوات المخصصة لخوادم الويب وتطبيقات الأجهزة المحمولة).
4.3.5	المستوى الثالث	تحسين تصنيف الثغرات وإعداد التقارير بناءً على المدخلات الواردة من مصادر أخرى (على سبيل المثال: اختبار الاختراق، والمعلومات الاستباقية).
4.3.6	المستوى الثالث	قياس ومراجعة وتحسين [متطلبات إدارة الثغرات] وكذلك فاعلية الإجراءات ذات الصلة بشكل مستمر.
المراجع		ISO 27002 - 12.6 SANS v7 - 3 SANS v6.1 - 4.1 SANS v6.1 - 4.8 NIST.sp.800-53r4 - RA-5 NIST.sp.800-53r4 - CA-8 NCA ECC - 2-10-1 NCA ECC - 2-10-2 NCA ECC - 2-10-3 NCA ECC - 2-10-4 NCA CSCC - 2-9-2 NCA CSCC - 2-10-1 NCA CSCC - 2-10-2 NCA CSCC - 2-10-3
4.4	إدارة حزم التحديثات والإصلاحات	
الضوابط		
4.4.1	المستوى الأول	تحديد وتوثيق [متطلبات إدارة حزم التحديثات والإصلاحات] مع مراعاة ما يلي: • نطاق إدارة حزم التحديثات والإصلاحات. • الأدوات والتقنيات ومحفزات إدارة حزم التحديثات والإصلاحات. • بيئة اختبار حزم التحديثات والإصلاحات. • معدل التكرار (يتضمن حزم التحديثات والإصلاحات الدورية).
4.4.2	المست	تحديد وتنفيذ {عملية إدارة حزم التحديثات والإصلاحات} التي تساهم في

	وى الأول	وضع [خطة المعالجة] مع مراعاة الجوانب التالية: • [تقرير الثغرات]. • [تقييم مخاطر الأمن السيبراني]. • اختبار حزم التحديثات والإصلاحات قبل تطبيقها على بيئة الإنتاج وإنشاء النسخ الاحتياطية اللازمة بناءً على نتائج تقييم المخاطر. • [إدارة التغيير]. • إصدارات حزم التحديثات والإصلاحات الدورية.
4.4.3	المستوى الثاني	التأكد من تثبيت حزم التحديثات والإصلاحات بنجاح ومعالجتها للثغرات التي تم اكتشافها.
4.4.4	المستوى الثاني	تحسين وتنفيذ [متطلبات إدارة حزم التحديثات والإصلاحات] لتشمل أنشطة تثبيت حزم التحديثات والإصلاحات في الحالات الطارئة للثغرات عالية الخطورة.
4.4.5	المستوى الثاني	تطبيق حزم التحديثات والإصلاحات (أو تحديثات البرمجيات) بصفة منتظمة على جميع الأصول المعلوماتية.
4.4.6	المستوى الثاني	أتمتة إدارة حزم التحديثات والإصلاحات وتطبيقها كلما أمكن ذلك (على سبيل المثال: أجهزة المستخدمين).
4.4.7	المستوى الثاني	تحسين [خطة المعالجة] وتنفيذها بناءً على المدخلات من مصادر مختلفة على سبيل المثال المعلومات الاستباقية و[اختبار الاختراق]، وغيرها من المصادر.
4.4.8	المستوى الثالث	قياس ومراجعة وتحسين [متطلبات إدارة حزم التحديثات والإصلاحات] وكذلك فاعلية الإجراءات ذات الصلة بشكل مستمر.
المراجع		SANS v6.1 - 4.4 SANS v6.1 - 4.5 SANS v6.1 - 4.7 SANS v7.0 - 3.7 NCA ECC - 2-3-3-3 NCA ECC - 2-10-3-4 NCA CSCC - 2-3-1 NCA CSCC - 2-9-1
4.5	أمن الشبكات	
الضوابط		
4.5.1	المستوى الأول	تحديد وتوثيق [متطلبات أمن الشبكات] مع مراعاة ما يلي: • إدارة ومراقبة أمن الشبكات التي تديرها الجهة والأصول المعلوماتية المرتبطة بها. • فصل الشبكات.

		• متطلبات الأمن لحماية خدمات الشبكة والمعلومات المنقولة من خلالها.
4.5.2	المستوى الأول	توثيق [مخطط الشبكات] التي تعكس بوضوح الحالة الفعلية للشبكات (على سبيل المثال: جميع الاتصالات في الشبكات، وأجهزة الشبكة، والخوادم الحساسة).
4.5.3	المستوى الأول	ضمان التحكم في حركة مرور البيانات الواردة والصادرة (على سبيل المثال: منع حركة البيانات الخبيثة، ومراقبة أحمال المحولات الشبكية، والتحكم في الاتصالات غير المرغوب فيها، على سبيل المثال: البريد الإلكتروني والرسائل القصيرة) بناءً على [متطلبات أمن الشبكات].
4.5.4	المستوى الأول	ضمان السماح للبروتوكولات ونطاقات عناوين IP الموثوقة والمصرح لها فقط بعبور الشبكة (على سبيل المثال: استخدام جدران الحماية) وتعطيل البروتوكولات غير المستخدمة (على سبيل المثال: تعطيل IPv6 إذا لم يكن مستخدماً) في الأجهزة لتقليل احتمالية الهجوم على الشبكة.
4.5.5	المستوى الأول	حماية المعلومات أثناء نقلها من خلال شبكة الجهة (على سبيل المثال: من الاعتراض والنسخ والتعديل) والتأكد من الحفاظ على سرية وسلامة المعلومات (على سبيل المثال: من خلال التشفير).
4.5.6	المستوى الأول	فصل وتقسيم الشبكة إلى مناطق (على سبيل المثال: نطاقات وشبكات فرعية) بناءً على أهمية الأصول المعلوماتية أو الخدمات الموجودة في تلك المناطق (على سبيل المثال: عزل شبكة الإنتاج عن شبكات التطوير والاختبار، وفصل الشبكة التي تحتوي على أجهزة المستخدمين عن خوادم التحقق).
4.5.7	المستوى الأول	التحكم في الدخول إلى شبكة الجهة (الشبكات السلكية واللاسلكية على حد سواء) بناءً على قائمة التحكم في الدخول [إدارة هويات الدخول والصلاحيات].
4.5.8	المستوى الأول	تأمين بيانات العملاء ومعلومات الاتصالات الصوتية والإشارات المنقولة عبر شبكة الاتصالات الخاصة بالجهة (على سبيل المثال: VOIP، وSIP، وSS7، وبروتوكولات الاتصالات ونقل الإشارات).
4.5.9	المستوى الأول	فصل شبكة العملاء المُستضافة عن الشبكة التشغيلية لاتصالات الجهة.
4.5.10	المستوى الثاني	ضمان التعاون مع الجهات التي تمتلك أو تشغل شبكات اتصالات مترابطة مع شبكة الجهة لكشف ومنع الأضرار على الشبكة والمستخدمين (على سبيل المثال: حظر الرسائل الاقتحامية SPAM، وهجمات تعطيل الخدمات الموزّعة DDoS، وأنماط حركات البيانات غير الطبيعية، ومصادقة هوية المتصل لتعطيل الهويات الغير قانونية).
4.5.11	المستوى الثاني	ضمان أن الواجهات (على سبيل المثال: Internet Exchange Points) للشبكات الأخرى محمية بشكل مناسب (على سبيل المثال: تأمين البنية التحتية لـ BGP، وتنفيذ التوافر العالي من خلال المنصات البديلة

		Redundancy، استخدام تشفير قوي).
4.5.12	المستوى الثاني	تحسين وتنفيذ [متطلبات أمن الشبكات] للتعامل مع الهجمات الداخلية والخارجية (على سبيل المثال: هجمات تعطيل الخدمات DoS/هجمات تعطيل الخدمات الموزعة DDoS) ضد شبكة الجهة.
4.5.13	المستوى الثاني	ضمان توفر آليات في مرافق الجهة لاكتشاف ومعالجة التحميل الزائد على الشبكة والذي يؤدي إلى انقطاع الخدمات (على سبيل المثال: إنشاء مرافق إضافية لتحقيق التوازن في أحمال الاستخدام بالشبكة).
4.5.14	المستوى الثاني	استخدام أدوات محددة لتحليل وتصفية جميع حركات البيانات (على سبيل المثال: تصفية المنافذ ports، التصفية القائمة على الاستضافة host based filtering) لاكتشاف أي حركة مرور للبيانات غير مصرح بها في الشبكة.
4.5.15	المستوى الثالث	قياس ومراجعة وتحسين [متطلبات أمن الشبكات] وكذلك فاعلية الإجراءات ذات الصلة بشكل مستمر.
المراجع		ISO 27002 - 13.1.1 ISO 27002 - 13.1.3 ISO 27002 - 13.2.1 ISO 27011 - X.1051 - TEL.11.3.3 ISO 27011 - X.1051 - TEL.13.1.3 ISO 27011 - X.1051 - TEL.13.1.4 ISO 27011 - X.1051 - TEL.13.1.5 ISO 27011 - X.1051 - TEL.13.1.6 SANS v7.0 - 9.4 SANS v7.0 - 12.3 SANS v7.0 - 12.4 SANS v7.0 - 12.6 SANS v7.0 - 12.7 NCA ECC - 2-5-1 NCA ECC - 2-5-2 NCA ECC - 2-5-3 NCA ECC - 2-5-4 NCA ECC - 2-5-3-6 NCA CSCC - 2-5-3 NCA CSCC - 2-4-1
4.6	سجل الأحداث والمراقبة	
الضوابط		
4.6.1	المستوى الأول	تحديد وتوثيق [متطلبات سجل الأحداث والمراقبة] مع مراعاة ما يلي: • تسجيل الأحداث (على سبيل المثال: محاولات تسجيل الدخول، تغييرات الإعدادات، سجلات جدار الحماية) المتعلقة بالأصول المعلوماتية التي

		تملكها الجهة. • مراقبة سجلات الأحداث وتحليل الأحداث المكتشفة. • مدة الاحتفاظ المطلوبة وحماية سجلات الأحداث.
4.6.2	المستوى الأول	تفعيل تسجيل الأحداث (على سبيل المثال: أنشطة المستخدم، والاستثناءات، وأحداث الأمن السيبراني، والعمليات الحساسة) المتعلقة بالأصول المعلوماتية.
4.6.3	المستوى الأول	حماية معلومات السجلات ومرافق التسجيل من الوصول غير المصرح به والتلاعب بها.
4.6.4	المستوى الأول	المراجعة الدورية لسجلات الأحداث والإبلاغ عن الأحداث المشبوهة والكشف عن الأمور غير الطبيعية للمسؤولين [إدارة الحوادث].
4.6.5	المستوى الأول	الاحتفاظ بالسجلات لفترة زمنية محددة على النحو المحدد في [متطلبات سجل الأحداث والمراقبة] (على سبيل المثال: 12 شهراً).
4.6.6	المستوى الثاني	جمع الأحداث ومراقبتها وتحليلها باستخدام أداة إدارة السجلات (على سبيل المثال: نظام إدارة سجلات الأحداث ومراقبة الأمن السيبراني SIEM) التي تحتوي على قدرات كشف وتكامل متقدمة.
4.6.7	المستوى الثاني	المراقبة الآنية ومراجعة سجلات الأحداث للأصول المعلوماتية الهامة.
4.6.8	المستوى الثاني	تحسين طرق كشف الأحداث من خلال استخدام أدوات مخصصة (على سبيل المثال: منصات المعلومات الاستباقية) لتحديث قواعد الاكتشاف الخاصة بأدوات إدارة السجل.
4.6.9	المستوى الثالث	قياس ومراجعة وتحسين [متطلبات سجل الأحداث والمراقبة].
المراجع		ISO 27002 - 12.4.1 ISO 27002 - 12.4.2 SANS v7.0 - 6.6 NIST CSWP - DE.AE-4 NIST CSWP - DE.DP-5 NCA ECC - 2-12-1 NCA ECC - 2-12-2 NCA ECC - 2-12-3 NCA ECC - 2-12-4 NCA CSCC - 2-12-3 NCA CSCC - 2-11-1 NCA CSCC - 2-11-2

	NCA CSCC - 2-12-1	
4.7	إدارة هويات الدخول والصلاحيات	
الضوابط		
4.7.1	المستوى الأول	تحديد وتوثيق [متطلبات إدارة هويات الدخول والصلاحيات] مع مراعاة ما يلي: • حسابات المستخدم، والحسابات ذات الصلاحيات الهامة، ومنح وإلغاء صلاحيات الدخول. • متطلبات التحقق من هوية المستخدم وصلاحياته (على سبيل المثال: في حالة الدخول عن بُعد، التحقق الثنائي من الهوية). • متطلبات إدارة كلمات المرور.
4.7.2	المستوى الأول	تحديد وتنفيذ {عملية تعيين/إلغاء صلاحيات المستخدم} مع مراعاة الآتي: • تعيين صلاحيات الوصول للمستخدمين بناءً على ما يصرح لهم باستخدامه (على سبيل المثال: التحكم بالوصول بناءً على الدور الوظيفي). • إعادة تعيين صلاحيات دخول المستخدمين في حالة تغير وظائف العمل (على سبيل المثال: تغيير الإدارات). • إدارة التحقق من هوية المستخدم وصلاحياته بناءً على مبادئ التحكم بالوصول (على سبيل المثال: مبدأ الحاجة إلى المعرفة، والحاجة إلى الاستخدام، ومبدأ الحد الأدنى من الصلاحيات والامتيازات، ومبدأ فصل المهام) والتأكد من تحديث [قائمة التحكم بالدخول]. • إلغاء صلاحيات الدخول إلى أنظمة المعلومات عند انتفاء الحاجة لذلك (على سبيل المثال: إنهاء العمل مع الجهة).
4.7.3	المستوى الأول	مراقبة وتقييد تعيين واستخدام الصلاحيات الهامة والحساسة.
4.7.4	المستوى الأول	توفير التحقق من الهوية متعدد العناصر للدخول إلى أنظمة المعلومات الحساسة وكذلك للدخول عن بعد.
4.7.5	المستوى الأول	إنفاذ متطلبات إدارة كلمات المرور (على سبيل المثال: استخدام كلمات مرور قوية، والتغيير المنتظم لكلمة المرور، وتعليق الحساب بعد محاولات تسجيل دخول فاشلة متعددة) وحماية معلومات التحقق من هوية المستخدم من الوصول غير المصرح به (على سبيل المثال: استخدام آليات تشفير أثناء نقل معلومات التحقق).
4.7.6	المستوى الثاني	المراجعة المنتظمة لهوية المستخدم وصلاحية الدخول (يراعي معدل تكرار المراجعة، على سبيل المثال: أنواع الحسابات المختلفة، وأهمية الأصول المعلوماتية)، والتأكد من مطابقتها لمبادئ التحكم بالدخول (على سبيل المثال: يجب على مالك الأصول مراجعة صلاحيات دخول المستخدم بانتظام).
4.7.7	المست	تحسين وتنفيذ [متطلبات إدارة هويات الدخول والصلاحيات] باستخدام

	وى الثاني	أدوات لأتمتة وإدارة هويات الدخول والصلاحيات بشكل مركزي.
4.7.8	المستوى الثاني	استخدام أنظمة مخصصة للمهام التي تتطلب صلاحيات مسؤول النظام (على سبيل المثال: إعدادات الأنظمة الحساسة).
4.7.9	المستوى الثالث	قياس ومراجعة وتحسين [متطلبات إدارة هويات الدخول والصلاحيات] وكذلك فاعلية الإجراءات ذات الصلة بشكل مستمر.
المراجع		ISO 27002 - 9.1.2 ISO 27002 - 9.2.1 ISO 27002 - 9.2.2 ISO 27002 - 9.2.3 ISO 27002 – 9.2.5 ISO 27002 - 9.2.6 ISO 27002 - 9.4.3 SANS v7.0 - 4.6 NCA ECC - 2-2-1 NCA ECC - 2-2-2 NCA ECC - 2-2-3 NCA ECC - 2-2-4 NCA CSCC - 2-2-1 NCA CSCC - 2-2-2 NCA CSCC - 2-2-3

4.8	السماح بقائمة محددة من التطبيقات (القائمة البيضاء للتطبيقات)	
الضوابط		
4.8.1	المستوى الأول	تحديد وتوثيق [متطلبات القائمة البيضاء للتطبيقات] مع مراعاة ما يلي: • قائمة بالبرمجيات المصرح بها. • اعتماد أدوات القائمة البيضاء للتطبيقات.
4.8.2	المستوى الأول	إعداد ونشر [فهرس البرمجيات المعتمدة] بما في ذلك تطبيقات البرمجيات ومكتبات البرمجيات (على سبيل المثال: *.dll، و*.ocx، و*.so) والبرامج النصية الموقعة رقمياً (على سبيل المثال: *.ps1، و*.py، و macros).
4.8.3	المستوى الأول	مراجعة وتحديث [فهرس البرمجيات المعتمدة] بصفة دورية.
4.8.4	المستوى الثاني	استخدام أدوات القائمة البيضاء للتطبيقات لضمان صلاحية الوصول إلى جميع الأصول المعلوماتية على البرمجيات المصرح بها والتأكد من عدم إمكانية تعطيل أو تجاوز أدوات القائمة البيضاء للتطبيقات.

4.8.5	المستوى الثالث	قياس ومراجعة وتحسين [متطلبات القائمة البيضاء للتطبيقات].
المراجع		SANS v6.1 - 2.2 SANS v7.0 - 2.6 SANS v7.0 - 2.7 SANS v7.0 - 2.8 SANS v7.0 - 2.9 NCA CSCC - 2-3-1-1
4.9	إدارة الحوادث	
الضوابط		
4.9.1	المستوى الأول	تحديد وتوثيق [متطلبات إدارة الحوادث] مع مراعاة ما يلي: • تعريف الحادثة، وتحديدها، وتصنيفها، وتحديد أولوياتها، وطرق الاستجابة لها. • هيكلية الإبلاغ عن الحوادث. • اختبار عملية الاستجابة للحوادث. • جمع الأدلة. • الدروس المستفادة من حوادث الأمن السيبراني.
4.9.2	المستوى الأول	تحديد وتنفيذ {عملية الاستجابة للحوادث} مع مراعاة ما يلي: • الكشف عن الحوادث من خلال تحليل الأحداث المبلغ عنها [سجل الأحداث والمراقبة]. • تصنيف الحوادث بناءً على معايير محددة مسبقاً كما هو محدد في المتطلبات. • الاستجابة لحوادث الأمن السيبراني (احتوائها، ومعالجتها ، والتعافي منها) ضمن الأطر الزمنية المحددة للجهة [إدارة التغيير]. • إعداد [تقرير الحوادث] والدروس المستفادة. • الإبلاغ عن حوادث الأمن السيبراني وتفاصيلها للهيئة.
4.9.3	المستوى الأول	إجراء تدريبات منتظمة لاختبار {عملية الاستجابة للحوادث} للتأكد من فعاليتها (على سبيل المثال: اختبار قنوات الاتصال ومدة الاستجابة).
4.9.4	المستوى الثاني	تحسين وتنفيذ [متطلبات إدارة الحوادث] باستخدام أدوات إدارة الحوادث لأتمتة العملية والربط مع الأنظمة الأخرى ذات الصلة لزيادة الكفاءة.
4.9.5	المستوى الثاني	جمع المعلومات الاستباقية واستخدامها خلال تحليل أحداث الأمن السيبراني.
4.9.6	المستوى الثاني	تشكيل فريق التحليل الجنائي الرقمي للتحقيق في حوادث الأمن السيبراني.

4.9.7	المستوى الثاني	تحديد وجمع الأدلة المتعلقة بحوادث الأمن السيبراني، والاحتفاظ بها، وكذلك الدروس المستفادة من حوادث الأمن السيبراني لتقليل احتمالية وآثار وقوع حوادث أمن سيبراني مستقبلية.
4.9.8	المستوى الثالث	قياس ومراجعة وتحسين [متطلبات إدارة الحوادث] وكذلك فاعلية الإجراءات ذات الصلة بشكل مستمر.
المراجع		ISO 27002 - 16.1 ISO 27002 - 16.1.2 ISO 27002 - 16.1.3 ISO 27002 - 16.1.4 ISO 27002 - 16.1.6 ISO 27002 - 16.1.7 NIST.sp.800-53r4 - IR-1 NIST.sp.800-53r4 - IR-2 NIST.sp.800-53r4 - IR-3 NIST.sp.800-53r4 - IR-4 NIST.sp.800-53r4 - IR-6 NIST CSWP RS.AN-3 NCA ECC - 2-13-1 NCA ECC - 2-13-2 NCA ECC - 2-13-3 NCA ECC - 2-13-4
4.10	التعامل مع البرمجيات الضارة	
الضوابط		
4.10.1	المستوى الأول	تحديد وتوثيق [متطلبات التعامل مع البرمجيات الضارة] مع مراعاة ما يلي: • ضوابط الكشف والوقاية للحماية من البرمجيات الضارة. • تنفيذ الضوابط التقنية لحماية الأصول المعلوماتية للجهة.
4.10.2	المستوى الأول	استخدام أدوات حماية نقطة النهاية على الأجهزة وضمان التحديث لقاعدة بيانات المعرفة المسبقة بانتظام واتخاذ تدابير أمنية لمنع تعطيل هذا البرنامج أو تعديله من قبل المستخدمين.
4.10.3	المستوى الأول	اتخاذ تدابير أمنية مناسبة لحظر مصادر مختلفة من حركات البيانات الخبيثة (على سبيل المثال: استخدام أدوات تحليل وتصفية الإنترنت وأدوات تصفية رسائل البريد الإلكتروني لحظر رسائل التصيد وتقييد عملية تنزيل محتوى خطر) [حماية البريد الإلكتروني ومتصفح الويب].
4.10.4	المستوى الأول	اتخاذ تدابير وقائية لحماية الوسائط المتنقلة من البرمجيات الضارة (على سبيل المثال: إجراء فحص لمكافحة البرمجيات الضارة للوسائط المتنقلة عند إدخالها أو توصيلها).
4.10.5	المستوى	تطبيق تقنيات متقدمة للكشف عن البرمجيات الضارة (على سبيل المثال:

	وى الثاني	تفعيل تسجيل الاستعلام عن نظام أسماء النطاقات DNS لاكتشاف عمليات البحث عن اسم المضيف للنطاقات الضارة المعروفة).
4.10.6	المست وى الثاني	استخدام أدوات سجل الأحداث والمراقبة المتقدمة لتحليل أحداث البرمجيات الضارة التي تم اكتشافها والتحذير منها [سجل الأحداث والمراقبة].
4.10.7	المست وى الثالث	مراجعة وتحسين [متطلبات التعامل مع البرمجيات الضارة] بشكل مستمر.
المراجع		NIST.sp.800-53r4 - SI-3 SANS v7.0 - 7.9 SANS v7.0 - 8.1 SANS v7.0 - 8.2 SANS v7.0 - 8.4 SANS v7.0 - 8.6 SANS v7.0 - 8.7 NCA ECC - 2-4-3 NCA ECC - 2-5-3 NCA CSCC - 2-5-3
4.11	حماية المعلومات	
الضوابط		
4.11.1	المست وى الأول	تحديد وتوثيق [متطلبات حماية المعلومات] مع مراعاة ما يلي: • مستوى ومعايير التصنيف (على سبيل المثال: مقيدة، سرية، عامة) {عملية تصنيف الأصول}. • خصوصية المعلومات، وملكيتها، وحمايتها، ونقلها والاحتفاظ بها. • ضمان خصوصية المعلومات الشخصية أو غيرها من المعلومات الحساسة في الجهة [الالتزام بالأمن السيبراني].
4.11.2	المست وى الأول	تحديد وتنفيذ {عملية تصنيف المعلومات} مع مراعاة: • تصنيف المعلومات بناءً على معايير التصنيف المحددة في المتطلبات. • التعامل مع المعلومات الحساسة وفقاً للمعايير المحددة (على سبيل المثال: القيمة التجارية، والمتطلبات القانونية والتقنية والوطنية والدولية).
4.11.3	المست وى الأول	تنفيذ آليات أمنية لحماية المعلومات (أثناء النقل، والتخزين، والاستخدام) مع الأخذ في الاعتبار [متطلبات التشفير] وتقنيات منع فقدان البيانات.
4.11.4	المست وى الأول	منع نقل المعلومات من بيئة الإنتاج إلى بيئة أخرى واستخدام بيانات الأنظمة الحساسة في بيئات الاختبار والتطوير.
4.11.5	المست	تحديد مدة الاحتفاظ بالمعلومات وفقاً للمتطلبات التنظيمية

	وى الثاني	والتشريعات ذات الصلة وحصر الاحتفاظ بالمعلومات اللازمة على الأنظمة الحساسة للمتطلبات الضرورية. [الالتزام بالأمن السيبراني]
4.11.6	المستوى الثالث	قياس ومراجعة وتحسين [متطلبات حماية المعلومات] وكذلك فاعلية الإجراءات ذات الصلة بشكل مستمر.
المراجع		ISO 27002 - 8.2.1 SANS v6.1 - 13.3 NCA ECC - 2-7-1 NCA ECC - 2-7-2 NCA ECC - 2-7-3 NCA ECC - 2-7-4 NCA CSCC - 2-6-1 NCA CSCC - 2-7-3
4.12	إدارة النسخ الاحتياطي والاستعادة	
الضوابط		
4.12.1	المستوى الأول	تحديد وتوثيق [متطلبات إدارة النسخ الاحتياطي والاستعادة] مع مراعاة ما يلي: • نطاق النسخ الاحتياطي المتصل وغير المتصل بما فيه مدة الاحتفاظ. • مدة استعادة المعلومات بعد حوادث الأمن السيبراني. • النسخ الاحتياطي الدوري للأصول المعلوماتية. • حماية النسخ الاحتياطية. • توافر النسخ الاحتياطية.
4.12.2	المستوى الأول	تحديد وتنفيذ {عملية النسخ الاحتياطي} مع مراعاة ما يلي: • متطلبات العمل (على سبيل المثال: نقطة الاستعادة المستهدفة). • نطاق النسخ الاحتياطية المتصلة وغير المتصلة وشمولها للأصول المعلوماتية (على سبيل المثال: عمليات النسخ الاحتياطي للنظام كاملاً).
4.12.3	المستوى الأول	تحديد وتنفيذ {عملية الاستعادة} لضمان استعادة الأصول المعلوماتية ضمن مدة زمنية مقبولة بناءً على أهميتها المحددة في {تصنيف الأصول}.
4.12.4	المستوى الأول	ضمان سرية النسخ الاحتياطية، وسلامتها، وتوافرها في الأوضاع المضادة (على سبيل المثال: استخدام التشفير، وحماية النسخ الاحتياطية عن طريق الأمن المادي) [حماية الأصول المعلوماتية المادية].
4.12.5	المستوى الثاني	إنشاء موقع تخزين/نسخ احتياطي بديل يوفر تدابير أمنية مكافئة للموقع الأساسي.
4.12.6	المستوى الثاني	اختبار ومراجعة {عمليات النسخ الاحتياطي} و{الاستعادة} للتحقق من فعاليتها بشكل مستمر.

4.12.7	المستوى الثاني	تحسين وتنفيذ [متطلبات إدارة النسخ الاحتياطي والاستعادة] باستخدام أدوات لأتمتة عمليات {النسخ الاحتياطي} و{الاستعادة}.
4.12.8	المستوى الثالث	قياس ومراجعة وتحسين [متطلبات إدارة النسخ الاحتياطي والاستعادة] وكذلك فاعلية الإجراءات ذات الصلة بشكل مستمر.
المراجع		ISO 27002 - 12.3.1 NIST.sp.800-53r4 - CP-6 NIST.sp.800-53r4 - CP-9 NCA ECC - 2-9-1 NCA ECC - 2-9-2 NCA ECC - 2-9-3 NCA CSCC - 2-8-1 NCA CSCC - 2-9-3
4.13	إدارة الإعدادات والتحصين	
الضوابط		
4.13.1	المستوى الأول	تحديد وتوثيق [متطلبات إدارة الإعدادات والتحصين] مع مراعاة ما يلي: • تأمين النسخ والإعدادات الأساسية للأصول المعلوماتية والبرمجيات/الأجهزة.
4.13.2	المستوى الأول	تطبيق ضبط الإعدادات الأساسية المحددة للأصول المعلوماتية.
4.13.3	المستوى الأول	استخدام تحصين الأنظمة والأجهزة وفقاً لأفضل الممارسات المعترف بها في الصناعة (على سبيل المثال: تعطيل الإعدادات الافتراضية التي تم تثبيتها على أجهزة الشبكة).
4.13.4	المستوى الأول	تقييد استخدام الوظائف غير الضرورية (على سبيل المثال: استخدام المنافذ والخدمات غير المصرح بها) وتهيئة الأصول المعلوماتية لتوفير القدرات الأساسية فقط.
4.13.5	المستوى الأول	مراقبة ضبط الإعدادات والتحقق منها مقارنة بالإعدادات الأساسية.
4.13.6	المستوى الثاني	استخدام أداة مخصصة لمراقبة ضبط الإعدادات والتحقق منها والتنبيه عند التعديل غير المصرح به عن الإعدادات الأساسية.
4.13.7	المستوى الثاني	استخدام أدوات مخصصة قادرة على ضبط/تهيئة الإعدادات آلياً [إدارة التغيير] على جميع الأصول المعلوماتية.
4.13.8	المست	قياس ومراجعة وتحسين [متطلبات إدارة الإعدادات والتحصين] بشكل

	وى الثالث	مستمر.
المراجع	NIST.sp.800-53r4 - CM-6 NIST.sp.800-53r4 - CM-7 SANS v6.1 - 3.1 SANS v7.0 - 5.4 SANS v7.0 - 5.5 SANS v7.0 - 11.3 NCA ECC 1-6-2-2 NCA ECC 1-6-3-5 NCA ECC 2-5-3-5	
4.14	تطوير البرمجيات الآمنة	
الضوابط		
4.14.1	المستوى الأول	تحديد وتوثيق [متطلبات تطوير البرمجيات الآمنة] مع مراعاة ما يلي: • استخدام المعايير الأمنية لتطوير البرامج والتطبيقات (على سبيل المثال: المكتبات المعتمدة للبرمجيات، واجهات برمجة التطبيقات). • الفصل بين صلاحيات الوصول وتخصيصها إلى بيئات مختلفة. • إجراء اختبارات للتحقق من امتثال البرنامج المطور لمتطلبات الأمن السيبراني للجهة.
4.14.2	المستوى الأول	التأكد من حصر الوصول إلى البيئة المناسبة على العاملين المصرح لهم [إدارة هويات الدخول والصلاحيات].
4.14.3	المستوى الأول	استخدام المعايير والممارسات الأمنية لشفرة البرمجيات والتطبيقات (على سبيل المثال: مبادئ الأمن حسب التصميم المدعومة بأدوات التحليل الثابتة أو الديناميكية) وضمان التكامل الآمن بين التطبيقات.
4.14.4	المستوى الأول	ضمان النقل الآمن والموثوق للبرمجيات بين البيئات.
4.14.5	المستوى الأول	استخدام مكونات الأطراف الخارجية الموثوقة والحديثة للبرمجيات المطورة داخلياً.
4.14.6	المستوى الثاني	إجراء وتوثيق مراجعة أمنية للبرمجيات المطورة والشفرة المصدرية (على سبيل المثال: إجراء فحص الأخطاء لجميع مدخلات البرمجيات والتطبيقات المطورة).
4.14.7	المستوى الثاني	إجراء اختبارات أمنية للتحقق من مدى امتثال البرمجيات المطورة لمتطلبات الأمن السيبراني للجهة.
4.14.8	المستوى	قياس ومراجعة وتحسين [متطلبات تطوير البرمجيات الآمنة] بشكل مستمر.

	الثالث	
المراجع		ISO 27002 - 14.2.1 SANS v7.0 - 18.1 SANS v7.0 - 18.9 SANS v7.0 - 18.3 SANS v7.0 - 18.2 NIST.sp.800-53-r4 SA-15-b NCA ECC - 1-6-3 NCA CSCC - 1-3-2 NCA CSCC -1-6-3
4.15	حماية البريد الإلكتروني ومتصفح الويب	
الضوابط		
4.15.1	المستوى الأول	تحديد وتوثيق [متطلبات حماية البريد الإلكتروني ومتصفح الويب] مع مراعاة ما يلي: • استخدام آليات أمنية موحدة لحماية البريد الإلكتروني ومتصفح الويب.
4.15.2	المستوى الأول	تنفيذ [متطلبات حماية البريد الإلكتروني ومتصفح الويب] (على سبيل المثال: تحليل البريد الإلكتروني وتصفيته للحماية من الرسائل الاقتحامية ورسائل التصيد، والتحقق من الهوية متعدد العناصر، والنسخ الاحتياطي لرسائل البريد الإلكتروني وأرشفتها، والحماية من التهديدات المتقدمة المستمرة، ومواقع الويب غير الموثوق بها).
4.15.3	المستوى الأول	تقييد الوصول إلى خدمات مواقع البريد الإلكتروني غير المصرح بها على شبكة الإنترنت (على سبيل المثال: إعدادات جدار الحماية وأدوات تصفية عناوين URL).
4.15.4	المستوى الثالث	قياس ومراجعة وتحسين [متطلبات حماية البريد الإلكتروني ومتصفح الويب] بشكل مستمر.
المراجع		SANS v7.0 – 7 NCA ECC - 2-5-3-3 NCA ECC - 2-4-1 NCA ECC - 2-4-2 NCA ECC - 2-4-3 NCA ECC - 2-4-4
4.16	اختبار الاختراق	
الضوابط		
4.16.1	المستوى الثاني	تحديد وتوثيق [متطلبات اختبار الاختراق] مع مراعاة ما يلي: • الغرض من اختبارات الاختراق وأهدافها العامة. • تحديد معدل تكرار إجراء اختبارات الاختراق.
4.16.2	المست	تحديد {عملية اختبار الاختراق} التي تتكون من نطاق اختبارات الاختراق

	وى الثاني	باستخدام منهجيات موحدة لتحديد الثغرات غير المعروفة (على سبيل المثال: اختبار الصندوق الرمادي واختبار الصندوق الأبيض) ومعدل تكرارها (على سبيل المثال: مرة كل ثلاثة أشهر على الأقل للأصول المعلوماتية الحساسة).
4.16.3	المست وى الثاني	استخدام [تقرير الثغرات] كمدخل لتوجيه اختبارات الاختراق اعتماداً على منهجية اختبار الاختراق المستخدمة.
4.16.4	المست وى الثاني	رفع [تقرير اختبار الاختراق] إلى الأطراف المعنية للبدء في إجراءات المعالجة عند الحاجة [إدارة حزم التحديثات والإصلاحات].
4.16.5	المست وى الثالث	قياس ومراجعة وتحسين [متطلبات اختبار الاختراق] وكذلك فاعلية الإجراءات ذات الصلة بشكل مستمر.
المراجع	SANS v6.1 – 20.1 SANS v6.1 – 20.6 NCA ECC – 2-11 NCA CSCC – 2-10	

5. الأمن المادي

5.1	حماية الأصول المعلوماتية المادية	
الضوابط		
5.1.1	المستوى الأول	تحديد وتوثيق [متطلبات حماية الأصول المعلوماتية المادية] مع مراعاة ما يلي: • حماية المرافق المادية التي تحتوي على الأصول المعلوماتية. • حماية الأصول المعلوماتية المادية والمرافق المادية في مواقع العمل الخارجية. • مناطق التوصيل والتحميل. • نقل الأصول المعلوماتية. • تحديد تدابير الحماية المادية ضد التهديدات البيئية.
5.1.2	المستوى الأول	تحديد المحيط الأمني من أجل حماية المرافق المادية (على سبيل المثال: المكاتب، والغرف، ومراكز البيانات، والمحطات الأرضية، ومعدات معالجة الاتصالات) التي تحتوي على أصول معلوماتية.
5.1.3	المستوى الأول	التأكد من وجود الأصول المعلوماتية المادية داخل مناطق أمنية مناسبة وتخزينها في مرافق مادية آمنة خارج ساعات العمل.
5.1.4	المستوى الأول	تأمين مناطق التوصيل/التحميل التي يمكن استخدامها من قبل أفراد غير مصرح لهم بالدخول إلى مباني الجهة (على سبيل المثال: الفصل

		المادي، إن أمكن، للشحنات الواردة والصادرة).
5.1.5	المستوى الأول	حماية الأصول المعلوماتية المادية من التلف الناتج عن التهديدات البيئية والمخاطر والوصول المادي غير المصرح به. بالإضافة إلى ذلك، يتم مراعاة العوامل التالية: • تنفيذ تدابير الحماية ضد التهديدات والمخاطر المادية (على سبيل المثال: الحرائق، انقطاعات التيار الكهربائي، الأعطال الناجمة عن الفشل في المرافق الداعمة، الكوارث البيئية). • تأمين الكابلات من التصنت أو التداخل أو التلف بالإضافة إلى الإدارة المناسبة للكابلات (على سبيل المثال: وضع علامات على الكابلات أو ترميزها بالألوان). • تشغيل الأصول المعلوماتية المادية وفقاً للمتطلبات المحددة من الشركة المصنعة والتحكم في مناخ العمل (على سبيل المثال: درجة الحرارة والرطوبة وجودة الهواء والمياه والضوء). • الحماية من الوصول غير المصرح به (على سبيل المثال: المراقبة من خلال الدوائر التلفزيونية المغلقة، أنظمة الإنذار، وأجهزة استشعار الحركة).
5.1.6	المستوى الأول	حماية الأصول المعلوماتية المادية أثناء نقلها مع الأخذ في الاعتبار (على سبيل المثال: المخاطر المتوقعة، والتأمين أثناء النقل).
5.1.7	المستوى الثالث	قياس ومراجعة وتحسين [متطلبات حماية الأصول المعلوماتية المادية] بشكل مستمر.
المراجع		ISO 27002 - 11.1.1 ISO 27002 - 11.1.4 ISO 27002 - 11.1.6 ISO 27002 - 11.2.1 ISO 27002 - 11.2.2 ISO 27002 - 11.2.3 ISO 27002 - 11.2.8 ISO 27002 - 11.2.9 ISO 27011 - X.1051 - TEL.11.1.7 ISO 27011 - X.1051 - TEL.11.1.8 ISO 27011 - X.1051 - TEL.11.1.9 ISO 27011 - X.1051 - TEL.11.3.1 NIST.sp.800-53r4 - PE -11 NIST.sp.800-53r4 - PE -12 NIST.sp.800-53r4 - PE -13 NIST.sp.800-53r4 - PE -14 NIST.sp.800-53r4 - PE -15 NIST.sp.800-53r4 - PE -17 NCA ECC - 3-1

	NCA ECC - 2-14-1 NCA ECC - 2-14-2 NCA ECC - 2-14-3 NCA ECC - 2-14-4	
5.2	إدارة الوصول المادي	
الضوابط		
5.2.1	المستوى الأول	تحديد وتوثيق [متطلبات إدارة الوصول المادي] مع مراعاة ما يلي: • تصاريح الوصول المادي والتحكم به. • مراقبة الوصول المادي.
5.2.2	المستوى الأول	إنشاء [قائمة التحكم بالوصول المادي] للأفراد الذين لديهم حق الوصول المصرح به إلى مرافق الجهة وإصدار تصاريح الدخول المناسبة.
5.2.3	المستوى الأول	تحديد وتنفيذ [عملية إدارة الوصول المادي] لمنح صلاحية الوصول (على سبيل المثال: المفاتيح الآمنة) إلى المرافق المادية وإدارتها.
5.2.4	المستوى الأول	تطبيق ضوابط الدخول المادي للزوار (على سبيل المثال: توفير شارات أمنية للزوار ومراقبة الأنشطة المشبوهة).
5.2.5	المستوى الثاني	مراجعة [قائمة التحكم بالوصول المادي] بشكل مستمر للأفراد الذين لديهم حق الوصول المصرح به إلى المرافق وإزالتهم من القائمة عند انتفاء الحاجة.
5.2.6	المستوى الثاني	مراجعة سجلات الوصول المادي بانتظام للكشف عن أي نشاط مشبوه [سجلات الأحداث والمراقبة].
5.2.7	المستوى الثالث	قياس ومراجعة وتحسين [متطلبات إدارة الوصول المادي] وكذلك فاعلية الإجراءات ذات الصلة بشكل مستمر.
المراجع	ISO 27002 - 11.1.2 NIST.sp.800-53r4 PE-2 NIST.sp.800-53r4 PE-3 NIST.sp.800-53r4 PE-6 NIST.sp.800-53r4 PE-8 NCA ECC - 2-14	

6. الأمن السيبراني المتعلق بالأطراف الخارجية

6.1	الخدمات السحابية	
الضوابط		
6.1.1	المستوى الأول	تحديد وتوثيق [متطلبات الخدمات السحابية] مع مراعاة ما يلي: • متطلبات الأمن السيبراني المتوقعة من مقدم الخدمات السحابية. • اتفاقيات مستوى الخدمة.
6.1.2	المستوى	إجراء تقييم المخاطر وفقاً لـ [تقييم مخاطر الخدمات السحابية] و

	الأول	[حماية المعلومات] قبل اعتماد الخدمات السحابية (أو في حالة حدوث تغييرات في المتطلبات التشريعية والتنظيمية ذات الصلة) لضمان تحديد ومعالجة المخاطر المتعلقة باستخدام الخدمات السحابية بشكل مناسب.
6.1.3	المستوى الأول	تحديد [متطلبات الأمن السيبراني للخدمة السحابية] بناءً على تقييم مخاطر الخدمة السحابية و [متطلبات تصنيف الأصول] لحماية سرية بيانات الجهة وسلامتها وتوافرها.
6.1.4	المستوى الأول	إعداد اتفاقيات مستوى الخدمة مع مقدم الخدمة السحابية التي تأخذ بعين الاعتبار بحد أدنى ما يلي: • [متطلبات الأمن السيبراني للخدمة السحابية]. • الإبلاغ عن حوادث الأمن السيبراني والتزامات استعادة الخدمة. • التأكد من إمكانية إنهاء الخدمة السحابية في حالة عدم الالتزام بالاتفاقيات التعاقدية. • تحديد إجراءات إنهاء الخدمة التي تغطي الحذف الآمن للبيانات (على سبيل المثال: حذف بيانات الجهة بشكل نهائي، وإتلاف الوسائط، وإعادة بيانات الجهة بصيغة قابلة للاستخدام، والاحتفاظ بالبيانات).
6.1.5	المستوى الأول	ضمان وجود موقع استضافة وتخزين بيانات الجهة داخل المملكة العربية السعودية.
6.1.6	المستوى الثاني	تدقيق ومراجعة امتثال مقدم الخدمة السحابية للالتزامات التعاقدية ومراقبته.
6.1.7	المستوى الثالث	قياس ومراجعة وتحسين [متطلبات الخدمات السحابية] بشكل مستمر.
المراجع		ISO 27002 - 15.1 ISO 27002 - 15.2.1 NCA ECC - 4-2-1 NCA ECC - 4-2-2 NCA ECC - 4-2-3 NCA ECC - 4-2-4 NCA CSCC - 4-2-1 NCA CSCC -4-2.3 NCA CSCC -4-2-3
6.2	خدمات الإسناد الخارجي	
الضوابط		
6.2.1	المستوى الأول	تحديد وتوثيق [متطلبات خدمات الإسناد الخارجي] مع مراعاة ما يلي: • تقييم المخاطر الخاصة بإسناد الأصول المعلوماتية للأطراف الخارجية. • معالجة متطلبات الأمن السيبراني المتوقعة من مقدم الخدمة الخارجي. • اتفاقيات مستوى الخدمة.

6.2.2	المستوى الأول	إجراء تقييم المخاطر وفقاً لـ [تقييم مخاطر الأمن السيبراني] و [حماية المعلومات] قبل التعاقد على الإسناد الخارجي للأصول المعلوماتية (أو في حالة حدوث تغييرات في المتطلبات التشريعية والتنظيمية ذات الصلة) لضمان تحديد ومعالجة المخاطر المتعلقة باستخدام خدمات الإسناد بشكل مناسب.
6.2.3	المستوى الأول	تحديد [متطلبات الأمن السيبراني للأطراف الخارجية] بناءً على تقييم المخاطر التي يجب أن يلتزم بها مقدم الخدمة الخارجي لحماية سرية بيانات الجهة وسلامتها وتوافرها (على سبيل المثال: بنود عدم الإفصاح).
6.2.4	المستوى الأول	إعداد اتفاقيات مستوى الخدمة مع مقدم الخدمة الخارجي التي تأخذ بعين الاعتبار بحد أدنى ما يلي: • [متطلبات الأمن السيبراني للأطراف الخارجية]. • إجراءات الاتصال والتصعيد في حالة وقوع حادثة أمن سيبراني. • التأكد من إمكانية إنهاء خدمة الإسناد الخارجي في حالة عدم الالتزام بالاتفاقيات التعاقدية. • تحديد إجراءات إنهاء الخدمة التي تغطي الحذف الآمن للبيانات (على سبيل المثال، إتلاف الوسائط، والتشفير).
6.2.5	المستوى الثاني	تدقيق ومراجعة امتثال مقدم الخدمة الخارجي للالتزامات التعاقدية ومراقبته.
6.2.6	المستوى الثاني	التأكد من خضوع موظفي الأطراف الخارجية للمسح الأمني عند التعاقد معهم للعمل على الأنظمة الحساسة.
6.2.7	المستوى الثالث	قياس ومراجعة وتحسين [متطلبات خدمات الإسناد الخارجي] بشكل مستمر.
المراجع		ISO 27002 - 15.1 ISO 27002 - 15.2.1 NIST CSWP - ID.SC-4 NIST CSWP - ID.SC-5 NCA ECC - 4-1-1 NCA ECC - 4-1-2 NCA ECC - 4-1-3 NCA ECC - 4-1-4 NCA CSCC - 4-1-1 NCA CSCC - 4-1-2 NCA CSCC - 4-1-3 NCA CSCC - 4-1-4 NCA CSCC - 4-1-1

الأدوار والمسؤوليات

1. مقدم الخدمة غير المصنف كبنى تحتية وطنية حساسة هو المسؤول عن أمنه السيبراني.
2. تقوم الهيئة بمتابعة التزام مقدمي الخدمة غير المصنفين كبنى تحتية وطنية حساسة بالمتطلبات والضوابط (المذكوره أعلاه) من خلال طرق مختلفة -على سبيل المثال ودون حصر- الالتزام الذاتي، وعمليات التفتيش الميدانية، وورش عمل الالتزام، وعمليات التدقيق الاستباقي أو الناتج عن البلاغات.
3. تقوم الهيئة بالمراجعة والتحديث الدوري للمتطلبات والضوابط.
4. تقوم الهيئة بتحديد مستهدفات الالتزام وتحديد المواعيد المستهدفة لضمان امتثال مقدمي الخدمة غير المصنفين كبنى تحتية وطنية حساسة للمتطلبات والضوابط.
5. يقوم مقدمي الخدمة غير المصنفين كبنى تحتية وطنية حساسة بتطبيق وتنفيذ المتطلبات والضوابط وفقاً لمستهدفات الالتزام المحددة.
6. يقوم مقدمي الخدمة غير المصنفين كبنى تحتية وطنية حساسة برفع تقارير الالتزام من خلال نماذج قياس الالتزام الذاتي على سبيل المثال، أو غيرها من الوسائل المختلفة بناءً على طلب الهيئة.
7. يقوم مقدمي الخدمة غير المصنفين كبنى تحتية وطنية حساسة بتقديم المعلومات والوثائق اللازمة إلى الهيئة عند الطلب بالإضافة إلى رفع التقارير المحددة في المتطلبات والضوابط.

8. المصطلحات والتعريفات

تكون للمصطلحات الواردة أدناه المعاني الموضحة لها ما لم يقتض السياق خلاف ذلك.

التحكم بالدخول	عملية منح أو رفض طلبات محددة للحصول على المعلومات وخدمات معالجة المعلومات ذات الصلة واستخدامها وكذلك الدخول إلى منشآت ومباني محددة.
الحماية من التهديدات المتقدمة المستمرة	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.
الفيروسات والبرمجيات الضارة غير المعروفة مسبقاً	عبارة عن برمجيات 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)
الأصل / الأصول المعلوماتية	أي شيء ملموس أو غير ملموس له قيمة بالنسبة للجهة. هناك أنواع كثيرة من الأصول؛ بعض هذه الأصول تتضمن أشياء واضحة، مثل: الأشخاص، والآلات، والمرافق، وبراءات الاختراع، والبرمجيات والخدمات. ويمكن أن يشمل المصطلح أيضاً أشياء أقل وضوحاً، مثل: المعلومات والخصائص (مثل: سمعة الجهة وصورتها العامة، أو المهارة والمعرفة).

الهجوم	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.
التدقيق	المراجعة المستقلة ودراسة السجلات والأنشطة لتقييم مدى فعالية ضوابط الأمن السيبراني ولضمان الالتزام بالسياسات، والإجراءات التشغيلية، والمعايير والمتطلبات التشريعية والتنظيمية ذات العلاقة.
التحقق	التأكد من هوية المستخدم أو العملية أو الجهاز، وغالباً ما يكون هذا الأمر شرطاً أساسياً للسماح بالوصول إلى الموارد في النظام.
صلاحية المستخدم	خاصية تحديد والتأكد من حقوق/تراخيص المستخدم للوصول إلى الموارد والأصول المعلوماتية والتقنية للجهة والسماح له وفقاً لما حدد مسبقاً في حقوق/تراخيص المستخدم.
توافر	ضمان الوصول إلى المعلومات والبيانات والأنظمة والتطبيقات واستخدامها في الوقت المناسب.
النسخ الاحتياطية	الملفات والأجهزة والبيانات والإجراءات المتاحة للاستخدام في حالة الأعطال أو الفقدان، أو إذا حذف الأصل منها أو توقف عن الخدمة.
النسخ الاحتياطي غير المتصل أو خارج الموقع	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	طريقة للتخزين يتم فيها النسخ الاحتياطي بانتظام عبر شبكة على خادم بعيد، (إما داخل شبكة الجهة أو بالاستضافة لدى مزود خدمة).
الإعدادات الأساسية	مجموعة موثقة من المواصفات لإحدى أنظمة المعلومات، أو عنصر تكوين داخل نظام، تمت مراجعته رسمياً والاتفاق عليه في وقت معين، ولا يمكن تغييره إلا من خلال إجراءات التحكم في التغيير.
أحضر الجهاز الخاص بك BYOD	يشير هذا المصطلح إلى سياسة جهة تسمح (سواءً 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	يستخدم التليفزيون ذو الدائرة المغلقة، والمعروف 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 مطلباً هاماً فيها.
إدارة التغيير	هو 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	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. يتألف نموذج الحوسبة السحابية من خمس خصائص أساسية: خدمة ذاتية حسب الطلب، ووصول إلى الشبكة بشكل واسع، ومجمع الموارد، ومرونة سريعة، والخدمة المقاسة. وهناك ثلاثة نماذج لتقديم خدمات الحوسبة السحابية وهي: البرمجيات السحابية كخدمة (Saas "Software-as-Service")، والنظام أو المنصة السحابية كخدمة ("PaaS" Platform-as-Service)، 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 السحابية الهجين.
السرية	الاحتفاظ بقيود مصرح بها على الوصول إلى المعلومات والإفصاح عنها بما في ذلك وسائل حماية معلومات الخصوصية والملكية الشخصية.
الأنظمة الحساسة	هي أي أنظمة أو شبكات، يؤدي تعطلها، أو التغيير غير المشروع لطريقة عملها، أو الدخول غير المصرح به لها، أو للبيانات والمعلومات التي تحفظها أو تعالجها؛ إلى التأثير السلبي على توافر الخدمات، أو أعمال الجهة العامة، أو إحداث آثار اقتصادية أو مالية أو أمنية، أو اجتماعية سلبية كبيرة، على المستوى الوطني.
المعلومات (أو البيانات) الحساسة	هي المعلومات أو البيانات التي تعتبر غاية في الحساسية والأهمية، حسب تصنيف الجهة، والمُعدة 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 مصرح به أو فقدها 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. وتشمل المعلومات الحساسة كل المعلومات التي يترتب على الإفصاح عنها بشكل غير مصرح به أو فقدها أو تخريبها مساءلة أو عقوبات نظامية.
البنى التحتية الوطنية الحساسة	تلك العناصر الأساسية للبنية التحتية (أي الأصول، والمرافق، والنظم، والشبكات، والعمليات، والعاملون الأساسيون الذين يقومون بتشغيلها ومعالجتها)، والتي قد يؤدي فقدانها أو تعرضها لانتهاكات أمنية إلى: • أثر سلبي كبير على توافر الخدمات الأساسية أو تكاملها أو تسليمها - بما في ذلك الخدمات التي يمكن أن تؤدي في حال تعرضت سلامتها للخطر

	إلى خسائر كبيرة في الممتلكات و/أو الأرواح و/أو الإصابات- مع مراعاة الآثار الاقتصادية و/أو الاجتماعية الكبيرة. • تأثير كبير على الأمن القومي و/أو الدفاع الوطني و/أو اقتصاد الدولة أو مقدراتها الوطنية.
التشفير	هي القواعد التي تشتمل مبادئ ووسائل وطرق تخزين ونقل البيانات أو المعلومات في شكل معين وذلك من أجل إخفاء محتواها الدلالي، ومنع الاستخدام غير المصرح به أو منع التعديل غير المكتشف، بحيث لا يمكن لغير الأشخاص المعنيين قراءتها ومعالجتها.
التهديدات أو الهجوم السيبراني	الاستغلال المتعمد لأنظمة الكمبيوتر والشبكات والجهات التي يعتمد عملها على الاتصالات وتقنية المعلومات الرقمية بهدف إلحاق الضرر.
الأمن 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 الأمن السيبراني أمن المعلومات والأمن الإلكتروني والأمن الرقمي ونحو ذلك.
الفضاء السيبراني	الشبكة المترابطة من البنية التحتية لتقنية المعلومات، والتي تشمل الإنترنت وشبكات الاتصالات وأنظمة الحاسب الآلي والأجهزة المتصلة بالإنترنت، إلى جانب المعالِجات وأجهزة التحكم المرتبطة بها. كما يمكن أن يشير المصطلح إلى عالم أو نطاق افتراضي كظاهرة مجربة أو مفهوم مجرد.
حدث	شيء يحدث في مكان محدد مثل الشبكة والأنظمة والتطبيقات وغيرها وفي وقت محدد.
حادثة	انتهاك أمني بمخالفة سياسات الأمن السيبراني أو سياسات الاستخدام المقبول أو ممارسات أو ضوابط أو متطلبات الأمن السيبراني.
حوادث الأمن السيبراني	خرق للسياسة الأمنية لنظام ما من أجل التأثير على سلامته أو توافره و/أو الوصول غير المصرح به إليه أو محاولة الوصول إلى نظام أو أنظمة.
مخاطر الأمن السيبراني	المخاطر التي تمس عمليات أعمال الجهة (بما في ذلك رؤية الجهة أو رسالتها أو إداراتها أو صورتها أو سمعتها) أو أصول الجهة أو الأفراد أو الجهات الأخرى أو الدولة، بسبب إمكانية الوصول غير المصرح به أو الاستخدام أو الإفصاح أو التعطيل أو التعديل أو تدمير المعلومات و/أو نظم المعلومات.
تصنيف البيانات والمعلومات	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.

أرشفة البيانات أو المعلومات	عملية نقل البيانات التي لم تعد مستخدمة بشكل فعال في جهاز تخزين منفصل للحفظ طويل الأجل. تتكون 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.
التعافي من الكوارث	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	نظام تقني يستخدم قاعدة بيانات يتم توزيعها عبر الشبكة و/أو الإنترنت تسمح بتحويل أسماء النطاقات إلى عناوين الشبكة (IP Addresses)، والعكس، لتحديد عناوين الخدمات مثل خوادم المواقع الإلكترونية والبريد الإلكتروني.
فعالية	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	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.
بروتوكول نقل النص التشعبي الآمن HTTPS	بروتوكول يستخدم التشفير لتأمين صفحات وبيانات الويب عند انتقالها عبر الشبكة. وهو عبارة عن نسخة آمنة من نظام بروتوكول نقل النص التشعبي (HTTP).
هوية	وسيلة التحقق من هوية المستخدم أو العملية أو الجهاز، وهي عادة شرط أساسي لمنح حق الوصول إلى الموارد في النظام.
التهديدات البيئية	السلوك البشري الذي يؤثر على البيئة أو الأثر الثانوي للكوارث الطبيعية، والذي قد يتسبب في انقطاع وظائف الأعمال لبعض الفترات المحددة سلفاً أو انتهاك الضوابط الأمنية.
الاعتبارات الخاصة بالاتصالات وتقنية المعلومات	الاتصالات وتقنية المعلومات مصطلح ممتد لتقنية المعلومات التي تؤكد على دور الاتصالات الموحدة وتكامل البنية التحتية للاتصالات (خطوط الهاتف، شبكات الكابلات، الإشارات اللاسلكية)، وأجهزة الكمبيوتر، والبرمجيات.
مقدمي الخدمات المرخصين	جميع مزودي الخدمة الحاصلين على ترخيص من قبل الهيئة لتوفير الخدمات، كما هو محدد في التراخيص ذات الصلة.
الأنشطة الخبيثة	الأنشطة التي تصيب الأنظمة بطريقة خفية لانتهاك سرية البيانات أو التطبيقات أو أنظمة التشغيل أو انتهاك سلامتها، أو دقتها، أو توافرها.

خدمات الإسناد الخارجي	الحصول على السلع أو الخدمات عن طريق التعاقد مع مورد أو مزود خدمة.
المعلومات الشخصية	المعلومات التي يمكن استخدامها لتحديد هوية الفرد أو تتبعها (على سبيل المثال، الاسم وسجلات السمات الحيوية) وحدها، أو عند دمجها مع معلومات شخصية أو معلومات تعريفية أخرى مرتبطة أو قابلة للربط بشخص معين (مثل تاريخ ومحل الميلاد).
الضرر المادي	الضرر أو الإصابة التي تلحق بالشخص أو الممتلكات أو النظام وينتج عنها اعتلال، أو فقدان وظيفة، أو فائدة، أو قيمة.
صمود الأمن السيبراني	القدرة الشاملة للجهة على الصمود أمام الأحداث الأمنية السيبرانية، ومسببات الضرر، والتعافي منها.
رسائل التصيد الإلكتروني	محاولة الحصول على معلومات حساسة مثل أسماء المستخدمين وكلمات المرور أو تفاصيل بطاقة الائتمان، غالباً لأسباب ونوايا ضارة وخبيثة، وذلك بالتنكر على هيئة جهة جديرة بالثقة في رسائل إلكترونية.
الأمن المادي	يصف الأمن 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 الأمن المادي على استخدام طبقات متعددة من نظم مترابطة، تشمل الدوائر التلفزيونية المغلقة (CCTV)، وحراس الأمن، وحدود أمنية، والأقفال، وأنظمة التحكم في الوصول، والعديد من التقنيات الأخرى.
الأمن المنطقي	التدابير الأمنية التي تم تصميمها لحماية أنظمة وشبكات الجهة من كافة التهديدات السيبرانية والأنشطة الضارة.
الأطراف الخارجية	أي جهة تعمل كطرف في علاقة تعاقدية لتقديم السلع أو الخدمات (وهذا يشمل موردي ومزودي الخدمات).
سلامة المعلومة	حماية ضد تعديل أو تخريب المعلومات بشكل غير مصرح به، وتتضمن ضمان عدم الإنكار للمعلومات (Non-Repudiation) والموثوقية.
البرمجيات الضارة	برنامج يصيب الأنظمة بطريقة خفية (في الغالب) لانتهاك سرية أو سلامة ودقة أو توافر البيانات أو التطبيقات أو نظم التشغيل.
حزم التحديثات والإصلاحات	حزم بيانات داعمة لتحديث أو إصلاح أو تحسين نظام التشغيل للحاسب الآلي أو لتطبيقاته أو برامجه. وهذا يشمل إصلاح الثغرات الأمنية وغيرها من الأخطاء، حيث تسمى هذه الحزم عادةً إصلاحات أو إصلاح الأخطاء وتحسين إمكانية الاستخدام أو الأداء.
اختبار الاختراق	ممارسة اختبار على نظام حاسب آلي أو شبكة أو تطبيق موقع إلكتروني أو تطبيق هواتف ذكية للبحث عن ثغرات يمكن أن يستغلها المهاجم.
سياسة	وثيقة تحدد بنودها التزاماً عاماً أو توجيهاً أو نية ما كما تم التعبير عن ذلك رسمياً من قبل صاحب الصلاحية للجهة. سياسة الأمن السيبراني هي وثيقة تعبر بنودها عن الالتزام الرسمي للإدارة العليا للجهة بتنفيذ وتحسين برنامج الأمن السيبراني في الجهة، وتشتمل السياسة على

	أهداف الجهة فيما يتعلق ببرنامج الأمن السيبراني وضوابطه ومتطلباته وآلية تحسينه وتطويره.
الخصوصية	الحرية من التدخل غير المصرح به أو الكشف عن معلومات شخصية حول فرد.
إجراء	وثيقة تحتوي على وصف تفصيلي للخطوات الضرورية لأداء عمليات أو أنشطة محددة في التوافق مع المعايير والسياسات ذات العلاقة. وتعرّف الإجراءات على أنها جزء من العمليات.
عملية	مجموعة من الأنشطة المترابطة أو التفاعلية تحول المدخلات إلى مخرجات. وهذه الأنشطة متأثرة بسياسات الجهة.
الاستعادة	إجراء أو عملية لاستعادة أو التحكم في شيء منقطع أو تالف أو مسروق أو ضائع.
مدة الاحتفاظ	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).
نظام إدارة سجلات الأحداث ومراقبة الأمن السيبراني	نظام يقوم بإدارة وتحليل بيانات سجلات الأحداث الأمنية في الوقت الفعلي لتوفير مراقبة للتهديدات، وتحليل نتائج القواعد المترابطة لسجلات الأحداث، والتقارير حول بيانات السجلات، والاستجابة للحوادث.
فصل المهام	مبدأ أساسي في الأمن 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.
تهديد	أي 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 مستغلًا 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	يوفر معلومات منظمة وتحليلها حول الهجمات الأخيرة والحالية والمحتملة التي يمكن أن تشكل تهديداً للأمن السيبراني للجهة.
الثغرة	أي نوع من نقاط الضعف في نظام الحاسب الآلي، أو برامجه أو تطبيقاته، أو في مجموعة من الإجراءات، أو في أي شيء يجعل الأمن السيبراني عرضة للتهديد.
نظام الحماية المتقدمة لاكتشاف ومنع الاختراقات	نظام لديه قدرات كشف الاختراقات، بالإضافة إلى القدرة على منع وإيقاف محاولات الأنشطة والحوادث المشبوهة أو المحتملة.
مؤشر قياس الأداء	نوع من أدوات قياس مستوى الأداء يُقيم مدى نجاح نشاط ما أو جهة تجاه تحقيق أهداف محددة.
ترميز أو علامة	عرض معلومات (بتسمية وترميز محدد وقياسي) توضع على أصول الجهة (مثل: الأجهزة والتطبيقات والمستندات وغيرها) ليستدل بها للإشارة إلى بعض المعلومات المتعلقة بتصنيف الأصل وملكيته ونوعه وغيرها من المعلومات المتعلقة بإدارة الأصول.

الحد الأدنى من الصلاحيات	مبدأ أساسي في الأمن السيبراني يهدف إلى منح المستخدمين صلاحيات الوصول التي يحتاجونها لتنفيذ مسؤولياتهم الرسمية فقط.
التحقق من الهوية متعدد العناصر	نظام أمني يتحقق من هوية المستخدم، يتطلب استخدام عدة عناصر مستقلة من آليات التحقق من الهوية. تتضمن آليات التحقق عدة عناصر: • المعرفة (شيء يعرفه المستخدم فقط "مثل كلمة المرور"). • الحيازة (شيء يملكه المستخدم فقط "مثل برنامج أو جهاز توليد أرقام عشوائية أو الرسائل القصيرة المؤقتة لتسجيل الدخول"، ويطلق عليها ("One-Time-Password"). • الملازمة (صفة أو سمة حيوية متعلقة بالمستخدم نفسه فقط "مثل بصمة الإصبع").
المعمارية متعددة المستويات	معمارية أو بنية تُطبق أسلوب عميل-خادم الذي يتم فيه تطوير وصيانة منطق العملية الوظيفية، والوصول إلى البيانات، وتخزين البيانات وواجهة المستخدم كوحدات مستقلة على منصات منفصلة.
الحاجة إلى المعرفة والحاجة إلى الاستخدام	القيود المفروضة على البيانات، والتي تعتبر حساسة ما لم يكن لدى الشخص حاجة محددة للاطلاع على البيانات لغرض ما متعلق بأعمال ومهام رسمية.
العاملون في الجهة	الأشخاص الذين يعملون في الجهة (بما في ذلك الموظفون الرسميون والموظفون المؤقتون والمتعاقدون).
المعايير الأمنية لشفرة البرامج والتطبيقات	ممارسة تطوير برمجيات وتطبيقات الحاسب الآلي بطريقة تحمي من التعرض غير المقصود لثغرات الأمن السيبراني المتعلقة بالبرمجيات والتطبيقات.
مراجعة الإعدادات والتحصين	حماية وتحصين وضبط إعدادات جهاز الحاسب الآلي، والنظام، والتطبيق، وجهاز الشبكة، والجهاز الأمني لمقاومة الهجمات السيبرانية. مثل: إيقاف أو تغيير الحسابات المصنعية والافتراضية، إيقاف الخدمات غير المستخدمة، إيقاف منافذ الشبكة غير المستخدمة.
الاختبار الأمني	عملية تهدف إلى التأكد من أن النظام أو التطبيق المعدل أو الجديد يتضمن ضوابط وحمايات أمنية مناسبة ولا يحتوي على أي ثغرات أمنية قد تضر بالأنظمة أو التطبيقات الأخرى، أو تؤدي إلى سوء استخدام النظام أو التطبيق أو معلوماته، وكذلك للحفاظ على وظيفة النظام أو التطبيق على النحو المنشود.
انتهاك أمني	الإفصاح عن أو الحصول على معلومات لأشخاص غير مصرح تسريبها أو الحصول عليها، أو انتهاك السياسة الأمنية السيبرانية للجهة بالإفصاح عن أو تغيير أو تخريب أو فقد شيء سواءً بقصد أو بغير بقصد. ويقصد بالانتهاك الأمني الإفصاح عن أو الحصول على بيانات حساسة أو تسريبها أو تغييرها أو تبديلها أو استخدامها بدون تصريح (بما في ذلك مفاتيح تشفير النصوص وغيرها من المعايير الأمنية السيبرانية الحرجة).
المتطلبات الوطنية والدولية	المتطلبات الوطنية هي متطلبات طورتها جهة تشريعية في المملكة العربية السعودية للاستخدام بشكل تنظيمي (مثل: الضوابط الأساسية للأمن السيبراني)

	المتطلبات الدولية هي متطلبات طورتها جهة أو منظمة دولية عالمية للاستخدام بشكل تنظيمي في جميع أنحاء العالم (مثل: SWIFT، PCI وغيرها).
الأمن من خلال التصميم	منهجية لتطوير الأنظمة والتطبيقات وتصميم الشبكات التي تسعى إلى جعلها خالية من نقاط الضعف والثغرات الأمنية السيبرانية، والمقدرة على صد الهجوم السيبراني قدر الإمكان من خلال عدة تدابير على سبيل المثال: الاختبار المستمر، وحماية المصادقة والتمسك بأفضل ممارسات البرمجة والتصميم، وغيرها.

9. الملحق

I. نطاق الملحق

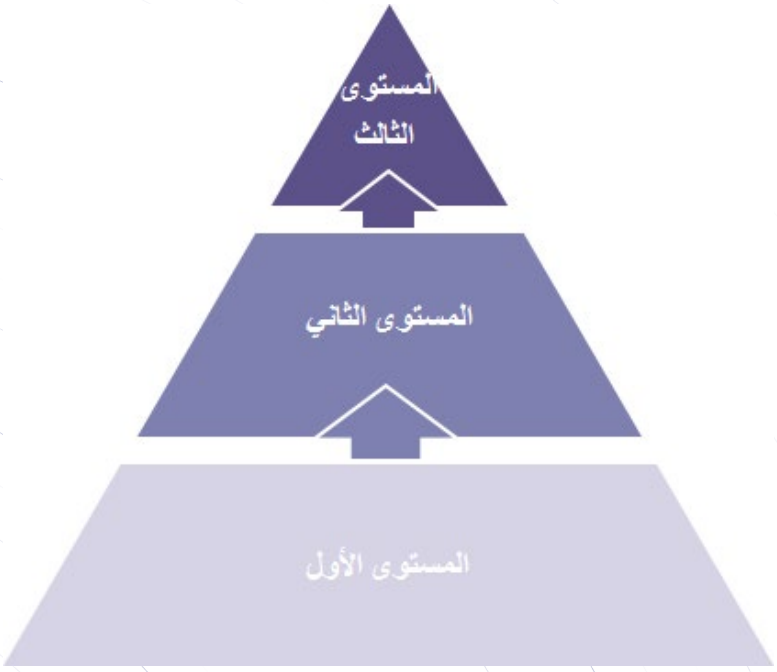
يختص هذا الملحق بتوضيح مستهدفات الالتزام، وهيكلية المتطلبات والضوابط المتعلقة بمقدمي الخدمة غير المصنفين كبنى تحتية وطنية حساسة.

II. مستهدفات الالتزام

تقوم الهيئة بوضع مستهدفات الالتزام من خلال تحديد ثلاث مستويات باتباع منهجية قائمة على إدارة المخاطر، ويحتوي كل مستوى على مجموعة من ضوابط الأمن السيبراني، وتختلف المستويات الثلاثة في متطلبات الضوابط:

- المستوى الأول: يشمل متطلبات الحد الأدنى من الضوابط.
- المستوى الثاني: يشمل متطلبات متقدمة من الضوابط.
- المستوى الثالث: يشمل متطلبات تعمل على مراقبة الكفاءة والتحسين المستمر لضوابط المستويين الأول والثاني.

تحقيق الالتزام بأحد المستويات يتطلب تحقيق الالتزام بالمستويات السابقة.



الشكل 1 - مستويات الالتزام

تشتمل مستهدفات الالتزام لمقدمي الخدمة غير المصنفين كبنى تحتية وطنية حساسة على مستوى الالتزام المطلوب وتاريخه، وهو ما سيتم تحديده والرفع به رسمياً من قبل الهيئة.

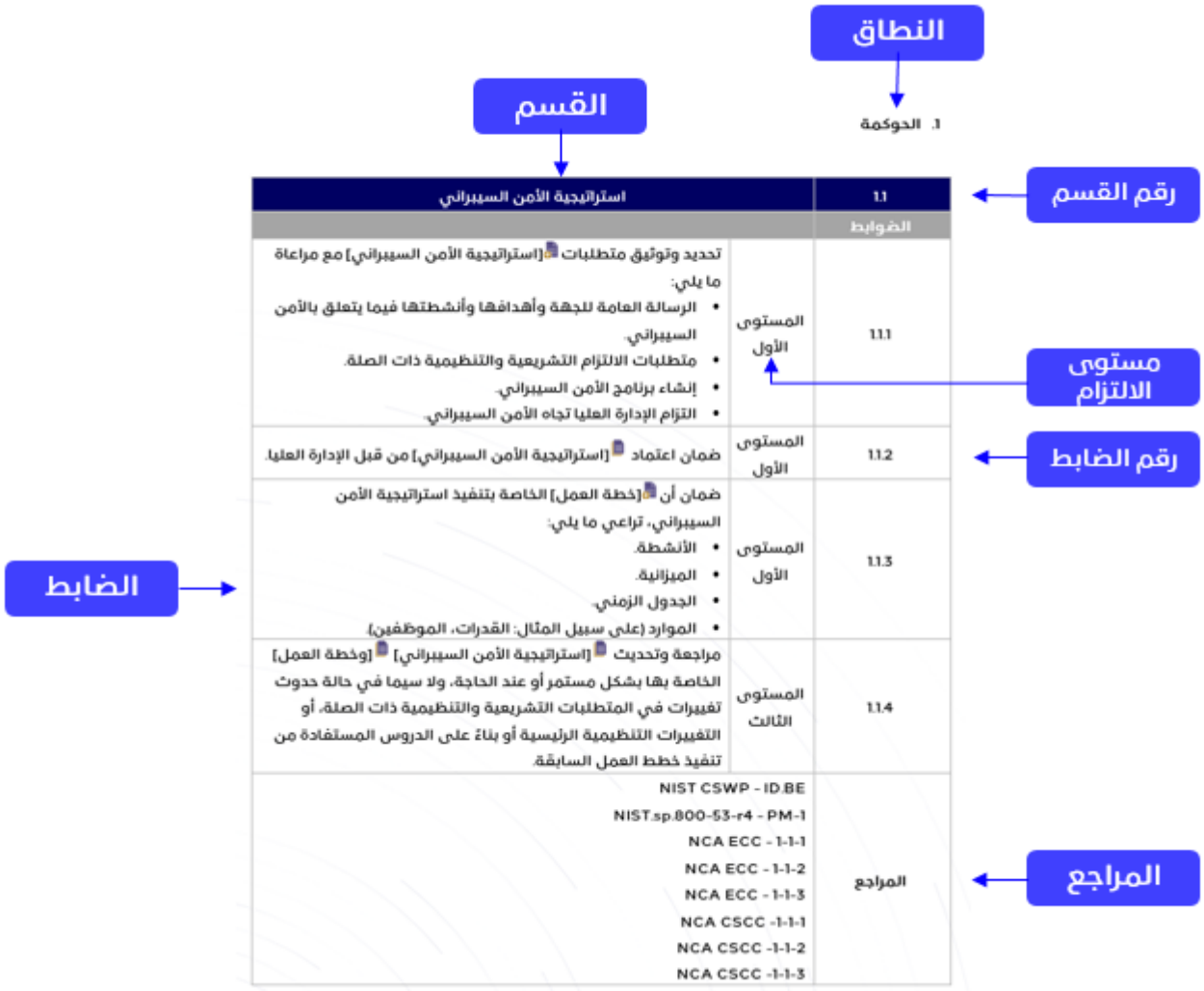
III. هيكلية المتطلبات

تنقسم متطلبات الأمن السيبراني لمقدمي الخدمة غير المصنفين كبنى تحتية وطنية حساسة إلى ست نطاقات:

الشكل 2 - نطاقات متطلبات الأمن السيبراني لمقدمي الخدمة غير المصنفين كبنى تحتية وطنية حساسة

تم تقسيم كل نطاق إلى أقسام أكثر تخصصاً تجمع ضوابط الأمن السيبراني ذات الصلة بالموضوع المحدد وتشترك في نفس الهدف.

الشكل 3 - نطاقات وأقسام متطلبات الأمن السيبراني لمقدمي الخدمة غير المصنفين كبنى تحتية وطنية حساسة



الشكل 4 - هيكل المتطلبات

ملاحظات هامة

يتم ترميز معلومات الضابط الخاصة على سبيل المثال: [العمليات]، و[المُخرجات]، و[المراجع] (على سبيل المثال فيما يتعلق بغيرها من الضوابط والأقسام والعمليات ووثائق الهيئة) بشكل منفصل في كافة أجزاء المتطلبات. عند التطابق، يتم أيضًا تظليل اعتبارات الضابط [الخاصة بالاتصالات وتقنية المعلومات].

ترتبط الضوابط الواردة في المتطلبات ببعضها البعض، فعلى سبيل المثال يمكن أن تكون نتيجة ضابط ما في قسم ما مدخلًا لضابط آخر في قسم مختلف (على سبيل المثال يعمل [تقرير الثغرات] الذي يتم إعداده في قسم إدارة الثغرات الأمنية كمدخل إلى قسم إدارة حزم التحديثات والإصلاحات).

تغطي العمليات والمخرجات المُظللة أبرز تدابير الأمن السيبراني وليس بالضرورة جميعها. حيث أنها تهدف للتركيز على العمليات والمخرجات المتوقعة من أجل تحسين قابلية استخدام ضوابط المتطلبات ووضوحها.

فيما يلي الرموز المستخدمة في المتطلبات وتفسيراتها:


مُخرج جديد


مُخرج


عملية جديدة


عملية

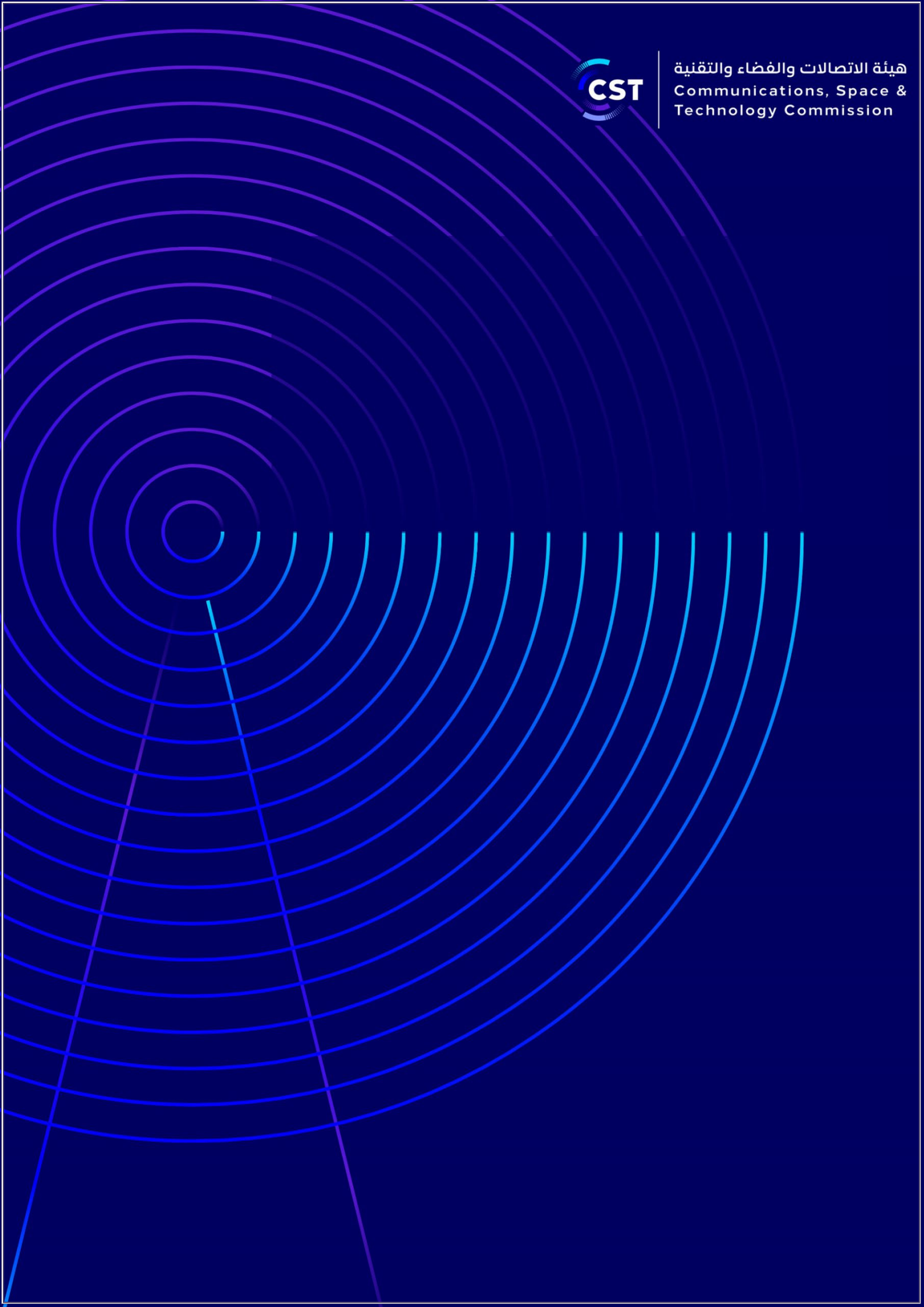

مرجع


الاعتبارات الخاصة بالاتصالات وتقنية المعلومات

IV. المراجع

أخذت الهيئة في الاعتبار الإسهامات المتوفرة من عدد من المعايير والأطر واللوائح المرتبطة بالأمن السيبراني والأعمال المماثلة التي أعدتها جهات تنظيمية أخرى حيث تمت مراعاة المراجع التالية أثناء وضع الإطار التنظيمي:

- ISO/IEC 27001 (2013)
- ISO/IEC 27002 (2013)
- ISO 27011/ITU-T X.1051 (2016)
- ISO/IEC 27004 (2016)
- ITU-T X series
- SANS CIS Critical Security Controls Version 6.1 (2016) and 7 (2018)
- National Institute of Standards & Technologies: Framework for Improving Critical Infrastructure Cybersecurity (NIST CSWP, 2018)
- National Institute of Standards & Technologies: Security and Privacy Controls for Federal Information Systems and Organizations (NIST Special Publication 800-53, Revision 4, (2013)
- الضوابط الأساسية للأمن السيبراني الصادرة عن الهيئة الوطنية للأمن السيبراني (2018)
- وضوابط الأمن السيبراني للأنظمة الحساسة الصادرة عن الهيئة الوطنية للأمن السيبراني (2018)


CST
هيئة الاتصالات والفضاء والتقنية
Communications, Space &
Technology Commission