الإطار التنظيمي للأمن السيبراني لقطاع الاتصالات وتقنية المعلومات

الإصدار: ١,٠

التاريخ: ٢٠١٩/٠٥/٢٩

التصنيف: متاح

المحتويات

١. مقدمة

وفقًا للأحكام الواردة في نظام الاتصالات (النظام) ولائحة الاتصالات (اللائحة) المتعلقة بحماية المصلحة العامة ومصالح المستخدمين والمحافظة على سرية الاتصالات وأمن المعلومات، وتماشيًا مع رؤية المملكة ٢٠٣٠، أعدت هيئة الاتصالات وتقنية المعلومات (الهيئة) إطار تنظيمي شامل للأمن السيبراني (الإطار) بهدف زيادة مستوى نضج الأمن السيبراني في قطاع الاتصالات وتقنية المعلومات.

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 البيانات الحساسة، أصبح تعزيز الأمن السيبراني في المملكة العربية السعودية أمرًا في غاية الأهمية لزيادة ثقة الوطن الرقمي في سلامة وصمود البنية التحتية لقطاع الاتصالات وتقنية المعلومات وخدماته.

٢. الغرض

يوفر الإطار التنظيمي للأمن السيبراني 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 في قطاع الاتصالات وتقنية المعلومات.
- زيادة مستوى نضج الأمن السيبراني في قطاع الاتصالات وتقنية المعلومات.
- تبني منهجية إدارة المخاطر لتحقيق متطلبات الأمن السيبراني.
- تشجيع قطاع الاتصالات وتقنية المعلومات على تطبيق أفضل الممارسات لوضع تدابير الأمن السيبراني المناسبة.
- ضمان سرية الخدمات المقدمة للعملاء، وسلامتها، وتوافرها.

٣. النطاق

يوفر هذا الإطار مجموعة شاملة من متطلبات الحد الأدنى لضوابط الأمن السيبراني التي يجب على مقدمي الخدمات المرخصين تنفيذها.

مع عدم الإخلال بالأحكام الواردة في أنظمة الهيئة والأنظمة ذات الصلة، تطبق أحكام هذا الإطار على مقدمي الخدمة المرخصين. وتجدر الإشارة إلى أن هذا الإطار لا يهدف إلى استبدال الأطر التنظيمية الصادرة، ولا ينبغي اعتباره بديلًا لأي منها.

٤. قابلية التطبيق

تنطبق أحكام هذا الإطار على جميع مقدمي الخدمات المرخصين، وشركاتهم التابعة، وموظفيهم، والأطراف الخارجية لديهم، وعملائهم. كما يجب على كل مقدم خدمة الالتزام بجميع المتطلبات القابلة للتطبيق لديه من خلال وضع منهجية خاصة به لتحقيق الأهداف المتعلقة بكل ضابط من ضوابط الأمن السيبراني.

نظرًا لشمولية المتطلبات، قد لا تسري بعض المتطلبات على كل مقدم خدمة مرخص. على سبيل المثال، إذا لم يكن أحد مقدمي الخدمة المرخصين يقوم بتطوير البرمجيات، ففي هذه الحالة ستكون المتطلبات المتعلقة بتطوير البرمجيات الآمنة غير قابلة للتطبيق لديه (القسم: 4.14). بينما ستظل الضوابط قابلة للتطبيق في

حالة تطوير البرمجيات عن طريق طرف خارجي.

٥. الأدوار والمسؤوليات

تتضمن مسؤوليات الهيئة القيام بالآتي:

١. متابعة التزام مقدمي الخدمات المرخصين للمتطلبات المحددة من خلال طرق مختلفة، على سبيل المثال عمليات التفتيش الميدانية، وورش عمل الالتزام، ومصفوفة الالتزام، وعمليات التدقيق الاستباقي أو الناتج عن البلاغات.
٢. المراجعة والتحديث الدوري للإطار.
٣. تحديد مستهدفات الالتزام وتحديد المواعيد المستهدفة لضمان امتثال مقدمي الخدمة للإطار.

تتضمن مسؤوليات مقدمي الخدمات المرخصين الالتزام بالآتي:

١. تطبيق وتنفيذ الإطار وفقًا لمتطلبات الالتزام المحددة.
٢. رفع تقارير الالتزام من خلال التقييمات الذاتية على سبيل المثال، أو غيرها من الوسائل المختلفة بناءً على طلب الهيئة.
٣. تقديم المعلومات والوثائق اللازمة إلى الهيئة عند الطلب بالإضافة إلى رفع التقارير المحددة في الإطار.

٦. المصطلحات والتعريفات

يجب أن تكون للكلمات والعبارات المحددة في قوانين الهيئة نفس المعاني المستخدمة في هذه الوثيقة. ويبين الجدول التالي تلك الكلمات والعبارات ومعانيها، ما لم ينص السياق على 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.
التهديدات المتقدمة المستمرة	هجوم خفي على شبكة كمبيوتر يحصل من خلاله شخص ما أو مجموعة على وصول غير مصرح به إلى شبكة ما ويظل غير مكتشف لفترة طويلة.
الإعدادات الأساسية	مجموعة موثقة من المواصفات لإحدى أنظمة المعلومات، أو عنصر تكوين داخل نظام، تمت مراجعته رسميًا والاتفاق عليه في وقت معين، ولا يمكن تغييره إلا من خلال إجراءات التحكم في التغيير.
أحضر الجهاز الخاص بك	تشير سياسة أحضر الجهاز الخاص بك إلى الأجهزة الشخصية (أجهزة الكمبيوتر المحمولة والأجهزة اللوحية والهواتف الذكية) التي يُسمح للموظفين والمقاولين باستخدامها لتنفيذ وظائف العمل.
الحوسبة السحابية	استخدام مجموعة قابلة للتطوير من الموارد المادية أو الافتراضية المشتركة (مثل الخوادم، والأنظمة التشغيلية، والشبكات، والبرمجيات، والتطبيقات ومعدات التخزين) التي يمكن توفيرها بالجهد الإداري التشغيلي والتدخل لإعداد الخدمة من مزود الخدمة.
الأنظمة الحساسة	أي أنظمة تؤدي فيها الأعطال، والتغييرات غير المصرح بها في عملياتها، والوصول غير المصرح به إلى معلوماتها إلى التأثير بشكل كبير على توفر الخدمات، أو عمليات الجهة، أو جوانبها الاقتصادية أو المالية أو الاجتماعية على المستوى الوطني.
التشفير	القواعد التي تشمل مبادئ ووسائل وطرق تخزين ونقل البيانات أو المعلومات في شكل معين وذلك من أجل إخفاء محتواها، ومنع الاستخدام غير المصرح به أو منع التعديل غير المكتشف، بحيث لا يمكن لغير الأشخاص المعنيين قراءتها ومعالجتها.
التهديدات السيبرانية	الاستغلال المتعمد لأنظمة الكمبيوتر والشبكات والجهات التي يعتمد عملها على الاتصالات وتقنية المعلومات الرقمية بهدف إلحاق الضرر.
الأمن السيبراني	حماية الشبكات، والأنظمة والعمليات، ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات، وما تحتويه من بيانات، من أي اختراق أو تعطيل أو دخول أو استخدام غير مشروع. ويشمل مفهوم الأمن السيبراني أمن المعلومات والأمن الرقمي.
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	حدث غير مرغوب فيه أو التعرض لعواقب سلبية محتملة.
التعافي من الكوارث	يُقصد بالتخطيط للتعافي من الكوارث وضع الإجراءات التي يتم اتخاذها لاستعادة الوضع الطبيعي للعمليات في أعقاب الكوارث. ويتضمن ذلك تحديد استراتيجيات التعافي لجميع وظائف الأعمال الحساسة، ووضع إجراءات لإدارة التعافي، ووضع خطط تعافي لمختلف مستويات وظائف الأعمال.
التهديدات البيئية	السلوك البشري الذي يؤثر على البيئة أو الأثر الثانوي للكوارث الطبيعية، والذي قد يتسبب في انقطاع وظائف الأعمال لبعض الفترات المحددة سلفًا 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.
الأصول المعلوماتية	مجموعة الأجهزة والأنظمة والبيانات والمعلومات التي تمكن جهة ما من أداء وظائفها التجارية وبالتالي تلبية متطلبات الجهة المعترف بها.

ITU	الاتحاد الدولي للاتصالات.
مقدمو الخدمات المرخصين	جميع مزودي الخدمة الذين طلبوا الحصول 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 والخدمات عن طريق التعاقد مع مورد أو مزود خدمة.
المعلومات الشخصية	المعلومات التي يمكن استخدامها لتحديد هوية الفرد أو تتبعها (على سبيل المثال، الاسم والسجلات البيومترية) 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.
الصمود	القدرة الشاملة للجهة على الصمود أمام الأحداث السيبرانية، ومسببات الضرر، والتعافي منها
رسائل التصيد النصية	ممارسة احتيالية متمثلة في إرسال رسائل نصية تزعم أنها من شركات مرموقة من أجل حث الأفراد على الكشف عن المعلومات الشخصية، مثل كلمات المرور أو أرقام بطاقات الائتمان.
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).
الأمن المنطقي	التدابير الأمنية التي تم تصميمها لحماية أنظمة وشبكات الجهة من كافة التهديدات السيبرانية والأنشطة الضارة.
الأطراف الخارجية	الجهات التي يتم التعاقد معها للحصول على السلع والخدمات.

٧. الإطار التنظيمي

يحدد الإطار التنظيمي للأمن السيبراني الأحكام التنظيمية التالية التي يجب على مقدمي الخدمات المرخصين الالتزام بها. يمكن الاطلاع على المتطلبات التفصيلية المتعلقة بكل حكم تنظيمي في الملحق.

١. الحوكمة

يجب على مقدمي الخدمات المرخصين القيام بما يلي:

١,١. تحديد استراتيجية الأمن السيبراني ووضع خارطة التنفيذ لتحقيق الأهداف الاستراتيجية المحددة.
١,٢. تحديد وتطبيق الهيكل التنظيمي المناسب الذي سيتولى مسؤولية أنشطة الأمن السيبراني داخل الجهة.
١,٣. تحقيق الالتزام بالمتطلبات التنظيمية الداخلية والخارجية (المحلية والعالمية) ذات الصلة.
١,٤. إجراء عمليات تدقيق مستقلة للأمن السيبراني بصفة دورية تغطي متطلبات الالتزام الداخلية والخارجية لقياس مستوى امتثال الجهة.
١,٥. عقد حملات توعية ودورات تدريبية بصفة دورية لموظفيهم عن الأمن السيبراني لضمان حصولهم على المؤهلات والمهارات اللازمة للقيام بمسؤولياتهم.
١,٦. تزويد عملائهم بمعلومات الأمن السيبراني ذات الصلة بالخدمات المقدمة لتحسين الوعي بالأمن السيبراني.
١,٧. ضمان إدراج المتطلبات التنظيمية للأمن السيبراني في منهجية إدارة المشاريع المطبقة.
١,٨. ضمان تلبية متطلبات الأمن السيبراني المتعلقة بالموارد البشرية في حالة حدوث أي تغييرات في العلاقة الوظيفية.

٢. إدارة الأصول

يجب على مقدمي الخدمات المرخصين القيام بما يلي:

٢,١. الاحتفاظ بقائمة جرد محدثة لجميع الأصول المعلوماتية التي تتضمن جميع التفاصيل ذات الصلة لتسهيل الحماية الفعّالة للأصول المعلوماتية.
٢,٢. تصنيف الأصول المعلوماتية لضمان الحماية القائمة على المخاطر للأصول المعلوماتية.
٢,٣. إدارة استخدام أجهزة الموظفين لأغراض العمل لحماية الجهة من المخاطر الناجمة عن استخدامها.
٢,٤. تحديد وتطبيق سياسة الاستخدام المقبول لحماية الجهة من المخاطر الناجمة عن الاستخدام غير المناسب للأصول المعلوماتية.
٢,٥. الحفاظ على الأصول المعلوماتية واستعادتها لضمان استمرار توافرها وسلامتها في حالة وقوع حادثة أمن سيبراني.
٢,٦. ضمان التخلص الآمن من الأصول المعلوماتية من أجل منع الاطلاع غير المصرح به أو تعديل المعلومات المخزنة عليها.

٣. إدارة المخاطر للأمن السيبراني

يجب على مقدمي الخدمات المرخصين القيام بما يلي:

٣,١. إعداد وتنفيذ منهجية مناسبة لتحديد مخاطر الأمن السيبراني وتحليلها وتقييمها لحماية الأصول المعلوماتية.
٣,٢. إعداد وتنفيذ منهجية مناسبة لمراقبة مخاطر الأمن السيبراني ومعالجتها بما يتيح التعامل مع المخاطر التي تم تحديدها ومراقبة خطط المعالجة.

٤. الأمن المنطقي

يجب على مقدمي الخدمات المرخصين القيام بما يلي:

٤,١. استخدام التشفير لضمان سرية وموثوقية وسلامة المعلومات أثناء النقل والتخزين والاستخدام.
٤,٢. إدارة التغييرات التي تُجرى على الأصول المعلوماتية لمنع التعديلات الغير مصرح بها أو الغير مخطط لها.
٤,٣. تحديد الثغرات الأمنية في الأصول المعلوماتية وترتيب أولويات إجراءات المعالجة الموصى بها.
٤,٤. التأكد من تطبيق حزم التحديثات والإصلاحات الأمنية على الأصول المعلوماتية ضمن إطار زمني مناسب لإصلاح المشكلات المعروفة وتعزيز صمود تلك الأصول.
٤,٥. حماية الشبكات التي تديرها الجهة من الأنشطة الخبيثة وضمان صمود الشبكات ضد التهديدات السيبرانية.
٤,٦. مراقبة وحماية سجلات الأحداث الخاصة بالأصول المعلوماتية والإبلاغ عن أي أنشطة مشبوهة تحتاج إلى مزيد من التحقيق.
٤,٧. إدارة صلاحيات الوصول وتطبيق آليات تحقق مناسبة لمنع الوصول غير المصرح به إلى الأصول المعلوماتية.
٤,٨. إنشاء وتطبيق قائمة بتطبيقات البرمجيات المسموح بتثبيتها واستخدامها داخل الجهة.
٤,٩. الكشف عن حوادث الأمن السيبراني والاستجابة لها لاحتوائها والحد من أثرها.
٤,١٠. الكشف عن البرمجيات الضارة ومنع انتشارها في الجهة.
٤,١١. تصنيف معلومات الجهة لضمان حمايتها بشكل ملائم.
٤,١٢. اتخاذ التدابير اللازمة بما في ذلك النسخ الاحتياطي لضمان استعادة المعلومات بعد وقوع أي حادثة.
٤,١٣. تطبيق الإعدادات الأساسية للأنظمة بهدف زيادة صمود الأصول المعلوماتية.
٤,١٤. تنفيذ منهجية دورة حياة تطوير البرمجيات بطريقة آمنة.
٤,١٥. حماية البريد الإلكتروني ومتصفحات الويب من تهديدات الأمن السيبراني.
٤,١٦. إجراء اختبارات الاختراق لتقييم القدرات الدفاعية للجهة وكشف الثغرات.

٥. الأمن المادي

يجب على مقدمي الخدمات المرخصين القيام بما يلي:

٥,١. حماية الأصول المعلوماتية من الأضرار المادية والتهديدات.
٥,٢. إدارة الوصول المادي إلى المرافق التي تحتوي الأصول المعلوماتية لمنع الوصول غير المصرح به.
٥,٣. حماية الأصول المعلوماتية من التهديدات البيئية.
٥,٤. حماية الأصول المعلوماتية الموجودة خارج مباني الجهة من التهديدات المادية والبيئية.

٦. الأمن المتعلق بالأطراف الخارجية

يجب على مقدمي الخدمات المرخصين القيام بما يلي:

٦,١. تضمين متطلبات الأمن السيبراني في العقود وإلزام مقدم الخدمة السحابية بتطبيقها.
٦,٢. تضمين متطلبات الأمن السيبراني في العقود وإلزام الأطراف الخارجية التي تقدم خدمات الإسناد الخارجي للجهة بتطبيقها.

الملحق

١. مستويات الالتزام

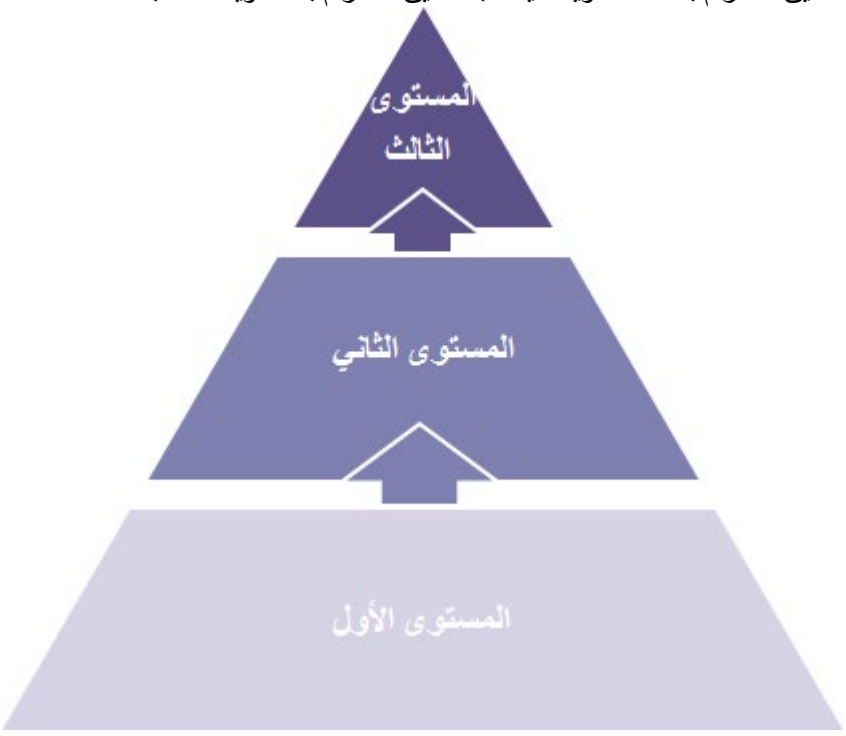
تقوم الهيئة بوضع مستهدفات الالتزام من خلال تحديد ثلاث مستويات باتباع منهجية قائمة على إدارة المخاطر، ويتكون كل مستوى من مجموعة من ضوابط الأمن السيبراني، وتختلف المستويات الثلاثة في متطلبات الضوابط:

المستوى الأول يشمل متطلبات الحد الأدنى من الضوابط.

المستوى الثاني يشمل متطلبات متقدمة من الضوابط.

المستوى الثالث يشمل متطلبات تركز على مراقبة الكفاءة والتحسين المستمر لضوابط المستويين الأول والثاني.

تحقيق الالتزام بأحد المستويات يتطلب تحقيق الالتزام بالمستويات السابقة.



الشكل ١ - مستويات الالتزام

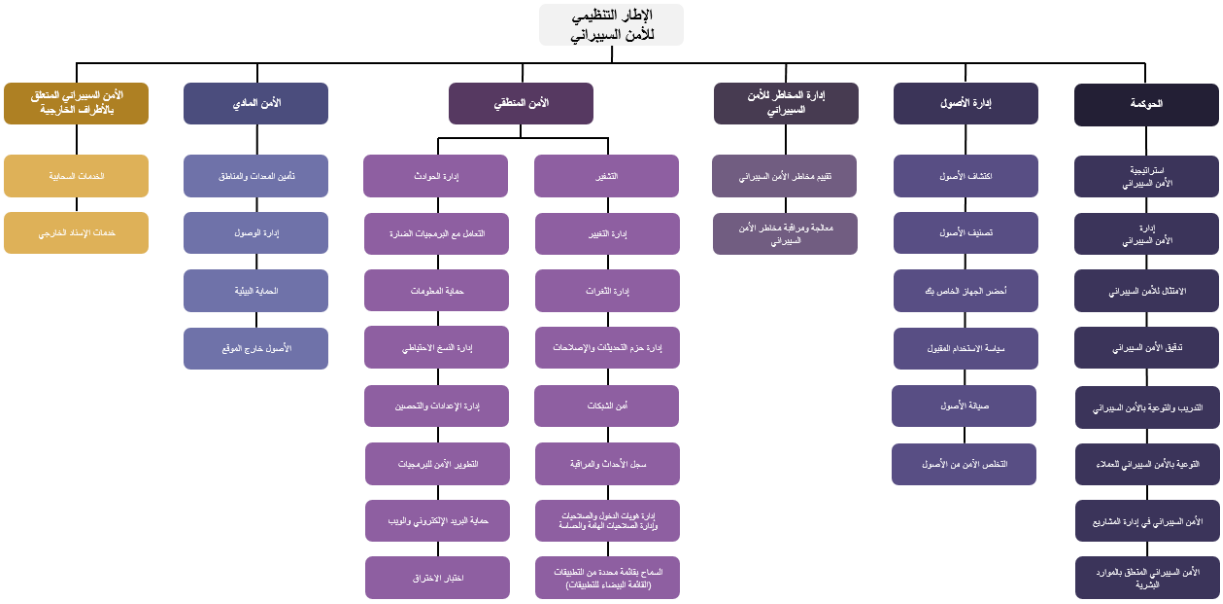
تشتمل مستهدفات الالتزام لمقدمي الخدمات المرخصين على مستوى الالتزام المستهدف وتاريخه، وهو ما سيتم تحديده والرفع به رسميًا من قبل الهيئة.

٢. هيكل الضوابط

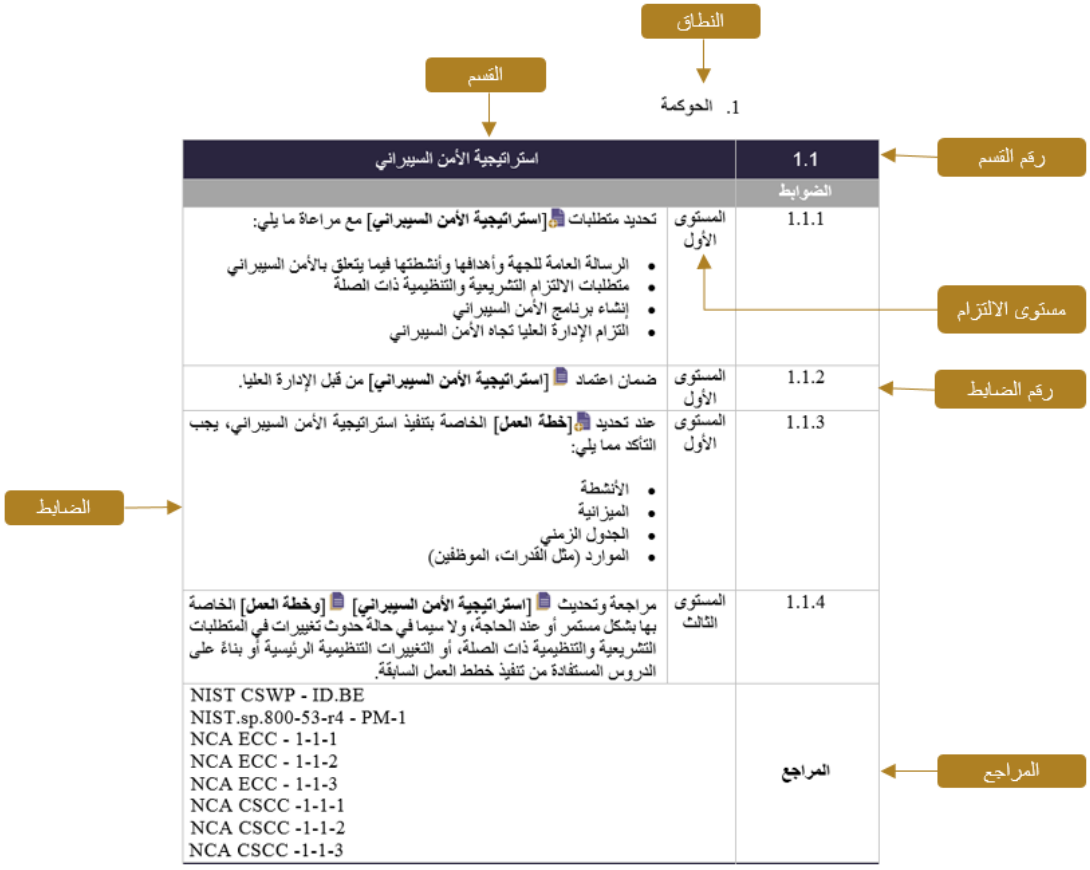
تُجمع ضوابط الإطار التنظيمي للأمن السيبراني في ستة مجالات:

الشكل ٢ - مجالات الإطار التنظيمي للأمن السيبراني

يتم تقسيم كل مجال إلى أقسام أكثر تحديدًا تجمع ضوابط الأمن السيبراني ذات الصلة بالموضوع المحدد وتشترك في نفس الهدف.



الشكل ٣ - مجالات وأقسام الإطار



الشكل ٤ - هيكل الإطار التنظيمي للأمن السيبراني

ملاحظات هامة

يتم تظليل معلومات الضابط الخاصة مثل[**العمليات**]، و[**المخرجات**]، و[**المراجع**] (على سبيل المثال فيما يتعلق بغيرها من الضوابط والأقسام والعمليات ووثائق الهيئة) بشكل منفصل في كافة أجزاء الإطار. عند الاقتضاء، يتم أيضًا تظليل اعتبارات الضابط [**الخاصة بالاتصالات وتقنية المعلومات**].

ترتبط الضوابط الواردة في الإطار ببعضها البعض، فعلى سبيل المثال يمكن أن تكون نتيجة ضابط ما في قسم ما مدخلًا لضابط آخر داخل 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 والنتائج المُظللة معظم تدابير الأمن السيبراني وليس بالضرورة جميعها. حيث أنها تهدف للتركيز على العمليات والمخرجات المتوقعة من أجل تحسين قابلية استخدام ضوابط الإطار ووضوحه.

فيما يلي الرموز المستخدمة في الإطار التنظيمي للأمن السيبراني:

شكل تفسيري لرموز الإطار

مخرج جديد
مخرج
عملية جديدة
عملية
مرجع
الاعتبارات الخاصة بالاتصالات وتقنية المعلومات

٣. توثيق المتطلبات

سيكون توثيق المتطلبات هو الخطوة الأولى في جميع أقسام الإطار تقريباً. ولا ينص الإطار على صيغة موحدة لتوثيق المتطلبات المذكورة في كل قسم من الأقسام، حيث يمكن تحديد هذه المتطلبات في شكل توجيهات أو قواعد أو معايير أو سياسات. ومع ذلك، يجب أن تتضمن وثيقة المتطلبات - بغض النظر عن اسمها - على الأقل ما يلي:

- عنوان مرجعي لتمييز كل وثيقة عن الأخرى
- رقم وتاريخ إصدار الوثيقة
- أداة تتبع التغييرات بالوثيقة
- مالك الوثيقة المسؤول عن التغييرات
- يجب اعتماد وثيقة المتطلبات رسميًا من قبل الموظفين/اللجنة المعتمدين داخل الجهة
- يجب نشر وثائق المتطلبات على نحو مناسب ونقلها إلى جميع الأطراف المعنية ذات الصلة داخل الجهة
- الأدوار والمسؤوليات المتعلقة بتحديد واعتماد متطلبات القسم والموافقة عليها.

الوثائق التي لا تفي بالمتطلبات المذكورة أعلاه ستعتبر غير متوافقة مع متطلبات الضابط.

٤. نطاقات الضوابط

١. الحوكمة

1.1	استراتيجية الأمن السيبراني	
الضوابط		
1.1.1	المستوى الأول	تحديد 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	عند تحديد [**خطة العمل**] الخاصة بتنفيذ استراتيجية الأمن السيبراني، يجب التأكد مما يلي: • الأنشطة • الميزانية • الجدول الزمني • الموارد (مثل 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 متطلبات [**الهيكل التنظيمي للأمن السيبراني**] مع مراعاة ما يلي: • لجنة الأمن السيبراني وتحديد أعضاء يمثلون تخصصات مختلفة داخل الجهة • مهام/إدارات الأمن السيبراني اللازمة لتنفيذ [**خطة العمل**] • 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**] المحددة.
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.
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 [**متطلبات الالتزام بالأمن السيبراني**] مع مراعاة ما يلي: • المتطلبات التشريعية والتنظيمية الوطنية المتعلقة بالأمن السيبراني • المتطلبات الدولية/الخارجية المعتمدة محليًا (على سبيل المثال المدرجة في الاتفاقيات أو الالتزامات الدولية) • المتطلبات الداخلية للجهة
1.3.2	المستوى الأول	تحديد {**عملية الالتزام**} لضمان تحديد متطلبات الالتزام بصفة دورية وتوثيقها والرفع بها (على سبيل المثال، إذا أصبحت متطلبات تنظيمية جديدة سارية ونافذة، يجب تحديث متطلبات الأمن السيبراني للجهة).
1.3.3	المستوى الأول	ضمان إدراج ومراعاة متطلبات الالتزام في جميع أعمال الجهة.
1.3.4	المستوى الثاني	أتمتة أنشطة الالتزام من خلال استخدام أدوات مخصصة (مثل أداة الحوكمة وإدارة المخاطر والالتزام).
1.3.5	المستوى الثالث	مراجعة 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 [**المتطلبات الخاصة بتدقيق الأمن السيبراني**] مع مراعاة ما يلي: • إجراء عمليات التدقيق الدورية (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	توثيق النتائج والتوصيات وتقديمها إلى الإدارة العليا.
1.4.4	المستوى الثاني	حماية [**سجلات التدقيق**] من الوصول غير المصرح به، أو تعديلها، أو إتلافها.
1.4.5	المستوى الثاني	ضمان الاحتفاظ بـ [**سجلات التدقيق**] كدليل، على سبيل المثال، على الالتزام بالمتطلبات التشريعية والتنظيمية.
1.4.6	المستوى الثالث	مراجعة 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 [**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 مثل: الحيل الهاتفية ومكالمات انتحال الشخصية) • توعية العاملين بعدم محاولة القيام بأنشطة غير مصرح بها (مثل 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
1.5.3	المستوى الثاني	تحسين وتنفيذ [**متطلبات التدريب والتوعية المتعلقة بالأمن السيبراني**] لتشمل إجراء اختبارات تحقق دورية لتقييم فاعلية برنامج التوعية والتدريب 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] (مثل التدريب الأولي على الأمن السيبراني للمستخدمين الجدد، والتدريب عند حدوث تغييرات في أنظمة المعلومات أو في الأدوار الوظيفية).
1.5.5	المستوى الثاني	تصميم **[برنامج التدريب والتوعية المتعلق بالأمن السيبراني]** بحيث يشمل المهارات المتخصصة أو المتعلقة بالأمن وكذلك تدريب فئات محددة من الموظفين، مثل: • موظفي الإدارة المعنية بالأمن السيبراني • الموظفين العاملين في تطوير البرمجيات • الموظفين المعنيين بإدارة تقييم مخاطر الأمن السيبراني • الموظفين الذين يتمتعون بصلاحيات الدخول إلى الأصول المعلوماتية الحساسة • الموظفين التنفيذيين
1.5.6	المستوى الثالث	مراجعة وتحسين **[متطلبات التدريب والتوعية المتعلقة بالأمن السيبراني]** وكذلك **[برنامج التدريب والتوعية المتعلق بالأمن السيبراني]** بشكل مستمر.
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
١,٦	التوعية بالأمن السيبراني للعملاء	
الضوابط		
1.6.1	المستوى الأول	تحديد **[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، وقناة 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 مثل: الحيل الهاتفية ومكالمات انتحال الشخصية) • توصيات محددة متعلقة بالخدمة المقدمة (على سبيل المثال: كيف تكون آمناً أثناء استخدام الإنترنت، رسائل التصيد النصية، وحماية جهازك المحمول)

1.6.3	المستوى الثاني	تحسين وتنفيذ [**متطلبات التوعية بالأمن السيبراني للعملاء**] لتنفيذ [**برنامج التوعية بالأمن السيبراني للعملاء**] بشكل دوري.
1.6.4	المستوى الثالث	مراجعة وتحسين [**متطلبات التوعية بالأمن السيبراني للعملاء**] بالإضافة إلى [**برنامج التوعية بالأمن السيبراني للعملاء**] بشكل مستمر.
المراجع		ISO 27002 - 7.2.2 NCA ECC - 1-10-3
١,٧	الأمن السيبراني في إدارة المشاريع	
الضوابط		
1.7.1	المستوى الأول	تحديد [**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 وفقًا لـ [**متطلبات 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	مراجعة 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
١,٨	الأمن السيبراني المتعلق بالموارد البشرية	
الضوابط		
1.8.1	المستوى الأول	تحديد [**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 (مثل 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	ضمان تنفيذ الإجراءات اللازمة (مثل تعديل تصاريح وصلاحيات الوصول وفقًا

	الأول	للدور الوظيفي الجديد) عند إعادة تعيين العاملين أو نقلهم إلى وظائف أخرى داخل الجهة.
1.8.3	المستوى الأول	إنفاذ الإجراءات التأديبية ضد العاملين الذين لا يمتثلون لمتطلبات الأمن السيبراني للجهة.
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 سابقًا تحت إشراف العامل الذي تم إنهاء عمله) عند انتهاء/إنهاء الخدمة للعاملين في الجهة.
1.8.5	المستوى الثالث	مراجعة 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

٢. إدارة الأصول

٢,١	اكتشاف الأصول	
الضوابط		
2.1.1	المستوى الأول	تحديد **[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 وتيرة تحديث **[قائمة جرد الأصول]** • ملكية الأصول المعلوماتية
2.1.2	المستوى الأول	تحديد وتنفيذ **{عملية اكتشاف الأصول}** لتحديد جميع الأصول المعلوماتية التي تملكها الجهة (باستخدام أداة اكتشاف الأصول على سبيل المثال) وتحديث **[قائمة جرد الأصول]**، وتعيين مالك لكل أصل من الأصول المعلوماتية.
2.1.3	المستوى	مراجعة وتحديث **[قائمة جرد الأصول]** بناءً على معدل التكرار المحدد في

	الأول	المتطلبات أو في حالة وجود تعديلات على الأصول المعلوماتية (على سبيل المثال أي إضافة أو حذف للأصول).
2.1.4	المستوى الثاني	استخدام أدوات مخصصة ومؤتمتة لاكتشاف الأصول المعلوماتية، وربط الأصول المعلوماتية ببعضها وتتبعها من نظام مركزي.
2.1.5	المستوى الثالث	مراجعة وتحسين **[متطلبات اكتشاف الأصول]** و**{عملية اكتشاف الأصول}** 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 ETSI TR 103 305 - 2.11 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
٢,٢	تصنيف الأصول	
الضوابط		
2.2.1	المستوى الأول	تحديد **[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 (مثل الأهمية، والقيمة التجارية، والمتطلبات القانونية، والسرية، والسلامة، والتوافر) و**[متطلبات حماية المعلومات]**.
2.2.3	المستوى الأول	تنفيذ عملية معالجة الأصول وفقًا **{لعملية تصنيف الأصول}**.
2.2.4	المستوى الثالث	مراجعة وتحسين **[متطلبات تصنيف الأصول]** **{وعملية تصنيف الأصول}** 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
٢,٣	أحضر الجهاز الخاص بك	
الضوابط		
2.3.1	المستوى	تحديد **[متطلبات الأمن السيبراني لسياسة أحضر الجهاز الخاص بك]** داخل الجهة

	الأول	مع مراعاة ما يلي: • فصل المعلومات الشخصية عن المعلومات المتعلقة بالعمل • القيود المفروضة على استخدام الأجهزة حسب توجهات الجهة • الوصول إلى الأنظمة الحساسة
2.3.2	المستوى الأول	إنفاذ **[متطلبات الأمن السيبراني لسياسة أحضر الجهاز الخاص بك]** المحددة داخل الجهة.
2.3.3	المستوى الثاني	ضمان تشفير معلومات الجهة المُخزنة على الأجهزة.
2.3.4	المستوى الثالث	مراجعة 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
٢,٤		سياسة الاستخدام المقبول
الضوابط		
2.4.1	المستوى الأول	تحديد **[متطلبات الاستخدام المقبول للأصول المعلوماتية]** مع مراعاة ما يلي: • الاستخدام المقبول للأصول المعلوماتية (مثل عدم تثبيت البرمجيات أو الأجهزة إلا بعد الحصول على موافقة رسمية من الإدارات المحددة ذات الصلة مثل إدارة تقنية المعلومات)
2.4.2	المستوى الأول	ضمان تنفيذ **[متطلبات الاستخدام المقبول للأصول المعلوماتية]** من قبل العاملين في الجهة (على سبيل المثال حظر تثبيت البرمجيات والتطبيقات غير المرغوب بها، والتحكم بالوصول إلى صفحات الويب وحظر الوصول إلى المواقع الضارة أو المواقع الخطرة).
2.4.3	المستوى الثالث	مراجعة وتحسين **[متطلبات الاستخدام المقبول للأصول المعلوماتية]** بشكل مستمر.
المراجع		ISO 27002 - 8.1.3 NCA ECC - 2-1-3 NCA ECC - 2-1-4
٢,٥		صيانة الأصول
الضوابط		
2.5.1	المستوى الثاني	تحديد **[متطلبات صيانة الأصول]** مع مراعاة ما يلي: • صيانة الأصول • التتبع والمراقبة • خطة الاستعادة
2.5.2	المستوى	تحديد وتنفيذ **{عملية صيانة الأصول}** لصيانة الأصول المعلوماتية للجهة

	الثاني	وإصلاحها (بما في ذلك الأصول خارج الموقع) والاحتفاظ بسجلات لهذه الأنشطة.
2.5.3	المستوى الثاني	وفقًا 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 (مثل استخدام تقنيات تتبع المواقع) للأصول المعلوماتية والتأكد من الاحتفاظ بها داخل المناطق التي تقع تحت إشراف الجهة.
2.5.5	المستوى الثالث	مراجعة وتحسين **[متطلبات صيانة الأصول]** و**{عملية صيانة الأصول}** 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
٢,٦	التخلص الآمن من الأصول	
الضوابط		
2.6.1	المستوى الأول	تحديد **[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]**. استخدم التقنيات المناسبة في حالة عدم الحاجة إليها أو عند إعادة استخدامها (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	مراجعة وتحسين **[متطلبات التخلص الآمن من الأصول]** و**{عملية التخلص الآمن من الأصول}** بشكل مستمر.
المراجع		ISO 27002 - 8.3.2 SANS v7.0 - 1.6 SANS v7.0 - 2.6 NCA ECC 2-14-3-4

٣. إدارة المخاطر للأمن السيبراني

٣,١	تقييم مخاطر الأمن السيبراني	
الضوابط		
3.1.1	المستوى الأول	تحديد **[متطلبات تقييم مخاطر الأمن السيبراني]** مع مراعاة ما يلي: • أهداف ونطاق تقييم المخاطر السيبرانية في الجهة • الحالات التي ينبغي بموجبها إجراء تقييم للمخاطر السيبرانية في الجهة ومعدل تكرار إجراء التقييم • ضمان تغطية **[متطلبات تقييم مخاطر الأمن السيبراني]** لمخاطر الأصول المعلوماتية وخدمات الجهة، والأفراد، والمؤسسات الأخرى، والدول المرتبطة بأنظمة معلومات الجهة
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]**. تسجيل 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 رسميًا من قبل الإدارة العليا. • عند الطلب، يتم الإبلاغ عن أهم مخاطر الأمن السيبراني الواردة في **[سجل المخاطر] وخطط المعالجة** إلى هيئة الاتصالات وتقنية المعلومات.
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 المبكرة للمشاريع التقنية الكبرى أو عند إجراء تغييرات جوهرية في البنية التنظيمية أو التقنية • قبل إطلاق منتجات وخدمات جديدة
3.1.4	المستوى الثاني	أتمتة أنشطة تقييم المخاطر من خلال استخدام أدوات مخصصة (مثل أداة الحوكمة وإدارة المخاطر والإلتزام).
3.1.5	المستوى الثالث	مراجعة وتحسين **[متطلبات تقييم مخاطر الأمن السيبراني]** 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
٣,٢	معالجة ومراقبة مخاطر الأمن السيبراني	
الضوابط		
3.2.1	المستوى الأول	تحديد **[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 تتكون من الأنشطة المتعلقة بمراقبة المخاطر المحددة، ومراقبة تنفيذ خطة معالجة المخاطر بشكل دوري، بالإضافة إلى مراقبة المخاطر المتبقية، وحالة المخاطر المقبولة.
3.2.4	المستوى الثاني	أتمتة أنشطة معالجة ومراقبة المخاطر من خلال استخدام أدوات مخصصة (مثل أداة الحوكمة وإدارة المخاطر والإلتزام).
3.2.5	المستوى الثالث	مراجعة وتحسين **[متطلبات معالجة ومراقبة مخاطر الأمن السيبراني]** 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

٤. الأمن المنطقي

٤,١	التشفير	
الضوابط		
4.1.1	المستوى الأول	تحديد **[متطلبات التشفير]** مع مراعاة ما يلي: • تحديد بروتوكولات وتقنيات التشفير الأساسية (على سبيل المثال AES 256، وRSA 2048، وPKI) بالإضافة إلى القيود ذات الصلة (مثل الشهادات الموقعة ذاتيًا، MD-5) • الحالات التي ينبغي بموجبها تطبيق بروتوكولات التشفير المعتمدة (أثناء نقل وتخزين واستخدام البيانات) مع مستوى الحماية المطلوب.
4.1.2	المستوى الأول	إعداد قائمة **[حلول التشفير]** (مثل المنتجات والخوارزميات والبروتوكولات) وفقًا للقيود ذات الصلة (مثل 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) ووفقًا 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	مراجعة وتحسين **[متطلبات التشفير]** وقائمة **[حلول التشفير]** المعتمدة وكذلك فاعلية حلول التشفير المستخدمة 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

٤,٢	إدارة التغيير	
الضوابط		
4.2.1	المستوى الأول	تحديد **[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 (مثل تطبيق حزم التحديثات والإصلاحات، أو تغييرات الإعدادات كجزء من المعالجة، أو ترقية الأنظمة، أو استخدام معدات جديدة).
4.2.3	المستوى	التخطيط للتغييرات المحددة واختبارها وتقييم الأثر المحتمل **[تقييم مخاطر الأمن**

	الأول	**السيبراني]** للتغيرات على الأمن السيبراني، والإبلاغ عن التغييرات، والحصول على موافقة المسؤولين (الموظفين/اللجنة).
4.2.4	المستوى الثاني	تحسين وتنفيذ **[متطلبات إدارة التغيير]** لمراعاة الإجراءات الخاصة بالتغيير في حالات الطوارئ.
4.2.5	المستوى الثالث	مراجعة وتحسين **[متطلبات إدارة التغيير]** وكذلك **{عملية إدارة التغيير}** بشكل مستمر.
المراجع		ISO 27002 - 12.1.2 NCA ECC - 1-6-2 NCA CSCC -1-6-2
٤,٣	إدارة الثغرات	
الضوابط		
4.3.1	المستوى الأول	تحديد **[متطلبات إدارة الثغرات]** مع مراعاة ما يلي: • النطاق، والأدوات، والتقنية، ورفع التقارير • معدل تكرار عمليات الفحص • الأطر الزمنية لعلاج الثغرات (بناءً على الخطورة)
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 وفقًا لمعدل التكرار المحدد في **[متطلبات إدارة الثغرات]** (على سبيل المثال، الفحص شهريًا للأنظمة الحساسة) • التحليل: تحليل أثر وجود ثغرات على الأصول المعلوماتية الحساسة وتحديد مستوى خطورتها. تحديد وتعيين الأطر الزمنية (اعتمادًا 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 (مثل إصدار منتج، وتغيير تقني جوهري، وإضافة معدات جديدة إلى الشبكات).
4.3.4	المستوى الثاني	استخدام أدوات الفحص المتخصصة والمؤتمتة (مثل الأدوات المخصصة لخوادم الويب وتطبيقات الأجهزة المحمولة).
4.3.5	المستوى الثالث	تحسين تصنيف الثغرات وإعداد التقارير بناءً على المدخلات الواردة من مصادر أخرى (مثل اختبار الاختراق، والمعلومات الاستباقية).
4.3.6	المستوى الثالث	مراجعة وتحسين **[متطلبات إدارة الثغرات]** بالإضافة إلى **{عملية إدارة الثغرات}** 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
٤,٤	إدارة حزم التحديثات والإصلاحات	
الضوابط		
4.4.1	المستوى الأول	تحديد **[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	المستوى الأول	تحديد وتنفيذ **{عملية إدارة حزم التحديثات والإصلاحات}** التي تساهم في 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 (مثل 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	مراجعة وتحسين **[متطلبات إدارة حزم التحديثات والإصلاحات]** بشكل مستمر بالإضافة إلى **{عملية إدارة حزم التحديثات والإصلاحات}**.
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
٤,٥	أمن الشبكات	

الضوابط		
4.5.1	المستوى الأول	تحديد **[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 (مثل 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، مثل 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). تعطيل البروتوكولات غير المستخدمة (على سبيل المثال IPv6 إذا لم يكن مستخدماً) في الأجهزة لتقليل احتمالية الهجوم على الشبكة.
4.5.5	المستوى الأول	حماية المعلومات أثناء نقلها (على سبيل المثال، من الاعتراض والنسخ والتعديل) من خلال شبكة الجهة والتأكد من الحفاظ على سرية وسلامة المعلومات (على سبيل المثال من خلال التشفير).
4.5.6	المستوى الأول	فصل وتقسيم الشبكة إلى مناطق (مثل نطاقات وشبكات فرعية) بناءً على أهمية الأصول المعلوماتية أو الخدمات الموجودة في تلك المناطق (مثل 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 وإدارة الصلاحيات الهامة والحساسة]**.
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 والعمل 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 Malicious Traffic)
4.5.11	المستوى الثاني	تحسين وتنفيذ **[متطلبات أمن الشبكات]** للتعامل مع الهجمات الداخلية والخارجية (مثل هجمات تعطيل الخدمات DoS/هجمات تعطيل الخدمات الموزعة DDoS) ضد شبكة الجهة.
4.5.12	المستوى الثاني	ضمان توفر آليات في مرافق الجهة لاكتشاف ومعالجة التحميل الزائد على الشبكة والذي يؤدي إلى انقطاع الخدمات (مثل إنشاء مرافق إضافية لتحقيق التوازن في أحمال الاستخدام بالشبكة).
4.5.13	المستوى الثاني	استخدام أدوات محددة لتحليل وتصفية جميع حركات البيانات (مثل تصفية المنافذ ports، التصفية القائمة على الاستضافة host based filtering) لاكتشاف

		أي حركة مرور غير مصرح بها في الشبكة.
4.5.14	المستوى الثالث	مراجعة وتحسين **[متطلبات أمن الشبكات]** وكذلك الضوابط اللازمة لتأمين شبكة الاتصالات في الجهة بشكل مستمر.
المراجع		ISO 27002 - 13.1.1 ISO 27002 - 13.1.3 ISO 27002 - 13.2.1 ISO 27011 - 13.1.3 ISO 27011 - 13.1.4 ISO 27011 - 13.1.5 ISO 27011 - 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
٤,٦	سجل الأحداث والمراقبة	
الضوابط		
4.6.1	المستوى الأول	تحديد **[متطلبات سجل الأحداث والمراقبة]** مع مراعاة ما يلي: • تسجيل الأحداث (التي يجب مراقبتها) المتعلقة بالأصول المعلوماتية التي تملكها الجهة • مراقبة سجلات الأحداث وتحليل الأحداث المكتشفة • مدة الاحتفاظ المطلوبة وحماية سجلات الأحداث
4.6.2	المستوى الأول	تنشيط تسجيل الأحداث (مثل أنشطة المستخدم، والاستثناءات، وأحداث أمن المعلومات، 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 المتطلبات (على سبيل المثال ١٢ شهرًا).
4.6.6	المستوى الثاني	جمع الأحداث ومراقبتها وتحليلها باستخدام أداة إدارة السجلات (مثل 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	تحسين طرق كشف الأحداث من خلال استخدام أدوات مخصصة (مثل أدوات

	الثاني	المعلومات الاستباقية) لتحديث قواعد الاكتشاف الخاصة بأدوات إدارة السجل.
4.6.9	المستوى الثالث	مراجعة وتحسين **[متطلبات سجل الأحداث والمراقبة]** وكذلك فاعلية سجلات الأحداث والمراقبة بشكل مستمر.
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
٤,٧		إدارة هويات الدخول والصلاحيات وإدارة الصلاحيات الهامة والحساسة
الضوابط		
4.7.1	المستوى الأول	تحديد **[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) • تحديد 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 (مثل التحكم بالوصول بناءً على الدور الوظيفي) • إعادة تعيين صلاحيات دخول المستخدمين في حالة تغير وظائف العمل (مثل تغيير الإدارات) • إدارة التحقق من هوية المستخدم وصلاحياته بناءً على مبادئ التحكم بالوصول (مثل 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 (مثل إنهاء العمل مع الجهة، تغيير الإدارات)
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 (مثل استخدام كلمات مرور قوية، والتغيير المنتظم لكلمة المرور) 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 الأول	إقفال الحسابات بعد عدد معين من محاولات تسجيل الدخول الفاشلة (على سبيل المثال، ٥ محاولات تسجيل دخول) والتحقيق في تكرار إقفال الحساب قبل تفعيل صلاحية الدخول **[سجل الأحداث والمراقبة].**
4.7.7	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).
4.7.8	المستوى الثاني	تحسين وتنفيذ **[متطلبات إدارة هويات الدخول والصلاحيات]** لاستخدام الأدوات لأتمتة وإدارة هويات الدخول والصلاحيات بشكل مركزي.
4.7.9	المستوى الثاني	استخدام أنظمة مخصصة للمهام التي تتطلب الوصول الإداري للأنظمة (Administrative Access).
4.7.10	المستوى الثالث	مراجعة وتحسين **[متطلبات إدارة هويات الدخول والصلاحيات]** 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
٤,٨		السماح بقائمة محددة من التطبيقات (القائمة البيضاء للتطبيقات)
الضوابط		
4.8.1	المستوى الأول	تحديد **[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 (مثل *.dll، و*.ocx، و*.so) والبرامج النصية الموقعة رقميًا (مثل *.ps1، و*.py، وmacros).
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	مراجعة وتحسين **[متطلبات القائمة البيضاء للتطبيقات]** وكذلك فاعلية القائمة

	الثالث	البيضاء للتطبيقات بشكل مستمر.
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
٤,٩	إدارة الحوادث	
الضوابط		
4.9.1	المستوى الأول	تحديد **[متطلبات إدارة الحوادث]** مع مراعاة ما يلي: • تعريف الحادثة، وتحديدها، وتصنيفها، وتحديد أولوياتها، وطرق الاستجابة لها • هيكل الإبلاغ عن الحوادث • اختبار عملية الاستجابة للحوادث • جمع الأدلة • التعلم 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 مسبقًا 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 الحوادث الكبرى وتفاصيلها لهيئة الاتصالات وتقنية المعلومات.
4.9.3	المستوى الأول	إجراء تدريبات منتظمة لاختبار **{عملية الاستجابة للحوادث}** للتأكد من فعاليتها (مثل 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 حوادث 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 الاستفادة من المعرفة المكتسبة من حوادث الأمن السيبراني لتقليل احتمالية وآثار وقوع حوادث أمن سيبراني مستقبلية.
4.9.8	المستوى الثالث	مراجعة وتحسين **[متطلبات إدارة الحوادث]** و**{عملية الاستجابة للحوادث}** المرتبطة بها 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
٤,١٠	التعامل مع البرمجيات الضارة	
الضوابط		
4.10.1	المستوى الأول	تحديد **[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 برنامج حماية نقطة النهاية على الأجهزة وضمان التحديث لقاعدة بيانات المعرفة المسبقة بانتظام. اتخاذ 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 (مثل استخدام أدوات تحليل وتصفية الإنترنت وأدوات تصفية رسائل البريد الإلكتروني لحظر رسائل التصيد وتقييد عملية تنزيل محتوى خطر) **[حماية البريد الإلكتروني والويب].**
4.10.4	المستوى الأول	اتخاذ تدابير وقائية لحماية الوسائط المتنقلة من البرمجيات الضارة (مثل إجراء فحص لمكافحة البرمجيات الضارة للوسائط المتنقلة عند إدخالها أو توصيلها).
4.10.5	المستوى الثاني	تطبيق تقنيات متقدمة للكشف عن البرمجيات الضارة (مثل تفعيل تسجيل الاستعلام عن نظام أسماء النطاقات DNS لاكتشاف عمليات البحث عن اسم المضيف للنطاقات الضارة المعروفة).
4.10.6	المستوى الثاني	استخدام أدوات سجل الأحداث والمراقبة المتقدمة لتحليل أحداث البرمجيات الضارة التي تم اكتشافها والتحذير منها **[سجل الأحداث والمراقبة].**
4.10.7	المستوى الثالث	مراجعة وتحسين **[متطلبات التعامل مع البرمجيات الضارة]** بشكل مستمر، وكذلك الضوابط التقنية المستخدمة لحماية الأصول المعلوماتية من انتشار البرمجيات الضارة.
المراجع		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
٤,١١	حماية المعلومات	

الضوابط		
4.11.1	المستوى الأول	تحديد **[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	المستوى الأول	تحديد وتنفيذ **{عملية تصنيف المعلومات}** مع مراعاة: • تصنيف المعلومات بناءً على معايير التصنيف المحددة في المتطلبات • التعامل مع المعلومات الحساسة وفقًا للمعايير المحددة (مثل القيمة التجارية، والمتطلبات القانونية والتقنية والوطنية والدولية)
4.11.3	المستوى الأول	تنفيذ آليات أمنية لحماية المعلومات (أثناء النقل، والتخزين، والاستخدام) مع الأخذ في الاعتبار **[متطلبات التشفير]** وتقنيات منع فقدان البيانات.
4.11.4	المستوى الأول	منع نقل المعلومات من بيئة الإنتاج إلى بيئة أخرى واستخدام بيانات الأنظمة الحساسة في بيئات الاختبار والتطوير.
4.11.5	المستوى الثاني	تحديد مدة الاحتفاظ بالمعلومات وفقًا للمتطلبات التنظيمية والتشريعات ذات الصلة و حصر الاحتفاظ بالمعلومات اللازمة في بيئة الإنتاج على الأنظمة الحساسة.
4.11.6	المستوى الثالث	مراجعة وتحسين **[متطلبات حماية المعلومات]** والعمليات المرتبطة بها 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
٤,١٢	إدارة النسخ الاحتياطي والاستعادة	
الضوابط		
4.12.1	المستوى الأول	تحديد **[متطلبات إدارة النسخ الاحتياطي والاستعادة]** مع مراعاة ما يلي: • نطاق النسخ الاحتياطي المتصل وغير المتصل بما فيه مدة الاحتفاظ • سرعة 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}** المكونة من نطاق النسخ الاحتياطية المتصلة وغير المتصلة وشمولها للأصول المعلوماتية (مثل عمليات النسخ الاحتياطي للنظام كاملا).
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	تنفيذ {**عملية النسخ الاحتياطي**} عن طريق إجراء نسخ احتياطية للأصول المعلوماتية بشكل دوري بناءً على متطلبات العمل (على سبيل المثال الهدف الخاص بوقت الاستعادة).
4.12.5	المستوى الأول	ضمان الحماية المناسبة للنسخ الاحتياطية عن طريق الأمن المادي **[تأمين المعدات والمناطق].**
4.12.6	المستوى الثاني	إنشاء موقع تخزين/نسخ احتياطي بديل يوفر تدابير أمنية مكافئة للموقع الأساسي.
4.12.7	المستوى الثاني	ضمان سرية النسخ الاحتياطية، وسلامتها، وتوافرها في الأوضاع المضادة (مثل استخدام التشفير).
4.12.8	المستوى الثاني	اختبار ومراجعة {**عمليات النسخ الاحتياطي**} {**والاستعادة**} للتحقق من فعاليتها بشكل مستمر.
4.12.9	المستوى الثاني	تحسين وتنفيذ **[متطلبات إدارة النسخ الاحتياطي]** باستخدام أدوات لأتمتة عمليات {**النسخ الاحتياطي**} {**والاستعادة**}.
4.12.10	المستوى الثالث	مراجعة وتحسين **[متطلبات إدارة النسخ الاحتياطي]** والعمليات المرتبطة بها 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
٤,١٣		إدارة الإعدادات والتحصين
الضوابط		
4.13.1	المستوى الأول	تحديد **[متطلبات إدارة الإعدادات والتحصين]** مع مراعاة ما يلي: • تأمين النسخ والإعدادات الأساسية للأصول المعلوماتية والبرمجيات/الأجهزة المستخدمة
4.13.2	المستوى الأول	تطبيق ضبط الإعدادات الأساسية المحددة للأصول المعلوماتية.
4.13.3	المستوى الأول	استخدام تحصين الأنظمة والأجهزة وفقًا لأفضل الممارسات المعترف بها في الصناعة (مثل تعطيل الإعدادات الافتراضية التي تم تثبيتها على أجهزة الشبكة).
4.13.4	المستوى الأول	تقييد استخدام الوظائف غير الضرورية (مثل 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 آليًا **[إدارة التغيير]** على جميع الأصول المعلوماتية.
4.13.8	المستوى الثالث	مراجعة وتحسين **[متطلبات إدارة الإعدادات والتحصين]** بشكل 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
٤,١٤	تطوير البرمجيات الآمنة	
الضوابط		
4.14.1	المستوى الأول	تحديد **[متطلبات تطوير البرمجيات الآمنة]** مع مراعاة ما يلي: • استخدام المعايير الأمنية لتطوير البرامج والتطبيقات (مثل المكتبات المعتمدة، 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 وإدارة الصلاحيات الهامة والحساسة]**.
4.14.3	المستوى الأول	استخدام المعايير والممارسات الأمنية لشفرة البرمجيات والتطبيقات (مثل مبادئ الأمن حسب التصميم المدعومة بأدوات التحليل الثابتة أو الديناميكية) وضمان التكامل الأمني بين التطبيقات.
4.14.4	المستوى الأول	ضمان النقل الآمن والموثوق للبرمجيات بين البيئات.
4.14.5	المستوى الأول	استخدام مكونات الطرف الخارجي الموثوقة والحديثة للبرمجيات المطورة داخليًا.
4.14.6	المستوى الثاني	إجراء وتوثيق مراجعة أمنية للبرمجيات المطورة والشفرة المصدرية (على سبيل المثال إجراء فحص الأخطاء لجميع مدخلات البرمجيات والتطبيقات المطورة). إجراء اختبارات أمنية للتحقق من مدى امتثال البرمجيات المطورة لمتطلبات الأمن السيبراني للجهة.
4.14.7	المستوى الثالث	مراجعة وتحسين **[متطلبات تطوير البرمجيات الآمنة]** بشكل مستمر.
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
٤,١٥	حماية البريد الإلكتروني ومتصفح الويب	
الضوابط		

4.15.1	المستوى الأول	تحديد **[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 (مثل قواعد جدار الحماية وأدوات تصفية عناوين URL).
4.15.4	المستوى الثالث	مراجعة 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
٤,١٦	اختبار الاختراق	
الضوابط		
4.16.1	المستوى الثاني	تحديد **[متطلبات اختبار الاختراق]** مع مراعاة ما يلي: • الغرض من اختبارات الاختراق وأهدافها العامة • تحديد تكرار إجراء اختبارات الاختراق
4.16.2	المستوى الثاني	تحديد **{عملية اختبار الاختراق}** التي تتكون من نطاق اختبارات الاختراق باستخدام منهجيات موحدة لتحديد الثغرات غير المعروفة (مثل اختبار الصندوق الرمادي واختبار الصندوق الأبيض) ومعدل تكرارها (على سبيل المثال مرة واحدة كل ثلاثة أشهر على الأقل للأصول المعلوماتية الحساسة).
4.16.3	المستوى الثاني	اعتمادًا على منهجية اختبار الاختراق المستخدمة، يمكن استخدام **[تقرير الثغرات]** كمدخل لتوجيه اختبارات الاختراق.
4.16.4	المستوى الثاني	رفع **[تقرير اختبار الاختراق]** إلى الأطراف المعنية للبدء في إجراءات المعالجة عند الحاجة **[إدارة حزم التحديثات والإصلاحات]**.
4.16.5	المستوى الثالث	مراجعة وتحسين **[متطلبات اختبار الاختراق]** بشكل مستمر وكذلك الطرق المستخدمة في إجراء اختبارات الاختراق والعمليات المرتبطة بها.
المراجع		SANS v6.1 – 20.1 SANS v6.1 – 20.6 NCA ECC – 2-11 NCA CSCC – 2-10

٥. الأمن المادي

٥,١	تأمين المعدات والمناطق	
الضوابط		
5.1.1	المستوى الأول	تحديد **[متطلبات تأمين المعدات والمناطق]** مع مراعاة ما يلي: • حماية المعدات والمرافق المادية • مناطق التوصيل والشحن • نقل المعدات
5.1.2	المستوى الأول	تحديد المحيط الأمني (مع مراعاة **[متطلبات إدارة الأصول]**) من أجل حماية المرافق المادية (مثل المكاتب، والغرف، ومراكز البيانات، والمحطات الأرضية، ومعدات معالجة الاتصالات) التي تحتوي على أصول معلوماتية حساسة أو هامة.
5.1.3	المستوى الأول	التأكد من وجود المعدات داخل مناطق أمنية مناسبة وتخزينها في مرافق مادية آمنة خلال ساعات خارج العمل.
5.1.4	المستوى الأول	تأمين مناطق التوصيل/الشحن التي يمكن استخدامها من قبل أفراد غير مصرح لهم بالدخول إلى مباني الجهة (مثل الفصل المادي، إن أمكن، للشحنات الواردة والصادرة).
5.1.5	المستوى الأول	حماية المعدات من التلف الناتج عن التهديدات البيئية والمخاطر والوصول غير المصرح به. بالإضافة إلى ذلك، يتم مراعاة العوامل التالية لحماية المعدات: • انقطاعات التيار الكهربائي (نتيجة فشل المرافق الداعمة) • تأمين الكابلات من التداخل أو التلف فضلاً عن الإدارة المناسبة للكابلات (مثل وضع علامات على الكابلات أو ترميزها بالألوان) • تشغيل المعدات وفقًا للمتطلبات المحددة من الشركة المصنعة والتحكم في مناخ العمل (مثل درجة الحرارة والرطوبة وجودة الهواء والمياه والضوء) • الحماية من الوصول غير المصرح به (مثل المراقبة من خلال الدوائر التلفزيونية المغلقة) • سياسة المكتب النظيف والشاشة الخالية (مثل تأمين المعلومات الحساسة المخزنة على الأوراق في مكان آمن، وإغلاق شاشات أجهزة الكمبيوتر و/أو الوحدات الطرفية في حالة عدم الاستخدام أو عدم المراقبة).
5.1.6	المستوى الأول	حماية المعدات أثناء نقلها مع الأخذ في الاعتبار على سبيل المثال المخاطر المتوقعة، والتأمين أثناء النقل
5.1.7	المستوى الثالث	مراجعة وتحسين **[متطلبات تأمين المعدات والمناطق]** بشكل مستمر.
المراجع		ISO 27002 - 11.1.1 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 NCA ECC - 2-14-1 NCA ECC - 2-14-2 NCA ECC - 2-14-3 NCA ECC - 2-14-4
٥,٢	إدارة الوصول المادي	
الضوابط		
5.2.1	المستوى الأول	تحديد **[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]** والموافقة عليها 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 (مثل المفاتيح الآمنة) إلى المرافق المادية وإدارتها.
5.2.4	المستوى الأول	إنشاء ضوابط الدخول المادي للزوار (مثل توفير شارات أمنية للزوار ومراقبة الأنشطة مشبوهة).
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	مراجعة وتحسين **[متطلبات إدارة الوصول المادي]** بشكل مستمر وكذلك فاعلية الضوابط المستخدمة للتعامل مع إدارة الوصول المادي.
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
٥,٣	الحماية البيئية	
الضوابط		
5.3.1	المستوى الأول	تحديد **[متطلبات الحماية البيئية]** مع مراعاة ما يلي: • تحديد تدابير الحماية المادية ضد التهديدات البيئية الداخلية والخارجية
5.3.2	المستوى الأول	تنفيذ تدابير الحماية المادية (على سبيل المثال استخدام وصيانة أجهزة/أنظمة الكشف عن الحرائق وإخمادها) ضد التهديدات والمخاطر البيئية الداخلية (مثل الحوادث، انقطاعات التيار الكهربائي، وغيرها من أوجه التعطيل الناجمة عن الفشل في المرافق الداعمة) والخارجية (مثل الكوارث الطبيعية).
5.3.3	المستوى الثالث	مراجعة وتحسين **[متطلبات الحماية البيئية]** بشكل مستمر وكذلك فاعلية الضوابط الموضوعة لحالات الطوارئ.
المراجع		ISO 27002 - 11.1.4 ISO 27002 - 11.2.2

		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 NCA ECC - 3-1
٥,٤	الأصول خارج الموقع	
الضوابط		
5.4.1	المستوى الأول	تحديد **[متطلبات الأصول خارج الموقع]** مع مراعاة ما يلي: • حماية المعدات والمرافق المادية المثبتة في مباني العمل خارج الموقع • خدمات الاتصالات المترابطة
5.4.2	المستوى الأول	اتخاذ التدابير الأمنية المناسبة لحماية معدات الجهة المثبتة خارج الموقع الرئيسي (مثل مواقع العمل البديلة والمواقع المشتركة) والتأكد من أن الأصول الموجودة خارج الموقع مؤمنة بشكل فعّال (على سبيل المثال ضد التهديدات المادية والبيئية).
5.4.3	المستوى الأول	تحديد الحدود والواجهات الواضحة المعالم مع جهات الأخرى التي تقدم خدمات الاتصالات في حالة ترابط خدمات الاتصالات.
5.4.4	المستوى الثالث	مراجعة وتحسين **[متطلبات الأصول خارج الموقع]** بشكل مستمر وكذلك فاعلية ضوابط الأمن السيبراني لحماية الأصول خارج الموقع.
المراجع		ISO 27011 - X.1051 - 11.1.9 ISO 27011 - X.1051 - 11.3.1 ISO 27011 - X.1051 - 11.3.3 NIST.sp.800-53r4 PE-17

٦. الأمن السيبراني المتعلق بالأطراف الخارجية

٦,١	الخدمات السحابية	
الضوابط		
6.1.1	المستوى الأول	تحديد **[متطلبات الخدمات السحابية]** مع مراعاة ما يلي: • تقييم مخاطر الخدمات السحابية • تحديد متطلبات الأمن السيبراني المتوقعة من مقدم الخدمات السحابية • اتفاقيات مستوى الخدمة
6.1.2	المستوى الأول	إجراء تقييم المخاطر وفقًا لـ**[متطلبات تقييم مخاطر الأمن السيبراني]** قبل اعتماد الخدمات السحابية (أو في حالة حدوث تغييرات في المتطلبات التشريعية والتنظيمية ذات الصلة) لضمان معالجة المخاطر المتعلقة باستخدام الخدمات السحابية بشكل مناسب.
6.1.3	المستوى الأول	تحديد متطلبات الأمن السيبراني (مثل تصنيف البيانات قبل الاستضافة على الخدمة السحابية، وحماية سرية بيانات الجهة وسلامتها وتوافرها، وفصل بيانات الجهة في الخدمة السحابية عن البيانات الأخرى) والتي يجب أن يلتزم بها مقدم الخدمة السحابية بناء على **{تصنيف المعلومات}**.
6.1.4	المستوى الأول	إعداد اتفاقيات مستوى الخدمة مع مقدم الخدمة السحابية التي تأخذ بعين الاعتبار بحد أدنى ما يلي: • متطلبات الأمن السيبراني المحددة مسبقًا • إجراءات الاتصال والتصعيد في حالة وقوع حادثة أمن سيبراني • الحق في إنهاء الخدمة السحابية (إرجاع بيانات الجهة في صيغة قابلة للاستخدام، حذف بيانات الجهة نهائيًا)
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	مراجعة وتحسين **[متطلبات الخدمة السحابية]** بشكل مستمر وكذلك الإجراءات المتضمنة في اختيار الخدمات السحابية ومتطلبات الأمن السيبراني المتوقعة.
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
٦,٢	خدمات الإسناد الخارجي	

الضوابط		
6.2.1	المستوى الأول	تحديد **[متطلبات خدمات الإسناد الخارجي]** مع مراعاة ما يلي: • تقييم المخاطر الخاصة بخدمات الإسناد للأطراف الخارجية. • معالجة متطلبات الأمن السيبراني المتوقعة من مقدم الخدمة الخارجي • اتفاقيات مستوى الخدمة
6.2.2	المستوى الأول	إجراء تقييم المخاطر وفقًا **[متطلبات تقييم مخاطر الأمن السيبراني]** قبل التعاقد على خدمات الإسناد الخارجي (أو في حالة حدوث تغييرات في المتطلبات التشريعية والتنظيمية ذات الصلة) لضمان معالجة المخاطر المتعلقة باستخدام خدمات الإسناد بشكل مناسب.
6.2.3	المستوى الأول	تحديد متطلبات الأمن السيبراني التي يجب أن يلتزم بها مقدم الخدمة الخارجي (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 المحددة مسبقًا • إجراءات الاتصال والتصعيد في حالة وقوع حادثة أمن سيبراني • الحق في إنهاء الالتزام التعاقدي مع مقدم الخدمة الخارجي
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	مراجعة وتحسين **[متطلبات الإسناد الخارجي]** بشكل مستمر وكذلك الإجراءات المتضمنة في اختيار مقدم الخدمة الخارجي ومتطلبات الأمن السيبراني المتوقعة.
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

المراجع

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

- 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)
- ETSI TR 103 305 - 2.11 (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)
- الأطر الوطنية والقطاعية (الضوابط الأساسية للأمن السيبراني ٢٠١٨ الصادرة عن الهيئة الوطنية للأمن السيبراني، وضوابط الأمن السيبراني للأنظمة الحساسة ٢٠١٨ الصادرة عن الهيئة الوطنية للأمن السيبراني)