٢ تعزيز الأمن السيبراني (Cybersecurity Defense)

٢-١	إدارة الأصول (Asset Management)
الهدف	للتأكد من أن الجهة لديها قائمة جرد دقيقة وحديثة للأصول تشمل التفاصيل ذات العلاقة لجميع الأصول المعلوماتية والتقنية المتاحة للجهة، من أجل دعم العمليات التشغيلية للجهة ومتطلبات الأمن السيبراني، لتحقيق سرية وسلامة الأصول المعلوماتية والتقنية للجهة ودقتها وتوافرها.
الضوابط	
٢-١-١	يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني لإدارة الأصول المعلوماتية والتقنية للجهة.
٢-١-٢	يجب تطبيق متطلبات الأمن السيبراني لإدارة الأصول المعلوماتية والتقنية للجهة.
٢-١-٣	يجب تحديد وتوثيق واعتماد ونشر سياسة الاستخدام المقبول للأصول المعلوماتية والتقنية للجهة.
٢-١-٤	يجب تطبيق سياسة الاستخدام المقبول للأصول المعلوماتية والتقنية للجهة.
٢-١-٥	يجب تصنيف الأصول المعلوماتية والتقنية للجهة وترميزها (Labeling) والتعامل معها وفقاً للمتطلبات التشريعية والتنظيمية ذات العلاقة.
٢-١-٦	يجب مراجعة متطلبات الأمن السيبراني لإدارة الأصول المعلوماتية والتقنية للجهة دورياً.
٢-٢	إدارة هويات الدخول والصلاحيات (Identity and Access Management)
الهدف	ضمان حماية الأمن السيبراني للوصول المنطقي (Logical Access) إلى الأصول المعلوماتية والتقنية للجهة من أجل منع الوصول غير المصرح به وتقييد الوصول إلى ما هو مطلوب لإنجاز الأعمال المتعلقة بالجهة.
الضوابط	
٢-٢-١	يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني لإدارة هويات الدخول والصلاحيات في الجهة.
٢-٢-٢	يجب تطبيق متطلبات الأمن السيبراني لإدارة هويات الدخول والصلاحيات في الجهة.
٢-٢-٣	يجب أن تغطي متطلبات الأمن السيبراني المتعلقة بإدارة هويات الدخول والصلاحيات في الجهة بحد أدنى ما يلي: ٢-٢-٣-١ التحقق من الهوية أحادي العنصر (Single-factor authentication) بناءً على إدارة تسجيل المستخدم، وإدارة كلمة المرور. ٢-٢-٣-٢ التحقق من الهوية متعدد العناصر (Multi-Factor Authentication) وتحديد عناصر التحقق المناسبة وعددها وكذلك تقنيات التحقق المناسبة بناء على نتائج تقييم الأثر المحتمل لفشل عملية التحقق وتخطيها، وذلك لعمليات الدخول عن بعد والحسابات ذات الصلاحيات الهامة والحساسة. ٢-٢-٣-٣ إدارة تصاريح وصلاحيات المستخدمين (Authorization) بناءً على مبادئ التحكم بالدخول والصلاحيات (مبدأ الحاجة إلى المعرفة والاستخدام "Need-to-know and Need-to-use"، ومبدأ الحد الأدنى من الصلاحيات والامتيازات "Least Privilege"، ومبدأ فصل المهام "Segregation of Duties"). ٢-٢-٣-٤ إدارة الصلاحيات الهامة والحساسة (Privileged Access Management). ٢-٢-٣-٥ المراجعة الدورية لهويات الدخول والصلاحيات.
٢-٢-٤	يجب مراجعة تطبيق متطلبات الأمن السيبراني لإدارة هويات الدخول والصلاحيات في الجهة دورياً.
٢-٣	حماية الأنظمة وأجهزة معالجة المعلومات (Information System and Processing Facilities Protection)
الهدف	ضمان حماية الأنظمة وأجهزة معالجة المعلومات بما في ذلك أجهزة المستخدمين والبنى التحتية للجهة من المخاطر السيبرانية.
الضوابط	
٢-٣-١	يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني لحماية الأنظمة وأجهزة معالجة المعلومات للجهة.
٢-٣-٢	يجب تطبيق متطلبات الأمن السيبراني لحماية الأنظمة وأجهزة معالجة المعلومات للجهة.
٢-٣-٣	يجب أن تغطي متطلبات الأمن السيبراني لحماية الأنظمة وأجهزة معالجة المعلومات للجهة بحد أدنى ما يلي:

	٢-٣-٣-١ الحماية من الفيروسات والبرامج والأنشطة المشبوهة والبرمجيات الضارة (Malware) على أجهزة المستخدمين والخوادم باستخدام تقنيات وآليات الحماية الحديثة والمتقدمة، وإدارتها بشكل آمن. ٢-٣-٣-٢ التقييد الحازم لاستخدام أجهزة وسائط التخزين الخارجية والأمن المتعلق بها. ٢-٣-٣-٣ إدارة حزم التحديثات والإصلاحات للأنظمة والتطبيقات والأجهزة (Patch Management). ٢-٣-٣-٤ مزامنة التوقيت (Clock Synchronization) مركزياً ومن مصدر دقيق وموثوق، ومن هذه المصادر ما توفره الهيئة السعودية للمواصفات والمقاييس والجودة.
٢-٣-٤	يجب مراجعة متطلبات الأمن السيبراني لحماية الأنظمة وأجهزة معالجة المعلومات للجهة دورياً.
٢-٤	حماية البريد الإلكتروني (Email Protection)
الهدف	ضمان حماية البريد الإلكتروني للجهة من المخاطر السيبرانية.
الضوابط	
٢-٤-١	يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني لحماية البريد الإلكتروني للجهة.
٢-٤-٢	يجب تطبيق متطلبات الأمن السيبراني لحماية البريد الإلكتروني للجهة.
٢-٤-٣	يجب أن تغطي متطلبات الأمن السيبراني لحماية البريد الإلكتروني للجهة بحد أدنى ما يلي: ٢-٤-٣-١ تحليل وتصفية (Filtering) رسائل البريد الإلكتروني (وخصوصاً رسائل التصيّد الإلكتروني "Phishing Emails" والرسائل الإقتحامية "Spam Emails") باستخدام تقنيات وآليات الحماية الحديثة والمتقدمة للبريد الإلكتروني. ٢-٤-٣-٢ التحقق من الهوية متعدد العناصر (Multi-Factor Authentication) وتحديد عناصر التحقق المناسبة وعددها وكذلك تقنيات التحقق المناسبة بناء على نتائج تقييم الأثر المحتمل لفشل عملية التحقق وتخطيها، وذلك للدخول عن بعد والدخول عن طريق صفحة موقع البريد الإلكتروني (Webmail). ٢-٤-٣-٣ النسخ الاحتياطي والأرشفة للبريد الإلكتروني. ٢-٤-٣-٤ الحماية من التهديدات المتقدمة المستمرة (APT Protection)، التي تستخدم عادة الفيروسات والبرمجيات الضارة غير المعروفة مسبقاً (Zero-Day Malware)، وإدارتها بشكل آمن. ٢-٤-٣-٥ توثيق مجال البريد الإلكتروني للجهة باستخدام إطار سياسة المرسل (Sender Policy Framework "SPF") والبريد المعرّف بمفاتيح النطاق (Domain Keys Identified Mail "DKIM") وسياسة مصادقة الرسائل والإبلاغ عنها (Domain Message Authentication Reporting and Conformance "DMARC").
٢-٤-٤	يجب مراجعة تطبيق متطلبات الأمن السيبراني الخاصة بحماية البريد الإلكتروني للجهة دورياً.
٢-٥	إدارة أمن الشبكات (Networks Security Management)
الهدف	ضمان حماية شبكات الجهة من المخاطر السيبرانية.
الضوابط	
٢-٥-١	يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني لإدارة أمن شبكات الجهة.
٢-٥-٢	يجب تطبيق متطلبات الأمن السيبراني لإدارة أمن شبكات الجهة.
٢-٥-٣	يجب أن تغطي متطلبات الأمن السيبراني لإدارة أمن شبكات الجهة بحد أدنى ما يلي: ٢-٥-٣-١ العزل والتقسيم المادي أو المنطقي لأجزاء الشبكات بشكل آمن، واللازم للسيطرة على مخاطر الأمن السيبراني ذات العلاقة، باستخدام جدار الحماية (Firewall) ومبدأ الدفاع الأمني متعدد المراحل (Defense-in-Depth). ٢-٥-٣-٢ عزل شبكة بيئة الإنتاج عن شبكات بيئات التطوير والاختبار. ٢-٥-٣-٣ أمن التصفح والاتصال بالإنترنت، ويشمل ذلك التقييد الحازم للمواقع الإلكترونية المشبوهة، ومواقع مشاركة وتخزين الملفات، ومواقع الدخول عن بعد. ٢-٥-٣-٤ أمن الشبكات اللاسلكية وحمايتها باستخدام وسائل آمنة للتحقق من الهوية والتشفير، وعدم ربط الشبكات اللاسلكية بشبكة الجهة الداخلية إلا بناءً على دراسة متكاملة للمخاطر المترتبة على ذلك والتعامل معها بما يضمن حماية الأصول التقنية للجهة. ٢-٥-٣-٥ قيود وإدارة منافذ وبروتوكولات وخدمات الشبكة. ٢-٥-٣-٦ أنظمة الحماية المتقدمة لاكتشاف ومنع الاختراقات (Intrusion Prevention Systems).