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: