

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