	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).

	٢-٥-٣-٧ أمن نظام أسماء النطاقات (DNS). ٢-٥-٣-٨ حماية قناة تصفح الإنترنت من التهديدات المتقدمة المستمرة (APT Protection)، التي تستخدم عادة الفيروسات والبرمجيات الضارة غير المعروفة مسبقاً (Zero-Day Malware)، وإدارتها بشكل آمن. ٢-٥-٣-٩ الحماية من هجمات تعطيل الشبكات (Distributed Denial of Service Attack "DDoS") للحد من المخاطر السيبرانية الناتجة عن هجمات تعطيل الشبكات.
٢-٥-٤	يجب مراجعة تطبيق متطلبات الأمن السيبراني لإدارة أمن شبكات الجهة دورياً.
٢-٦	أمن الأجهزة المحمولة (Mobile Devices Security)
الهدف	ضمان حماية أجهزة الجهة المحمولة (بما في ذلك أجهزة الحاسب المحمول والهواتف الذكية والأجهزة الذكية اللوحية) من المخاطر السيبرانية. وضمان التعامل بشكل آمن مع المعلومات الحساسة والمعلومات الخاصة بأعمال الجهة وحمايتها أثناء النقل والتخزين عند استخدام الأجهزة الشخصية للعاملين في الجهة (مبدأ "BYOD").
الضوابط	
٢-٦-١	يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني الخاصة بأمن الأجهزة المحمولة والأجهزة الشخصية للعاملين (BYOD) عند ارتباطها بشبكة الجهة.
٢-٦-٢	يجب تطبيق متطلبات الأمن السيبراني الخاصة بأمن الأجهزة المحمولة وأجهزة (BYOD) للجهة.
٢-٦-٣	يجب أن تغطي متطلبات الأمن السيبراني الخاصة بأمن الأجهزة المحمولة وأجهزة (BYOD) للجهة بحد أدنى ما يلي: ٢-٦-٣-١ فصل وتشفير البيانات والمعلومات (الخاصة بالجهة) المخزنة على الأجهزة المحمولة وأجهزة (BYOD). ٢-٦-٣-٢ الاستخدام المحدد والمقيد بناءً على ما تتطلبه مصلحة أعمال الجهة. ٢-٦-٣-٣ حذف البيانات والمعلومات (الخاصة بالجهة) المخزنة على الأجهزة المحمولة وأجهزة (BYOD) عند فقدان الأجهزة أو بعد انتهاء/إنهاء العلاقة الوظيفية مع الجهة. ٢-٦-٣-٤ التوعية الأمنية للمستخدمين.
٢-٦-٤	يجب مراجعة تطبيق متطلبات الأمن السيبراني الخاصة لأمن الأجهزة المحمولة وأجهزة (BYOD) للجهة دورياً.
٢-٧	حماية البيانات والمعلومات (Data and Information Protection)
الهدف	ضمان حماية السرية وسلامة بيانات ومعلومات الجهة ودقتها وتوافرها، وذلك وفقاً للسياسات والإجراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية ذات العلاقة.
الضوابط	
٢-٧-١	يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني لحماية بيانات ومعلومات الجهة، والتعامل معها وفقاً للمتطلبات التشريعية والتنظيمية ذات العلاقة.
٢-٧-٢	يجب تطبيق متطلبات الأمن السيبراني لحماية بيانات ومعلومات الجهة، حسب مستوى تصنيفها.
٢-٧-٣	يجب مراجعة تطبيق متطلبات الأمن السيبراني لحماية بيانات ومعلومات الجهة دورياً.
٢-٨	التشفير (Cryptography)
الهدف	ضمان الاستخدام السليم والفعال للتشفير لحماية الأصول المعلوماتية الإلكترونية للجهة، وذلك وفقاً للمعايير الوطنية للتشفير الصادرة من الهيئة، وللسياسات والإجراءات التنظيمية للجهة، وبناء على تقييم المخاطر، وبحسب المتطلبات التشريعية والتنظيمية ذات العلاقة.
الضوابط	
٢-٨-١	يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني للتشفير في الجهة.
٢-٨-٢	يجب تطبيق متطلبات الأمن السيبراني للتشفير في الجهة.
٢-٨-٣	يجب أن تغطي متطلبات الأمن السيبراني للتشفير بحد أدنى المتطلبات المذكورة في المعايير الوطنية للتشفير الصادرة من الهيئة، مع تطبيق مستوى التشفير المناسب، وذلك بحسب طبيعة ومستوى حساسية البيانات والأنظمة والشبكات وبناءً على تقييم المخاطر من قبل الجهة وحسب المتطلبات التشريعية والتنظيمية ذات العلاقة، وفقاً لما يلي: ٢-٨-٣-١ معايير أنظمة وحلول التشفير المعتمدة والقيود المطبقة عليها (تقنياً وتنظيمياً). ٢-٨-٣-٢ الإدارة الآمنة لمفاتيح التشفير خلال عمليات دورة حياتها.