	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.

	٢-٨-٣-٣ تشفير البيانات أثناء النقل والتخزين والمعالجة بناءً على تصنيفها وحسب المتطلبات التشريعية والتنظيمية ذات العلاقة.
٢-٨-٤	يجب مراجعة تطبيق متطلبات الأمن السيبراني للتشفير في الجهة دورياً.
٢-٩	إدارة النسخ الاحتياطية (Backup and Recovery Management)
الهدف	ضمان حماية بيانات ومعلومات الجهة والإعدادات التقنية للأنظمة والتطبيقات الخاصة بالجهة من الأضرار الناجمة عن المخاطر السيبرانية، وذلك وفقاً للسياسات والإجراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية ذات العلاقة.
الضوابط	
٢-٩-١	يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني لإدارة النسخ الاحتياطية للجهة.
٢-٩-٢	يجب تطبيق متطلبات الأمن السيبراني لإدارة النسخ الاحتياطية للجهة.
٢-٩-٣	يجب أن تغطي متطلبات الأمن السيبراني لإدارة النسخ الاحتياطية بحد أدنى ما يلي: ٢-٩-٣-١ نطاق النسخ الاحتياطية وشموليتها للأصول المعلوماتية والتقنية الحساسة. ٢-٩-٣-٢ القدرة السريعة على استعادة البيانات والأنظمة بعد التعرض لحوادث الأمن السيبراني. ٢-٩-٣-٣ إجراء فحص دوري لمدى فعالية استعادة النسخ الاحتياطية.
٢-٩-٤	يجب مراجعة تطبيق متطلبات الأمن السيبراني لإدارة النسخ الاحتياطية للجهة.
٢-١٠	إدارة الثغرات (Vulnerabilities Management)
الهدف	ضمان اكتشاف الثغرات التقنية في الوقت المناسب ومعالجتها بشكل فعال، وذلك لمنع أو تقليل احتمالية استغلال هذه الثغرات من قبل الهجمات السيبرانية وتقليل الآثار المترتبة على أعمال الجهة.
الضوابط	
٢-١٠-١	يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني لإدارة الثغرات التقنية للجهة.
٢-١٠-٢	يجب تطبيق متطلبات الأمن السيبراني لإدارة الثغرات التقنية للجهة.
٢-١٠-٣	يجب أن تغطي متطلبات الأمن السيبراني لإدارة الثغرات بحد أدنى ما يلي: ٢-١٠-٣-١ فحص واكتشاف الثغرات دورياً. ٢-١٠-٣-٢ تصنيف الثغرات حسب خطورتها. ٢-١٠-٣-٣ معالجة الثغرات بناءً على تصنيفها والمخاطر السيبرانية المترتبة عليها. ٢-١٠-٣-٤ إدارة حزم التحديثات والإصلاحات الأمنية لمعالجة الثغرات، على أن يتم التحقق من سلامة وفعالية تلك التحديثات والإصلاحات الأمنية على بيئة غير بيئة الإنتاج قبل تطبيقها. ٢-١٠-٣-٥ التواصل والاشتراك مع مصادر موثوقة فيما يتعلق بالتنبيهات المتعلقة بالثغرات الجديدة والمحدثة.
٢-١٠-٤	يجب مراجعة تطبيق متطلبات الأمن السيبراني لإدارة الثغرات التقنية للجهة دورياً.
٢-١١	اختبار الاختراق (Penetration Testing)
الهدف	تقييم واختبار مدى فعالية قدرات تعزيز الأمن السيبراني في الجهة، وذلك من خلال عمل محاكاة لتقنيات وأساليب الهجوم السيبراني الفعلية. ولاكتشاف نقاط الضعف الأمنية غير المعروفة والتي قد تؤدي إلى الاختراق السيبراني للجهة. وذلك وفقاً للمتطلبات التشريعية والتنظيمية ذات العلاقة.
الضوابط	
٢-١١-١	يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني لعمليات اختبار الاختراق في الجهة.
٢-١١-٢	يجب تنفيذ عمليات اختبار الاختراق في الجهة.
٢-١١-٣	يجب أن تغطي متطلبات الأمن السيبراني لاختبار الاختراق بحد أدنى ما يلي: ٢-١١-٣-١ نطاق عمل اختبار الاختراق، ليشمل جميع الخدمات المقدمة خارجياً (عن طريق الإنترنت) ومكوناتها التقنية، ومنها: البنية التحتية، المواقع الإلكترونية، تطبيقات الويب، تطبيقات الهواتف الذكية واللوحية، البريد الإلكتروني والدخول عن بعد. ٢-١١-٣-٢ عمل اختبار الاختراق دورياً.
٢-١١-٤	يجب مراجعة تطبيق متطلبات الأمن السيبراني لعمليات اختبار الاختراق في الجهة دورياً.