	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.