٢-١٢	إدارة سجلات الأحداث ومراقبة الأمن السيبراني (Cybersecurity Event Logs and Monitoring Management)
الهدف	ضمان تجميع وتحليل ومراقبة سجلات أحداث الأمن السيبراني في الوقت المناسب من أجل الاكتشاف الاستباقي للهجمات السيبرانية وإدارة مخاطرها بفعالية لمنع أو تقليل الآثار المترتبة على أعمال الجهة.
الضوابط	
٢-١٢-١	يجب تحديد وتوثيق واعتماد متطلبات إدارة سجلات الأحداث ومراقبة الأمن السيبراني للجهة.
٢-١٢-٢	يجب تطبيق متطلبات إدارة سجلات الأحداث ومراقبة الأمن السيبراني للجهة.
٢-١٢-٣	يجب أن تغطي متطلبات إدارة سجلات الأحداث ومراقبة الأمن السيبراني بحد أدنى ما يلي: ٢-١٢-٣-١ تفعيل سجلات الأحداث (Event logs) الخاصة بالأمن السيبراني على الأصول المعلوماتية الحساسة لدى الجهة. ٢-١٢-٣-٢ تفعيل سجلات الأحداث الخاصة بالحسابات ذات الصلاحيات الهامة والحساسة على الأصول المعلوماتية وأحداث عمليات الدخول عن بعد لدى الجهة. ٢-١٢-٣-٣ تحديد التقنيات اللازمة (SIEM) لجمع سجلات الأحداث الخاصة بالأمن السيبراني. ٢-١٢-٣-٤ المراقبة المستمرة لسجلات الأحداث الخاصة بالأمن السيبراني. ٢-١٢-٣-٥ مدة الاحتفاظ بسجلات الأحداث الخاصة بالأمن السيبراني (على ألا تقل عن ١٢ شهر).
٢-١٢-٤	يجب مراجعة تطبيق متطلبات إدارة سجلات الأحداث ومراقبة الأمن السيبراني في الجهة دورياً.
٢-١٣	إدارة حوادث وتهديدات الأمن السيبراني (Cybersecurity Incident and Threat Management)
الهدف	ضمان تحديد واكتشاف حوادث الأمن السيبراني في الوقت المناسب وإدارتها بشكل فعّال والتعامل مع تهديدات الأمن السيبراني استباقياً من أجل منع أو تقليل الآثار المترتبة على أعمال الجهة. مع مراعاة ما ورد في الأمر السامي الكريم رقم ٣٧١٤٠ وتاريخ ١٤ / ٨ / ١٤٣٨ هـ
الضوابط	
٢-١٣-١	يجب تحديد وتوثيق واعتماد متطلبات إدارة حوادث وتهديدات الأمن السيبراني في الجهة.
٢-١٣-٢	يجب تطبيق متطلبات إدارة حوادث وتهديدات الأمن السيبراني في الجهة.
٢-١٣-٣	يجب أن تغطي متطلبات إدارة حوادث وتهديدات الأمن السيبراني بحد أدنى ما يلي: ٢-١٣-٣-١ وضع خطط الاستجابة للحوادث الأمنية وآليات التصعيد. ٢-١٣-٣-٢ تصنيف حوادث الأمن السيبراني. ٢-١٣-٣-٣ تبليغ الهيئة عند حدوث حادثة أمن سيبراني. ٢-١٣-٣-٤ مشاركة التنبيهات والمعلومات الاستباقية ومؤشرات الاختراق وتقارير حوادث الأمن السيبراني مع الهيئة. ٢-١٣-٣-٥ الحصول على المعلومات الاستباقية (Threat Intelligence) والتعامل معها.
٢-١٣-٤	يجب مراجعة تطبيق متطلبات إدارة حوادث وتهديدات الأمن السيبراني في الجهة دورياً.
٢-١٤	الأمن المادي (Physical Security)
الهدف	ضمان حماية الأصول المعلوماتية والتقنية للجهة من الوصول المادي غير المصرح به والفقدان والسرقة والتخريب.
الضوابط	
٢-١٤-١	يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني لحماية الأصول المعلوماتية والتقنية للجهة من الوصول المادي غير المصرح به والفقدان والسرقة والتخريب.
٢-١٤-٢	يجب تطبيق متطلبات الأمن السيبراني لحماية الأصول المعلوماتية والتقنية للجهة من الوصول المادي غير المصرح به والفقدان والسرقة والتخريب.
٢-١٤-٣	يجب أن تغطي متطلبات الأمن السيبراني لحماية الأصول المعلوماتية والتقنية للجهة من الوصول المادي غير المصرح به والفقدان والسرقة والتخريب بحد أدنى ما يلي: ٢-١٤-٣-١ الدخول المصرح به للأماكن الحساسة في الجهة (مثل: مركز بيانات الجهة، مركز التعافي من الكوارث، أماكن معالجة المعلومات الحساسة، مركز المراقبة الأمنية، غرف اتصالات الشبكة، مناطق الإمداد الخاصة بالأجهزة والعتاد التقنية، وغيرها). ٢-١٤-٣-٢ سجلات الدخول والمراقبة (CCTV). ٢-١٤-٣-٣ حماية معلومات سجلات الدخول والمراقبة.