	٢-١٤-٣-٤ أمن إتلاف وإعادة استخدام الأصول المادية التي تحوي معلومات مصنفة (وتشمل: الوثائق الورقية ووسائط الحفظ والتخزين). ٢-١٤-٣-٥ أمن الأجهزة والمعدات داخل مباني الجهة وخارجها.
٢-١٤-٤	يجب مراجعة متطلبات الأمن السيبراني لحماية الأصول المعلوماتية والتقنية للجهة من الوصول المادي غير المصرح به والفقدان والسرقة والتخريب دورياً.
٢-١٥	حماية تطبيقات الويب (Web Application Security)
الهدف	ضمان حماية تطبيقات الويب الخارجية للجهة من المخاطر السيبرانية.
الضوابط	
٢-١٥-١	يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني لحماية تطبيقات الويب الخارجية للجهة من المخاطر السيبرانية.
٢-١٥-٢	يجب تطبيق متطلبات الأمن السيبراني لحماية تطبيقات الويب الخارجية للجهة.
٢-١٥-٣	يجب أن تغطي متطلبات الأمن السيبراني لحماية تطبيقات الويب الخارجية للجهة بحد أدنى ما يلي: ٢-١٥-٣-١ استخدام جدار الحماية لتطبيقات الويب (Web Application Firewall). ٢-١٥-٣-٢ استخدام مبدأ المعمارية متعددة المستويات (Multi-tier Architecture). ٢-١٥-٣-٣ استخدام بروتوكولات آمنة (مثل بروتوكول HTTPS). ٢-١٥-٣-٤ توضيح سياسة الاستخدام الآمن للمستخدمين. ٢-١٥-٣-٥ التحقق من الهوية على أن يتم تحديد عناصر التحقق المناسبة وعددها وكذلك تقنيات التحقق المناسبة بناء على نتائج تقييم الأثر المحتمل لفشل عملية التحقق وتخطيها، وذلك لعمليات دخول المستخدمين.
٢-١٥-٤	يجب مراجعة متطلبات الأمن السيبراني لحماية تطبيقات الويب للجهة من المخاطر السيبرانية دورياً.