١-٤	أدوار ومسؤوليات الأمن السيبراني
الهدف	ضمان تحديد أدوار ومسؤوليات واضحة لجميع الأطراف المشاركة في تطبيق ضوابط الأمن السيبراني في الجهة.
الضوابط	
١-٤-١	يجب على صاحب الصلاحية تحديد وتوثيق واعتماد الهيكل التنظيمي للحوكمة والأدوار والمسؤوليات الخاصة بالأمن السيبراني للجهة، وتكليف الأشخاص المعنيين بها، كما يجب تقديم الدعم اللازم لإنفاذ ذلك، مع الأخذ بالاعتبار عدم تعارض المصالح.
٢-٤-١	يجب مراجعة أدوار ومسؤوليات الأمن السيبراني في الجهة وتحديثها على فترات زمنية مخطط لها (أو في حالة حدوث تغييرات في المتطلبات التشريعية والتنظيمية ذات العلاقة).
١-٥	إدارة مخاطر الأمن السيبراني
الهدف	ضمان إدارة مخاطر الأمن السيبراني على نحو ممنهج يهدف إلى حماية الأصول المعلوماتية والتقنية للجهة، وذلك وفقاً للسياسات والإجراءات التنظيمية للجهة والمتطلبات التشريعية والتنظيمية ذات العلاقة.
الضوابط	
١-٥-١	يجب على الإدارة المعنية بالأمن السيبراني في الجهة تحديد وتوثيق واعتماد منهجية وإجراءات إدارة مخاطر الأمن السيبراني في الجهة. وذلك وفقاً لاعتبارات السرية وتوافر وسلامة الأصول المعلوماتية والتقنية.
٢-٥-١	يجب على الإدارة المعنية بالأمن السيبراني تطبيق منهجية وإجراءات إدارة مخاطر الأمن السيبراني في الجهة.
٣-٥-١	يجب تنفيذ إجراءات تقييم مخاطر الأمن السيبراني بحد أدنى في الحالات التالية: ١-٣-٥-١ في مرحلة مبكرة من المشاريع التقنية. ٢-٣-٥-١ قبل إجراء تغيير جوهري في البنية التقنية. ٣-٣-٥-١ عند التخطيط للحصول على خدمات طرف خارجي. ٤-٣-٥-١ عند التخطيط وقبل إطلاق منتجات وخدمات تقنية جديدة.
٤-٥-١	يجب مراجعة منهجية وإجراءات إدارة مخاطر الأمن السيبراني وتحديثها على فترات زمنية مخطط لها (أو في حالة حدوث تغييرات في المتطلبات التشريعية والتنظيمية والمعايير ذات العلاقة)، كما يجب توثيق التغييرات واعتمادها.
٦-١	الأمن السيبراني ضمن إدارة المشاريع المعلوماتية والتقنية
الهدف	التأكد من أن متطلبات الأمن السيبراني مضمنة في منهجية وإجراءات إدارة مشاريع الجهة لحماية السرية وسلامة الأصول المعلوماتية والتقنية للجهة ودقتها وتوافرها، وذلك وفقاً للسياسات والإجراءات التنظيمية للجهة والمتطلبات التشريعية والتنظيمية ذات العلاقة.
الضوابط	
١-٦-١	يجب تضمين متطلبات الأمن السيبراني في منهجية وإجراءات إدارة المشاريع وفي إدارة التغيير على الأصول المعلوماتية والتقنية في الجهة لضمان تحديد مخاطر الأمن السيبراني ومعالجتها كجزء من دورة حياة المشروع التقني، وأن تكون متطلبات الأمن السيبراني جزء أساسي من متطلبات المشاريع التقنية.
٢-٦-١	يجب أن تغطي متطلبات الأمن السيبراني لإدارة المشاريع والتغييرات على الأصول المعلوماتية والتقنية للجهة بحد أدنى ما يلي: ١-٢-٦-١ تقييم الثغرات ومعالجتها. ٢-٢-٦-١ إجراء مراجعة للإعدادات والتحصين (Secure Configuration and Hardening) وحزم التحديثات قبل إطلاق وتدشين المشاريع والتغييرات.
٣-٦-١	يجب أن تغطي متطلبات الأمن السيبراني لمشاريع تطوير التطبيقات والبرمجيات الخاصة للجهة بحد أدنى ما يلي: ١-٣-٦-١ استخدام معايير التطوير الآمن للتطبيقات (Secure Coding Standards). ٢-٣-٦-١ استخدام مصادر مرخصة وموثوقة لأدوات تطوير التطبيقات والمكتبات الخاصة بها (Libraries). ٣-٣-٦-١ إجراء اختبار للتحقق من مدى استيفاء التطبيقات للمتطلبات الأمنية السيبرانية للجهة. ٤-٣-٦-١ أمن التكامل (Integration) بين التطبيقات. ٥-٣-٦-١ إجراء مراجعة للإعدادات والتحصين (Secure Configuration and Hardening) وحزم التحديثات قبل إطلاق وتدشين التطبيقات.
٤-٦-١	يجب مراجعة متطلبات الأمن السيبراني في إدارة المشاريع في الجهة دورياً.