الضوابط الأساسية للأمن السيبراني

تفاصيل الضوابط الأساسية للأمن السيبراني

١ حوكمة الأمن السيبراني (Cybersecurity Governance)

١-١	إستراتيجية الأمن السيبراني
الهدف	ضمان إسهام خطط العمل للأمن السيبراني والأهداف والمبادرات والمشاريع داخل الجهة في تحقيق المتطلبات التشريعية والتنظيمية ذات العلاقة.
الضوابط	
١-١-١	يجب تحديد وتوثيق واعتماد إستراتيجية الأمن السيبراني للجهة ودعمها من قبل رئيس الجهة أو من ينيبه (ويشار له في هذه الضوابط باسم "صاحب الصلاحية")، وأن تتماشى الأهداف الإستراتيجية للأمن السيبراني للجهة مع المتطلبات التشريعية والتنظيمية ذات العلاقة.
١-١-٢	يجب العمل على تنفيذ خطة عمل لتطبيق إستراتيجية الأمن السيبراني من قبل الجهة.
١-١-٣	يجب مراجعة إستراتيجية الأمن السيبراني على فترات زمنية مخطط لها (أو في حالة حدوث تغييرات في المتطلبات التشريعية والتنظيمية ذات العلاقة).
١-٢	إدارة الأمن السيبراني
الهدف	ضمان التزام ودعم صاحب الصلاحية للجهة فيما يتعلق بإدارة وتطبيق برامج الأمن السيبراني في تلك الجهة وفقاً للمتطلبات التشريعية والتنظيمية ذات العلاقة.
الضوابط	
١-٢-١	يجب إنشاء إدارة معنية بالأمن السيبراني في الجهة مستقلة عن إدارة تقنية المعلومات والاتصالات (ICT/ IT) (وفقاً للأمر السامي الكريم رقم ٣٧١٤٠ وتاريخ ١٤ / ٨ / ١٤٣٨ هـ). ويفضل ارتباطها مباشرة برئيس الجهة أو من ينيبه، مع الأخذ بالاعتبار عدم تعارض المصالح.
١-٢-٢	يجب شغل جميع وظائف الأمن السيبراني من قبل مواطنين متفرغين وذوي كفاءة في مجال الأمن السيبراني.
١-٢-٣	يجب إنشاء لجنة إشرافية للأمن السيبراني بتوجيه من صاحب الصلاحية للجهة لضمان التزام ودعم ومتابعة تطبيق برامج وتشريعات الأمن السيبراني، ويتم تحديد وتوثيق واعتماد أعضاء اللجنة ومسؤولياتها وإطار حوكمة أعمالها على أن يكون رئيس الإدارة المعنية بالأمن السيبراني أحد أعضائها. ويفضل ارتباطها مباشرة برئيس الجهة أو من ينيبه، مع الأخذ بالاعتبار عدم تعارض المصالح.
١-٣	سياسات وإجراءات الأمن السيبراني
الهدف	ضمان توثيق ونشر متطلبات الأمن السيبراني والتزام الجهة بها، وذلك وفقاً لمتطلبات الأعمال التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية ذات العلاقة.
الضوابط	
١-٣-١	يجب على الإدارة المعنية بالأمن السيبراني في الجهة تحديد سياسات وإجراءات الأمن السيبراني وما تشمله من ضوابط ومتطلبات الأمن السيبراني، وتوثيقها واعتمادها من قبل صاحب الصلاحية في الجهة، كما يجب نشرها إلى ذوي العلاقة من العاملين في الجهة والأطراف المعنية بها.
١-٣-٢	يجب على الإدارة المعنية بالأمن السيبراني ضمان تطبيق سياسات وإجراءات الأمن السيبراني في الجهة وما تشمله من ضوابط ومتطلبات.
١-٣-٣	يجب أن تكون سياسات وإجراءات الأمن السيبراني مدعومة بمعايير تقنية أمنية (على سبيل المثال: المعايير التقنية الأمنية لجدار الحماية وقواعد البيانات، وأنظمة التشغيل، إلخ).
١-٣-٤	يجب مراجعة سياسات وإجراءات ومعايير 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.