متطلبات الأمن السيبراني

- **المتطلبات العامة:**

١. الالتزام بمتطلبات الهيئة الوطنية للأمن السيبراني وجميع متطلبات الإدارة العامة للأمن السيبراني مع الالتزام بالمتطلبات التشريعية والتنظيمية الخاصة بوزارة البلديات والإسكان.
٢. التأكد من تطبيق جميع ضوابط الهيئة الوطنية للأمن السيبراني على جميع مخرجات وخدمات العقد / المشروع ذات العلاقة.
٣. إشعار وزارة البلديات والإسكان متمثلة بالإدارة العامة للأمن السيبراني في حالة حدوث أي أنشطة مشبوهة أو حادثة أمن سيبراني لديه تؤثر على الوزارة أو مخرجات وخدمات العقد / المشروع أو مخاوف تتعلق بالأمن السيبراني.
٤. تضمين مسؤوليات الأمن السيبراني وبنود المحافظة على سرية المعلومات (Non- Disclosure Clauses) في عقود فريق عمل المشروع (لتشمل خلال وبعد انتهاء/ إنهاء العلاقة التعاقدية مع الوزارة).
٥. إجراء مسح أمني (Screening and Vetting) لفريق عمل المشروع / العقد، للأطراف الخارجية التي تقدم خدمات إسناد لتقنية المعلومات أو خدمات مدارة - خاصة لمن لديهم صلاحيات الاطلاع على البيانات (سري، سري للغاية) والأنظمة الحساسة وتقديم ما يثبت ذلك لمدير المشروع أو لمسؤول العقد.
٦. إجراء تقييم لمخاطر الأمن السيبراني، والتأكد من وجود ما يضمن السيطرة على تلك المخاطر، قبل توقيع العقود والاتفاقيات أو عند تغيير المتطلبات التشريعية والتنظيمية ذات العلاقة.

- **بالإضافة للمتطلبات العامة في حال كان هناك خدمات إسناد لتقنية المعلومات أو خدمات مدارة:**

١. إجراء تقييم لمخاطر الأمن السيبراني، والتأكد من وجود ما يضمن السيطرة على تلك المخاطر، قبل توقيع العقود والاتفاقيات أو عند تغيير المتطلبات التشريعية والتنظيمية ذات العلاقة.
٢. أن تكون مراكز عمليات خدمات الأمن السيبراني المدارة للتشغيل والمراقبة، والتي تستخدم طريقة الوصول عن بعد، موجودة بالكامل داخل المملكة.
٣. أن تكون خدمات الإسناد، والخدمات المدارة على الأنظمة الحساسة؛ عن طريق شركات، وجهات وطنية؛ وفقًا للمتطلبات التشريعية، والتنظيمية ذات العلاقة.
٤. عند مشاركة البيانات خارج المملكة يجب التحقق من قدرة الجهة المستضيفة على حماية تلك البيانات والحصول على موافقة صاحب الصلاحية بالإضافة إلى الالتزام بالمتطلبات التشريعية والتنظيمية ذات العلاقة.

- **بالإضافة للمتطلبات العامة في حال كان هناك خدمات استشارية للمشاريع الاستراتيجية ذات الحساسية العالية:**

١. وجود ضمانات تعاقدية تشمل إلزام موظفي الخدمات الاستشارية بعدم إفشاء المعلومات وكذلك القدرة على حذف بيانات الجهة بطرق آمنة لدى شركات الخدمات الاستشارية عند الانتهاء/إنهاء العلاقة التعاقدية مع تقديم الأدلة على ذلك.
٢. توثيق كافة عمليات مشاركة البيانات مع شركات الخدمات الاستشارية، على أن يشمل ذلك مبررات مشاركة البيانات.