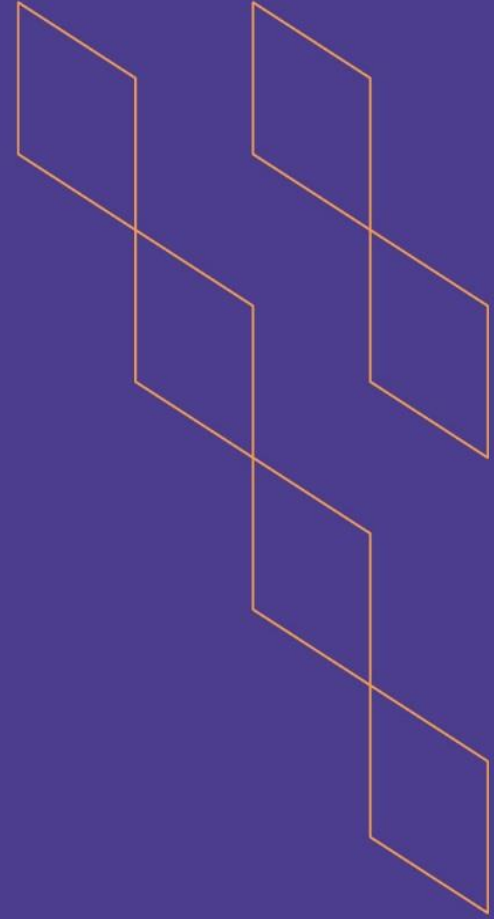




متطلبات الأمن السيبراني للمشاريع المتعلقة بالأطراف الخارجية والخدمات الاستشارية

الإدارة العامة للأمن السيبراني
مايو 2023م



المحتوى

3..... متطلبات الأمن السيبراني للمشاريع المتعلقة الأطراف الخارجية والخدمات الاستشارية.



متطلبات الأمن السيبراني للمشاريع المتعلقة بالأطراف الخارجية والخدمات الاستشارية

- تضمن اتفاقية مستوى الخدمة (SLA) مع الأطراف الخارجية التي قد تتأثر بإصابتها ببيانات الجهة أو الخدمات المقدمة لها .
- يجب توقيع اتفاقية عدم إفشاء المعلومات (Non-Disclosure Clauses).
- يجب أن يقوم مزود الخدمة بالحذف الآمن لبيانات الجهة عند إنتهاء الخدمة.
- إجراء المسح الأمني (Screening or Vetting) لموظفي الأطراف الخارجية وشركات الخدمات الاستشارية الذين لديهم صلاحيات الاطلاع على البيانات ذات التصنيف التالي: مقيد، سري، سري للغاية.
- توثيق كافة عمليات مشاركة البيانات مع الأطراف الخارجية، على أن يشمل ذلك مبررات مشاركة البيانات وتحديد مدة مشاركة البيانات والموعد النهائي للوصول إلى البيانات أو تخزينها.
- 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 والتنسيق مع مكتب إدارة البيانات الوطنية.
- إلزام الأطراف الخارجية بإبلاغ الجهة مباشرة عند حدوث حادثة أمن سيبراني قد تؤثر على البيانات التي تمت مشاركتها أو إنشائها.
- 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.
- إعادة تصنيف البيانات إلى أقل مستوى يحقق الهدف، قبل مشاركتها مع الأطراف الخارجية وذلك باستخدام تقنيات تعقيم البيانات (Data Masking) أو تقنيات مزج البيانات (Data Scrambling).
- يجب على مقدم الخدمة الالتزام بتطبيق متطلبات حماية وخصوصية البيانات الصادرة عن الهيئة السعودية للبيانات والذكاء الاصطناعي والمكتب الوطني لإدارة البيانات.
- يجب على مقدم الخدمة اتخاذ جميع التدابير اللازمة لتجنب التأثير على أنظمة الهيئة.
- يجب على الأطراف الخارجية عند استلامها للبيانات عدم مشاركتها مع طرف آخر أو جهة أخرى دون موافقة الهيئة.

