

محلقات منافسة (أرشفة الوثائق الورقية والالكترونية للمساهمات لمركز الاسناد والتصفية -
إنفاذ)

القوى العاملة						
عدد ساعات العمل	الحد الأدنى لسنوات الخبرة	أقل مؤهل للقبول	وصف البند	العدد	المسمى الوظيفي	
	5	بكالوريوس	إدارة المشروع	1	مدير مشروع	
	2	دبلوم	فرز وجرد الوثائق حسب تصنيف الوثائق	8	مختص الفرز والجرد	
	2	دبلوم	المسح الضوئي والتصوير للوثائق استعدادا لاستكمال أرشفتها داخل النظام	6	مختص المسح الضوئي والتصوير	
	3	بكالوريوس	ادخال بيانات الوثيقة داخل النظام	6	مختص ادخال بيانات	
	3	بكالوريوس	تدقيق والجودة على البيانات المدخلة	6	مختص الجودة	
	2	دبلوم	تحديد الموقع الفيزيائي داخل النظام ومستودع الحفظ الورقي	5	مسؤول الحفظ المكاني	

الشروط الخاصة:

- 1- على المتعاقد الالتزام بنسب التوطين وفقاً للإدلة الإجرائية لقرارات التوطين الصادر من وزارة الموارد البشرية والتنمية الاجتماعية.
- 2- يجب على المتعاقد الالتزام بتمكين السعوديين من العمل في وظائف المشروع مع الالتزام بتطبيق دليل توظيف عقود التشغيل والصيانة، على سبيل المثال لا الحصر مسؤولي إدخال البيانات واستكمال الأرشفة في النظام.
- 3- يشترط تنفيذ المشروع خلال مدة أقصاها 12 شهر من تاريخ توقيع محضر بدء أعمال المشروع، ويعد الالتزام الزمني من أبرز معايير التقييم والمتابعة، ويتربط على الإخلال به تطبيق الغرامات.
- 4- يجب على المورد الالتزام باتفاقية مستوى الخدمة التي يوافق عليها المركز، ويحق للمركز تنفيذ الجزاءات النظامية في حقه في حال تأخر في التنفيذ.
- 5- يجب أن تكون للجهة المنفذة خبرة مثبتة في مشاريع مماثلة لدى جهات مماثلة لا تقل عن 3 مشاريع في إطار حرص المركز على ضمان جودة التنفيذ وتقليل مخاطر الاعتماد على الأطراف الخارجية.
- 6- يتعين على الجهات المتقدمة الالتزام الكامل بشرط قبول المركز للمهندسين والمستشارين المقيمين قبل عملية اسنادهم مع شرط تقديم سيرهم الذاتية وتسهيل عمل مقابلة لهم لتحديد مدى كفاءتهم وخبرتهم.
- 7- يجب أن تكون جميع مخرجات المشروع من الوثائق باللغة العربية.
- 8- يجب أن يضمن المورد أن فريق العمل سبق وأن عمل على مشاريع مماثلة ومتوافق مع جدول المتطلبات الفنية لفريق العمل.
- 9- يلتزم مزود الخدمة بتوفير أجهزة حاسب آلي ومساحات ضوئية وأي أجهزة متطلبه لتنفيذ المشروع وتدار بشكل كلي من قبل المركز على أن يتم التخلص من أي بيانات في الأجهزة المستخدمة لتنفيذ المشروع بعد انتهائه بالطريقة المناسبة والأمنة التي يراها المركز.
- 10- متطلبات الامن السيبراني بشأن التعامل مع البيانات وحمايتها وفق المتطلبات الداخلية والتنظيمية والتشريعية ذات العلاقة:
 - O تخزين البيانات وحفظها حصراً في خوادم/أنظمة المركز، وعدم رفعها على أي منصات سحابية خارجية.
 - O يمنع مشاركة اي بيانات متعلقة بالمشروع او بالمركز عبر أي تطبيقات غير معتمدة.
 - O تشفير البيانات أثناء النقل والتخزين باستخدام بروتوكولات ومعايير معتمدة.
 - O منع توصيل أي وسائط خارجية (USB, HDD, CD)، مع تثبيت جميع الأنظمة التقنية الأمنية وأنظمة تقنية المعلومات.
 - O العمل يتم حصراً من داخل بيئة عمل آمنة ومعتمدة في المركز، وفي حال وجود أي استثناء يتم وفق شروط ومتطلبات الامن السيبراني.
 - O عزل بيئة تطوير/اختبار عن بيئة الإنتاج الخاصة بالمركز.
 - O تطبيق آليات واجراءات إتلاف البيانات بعد انتهاء الغرض من استخدامها.
- 11- القيود على التعاقد من الباطن: لا يجوز تفويض أي طرف ثالث بتنفيذ أي جزء جوهري من المشروع دون الحصول على موافقة خطية مسبقة من المركز، وتظل الجهة المتقدمة مسؤولة ومسؤولية كاملة عن أداء الأطراف الثانوية، إن وُجدت، بما يضمن الامتثال التام لجميع المتطلبات.
- 12- إدارة المخاطر: يجب على الجهة المتقدمة تقديم خطة مبدئية لإدارة المخاطر المرتبطة بالمشروع، تتضمن أسلوب التعامل مع مخاطر الطرف الثالث والموردين.
- 13- يجب على المتنافس الاطلاع على قرارات وأنظمة التوطين وتحديثاتها الخاصة بجميع أنواع النشاطات وفئات الوظائف الصادرة من الجهات الحكومية المختصة والالتزام بها عند تنفيذ العقد.
- 14- يحق لمركز الإسناد والتصفية (إنفاذ) في جميع الأحوال أن تطلب كتابةً من المتعاقد اثناء فترة تنفيذ العقد أو قبل البدء في التنفيذ استبدال أي شخص من فريق العمل للمتعاقدين بشكل كامل أو جزئي وعلى المتعاقد استبدال فريق العمل خلال (3) أيام عمل فقط من تاريخ اشعاره
- 15- يشترط لصرف المستحقات المالية عدم الإخلال بالمتطلبات أو تعاميم وتعليمات الجهات الحكومية أو العامة أو وجود ملاحظات منها جراء تنفيذ أعمال هذا المشروع بشكل مباشر أو غير مباشر.

16- يلتزم المتعاقد بتزويد المركز بقائمة بالعاملين المستهدف عملهم في تنفيذ العقد لغرض الحصول على التراخيص اللازمة وذلك خلال (10) أيام عمل من تاريخ توقيع العقد. وفي حال طرأ تحديث أو تغيير على هذه القائمة مستقبلاً ولأي سبب كان، فيلزم تزويد المركز بالقائمة المحدثة خلال يوم عمل من تاريخ التحديث أو التغيير.

17- مدير المشروع والتواصل الدوري:

- تلزم الجهة المتقدمة بتعيين مدير مشروع ذو خبرة مثبتة لا تقل عن خمس (5) سنوات في إدارة مشاريع مماثلة في مجال الجرد والتحليل والأرشفة الإلكترونية.
- يكون مدير المشروع هو نقطة الاتصال الرسمية والمسؤولة عن تنفيذ ومتابعة المشروع من طرف الشركة.
- يجب على مدير المشروع حضور اجتماع متابعة أسبوعي مع الفريق المعني من المركز، سواءً بشكل حضوري أو افتراضي، وتقديم تقارير مرحلية (Status Reports) تشمل نسبة الإنجاز، العوائق، والتوصيات.
- لا يجوز استبدال مدير المشروع إلا بموافقة خطية مسبقة من المركز، ويجب أن يتم تقديم سيرة ذاتية بديلة بمستوى خبرة ومؤهلات مكافئة أو أعلى.

18- الكفاءة الفنية

- يجب تقديم هيكل الفريق المقترح مع بيان الخبرات السابقة لكل عضو، والمشاريع التي شارك فيها.
 - لا يُقبل إدراج موظفين متدربين أو حديثي التخرج ضمن الفريق التنفيذي الأساسي للمشروع.
- يجب الالتزام بمتطلبات فريق العمل حسب المرفق

متطلبات مكتب البيانات وحماية البيانات الشخصية

متطلبات عامة:

1. يجب على المقاول الالتزام بتطبيق أفضل ممارسات حوكمة البيانات وحماية البيانات الشخصية على جميع أنشطته وموظفيه ومتعاquديه ممن لديهم وصول إلى بيانات الجهة أو يعملون ضمن نطاق المشروع.
2. يجب الالتزام بسياسات وإجراءات مكتب البيانات لدى الجهة، وبمعايير ولوائح وضوابط الهيئة السعودية للبيانات والذكاء الاصطناعي (سدايا)، ونظام حماية البيانات الشخصية (PDPL).
3. يقر المقاول بأن الجهة هي مالك البيانات، ويُعد المقاول معالجاً للبيانات، ولا يجوز له جمع أو معالجة أو مشاركة البيانات إلا لغرض تنفيذ المشروع وبالحد الأدنى اللازم.
4. يجب الالتزام بتصنيف البيانات وفق سياسة تصنيف البيانات المعتمدة وتطبيق الضوابط المناسبة حسب مستوى التصنيف، مع تقييد الوصول على العاملين المخولين فقط.
5. يلتزم المقاول بحماية البيانات باستخدام الوسائل المناسبة، بما في ذلك – على سبيل المثال لا الحصر – التشفير أثناء الجمع والنقل والتخزين، وضمان أمن مشاركة البيانات بين الأنظمة.
6. يجب الإبلاغ الفوري للجهة عن أي حادث أمني أو تسرب بيانات، والالتزام بالإجراءات المعتمدة للتعامل مع الحوادث والتعاون الكامل في التحقيق والمعالجة.
7. يلتزم المقاول بتوثيق جميع العمليات والإجراءات والمخرجات المتعلقة بالبيانات، وتقديم الأدلة عند الطلب، ومعالجة أي فجوات يتم رصدها وفق توصيات معتمدة.
8. في حال تصنيف المشروع أو أي من بياناته على مستوى سري أو أعلى، يلتزم المقاول بتطبيق الضوابط المشددة للمشاريع المصنفة وعدم استخدام أي أدوات أو قنوات غير معتمدة لمعالجة البيانات.
9. يُحظر نقل أو استضافة أو معالجة بيانات الجهة خارج المملكة العربية السعودية إلا بعد الحصول على موافقة خطية مسبقة من الجهة.
10. يلتزم المقاول بإتلاف أو حذف بيانات الجهة بشكل آمن بعد انتهاء المشروع أو العلاقة التعاقدية، وتقديم ما يثبت ذلك عند الطلب.
11. يلتزم المقاول بتوقيع اتفاقيات مكتب البيانات المعتمدة، بما في ذلك عقود معالجة البيانات الشخصية (DPA)، واتفاقيات مشاركة البيانات، واتفاقيات عدم الإفصاح (NDA)، متى ما تطلب نطاق المشروع ذلك.
12. يحق للجهة أو مكتب البيانات طلب أي تقارير أو أدلة للتأكد من التزام المقاول بمتطلبات حوكمة البيانات وحماية البيانات الشخصية.

متطلبات الامن السيبراني

متطلبات عامة:

1. يجب على المفاوض بذل العناية الواجبة في تطبيق أفضل ممارسات الأمن السيبراني على أصوله التقنية وموظفيه ومتعاquديه ممن لديهم وصول للأصول التقنية أو المعلوماتية الخاصة بالجهة الحكومية أو ممن يعملون ضمن المشروع مع الجهة الحكومية.
 2. يجب الالتزام بالسياسات والإجراءات والمعايير الخاصة بالأمن السيبراني لدى الجهة الحكومية، والمتطلبات التشريعية والتنظيمية الصادرة من الهيئة الوطنية للأمن السيبراني.
 3. يضمن المفاوض إجراء المسح الأمني والخلو من السوابق لعامله ممن لديهم وصول لأصول الجهة الحكومية التقنية والمعلوماتية، كما يتحمل المسؤولية الكاملة عن أي انتهاك من قبل عامله يؤثر سلباً على سرية ونزاهة وتوافر أصول الجهة الحكومية التقنية والمعلوماتية أثناء وبعد انتهاء مدة العقد أو المشروع.
 4. يجب أن تكون مراكز الخدمات المدارة للتشغيل والمراقبة والتي تستخدم طريقة الوصول عن بعد موجودة بالكامل داخل المملكة العربية السعودية.
 5. ضمان الالتزام بتوقيع اتفاقية عدم الإفصاح (Non-Disclosure Agreement) في بداية المشروع وفي حال الحاجة للتعامل مع أي بيانات مصنفة خاصة بالجهة الحكومية.
 6. يجب على المفاوض حذف أي بيانات ومعلومات لديه خاصة بالجهة الحكومية بشكل آمن بعد انتهاء العلاقة التعاقدية، وعدم الاحتفاظ بها من دون إذن رسمي مسبق من الجهة الحكومية.
 7. يجب على المفاوض ضمان ارجاع البيانات والحسابات ووسائل الوصول إلى أنظمة الجهة الحكومية بصيغة قابلة للقراءة والاستخدام.
 8. ضمان أن يُبلغ مزود الخدمة/المفاوض الجهة الحكومية حال اكتشاف أي انتهاك يؤثر مباشرةً على موارد الجهة الحكومية أو بياناتها وذلك عن طريق البريد الإلكتروني التالي SOC@infath.gov.sa
 9. ضمان أمن معلومات الجهة الحكومية وسريتها التي تتم مشاركتها من خلال المشروع وكذلك أمان وسرية الأنظمة المعلوماتية والشبكة التي يتم توفير الوصول إلى جزء منها أو كليتها كمتطلب في المشروع.
- لمركز إنفاذ الحق في طلب ما يضمن التزام المفاوض بالمتطلبات المذكورة، ويجب على المفاوض إطلاع الجهة الحكومية على أي أدلة يتم طلبها للتأكد من التزام المفاوض بمتطلبات الأمن السيبراني لمركز إنفاذ.