|  |  |
| --- | --- |
| Review For: |  |
| Completed by: |  |
| Requested by: |  |
| Review Type: | One of: Brief/Standard/Details |
| Review Date: |  |
| Review Status: | One of: IN PROGRESS OR COMPLETE – SUITABLE FOR GOAL USE |

# QUESTIONS

**Questions for vendor:**

1. How is your software\System hosted? Is the system hosted by your organization or a third-party data center? Or is it going to be fully installed in GOAL environment?
	1. If it is hosted by you, where will the data be stored geographically?
	2. What are your security policies for the datacentre and data security? (Please share your security policies)
2. Is the service\system compliant with General Data Protection Regulation (GDPR) or relevant regulations in country
	1. What policies and procedures do you have in place to manage client’s data? Do you have any certifications?
	2. How will you protect GOAL data?
	3. Do you follow secure data destruction process for data and IT equipment\media?
		1. Please share procedures\policies
	4. If the contract is terminated, will you return or securely destroy GOAL data?
3. Data encryption
	1. Is data encrypted at rest – while stored?
	2. Is data encrypted in transit – while users are accessing it?
4. Data management (audit trail)
	1. Are actions (create, delete, modify) on data in your system monitored and logged?
5. Backup and DR– is the service\system supports backup and DR?
	1. Please describe backup process.
	2. Please describe DR (Disaster Recovery) process.
6. Does your Software\System support Multi Factor Authentication (MFA) for accessing it?
	1. If not, what other measures are in place to minimize the risk of unauthorised access?
7. Does your Software\System support Single Sing On (SSO) with Azure AD?
8. Identity and access management
	1. Are there different levels of access possible such as admin, financial controller, junior staff?
		1. Can those roles be customised?
	2. Is access monitored and logged?
9. Vulnerabilities management
	1. Are the systems regularly patched to address security risks as recommended by vendors?
	2. How do you notify clients in the event of security incident or data breach in your system?
	3. Please provide details on your security incident management policies/procedures

**Additional questions**

* Does the service have an operational dependency on existing evaluated services and infrastructure? e.g. SharePoint
* Can a standard user read or write sensitive system data (e.g. SharePoint dependent services)?

**Declaration Statements**

As part of our submission to this Invitation to Tender, we hereby confirm the following:

1. **Authenticity and Accuracy**
 We confirm that all information provided in this security assessmnt is accurate, complete, and truthful, and we understand that any false declaration may result in disqualification.

|  |
| --- |
| **Declaration Box** |
| **Name** |  |
| **Signature** |  |
| **Date** |  |