**Attachment 3.1**

Technology

*Complete 1 Technology form per firm*

If the question does not fit the type of technology deployment in your proposal enter “NA” (Not Applicable) in the box and provide an explanation why it is “NA”.

**Type of Deployment**

|  |  |
| --- | --- |
| **Question** | **Answer** |
| Proposed solution is a hosted / SaaS solution? | Select one |
| All Applications do not require client software (i.e., VPN)? | Select one |
| All customers on proposed application must upgrade at same time? | Select one |

**Data Center**

|  |  |
| --- | --- |
| **Question** | **Answer** |
| Where are the data centers located? |  |
| Are any third-party providers used to deliver PaaS or IaaS services? If so, please list. |  |
| How many environments or tenants are proposed for: 1) Implementation and 2) Production? |  |
| List Data Center industry standard and regulations, such as SOC 1 and SOC 2 for internal controls, and ISO 27001 for information security management – include dates. |  |
| What physical security measures are in place at the data centers? |  |

**Hardware**

|  |  |
| --- | --- |
| **Question** | **Answer** |
| Are there any on-site hardware requirements. If “Yes”, list in your answer. |  |
| If your proposed solution requires customer managed servers, what are the server requirements? |  |
| What are the network requirements? |  |

**Updates**

|  |  |
| --- | --- |
| **Question** | **Answer** |
| How often is the solution updated? |  |
| How much advance notice are customers provided for new updates? |  |
| Does customer have the opportunity to test updates in a pre-production environment? |  |
| How long do customers have to test updates before the update is applied? |  |

**Security**

|  |  |
| --- | --- |
| **Question** | **Answer** |
| Does the system support SSO or LDAP? |  |
| Does the system support multi-factor authentication (MFA)? If so, what methods and what authenticators? |  |
| Is your integration protocol based on SOAP or REST? |  |
| Does the entire proposed solution follow the same integration protocol? |  |

**Information Security**

|  |  |
| --- | --- |
| **Question** | **Answer** |
| What protections are provided against data breach? |  |
| In the event of a cyber-incident, please define liability for the Library and vendor including any proposed mitigation services provided by vendor |  |

Please include information regarding cybersecurity standards, recent independent audits, notification process, remedy, and indemnification provided.

**Disentanglement**

|  |  |
| --- | --- |
| **Question** | **Answer** |
| Can customer data be exported in nonproprietary format? |  |

**Availability**

Provide historical availability for data center for past six months. Report all time in minutes.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Month** | **Total Minutes** | **Downtime** | **Scheduled Maintenance** | **Other Downtime** | **Total Downtime** | **% Availability** |
| Sep 2023 |  |  |  |  |  |  |
| Oct 2023 |  |  |  |  |  |  |
| Nov 2023 |  |  |  |  |  |  |
| Dec 2023 |  |  |  |  |  |  |
| Jan 2024 |  |  |  |  |  |  |
| Feb 2024 |  |  |  |  |  |  |

**Proposed Service Level Guarantees**

If SaaS services are proposed, please complete the following table identifying proposed service level guarantees. For each service, please indicate the metric, including definition, used to measure the service quality, the proposed requirement (target for service), and the proposed remedy or penalty if guarantee is not met.

|  |  |  |  |
| --- | --- | --- | --- |
| **Service** | **Metric** | **Requirement/Guarantee** | **Remedy** |
| **System Availability**  **(Unscheduled**  **Downtime)** |  |  |  |
| **System Response**  **(Performance)** |  |  |  |
| **Issue Response**  **Time** |  |  |  |
| **Issue Resolution**  **Time** |  |  |  |
| **Recovery Point**  **Objective (RPO)** |  |  |  |
| **Recovery Time**  **Objective (RTO)** |  |  |  |
| **System Data**  **Restore** |  |  |  |
| **Implementation of**  **System Patches** |  |  |  |
| **Notification of**  **Security Breach** |  |  |  |
| **Please list other**  **proposed service**  **levels** |  |  |  |

|  |  |
| --- | --- |
| **Question** | **Answer** |
| How is performance against service levels reported to the Library? |  |

**Detail Support and Maintenance**

|  |  |
| --- | --- |
| **Question** | **Answer** |
| How are support issues reported (online, phone, email) |  |
| How are customers notified of Maintenance Update? |  |
| What is the Frequency of Planned Updates? |  |

**Disaster Recovery and Backup**

|  |  |
| --- | --- |
| **Question** | **Answer** |
| Document comprehensive disaster recovery plan and regular backups to protect against data loss |  |
| What is backup frequency |  |
| How often are backups tested |  |
| Do you keep a Hot Site, Warm Site or Cold Site, please detail |  |
| Outline Data redundancy including offsite or cloud storage |  |
| Is all data stored onshore (within USA) |  |

**Incident Response and Management**

|  |  |
| --- | --- |
| **Question** | **Answer** |
| What are your procedures for detecting, responding to, and recovering from security incidents. |  |
| What are your communication protocols during and after an incident. |  |
| Please identify past security incidents and resolutions. |  |

### **Infrastructure and Scalability**

|  |  |
| --- | --- |
| **Question** | **Answer** |
| What is the underlying infrastructure used to host and deliver the solution? |  |
| How does the infrastructure support scalability to handle growth in users, data volume, and processing needs? |  |