—

Part D: PRIVACY AND CYBERSECURITY

Loan, security, settlement & recovery services RFT

# Overview

The successful tenderer will deal with personal and confidential information relating to IBA’s staff and customers. Please include the following information regarding the Tenderer’s IT network and data security measures.

If a Tenderer proposes to engage a Third Party Collaborator for part of the services, the Third Party Collaborator must also complete the questionnaires below.

# IT infrastructure and network environment

Tenderer may provide the following information in a separate document but please ensure the following information is given.

|  |  |
| --- | --- |
| **Question** | **Response** |
| Please provide a high level overview of your firm’s existing IT infrastructure and network environment. Include an outline of the tools, systems or software that you have in place or expect to use to perform the Services. |  |
| Do you have a secondary site / backup facility that can be used in case of a complete building failure? If yes, please provide details. |  |
| Do you have backup / redundancy in place in case of electrical failure at the proposed location(s) where Services will be performed from? If yes, please provide details. |  |
| Please provide a brief outline of your internet redundancy at the proposed location(s) where Services will be performed. |  |

# IT security and data protection

Tenderer may provide the following information in a separate document (e.g. by way of a Data Security Statement) but please ensure the following information is given.

Reference to ‘IBA Data’ includes any information (electronic and hard copy) provided to the successful Tenderer in connection with the Services (such as any contracts, personal and financial information of IBA’s clients and staff) and any files, documents and notes that the firm creates in relation to the Services.

|  |  |
| --- | --- |
| **Section 1: Contact Details** | |
| Please confirm the name, job title and contact details for the person within your organisation who is responsible for data privacy. |  |
| **Section 2: Physical security** | |
| Does your firm comply with the physical, technical and administrative control objectives of the Australian Government Information Security Manual? |  |
| Please describe the physical access controls in place in relation each of your firm’s offices where the Services will be carried out and where IBA’s Data are held (**Office**).  Please include responses to:   1. Are all entrance and exits to the Office controlled by physical barriers? 2. Is the Office controlled by swipe card access? 3. Are there physical and electronic access controls in place between staff working on different client accounts? |  |
| **Section 3: People and training** | |
| Do you require confidentiality agreements be signed by all your employees, subcontractors and third parties that have access to IBA Data? |  |
| Do staff and third party agents undergo mandatory privacy and data protection training? If yes, what form is this training in e.g., face to face, online etc. |  |
| How often do staff and agents undertake data protection and privacy refresher training? |  |
| **Section 4: Data Storage and Security** | |
| Do you hold any industry recognised security certifications, for example ISO 27001, PCI-DSS or approved IRAP ISM classification?  If yes, will the certifications cover the services that you are undertaking on behalf of IBA? |  |
| Does your firm have data security incident management procedures and data breach response plan in place? If yes, please provide details. |  |
| Where will IBA Data be processed and stored (including location of servers)? Please specify all location(s) including details of back-up data centres (if any).  If IBA Data is held in cloud network, then specify the location of those servers too. |  |
| Will IBA Data be encrypted, both in transit and at rest?  If yes, please provide details of the level of encryption you use for the secure storage and transmission of data. |  |
| Will any of IBA Data be made available to entities located outside Australia, even where the information is stored / hosted in Australia? |  |
| If yes, please indicate all countries where the data will be made available or transferred to. |  |
| If yes, please indicate what measures are in place to protect personal data when made available or transferred to another country. |  |
| **Section 5: Data retention policy** | |
| Please describe your firm’s retention and destruction policy, and include retention periods for IBA Data (both hard copy and electronic data) |  |
| **Section 6: Subcontractors & Third Parties** | |
| Will any Subcontractors or Third Parties have access to IBA Data?  If so, please provide the following details for all Subcontractors & Third Parties:   1. Their name 2. A description of the services they are providing 3. Details of the IBA Data which they will be accessing 4. Details of how they will access the data (for example, will the data be transferred to the contractor or agent, or will it be remotely accessed) 5. The location where the data will be processed by the Subcontractors / Third Parties |  |
| Please indicate whether there is a data processing agreement in place with each of the Subcontractors / Third Parties |  |
| Please also indicate whether data protection and information security compliance checks have been carried out and regularly updated in relation to each Subcontractors / Third Parties |  |
| **Section 7: Information security reviews** | |
| Do you have a documented Policy, Standard or process for Technical Vulnerability Management? |  |
| Has a network vulnerability assessment or penetration test been performed on the external-facing network within the last 12 months by an external 3rd party? If yes, please provide details including the coverage and scope of the scan. |  |
| Do you regularly conduct technical compliance reviews of your information systems? (e.g. control testing and system accreditation). If yes, how often? |  |