Attachment 3: As-a-Service Questionnaire

**This as-a-service questionnaire is necessary for the Department of <<Insert Department Name>> to complete its due diligence when having departmental data stored and used outside of the departmental network.**

*It is specifically designed to elicit a high-level overview of the service being considered in order to refine and direct cyber security and information security questions at a later procurement stage.*

The questions below directly relate to the requirements contained within the *Information Privacy Act 2009* (Qld) and the Queensland Government Information Security Classification Framework. Supplier’s responses will assist the Principal/Customer to assess, mitigate and monitor the risks associated with the offered solution.

For the purpose of this as-a-service questionnaire, a reference to “Solution” means the ICT system/s the Supplier intends to use to capture, store and access Customer Data. Please note Suppliers may be required to provide copies of certificates to support responses.

Responses provided may be used to inform any contractual arrangements entered with the Principal/Customer.

# Filling out this form

***Please note*** *this form is required only for products/goods/services that include an ICT component.*

*Supplier do not need to complete this form if the Offered product/good/service offering does not include an ICT component.*

*Suppliers who’s product/good/service offering includes only a minor ICT component, such as online ordering for your product/service offering, only respond to the questions that are relevant. Suppliers should leave field blank if they are unsure of any of the questions, or leave a comment.*

|  |  |
| --- | --- |
| **Description** | **Required information** |
| **Solution name***Title describing the product or solution which includes the ICT component.* |  |
| **Supplier Name & ABN***Name of responding company / Supplier.* |  |
| **Date***Date assessment completed.* |  |
| **Completed by***Name, position and company of person’s completing the form.* |  |

| **Question** | **Response** |
| --- | --- |
| **Supplier and solution details** |
| Are one or more third party services used for the proposed solutions? If so, who? |       |
| What service/s does the solution deliver? |       |
| Is there a data map available that includes a field description and whether it is mandatory? If so, please include/attach. |       |
| Does the Supplier have a current insurance policy including claims for data breaches/loss for at least $1 million? | Choose an item. |
| **Hosting services and locations** |
| Where is/would the solution be hosted? Select all that apply. | [ ]  On the Customer’s network[ ]  Private servers within Australia [ ]  Private servers outside of Australia[ ]  Third-party cloud service within Australia[ ]  Third-party cloud service outside of AustraliaHosting outside of Australia is located in:      |
| If any of the environments (back-ups/redundancy/testing) are hosted in other locations, provide details for each environment. | Environment:      Location:       |
| Where will your ICT support staff be accessing departmental data from? | [ ]  No access to departmental data[ ]  Support accessing from within Australia[ ]  Support accessing from outside Australia, located in:      |
| **Security measures** |
| Is the data contained within the solution to be encrypted in transit? Select all that apply. | [ ]  Data not encrypted in transit[ ]  Data encrypted in transit [ ]  Transport Layer Security (TLS) version:       [ ]  Secure Shell (SSH) [ ]  Secure Multipurpose Internet Mail Extension (S/MIME) [ ]  Open PGP Message Format [ ]  Internet Protocol Security (IPSec) [ ]  Other:       |
| Can the data contained within the solution be encrypted at rest? Select all that apply. | [ ]  Data cannot be encrypted at rest[ ]  Data can be encrypted at rest [ ]  3DES [ ]  AES128 [ ]  AES256 [ ]  Other:       |
| Can the solution facilitate federated access? | Choose an item.If yes, provide details:       |
| Does the solution include access controls to ensure only your authorised staff have access to the data? | Choose an item.If yes, provide details:       |
| If the solution requires the Customer to provide existing data, does the solution provide a secure method for uploading the data? Select all that apply. | [ ]  No data is transferred/up loadable[ ]  Data requires importing [ ]  Direct upload by Customer [ ]  Direct transfer from other Customer solution [ ]  Provided by encrypted USB [ ]  Provided by unencrypted USB [ ]  Other:       |
| Are criminal history checks conducted on your employees and sub-contractors? | Choose an item.If other, provide details:       |
| Do you offer a multifactor authentication service? | [ ]  Multifactor authentication not available[ ]  Multifactor authentication available [ ]  Electronic (SMS, email, etc) [ ]  Physical token [ ]  Other:       |
| How frequently do you conduct vulnerability assessments on the solution? | Choose an item.If other, provide details:      [ ]  Redacted report provided[ ]  Proof of assessment (or equivalent) provided |
| How frequently do you conduct penetration testing on the solution? | Choose an item.If other, provide details:      [ ]  Redacted report provided[ ]  Verification of pen test (or equivalent) provided |
| What is the mean time to remediate any identified vulnerabilities? | Comments:       |
| Do you conduct investigations into security breaches and implement remediation strategies? | Choose an item.Comments:       |
| Do you immediately notify Customers of any security breaches and/or data corruption/loss? | Choose an item.Comments:       |
| Provide details of any other user access controls that are in place. |       |
| Does the solution provide unique usernames and passwords for end users? | Choose an item. |
| Are passwords stored securely? | Choose an item.If yes, provide details:       |
| Does the solution provide role-based access? | Choose an item.Comments:       |
| **Quality controls** |
| Have processes been implemented to minimise disruption during business hours? | Choose an item.Comments:       |
| Does the solution have a Business Continuity Plan (BCP) in place? | Choose an item.Comments:       |
| What is the availability of the solution? | 24x7:      %Business hours:      %[ ]  NegotiableComments:       |
| What is the Recovery Time Objective? | [ ]  Yes[ ]  No[ ]  NegotiableIf other, provide details:       |
| What is the Recovery Point Objective? | [ ]  Yes[ ]  No[ ]  NegotiableIf other, provide details:       |
| Is data made available to the Customer in an agreed format, upon request? | [ ]  No[ ]  Yes [ ]  Predefined:       [ ]  Proprietary:       [ ]  Other/agreed on request:       |
| How long is data retained for? This includes backups and archives. |       |
| Is data deleted on Customer request? This includes backups and archives. | [ ]  Yes[ ]  NoComments:       |
| Is data deletion certified? | Choose an item.Comments:       |
| **Compliance controls** |
| Is the solution ISO27001 certified? | [ ]  No[ ]  Yes [ ]  Certificate provided [ ]  Certificate not providedComments:       |
| If an IRAP assessment has been undertaken (Australian InfoSec Registered Assessors Program), to what level has the solution been certified? | [ ]  Not IRAP assessed[ ]  IRAP assessed [ ]  Unclassified DLM [ ]  Protected [ ]  Other:       |
| If the solution processes electronic payments or holds credit card data, is it Payment Card Industry (PCI) Data Security Standards (DSS) compliant? | Choose an item.Comments:       |