The University of Aberdeen requires that all suppliers manage information security risk and implement appropriate controls to minimise the impact of a cyber-security incident. The scope of risk includes University data that the supplier has been given, has access to or has collected on behalf of the University, it also includes the suppliers own data, where a cyber-security incident affecting it, would significantly impact the supplier’s ability to meet their contracted obligations to the University.

# Part 1: Proposal

(For completion by University of Aberdeen purchaser)

|  |  |
| --- | --- |
| School / Professional Service |  |
| Contact member of staff |  |
| Internal reference (e.g. contract number, quote number): |  |
| What services will the supplier provide?  Describe the activities they will undertake (e.g. cloud hosting, analytical services etc) |  |
| What University activities will the service support? (e.g. collaboration between students for teaching purposes, delivering communications to external stakeholders) |  |
| What University data will the supplier process or store as part of the service?  Describe the type of data and estimate the amount of data |  |

# Part 2: Supplier details and responses

(For completion by proposed supplier)

|  |  |
| --- | --- |
| Organisation name: |  |
| Address: |  |
| Website: |  |

Please supply details of a contact who can provide clarification on any questions:

|  |  |
| --- | --- |
| Contact name: |  |
| Email address: |  |
| Telephone number: |  |

|  |  |
| --- | --- |
| Date form completed: |  |

Please complete the questionnaire by providing a response to each question. If you wish to submit any supporting documentation as part of your answer, please provide it with your completed questionnaire.

|  |  |  |
| --- | --- | --- |
| **1** | **CONDITIONS OF PURCHASE** | |
|  | Question | Response |
| 1.1 | Have you read and agree to the University’s General Conditions of Purchase which can be found [here](https://www.abdn.ac.uk/staffnet/working-here/legislations-7499.php#panel7530) |  |

|  |  |  |
| --- | --- | --- |
| **2** | **GOVERNANCE** | |
|  | Question | Response |
| 2.1 | Do you have an Information Security policy that is approved at board level or equivalent? |  |
| 2.2 | Do you have a security and data governance framework in place? Please provide details. |  |
| 2.3 | Where is our data stored and processed? Please list all locations including country. |  |

|  |  |  |
| --- | --- | --- |
| **3** | **ASSURANCE** | |
|  | Question | Response |
| 3.1 | Do you conduct regular third-party security assessments and/or penetration tests? Please provide details. |  |
| 3.2 | Do you conduct regular vulnerability scans? Please provide details. |  |
| 3.3 | Can the University of Aberdeen, at its own cost and by prior arrangement, commission penetration tests of your systems? |  |
| 3.4 | Do you hold any relevant information security certifications? E.g. ISO 27001, Cyber Essentials, etc. Please provide a copy of any certificates. |  |

|  |  |  |
| --- | --- | --- |
| **4** | **ACCESS** | |
|  | Question | Response |
| 4.1 | Do you have security controls in place to prevent unauthorised persons accessing data? Please provide details. |  |
| 4.2 | Do you mandate Multi-Factor Authentication for standard and privileged accounts? Please provide details. |  |
| 4.3 | Do you conduct screening and employment checks for new staff? |  |
| 4.4 | Do you require staff to complete Information Security awareness training? Please provide details. |  |
| 4.5 | Have you implemented appropriate segregation between users of the service to ensure that an incident affecting one customer will not affect others? Please provide details. |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **5** | | **MEASURES** | |
|  | Question | | Response |
| 5.1 | Do you have controls in place to ensure devices and data are protected from unauthorised access, damage, theft or interference? Please provide details. | |  |
| 5.2 | Do you encrypt data at rest? E.g. data stored on cloud storage services, physical servers, phones, laptops, computers, hard disks and other data storage devices. Please provide details. | |  |
| 5.3 | Do you encrypt data in transit both over the Internet and internally? Please provide details. | |  |
| 5.4 | Do you use a firewall to protect connections to and from the Internet? Please provide details. | |  |
| 5.5 | Do you have controls and policies in place to ensure that default settings and passwords been changed to appropriate values? | |  |
| 5.6 | Do you have policies and technical controls in place for the management and use of privileged accounts? Please provide details. | |  |
| 5.7 | Do you have measures in place to prevent malware? Please provide details. | |  |
| 5.8 | Are all your systems and software supported, with the latest security patches installed? | |  |
| 5.9 | How do you manage Information Security with your suppliers and do you align with the [NCSC supply chain security requirements](https://www.ncsc.gov.uk/collection/supply-chain-security/principles-supply-chain-security)? | |  |
| 5.10 | Will any administration, hosting or any aspects of the service provided be sub-contracted, outsourced or delegated to another party? If Yes, provide details. | |  |
| 5.11 | Are sub-contractors bound by your information security and governance requirements and covered by the responses in this assessment? | |  |
| 5.12 | Do you have appropriate security controls in place to protect the admin and management interfaces of the service? Provide details. | |  |
| 5.13 | Are you able to provide audit logs on request? Please provide details. | |  |
| 5.14 | Do you have a policy and process for securely erasing data from devices or securely destroying devices containing data before they leave your control? Please provide details. | |  |
| 5.15 | Will you securely delete University of Aberdeen data from your systems at the end of the contracted term or on request by the University. Please provide details. | |  |

|  |  |  |
| --- | --- | --- |
| **6** | **PERSONAL DATA** | |
| The University must comply with United Kingdom data protection laws for the way that personal data is handled.   * **Personal data** is information about identifiable people and can include names, identification numbers, email addresses and IP addresses as well as data that provides information about that person’s characteristics or behaviour, online or offline. * The **controller** is the organisation that has primary responsibility for compliance with the law. The controller determines the purposes and means for which personal data is collected and used. Usually, the controller for supplier arrangements is the University. * A **processor** of personal data acts on behalf of the controller. A processor may collect, use, store and delete personal data to meet the controller’s requirements, but the processor cannot use the personal data for its own purposes.   If you need further background to complete this section, please see the Information Commissioner’s data protection guidance pages at: [www.ico.org.uk/for-organisations/guide-to-data-protection/](http://www.ico.org.uk/for-organisations/guide-to-data-protection/) | | |
|  | Question | Response |
| 6.1 | Will you be processing any personal data in this arrangement whether as a controller or a processor?  If No, go to section 7 |  |
| 6.2 | Will you be acting as a controller of any personal data in this arrangement?  If Yes, provide details of the personal data involved and your privacy notice. |  |
| 6.3 | Will you be acting as a processor of any personal data on behalf of the University in this arrangement?  If yes, provide details of the personal data involved. |  |
| 6.4 | If you are acting as a processor, do you have data processing contract terms and a description of processing that apply to this arrangement?  If yes, please attach them for review. |  |
| 6.5 | In which countries will personal data be processed and stored in this arrangement by you or your sub-processors? |  |
| 6.6 | Do any of the technical or organisational measures you have described in this questionnaire not apply to the personal data involved in this arrangement? |  |
| 6.7 | Are there any additional technical or organisational measures in place to protect personal data not otherwise described in this questionnaire? |  |

|  |  |  |
| --- | --- | --- |
| **7** | **INCIDENT RESPONSE** | |
|  | Question | Response |
| 7.1 | Do you have an Incident Response Plan and a mechanism to report relevant incidents to the University? |  |
| 7.2 | Please provide emergency contact details where the University can contact you in the event of a security incident. |  |
| 7.3 | Do you monitor systems for unusual activity on your systems and networks? Provide details. |  |