**Supplier Cyber and Data Assessment**

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 supplier’s own data, where a cyber-security incident affecting it, would significantly impact the supplier’s ability to meet their contracted obligations to the University.

**Please note that both Part 1 and Part 2 need to be completed before the assessment can start. Provide as much information as possible or there may have to be follow up questions or clarifications, resulting in a delay to the process.**

**Part 1: Proposal – for completion by the University of Aberdeen purchaser or person proposing the supplier**

|  |  |
| --- | --- |
| School / Professional Service |  |
| Contact member of staff |  |
| What services will the supplier provide?  Describe the activities they will undertake (e.g. cloud hosting, analytical services etc) |  |
| What University activities or business processes will the service support? (e.g. collaboration between students for teaching purposes, delivering communications to external stakeholders) |  |
| Will the supplier have access to, store, manage, or process any University data, personal data, be provided with a University login account, provide cloud-based services/Software as a Service, or have a connection to the University network? |  |
| 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 the proposed supplier**

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

**Provide as much information as possible or there may have to be follow up questions or clarifications, resulting in a delay to the process.**

|  |  |
| --- | --- |
| 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: |  |

|  |  |  |
| --- | --- | --- |
| **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? Provide details. |  |
| 2.3 | Do you have staff with a responsibility for information security and data protection? Provide details. |  |
| 2.4 | 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? Provide details. |  |
| 3.2 | Do you conduct regular vulnerability scans? Provide details. |  |
| 3.3 | Can the University of Aberdeen, at its own cost and by prior arrangement, commission penetration tests or vulnerability assessments of your systems? |  |
| 3.4 | Do you hold any relevant information security certifications? E.g. ISO 27001, Cyber Essentials, etc. Provide a copy of any certificates. |  |

|  |  |  |
| --- | --- | --- |
| **4** | **ACCESS** | |
|  | Question | Response |
| 4.1 | Provide details on access management procedures and security controls that are in place to prevent unauthorised access to data? |  |
| 4.2 | Do you have least privilege approach and do users have the minimum level of access to data, systems and networks required to do their job. Provide details. |  |
| 4.3 | Describe procedures and controls you have in place for the management and use of privileged accounts. |  |
| 4.4 | Do you mandate Multi-Factor Authentication for standard and privileged accounts? Provide details. |  |
| 4.5 | Do you conduct screening and employment checks for new staff? |  |
| 4.6 | Do you require staff to complete Information Security awareness training? Provide details. |  |
| 4.7 | Have you implemented appropriate segregation between users of the service to ensure that an incident affecting one customer will not affect others? Provide details. |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **5** | | **MEASURES** | |
|  | Question | | Response |
| 5.1 | Provide information on controls that are in place to ensure devices and data are protected from unauthorised access, damage, theft or interference? | |  |
| 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. Provide details. | |  |
| 5.3 | Do you encrypt data in transit both over the Internet and internally? Provide details. | |  |
| 5.4 | Do you use a firewall to protect connections to and from the Internet? Provide details. | |  |
| 5.5 | Provide information on controls and policies in place to ensure that default settings and passwords been changed to appropriate values? | |  |
| 5.6 | Provide information on policies and technical controls in place for the management and use of privileged accounts? | |  |
| 5.7 | If cloud services or Software as a Service is being provided, is data segregated from other customers? Provide details on how this is achieved and the policy | |  |
| 5.8 | Provide information on measures in place to prevent malware? | |  |
| 5.9 | Are all your systems and software supported, with the latest security patches installed? Provide details. | |  |
| 5.10 | 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)? | |  |
| 5.11 | Will any administration, hosting or any aspects of the service provided be sub-contracted, outsourced or delegated to another party? If Yes, provide details here and answer question 5.12. | |  |
| 5.12 | Are sub-contractors bound by your information security and governance requirements and covered by the responses in this assessment? | |  |
| 5.13 | Do you have appropriate security controls in place to protect the admin and management interfaces of the service? Provide details. | |  |
| 5.14 | Do you have processes and systems in place to collect and store audit logs? Provide the details on process and retention period | |  |
| 5.15 | Are you able to provide audit logs relevant to the University of Aberdeen on request? Provide details. | |  |
| 5.16 | Describe processes you have in place to review and monitor logs for malicious activities. | |  |
| 5.17 | Do you monitor systems for unusual activity on your systems and networks? Provide details. | |  |
| 5.18 | Do you have a policy and process for securely erasing data from devices or securely destroying devices containing data before they leave your control? Provide details. | |  |
| 5.19 | Provide details on how you will securely delete University of Aberdeen data from your systems at the end of the contracted term or on request by the University. | |  |

**Provide as much information as possible or there may have to be follow up questions or clarifications, resulting in a delay to the process.**

|  |  |  |
| --- | --- | --- |
| **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.   Any processing of personal data should ideally take place in the UK or EU, otherwise [appropriate safeguards](https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/data-protection-now-the-transition-period-has-ended/the-gdpr/international-data-transfers/) will be required to ensure that the processing is lawful.  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 | Will you be utilising any sub-processors to deliver the service? If so, please list these and where they are based/where they store data. Where outwith the EU or UK, can you confirm that you have appropriate contractual safeguards in place. |  |
| 6.5 | 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. A signed contract must be in place before any data processing can begin. |  |
| 6.6 | In which countries will personal data be processed and stored in this arrangement by you or your sub-processors? |  |
| 6.7 | Do any of the technical or organisational measures you have described in this questionnaire not apply to the personal data involved in this arrangement? |  |
| 6.8 | 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? Provide details. |  |
| 7.2 | Is the Incident Response Plan tested at least annually? Provide details. |  |
| 7.3 | Does the plan specify how soon after discovery you will notify customers of a breach? Provide details. |  |
| 7.4 | Please provide emergency contact details where the University can contact you in the event of a security incident. |  |

|  |  |  |
| --- | --- | --- |
| **8** | **BUSINESS CONTINUITY AND DISASTER RECOVERY** | |
|  | Question | Response |
| 8.1 | Do you have a managed process in place for developing and maintaining business continuity and disaster recovery plan? Provide details. |  |
| 8.2 | Are BC/DR plans approved by management? Provide details. |  |
| 8.3 | Is there a schedule that specifies how and when the BC/DR plans are to be tested? Provide details. |  |
| 8.4 | When were the plans last tested? Provide details. |  |

The University must comply with United Kingdom accessibility regulations. Does the service provided by the supplier include websites, web or mobile applications that fall under the scope of the *Public Sector Bodies (Websites and Mobile Applications) (No. 2) Accessibility Regulations 2018*? If so, please complete the Section 9 below:

|  |  |  |
| --- | --- | --- |
| **9** | **ACCESSIBILITY** | |
|  | Question | Response |
| 9.1 | Describe your company accessibility governance process. Please give examples of established procedures or working practices. |  |
| 9.2 | Provide details on how you ensure your development team have knowledge of accessible coding techniques; what training is provided to staff, and how staff are kept apprised of new accessibility developments. |  |
| 9.3 | If websites, web or mobile applications are provided, do these comply with the latest [Web Content Accessibility Guidelines](https://www.w3.org/WAI/standards-guidelines/) AA standards? |  |
| 9.4 | Describe how you would remediate accessibility issues identified by users of your product. |  |