The University of Aberdeen requires that all Cloud and Managed Service Providers manage information security risk and implement appropriate controls to minimise the impact of a cyber-security incident. The scope of risk includes University data and Cloud hosted systems that the supplier has been entrusted to host 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.

# 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: Service Provider details and responses

|  |  |
| --- | --- |
| Cloud Service Provider name: |  |
| Address: |  |
| Website: |  |
| 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** | **SERVICE MANAGEMENT** | |
|  | Question | Response |
| 1.1 | What is the cloud service model (IaaS, PaaS, SaaS)? |  |
| 1.2 | What is the cloud delivery model (on premise, private, shared, or public) |  |
| 1.3 | Is the cloud service offered in multi or single tenant cloud? |  |
| 1.4 | Is there a contract in place? |  |
| 1.5 | Has the contract or terms and conditions covered cloud shared responsibilities between the Cloud Provider and University? |  |
| 1.6 | Has the contract or terms and conditions covered Incident management responsibilities and communication procedures? |  |
| 1.7 | Does the contract or terms and conditions cover data privacy, including data processor clauses? |  |
| 1.8 | Does the contract or terms and conditions cover Service Level Agreement clauses? |  |
| 1.9 | Have agreements been made for an exit procedure (how and in what format do we receive the data and what assurance do we get about erasure of data)  Exit should be possible at any given time and for any reason UoA has. Likely reasons may be:  a. change in risk posture or law and regulation  b. when the performance of the supplier is not conforming to UoA standards.  c. when the supplier terminates activities (e.g. bankruptcy)  d. when the supplier is outsourcing activities.  e. when the supplier is acquisitioned by another company |  |
| 1.10 | Where is our data stored and processed? Please list all locations including country. |  |
| 1.11 | Does the contract or terms and conditions cover log data retention and auditing? |  |

|  |  |  |
| --- | --- | --- |
| **2** | **VULNERABILITY MANAGEMENT** | |
|  | Question | Response |
| 2.1 | Does the Cloud Service provider have a Vulnerability Management Process that remediates critical vulnerabilities identified within 15days? |  |
| 2.2 | How often do external penetration tests take place on web-facing or internal servers? Please share the latest penetration test report.  Describe the formal risk management process that provides detail on when vulnerabilities will be mitigated based on their severity |  |
| 2.3 | Can the University of Aberdeen, at its own cost and by prior arrangement, commission penetration tests of your systems? |  |

|  |  |  |
| --- | --- | --- |
| **3** | **ASSURANCE** | |
|  | Question | Response |
| 3.1 | Does the cloud provider have a ISO27001:2013, Cyber Essentials, NIST (or similar) certificate.  a. what is the scope of the certificate  b. and what is the Statement of Applicability (which controls are in scope)  c. what are the results of the last external audit |  |
| 3.2 | Does the cloud provider have a SOC2 (or similar) report?  a. what is the scope of this report  b. can the cloud supplier provide the actual report and findings |  |
| 3.3 | Describe the threat detection and protection measures that are in place? |  |

|  |  |  |
| --- | --- | --- |
| **4** | **ACCESS** | |
|  | Question | Response |
| 4.1 | Do you mandate Multi-Factor Authentication for standard and privileged accounts for all service users including, but limited to, supplier and University specific users? Please provide details. |  |
| 4.2 | List the Authentication methods supported by Cloud Service. |  |
| 4.3 | Does the Cloud Service support Identity and Access Management Federation with UoA Identity systems(SAML/OIDC)?  What data types are required to enable Identity federation with the Cloud Service? |  |
| 4.4 | Will the Cloud service comply with the Password Policy, UoA Access Control and Authentication Policy if the Cloud service does not support Identity Federation or integration? |  |
| 4.5 | How does your system support monthly/quarterly access reviews if Identity Federation is not supported by the Cloud Service? |  |
| 4.6 | Are user access and intra-tenant access for the UoA tenant adequately segmented, segregated, monitored, and restricted from other tenants? Please provide details. |  |
| 4.7 | Are there any IP addresses, network ports, protocols, processes, and applications that UoA would need to allowlist as part of the cloud Service implementation? Please provide list |  |
| 4.8 | Do you use a Web Application Firewall (WAF) to safeguard internet-facing web applications? If not, please provide information on the measures implemented to secure the cloud workloads. |  |
| 4.9 | Is the service utilizing Content Delivery Networks (CDNs) for the purpose of optimizing performance and ensuring availability? |  |
| 4.10 | Does the Cloud service integrate with other systems/APIs to provide a service to UoA? Please list all UoA, 3rd party systems/APIs that will be required to integrate with the Cloud Service and provide. |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **5** | | **ENCRYPTION** | |
|  | Question | | Response |
| 5.1 | Please described how you encrypt data in transit and at rest? Please provide details including, but not limited to, technical standards and ciphers used. | |  |
| 5.2 | Is the encryption key management life cycle maintained by CSP or UoA? Please provide details | |  |

|  |  |  |
| --- | --- | --- |
| **6** | **DATA PROTECTION** | |
| 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 | How does the Cloud assure compliance with UK GDPR and Privacy? Please provide links to the relevant policies. |  |
| 6.6 | In which region 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? |  |

|  |  |  |
| --- | --- | --- |
| **7** | **DATA HANDLING** | |
|  | Question | Response |
| 7.1 | Is there a data backup process in place to protect University Cloud Data and which country is the data stored? |  |
| 7.2 | Does the service have data backup and retention functionality? Please provide details. |  |
| 7.3 | Is there a sanitisation software or method for the media or devices utilised before reallocating to the UoA? |  |
| 7.4 | 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. |  |

|  |  |  |
| --- | --- | --- |
| **8** | **BUSINESS CONTINUITY** | |
|  | Question | Response |
| 8.1 | What are the Cloud Service Providers Disaster Recovery capabilities?  a. How often are DR exercises performed?  b. What back up provisions have been made?  c. What guarantees do the supplier give on the Recovery Time Objective (RTO) and Recovery Point Objective (RPO) |  |

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. |  |