

**Digital Systems**

**and**

**Cloud Services Policy**

**Appendix A**

# **Appendix A – Digital Systems and Cloud Services Checklist**

## **A.1 Introduction**

This checklist is intended to assist in the evaluation, procurement or use of digital systems and cloud services. Where difficulties are experienced completing this checklist advice should be sought from ISS – clearly indicating where there is uncertainty with the answer.

As requirements can vary, this document should be regarded as a non-exhaustive checklist that highlights to sponsors the implications of using digital systems and cloud services.

Please note that this document cannot anticipate every issue that might arise in every project nor is it intended to take the place of a properly resourced project proposal or plan.

## **A.2 Checklist instructions**

The answers to the questions should be in the first instance compiled by the University department(s) in MS Word.

Questions should be answered as concisely and as fully as possible in the document.

The input of vendors should be incorporated as needed. Inclusion of vendor promotional materials or references should be avoided or kept to the minimum.

If the question is not considered relevant or cannot be answered by the department, please state this in the table below.

Where answers are very detailed, place a reference (e.g. NOTE 1) in the table below and then a full reply placed at the end of the document.

Where the information in an answer is considered confidential, please preface the answer with [CONFIDENTIAL].

## **A.3 Checklist roadmap**

Completed self-evaluation checklist and associated documents should be submitted to ISS for further advice and/or recording.

Some projects may require input from the other University offices such as Data Protection, Procurement, Finance and others. If required, please contact the relevant office for additional advice.

## **A.4 DCU stakeholder and institutional requirements**

This section deals with the service and the implications of its use for the University. This section should be completed by DCU.

| **Ref:** | **Question** | **Answer** |
| --- | --- | --- |
| **A4. 1** | Which University departments are stakeholders in the proposed system? |  |
| **A4. 2** | List the names of university sponsors for the system. These would normally be Heads of Department, Schools, or senior members of staff. |  |
| **A4 .3** | Name of University Project Manager. |  |
| **A4. 4** | Name of departmental contact person (usually person collating the information in this document). |  |
| **A4. 5** | What business need(s) does this system fulfil?  Please append if available. |  |
| **A4. 6** | Is this a new system or replacing an existing system?  If replacing an existing system, please specify the name of the existing system. |  |
| **A4. 7** | Have detailed user requirements been documented and agreed by the stakeholders?  Please append if available. |  |
| **A4. 8** | What groups of people will be using this system? e.g. postgraduate students, staff members etc. |  |
| **A4. 9** | What would be the impact to university if the service were unavailable? |  |
| **A4. 10** | Is this a public or private cloud service?  A public service is offered without modification by the vendor.  A private service is where the vendor modifies the service to meet specific University requirements. |  |
| **A4. 11** | Does the application contain personally identifiable information (PII)?  If Yes, please specify what PII data will be stored in the system. |  |
| **A4. 12** | Can data generated by the vendor product be supplied to other University systems that might need it e.g. Student system?  This is to identify potential “silo” systems. |  |
| **A4. 13** | How long in years is it projected that the service will be used? |  |
| **A4. 14** | Please list independent reference sites and contacts using this service.  Site name and address:  Year started usage:  Site contract name and email:  Has these sites been contacted by DCU? |  |
| **A4. 15** | Will the system need data from core University systems such as Student Information System, Personnel or Finance Systems?  The permission of the relevant University data owner will be needed to use data of this type. | List of Data Owners |

## **A.5. Application Security Considerations**

This section outlines issues and security considerations in relation to the vendor offering the service. **This section should be completed by the application vendor/service provider.**

| **Ref.** | **Question** | **Answer** |
| --- | --- | --- |
| **Vendor Detail** | | |
| **A5. 1** | Vendor Name |  |
| **A5. 2** | Product Name |  |
| **A5. 3** | Product Description |  |
| **A5. 4** | When was the vendor company established? |  |
| **A5. 5** | What year did the vendor start to supply this service? |  |
| **A5. 6** | Vendor contact name |  |
| **A5. 7** | Vendor contact title |  |
| **A5. 8** | Vendor contact email |  |
| **A5. 9** | Vendor contact phone number |  |
| **A5. 10** | Which country or jurisdiction is the vendor based in? |  |
| **A5. 11** | How many higher education, commercial customers and government customers do you serve in Ireland and Europe?  If applicable, please provide a list of higher education customers. |  |
| **A5. 12** | Describe the structure and size of the vendors IT Security Office and overall information security staff. |  |
| **A5. 13** | Describe the structure and size of the vendor Software and System Development teams. |  |
| **Documentation / Compliance** | | |
| **Ref:** | **Question** | **Answer** |
| **A5. 14** | Does the vendor have a complete and successful SOC2 or SOC3 reports? If so, please provide your company's latest reports. |  |
| **A5. 15** | Does the vendor have system and/or process certifications?  If yes, please provide current attestations. e.g. ISO-27001, PCI-DSS, SSAE16, Cloud Security Alliance self-assessment, etc. |  |
| **A5. 16** | Please supply current copies or links to the vendors IT Security Policy and supporting documentation. |  |
| **A5. 17** | Please supply current copies or links to the vendors Privacy Policies. |  |

|  |  |  |
| --- | --- | --- |
| **Application Compatibility / Integration** | | |
| **Ref:** | **Question** | **Answer** |
| **A5. 18** | List any client operating systems or versions that the vendor product cannot work on. |  |
| **A5. 19** | List any client web browsers or versions that the vendor’s product cannot work on. |  |
| **A5. 20** | Are standard API interfaces provided by the vendor’s product?  Please provide details of interface types (REST, SOAP, etc.) supported. |  |
| **A5. 21** | Please provide reference documentation for each interface type and highlight any data/functionality that cannot be accessed via APIs. |  |
| **A5. 22** | What percentage of data / functionality is exposed via APIs? |  |
| **A5.23** | Does the vendor’s product support consuming DCU-provided RESTful APIs in a JSON format over HTTPS? |  |

|  |  |  |
| --- | --- | --- |
| **Architecture** | | |
| **Ref.** | **Question** | **Answer** |
| **A5. 23** | How many environments are provided with the solution, e.g. Production/ Test/ Development / Training? |  |
| **A5. 24** | Can access to the application be restricted to the University’s network? |  |
| **A5. 25** | Please provide overall system and/or application architecture diagrams including a full description of the data communications architecture for all components of the system. |  |
| **Cloud Architecture (if applicable)** | | |
| **Ref:** | **Question** | **Answer** |
| **A5. 26** | Which type of cloud service is being provided; SaaS, IaaS or PaaS |  |
| **A5. 27** | Is the service a single-tenant or multi-tenant environment? |  |
| **A5. 28** | Is the institution's data physically and logically separated from that of other customers? |  |

|  |  |  |
| --- | --- | --- |
| **Authentication, Authorization, and Auditing** | | |
| **Ref:** | **Question** | **Answer** |
| **A5. 29** | Can user access be customised to allow read-only access, update access, or no-access to specific types of records, record attributes, components, or functions? |  |
| **A5. 30** | Are passwords required to be at least fourteen (14) characters and do they comply with the University password policy? |  |
| **A5. 31** | Does the application support Shibboleth/SAML Authentication Protocol? If not, please specify what authentication protocols are supported. |  |
| **A5. 32** | Can a second factor of authentication be used for this solution? If yes, please provide details of what 2FA solutions are supported. |  |
| **A5. 33** | Does the application support password expiration? |  |
| **A5. 34** | Does the application require a user to set their own password after an administrator reset or on first use of the account? |  |
| **A5. 35** | Can the application lock-out an account after a number of failed login attempts? |  |
| **A5. 36** | Can the application automatically lock or log-out an account after a period of inactivity? |  |
| **A5. 37** | Are audit logs available that include all of the following: login and logout actions performed, including source IP address of client? |  |
| **A5. 38** | What measures are in place to ensure robustness and prevent tampering with the audit logs? |  |
| **A5. 39** | How does the solution detect and prevent unauthorised access attempts, such as suspicious login patterns (Geolocation), brute force password attempts, credential stuffing, etc. |  |

|  |  |  |
| --- | --- | --- |
| **Data Security** | | |
| **Ref:** | **Question** | **Answer** |
| **A5. 40** | Does the application contain personally identifiable information?  If Yes, please specify what PII data will be stored in the system. |  |
| **A5. 41** | Please outline the application backup procedures and the frequency that it is tested. e.g. the frequency of backups, off site locations, how many copies are retained, how long are backups retained, what encryption standards are used, frequency of integrity checks, etc. |  |
| **A5. 42** | What protocols will be used to protect application data in transit (e.g., TLS, SSL, SFTP, FTP/S)? Please provide technical details, including version information. |  |
| **A5. 43** | What encryption standards are used to protect data at rest e.g. database encryption, disk encryption, backup encryption, etc. Please provide details of encryption standards. |  |
| **A5. 44** | Will the vendor allow other organizations access to the data stored on the system? |  |
| **A5. 45** | Will the University retain ownership of the data at all times? |  |
| **A5. 46** | Who controls access to the data within the vendor’s organization? |  |
| **A5. 47** | Are vendor employees allowed to take home customer data in any form? |  |

|  |  |  |
| --- | --- | --- |
| **Data Protection** | | |
| **Ref:** | **Question** | **Answer** |
| **A5. 48** | How does the service comply with E.U data protection regulations (GDPR)?  Please provide details. |  |
| **A5. 49** | In which jurisdiction will the data reside, including backups? E.g. European Economic Area (EEA), USA, Australia etc.  If the data is to reside outside of the EEA, please specify what data protection arrangements are in place to ensure the data is protected in line with the EU General Data Protection Regulation 2016.  E.g. Application of one of the following:  EU/US Privacy Shield Framework  or  Use of Standard Contractual Clauses  or  Use of Binding Corporate Rules etc.  Further details of the above may be found at the link below:  [EU Guidance](https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection_en) |  |
| **A5. 50** | What procedures does the provider have in the event of a data breach?  The University’s Data Protection Officer must be informed of both a suspected and actual breach within 24 hours of the breach being discovered.  Contact email: [data.protection@dcu.ie](mailto:data.protection@dcu.ie)  Contact Phone # 700 7476 |  |
| **A5. 51** | Does the contractual and financial terms protect the University from a data breach by the provider? |  |
| **A5. 52** | How would the vendor address:  Persons who wish to view their data under Data Protection, Freedom of Information or other legislation.  Persons who wishes to amend or remove their data (Right to be forgotten). |  |
| **Data Centre Security** | | |
| **Ref:** | **Question** | **Answer** |
| **A5. 53** | List all datacentres, including cities and countries, where the institution's data will be stored. Does your company own these data centres? |  |
| **A5. 54** | Does the vendor own the physical data centre where University data will reside? If so, do these servers reside in a co-located data centre? |  |
| **A5. 55** | Does the hosting provider have a SOC 2 Type 2 report available? |  |

|  |  |  |
| --- | --- | --- |
| **Disaster Recovery & Business Continuity** | | |
| **Ref:** | **Question** | **Answer** |
| **A5. 56** | What would be the impact to the University if the service were unavailable? |  |
| **A5. 57** | What is the company's disaster recovery/business continuity policy and process?  Please provide details, including the frequency of DR/BCP tests. |  |
| **A5. 58** | How often is the DR/BCP tested? What was the date of the last DR test? |  |
| **A5. 59** | What is the communication plan in your DR/BCP for impacted clients? |  |
| **A5. 60** | Are any disaster recovery locations outside the EEA? If so, please provide the locations. |  |
| **A5. 61** | List Disaster Recovery;  RTO (Recovery Time Objective).  RPO (Recovery Point (Objective). |  |

|  |  |  |
| --- | --- | --- |
| **Application Security Controls** | | |
| **Ref:** | **Question** | **Answer** |
| **A5. 62** | Describe the development language(s) (Java, .NET, iOS, etc.) the application was / will be developed with. |  |
| **A5. 63** | Do all developers receive formal software security training? |  |
| **A5. 64** | Does your company use industry standards (e.g. OWASP for security applications) to validate security risks in applications? |  |
| **A5. 65** | Has the service been securely developed and configured to be available directly from the internet? |  |
| **A5. 66** | Is the system utilizing a web application firewall (WAF) and / or a stateful packet inspection (SPI) firewall? |  |
| **A5. 67** | Is the service monitored for intrusions on a 24x7x365 basis? |  |
| **A5. 68** | Describe or provide a reference to how the system is monitored for and protected against common web application security vulnerabilities (e.g. SQL injection, XSS, XSRF, etc.). |  |
| **A5. 69** | Will the University be immediately alerted of intrusions or malicious events? |  |
| **A5. 70** | Has the application undergone an independent third-party penetration test or security audit in the last year? If so, please provide details of the external company who carried out the test, the date of the last test and include a high-level overview of the results. |  |
| **A5. 71** | Are your applications and infrastructure scanned for vulnerabilities on a regular basis?  Please provide details of what tool(s) are used to scan the application and infrastructure. |  |
| **A5. 72** | What was the date of your last application/Infrastructure vulnerability assessment? (dd/mm/yyyy) |  |
| **A5. 73** | Describe or provide a reference to any other safeguards, security controls or intrusion prevention controls used to monitor or prevent attacks? |  |

**A.6 Support arrangements**

| **Ref** | **Question** | **Answer** |
| --- | --- | --- |
| **A6. 1** | Is there a roadmap for the service/application in terms of product updates/support and testing? |  |
| **A6. 2** | How is support provided by the company to your environment e.g. Helpdesk, remote management, is admin rights required? |  |
| **A6. 3** | Can you provide the solution or sample service level agreement (SLA) detailing maintenance and support services including scheduled maintenance plans, uptime, and response times? |  |
| **A6. 4** | Within the SLA, please outline response and resolution times for priority 1 to 4 support issues and penalties in place if SLA is not met? |  |
| **A6. 5** | Outline system upgrade, maintenance, and patching schedule? |  |
| **A6. 6** | Can the University delay upgrades to avoid disruption during peak business periods? |  |
| **A6. 7** | Are solution performance and availability metrics available online or through regular reports? |  |
| **A6. 8** | Please indicate if any other third party manages any part of the support? If the solution is a multi-vendor solution, please provide details of how support calls are managed. |  |
| **A6. 9** | Please describe your support organisation, account management, including locations and total number of support staff. |  |

**A.7 Exit strategy**

This section clarifies what happens when the cloud service ends.

| **Ref:** | **Question** | **Answer** |
| --- | --- | --- |
| **A7 .1** | What notice must the University give to terminate the service? |  |
| **A7. 2** | What notice does the vendor have to give to terminate the service? |  |
| **A7. 3** | How and in what format will the University data be available after termination? |  |
| **A7. 4** | Will the returned data be in a format that can be migrated to another future system? |  |
| **A7. 5** | Will the vendor be allowed keep copies of the data after the termination? |  |
| **A7. 6** | Will the vendor be able to demonstrate that all copies of the data will be destroyed, including backups? |  |

**A.8 Document checklist**

These documents are likely to be needed.  The variety of applications means a definitive list is difficult to compile.

|  |  |
| --- | --- |
| **Document name** | **Question #** |
| Fully completed checklist (this document) |  |
| Data Processing Agreement |  |
| Vendor IT security policy |  |
| Vendor Business Continuity Plan |  |
| Independent IT security audit |  |
| Vendor Service Level Agreement |  |