Digital Systems

and

Cloud Services Policy

Table of Contents Page

Introduction

This document sets out the Dublin City University (DCU) Policy for evaluating Digital Systems and Cloud Services (also known as “Cloud Computing” or “Cloud”).

Purpose

The policy is a statement of DCU’s commitment to ensuring that all its legal, ethical and policy compliance requirements, including cybersecurity needs are met in the procurement, evaluation and use of all digital systems and cloud services.

Scope

Who does this policy apply to?

This Policy applies to all staff of the University, both academic and support, including campus companies and research centres.

What data and information does this policy apply to?

This policy applies to all University data and information including, but not limited to, personal data, sensitive personal data (or special categories of personal data) and confidential business data and information.

Policy Statement

Ownership & Implementation

Whereas this Digital Systems and Cloud Services Policy document is owned by the University, it will be maintained by the Director of Information Systems Services on behalf of the University. Compliance with this Policy will be monitored by the IS Governance Committee supported by ISS. A completed checklist, as outlined in Appendix A, must be submitted to ISS for review and/or consultation. ISS will keep a record of all checklists submitted and report to IS Governance Committee as required.

Policy

The steps involved in procuring and evaluating digital systems and cloud services can be complex and subject to legal, ethical and policy compliance requirements. These requirements, outlined below, must be evaluated and met prior to using such services. This is essential to ensure that personal, sensitive and confidential business data and information owned, controlled, or processed by the University, its staff, students and its agents is adequately protected at all times.

1. Procurement

The purchasing of all digital systems and cloud services, including cloud services must comply with relevant university procurement policies and procedures. Those involved in the purchase of digital systems and/or services should be cognizant of the risk that purchases by different University units of the same digital system and/or service may inadvertently result in procurement thresholds being breached.

2. Data Protection

The General Data Protection Regulation (GDPR), and related legislation, requires that Data Controllers such as DCU meet significant obligations with regard to how personal data is collected, used and protected. All digital systems and cloud services used to process personal data or information must allow the University to meets those obligations. The University Data Protection Unit should be consulted prior to any new system and/or service implementation. In particular, regard should be given to the possible requirement for a Data Protection Impact Assessment (DPIA) in addition to a comprehensive Data Processing Agreement duly reviewed by the University Data Protection Officer (contact: data.protection@dcu.ie) prior to signing.

3. Approval to use University data

Where a digital service is proposed to host University data or information, appropriate written sign-off must be received from the data or information owner.

4. System / Service Security

Notwithstanding any assurances given by a system vendor as part of any data sharing agreements or vendor literature, all digital systems and cloud services must be thoroughly reviewed to ensure that best industry practice is employed to ensure system or service security.

5. Interoperability

The University places great emphasis on the need for integration and interoperability of systems. These requirements must be considered and documented as part of any service evaluation. ISS must be contacted at evaluation stage for advice where data from a proposed cloud service is required to integrate with a University system. Where integration is required, all University Policies, Guidelines and Procedures must be adhered to. The prioritisation of projects must be considered as part of service planning.

6. Disaster Recovery / Business Continuity

The service must be selected to ensure that the data and information is secure at all times and that an adequate backup and recovery plan is in place to ensure that data and information can be retrieve in a timely manner to meet business needs. For more critical systems, the service must be built with high availability, with a business continuity and disaster recovery plan that fits business needs. ISS must be contacted for advice and sign-off in advance where a cloud services/hosting is being considered to provide a business critical IT system.

7. Vendor Management and Governance

Effective vendor management and governance is key to ensuring that the University derives the best value and service from its investment in digital systems and cloud services. All new and existing vendors of digital systems and cloud services should be subject to ongoing assessments in the areas of contract, financial, performance, relationship and risk management.

The appendices (Apx. A & Apx. B) to this document are intended to assist staff in ensuring that the legal, ethical and policy compliance requirements are met. Where doubt exists in answering the questions outlined in the appendices, staff should seek advice from the appropriate area of the University e.g. ISS, Procurement Unit, Data Protection Unit etc.

Roles and Responsibilities

This Policy applies to all staff and students and to all agents or organisations acting for, or on behalf of, the University in the evaluation, procurement or use of digital systems and cloud services. In order to comply with this Policy, the individual or agent must ensure that all criteria outlined in this Policy have been met and submit their checklist (Appendix A – Digital Systems and Cloud Services Checklist) to ISS for review/record and DCU Procurement Unit as required, so the service can be evaluated. In certain instances, the submitted checklist may be submitted to the IS Governance Committee for review.

Related Documentation

Legal and policy basis

The procurement, evaluation and use of Digital systems and cloud services must;

- Comply with all existing University Policies;
- Adhere to data protection legislation and the General Data Protection Regulation (GDPR);
- Respect the intellectual property rights of others and not breach copyright when using cloud services;
- Meet University Accessibility Requirements; &
- Comply with the relevant professional ethics and the University code of ethics. Where ethical issues arise in the use of digital systems or cloud services, the guidance of the University's Ethics Committee must be sought in advance.

Contacts

Further clarification on this policy can be sought from the Director of ISS.

Policy Review

The Director of Information Systems Services (ISS) will draft necessary changes and have them reviewed and approved by the IS Governance Committee as appropriate. Anyone in the University can determine the need for a modification to the existing policy. Recommendations for changes to this Policy should be communicated to the Director of ISS. This policy should be reviewed annually.

Version Control

Document Name	Digital Systems and Cloud Services Policy
Version Reference	1.0
Document Owner	Director of ISS
Approved by	DCU Executive
Date	June 23rd 2020

End.

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 considerably this document should be regarded as a non-exhaustive checklist that highlights to sponsors the likely 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 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 advice/record.

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.	NO/PUBLIC/PRIVATE

Ref:	Question	Answer
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.	

Ref.	Question	Answer
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 customized 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	

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 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	

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

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	

Appendix B – General Advice on Contractual Issues

The details provided below are for information purposes only and does not constitute legal advice. For specific legal advice, please contact the Office of the Chief Operations Officer.

B.1 Contracts

If you propose to use a digital system or service, you must have a contract in place with the third party that covers the provision of the service. Matters to be included in the contract are:

- Data protection;
- Intellectual property rights;
- Freedom of information obligations;
- Legal compliance;
- Law enforcement and loss of control;
- Licensing;
- Confidentiality of data;
- Monitoring by the cloud provider;
- Law and jurisdiction;
- Data retention schedules;
- Subcontracting;
- Acceptable use policy;
- Warranties;
- Indemnities;
- Exclusions and limitations of liability;
- Change of service by the cloud provider;
- Termination; &
- Disaster Recovery / Business Continuity.
-

B.2 Transfer of personal data outside of the EEA

If personal data is likely to be stored outside the EEA, you might be in breach of the General Data Protection Regulation (GDPR) unless there are adequate security measures in place for personal data. Compliance may be achieved if EU approved contract clauses are used with the provider. Alternatively, if using a US based provider, ensuring that they are signed up to the EU/US Privacy Shield provisions will be necessary.

Further details on your obligations when considering sending personal data outside the European Economic Area are available on the European Commission's website at the link below:

International Dimension of Data Protection

In all cases, please contact the DCU Data Protection Unit (DPU).

B.3 Service level agreement

A service level agreement (SLA) describes the service that the third party will provide, the performance targets (e.g. service availability, problem resolution, support, incident resolution, change control, security, etc.) and mechanisms for compensating the University if the SLA targets are not met. You must ensure that the contract for digital systems and cloud services includes an SLA that meets your business needs.

B.4 Agreeing the right terms with a vendor

The vendor contract on offer must be examined in detail and favourable and constructive terms negotiated with the provider to ensure that they are appropriate to the work that the University carries out.

Vendors are likely to offer the same (standard) service to multiple users so the University may have to change its applications and processes to match what is offered.

The key to the negotiation at this point is to ensure that enough control is maintained in house in order to minimise the legal risks while still taking advantage of the opportunities that digital services can bring.

End of Appendices