IT Disaster Recovery & Data Backup Policy

Policy Name – IT Disaster Recovery & Data Backup Policy	
Version number: 1.0	
Policy Owner	**Policy Author/Reviewer**
Digital Governance Risk & Compliance	Steve Coyle Digital GRC
Approving body	**Date of approval**
Digital Services Directorate	January 2024
	Equality Screened
	Yes
	Next Review date
	January 2026
Queries relating to this document should be directed to the Policy Owner – Digital Governance, Risk & Compliance via the Digital Services IT Service Desk https://www.ulster.ac.uk/ds/getting-help/service-desk. This document can be made available on request, in alternative formats and in minority languages to meet the needs of those who are not fluent in English.	

Contents

1 AIMS, PURPOSE & SCOPE 3
2 APPLICABLE SUBJECTS 3
3 POLICY STATEMENT 3
4 COMMUNICATION, IMPLEMENTATION & TRAINING 4
5 COMPLAINTS 4
6 RELEVANT LEGISLATION 5
7 RELATED DOCUMENTES REFERENCED 5
8 CONTACT DETAILS 5
9 DOCUMENT HISTORY 5

1 Aims, Purpose & Scope

The principles of information security require that all reasonable care be taken to prevent inappropriate access, modification, loss or manipulation of Ulster University data and systems.

Ulster University expects the highest standards of information security, regardless of whether information belongs to Ulster University, it's people (staff), it's third parties/interested parties, or its customers (students and research award bodies). Every person who uses Ulster University services has a shared responsibility to keep information safe. This policy sets out Ulster University's commitments to information security and what is expected from service users.

It is vital that information assets are protected from external and internal cyber threats (e.g., malware). by implementing technical controls, physical controls, training and awareness, personnel vetting and screening, and other applicable methods/controls.

In alignment with the Data Protection Act the university is obliged to ensure that information is only accessible by those who are entitled to access it and within the scope of the purpose it was obtained and stored.

Ulster University maintains a large amount of potentially sensitive data for both customers and Ulster employees. Should a major data breach occur Ulster University's reputation would be tarnished. In addition, there is a high risk of incurring GDPR fines imposed by the information Commissioners Office (ICO).

Ulster University working towards ISO27001 framework, and all its digital policies and standards are aligned to the requirements for ISO27001.

2 Applicable Subjects

All Ulster University staff, students, agency staff, visitors, contractors, and third-party users have a responsibility to ensure that they keep information safe. This is to be achieved by adhering to Digital Services policies and standards. A library of these policies and standards can be accessed at the following link IT Policies - Home (sharepoint.com).

3 Policy Statement

Every person that uses digital services provided by Ulster University has a responsibility to keep information and computer systems and the devices used to access these services safe.

As a result of this collaborative action Ulster University aims to maintain the confidentiality, integrity, and availability of information.

4 Communication, Implementation & Training

Training and communication will be via a learning management tool, which is auditable.

5 Complaints

Queries are to be directed to the Service Desk, contactable at servicedesk@ulster.ac.uk or +44 28 95367776 https://www.ulster.ac.uk/ds/getting-help/service-desk.

6 Relevant Legislation

Refer to Applicable Legislation Ulster University for a list of applicable legislation.

7 Related Documents Referenced

- Acceptable Use Standard
- Authentication Standard
- Bring Your Own Device Standard
- Data Centre Access Policy
- Digital Information Assurance Policy
- Disposal of IT Devices Standard
- End User Device Standard
- Enterprise Application Standard
- Enterprise Infrastructure Standard
- IT Documentation Life Cycle Process
- IT Monitoring Standard
- Network Standard
- Password Standard
- Physical Security Standard
- Protective Marking Standard
- Ransomware Communications
- Ransomware Policy
- Record Management Policy
- Records Retention and Disposal Schedule
- Remote Access Standard
- Secure Storage and Archival Standard
- Systems Administrators Standard

- User Account and Access Policy
- User Account Management Standard
- Wireless Network Standard

8 Contact Details

ICT Governance via the Digital Services IT Service Desk
https://www.ulster.ac.uk/ds/getting-help/service-desk

Security: In case of Emergency telephone 028 70123456

9 Document History

Author	Status	Version	Date	Description
ICT Governance (SC)	Draft	0.1	12/01/2022	Draft
ICT Governance (SMcA)	Draft	0.1	02/03/2022	Reviewed
ICT Governance (SC)	Draft	0.1	30/03/2023	Templated