Ransomware Policy

Policy Name – Ransomware 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 DOCUMENT MANAGEMENT 2
2 POLICY STATEMENT..... 4
3 RELEVANT LEGISLATION..... 4
4 CONTACT DETAILS 4
5 DOCUMENT HISTORY 4

1 Document Management

Name:	Data Destruction Policy
Version number	1.0
Current Status (of this document)	Accepted and published by OUS

Policy Owner	The Deputy Chief Digital and Information Officer
Department	Digital Services
Policy Author/Reviewer	ICT Governance

Approving Body	**Date of Approval**
Digital Services Directorate	January 2024
Version approval date	**Equality Screened**
	Next Review Date

Notes:

2 Aims, Purposes & Scope

This policy is to define a how the university deal with ransomware events.

3 Definitions

Ransomware is a type of malware that attackers use to infect systems and encrypt the data until a Ransom is paid. There is no guarantee that the data will be decrypted after the ransom has been paid, or that the attacker won't make the data available on the internet for others.

In some cases, certain types of Ransomware spreads itself to other connected systems, such as connected computers, file servers and removable storage devices. If it successfully connects, it will encrypt the data on those systems too.

In the event of a Ransomware incident, it is important that Ulster University understands what needs to happen and can respond in a calm and methodical manner to contain and eradicate the threat, in order to limit any impact to staff, students, and its partners

4 Policy Statement

Ransomware demands must not be paid.

5 Communication, Implementation and Training

Service Desk Officer will notify the Cyber Security Team of any ransomware events. The Cyber Security Team will manage the ransomware event in line with the Ransomware Playbook and Ransomware Communications Table
request a copy of the data deletion log to evidence the deletion of materials form cloud storage

6 Complaints Procedure

Complaints should be directed to ICT Governance via email:
ICT-Governance@ulster.ac.uk

7 Relevant Legislation

See Applicable Legislation Ulster University

8 Related Policy Documents Referenced

Ransomware Communications Table
Ransomware Playbook

9 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

10 Document History

Author	Status	Version	Date	Description
ICT Governance (SC)	Published	1.0	January 2024	Approved by DS Directorate
ICT Governance (SC)	Draft	1.0	02/10/2024	Template Formatting