IT Security Policy

Framework

Table of Contents

1. Purpose

A full list of Information Security Policies has been collated based on the ISO-27000 series of standards and ITIL best practices. This list is included in the Appendix.

Not all Information Security policies and procedures fall under IT Services. The purpose of this document is to focus on the IT Security related policies, to align the policies, procedures and guidelines that are needed to govern IT Security in University College Dublin. The interpretation of the meaning of "Policy", "Procedure" and "Guideline" have been taken from the UCD Policy Management Framework.

The University endeavours to ensure consistent, high quality implementations and management of its IT resources, processes, and practices. A comprehensive framework of well-defined Policies, Procedures and Guidelines is required to facilitate and ensure this.

2. Scope

The IT Security Policy Framework covers IT Security policies, procedures, and guidelines relating to the University's IT resources and electronic information assets.

The covers all users of IT services including but not limited to University students, faculty, staff, contractors, and visitors.

3. IT Security Policies, Procedures, and Guidelines

The following is a list of IT Security policies, procedures, and guidelines for University College Dublin. These documents will be reviewed on a regular basis, at a minimum of every 3 years. Links to a list of IT Security documents including policies, procedures, and guidelines are available on the IT Services website https://www.ucd.ie/itservices/ourservices/security/policiesandprocedures/

Name	In UCD Policy DB?	Date of last review	Document Owner	Governance	Comments
Policy					
Password Protection Policy	Y	Sept 2024	Programme & Risk Management	UMT	
Acceptable Use Policy	Y	Feb 2021	Programme & Risk Management	UMT	
Device Protection Policy	Y	Nov 2022	Programme & Risk Management	UMT	
Third Party Applications Integration Policy	N	Jun 2022	Programme & Risk Management	ITLG	

Firewall Technical Policy	N		Infrastructure		No university firewall policy but there are five technical policies (Bus systems, Server-Farm, Research, Wireless and LAN) implemented on the firewall. These are maintained locally by the teams in Infrastructure.
Digital Governance Policy	N		IT Services	UMT	A project is underway to create a new Digital Governance Policy
Procedures					
Wireless Access	N	2021	Infrastructure	ITLG	
Network Registration Procedure	N		Infrastructure	ITLG	Procedure to be reviewed as part of the Network Registration Renewals Project in the Cybersecurity Programme Plan.
IT Security Incident Response Procedure	N	Mar 2023	Programme & Risk Management	ITLG	
IT Security Review Procedure	N	Apr 2024	Programme & Risk Management	ITLG	
VPN Access Procedure	N		Infrastructure	ITLG	
Data Backup and Monitoring Procedure	N		Infrastructure	ITLG	There is no link available, but documentation is maintained locally per application.
IT Services Change Control Process	N	Feb 2024	Programme & Risk Management	ITLG	
IT Accounts and Access Services	N	Apr 2024	Customer and Academic Services	ITLG	Current link and Knowledge Article
Change Control for Business Systems	N	Aug 2017	Enterprise Applications	ITLG	
Oracle Development Standards	N	2015	Enterprise Applications	ITLG	
Testing Strategy	N	2012	Enterprise Applications	ITLG	
Managing Access to Business Systems	N	Jan 2021	Programme & Risk Management, Enterprise Applications, Registry, Finance &	Programme & Risk Management	.

			Human Resources		
Guidelines and Standards					
Cloud Computing Guidance	N	Jun 2023	Programme & Risk Management	Programme & Risk Management	
IT Security Cloud Security Checklist	N	Apr 2024	Programme & Risk Management	Programme & Risk Management	
Website Protection Guidelines	N	Sept 2016	Enterprise Applications	Enterprise Applications	
Encryption Guidelines	N	Sept 2022	Programme & Risk Management	Programme & Risk Management	
Server Security	N	Sept 2024	Infrastructure	Infrastructure	
Device Security	N	Sept 2022	Programme & Risk Management	Programme & Risk Management	
Information Protection	N	Sept 2022	Programme & Risk Management	Programme & Risk Management	
File Storage and Sharing Guide	N	Jun 2024	Enterprise Applications	Enterprise Applications	
Disposal of IT Equipment	N		Customer & Academic Services	ITLG	
Multi Factor Authentication & Duo	N	Jan 2021	Infrastructure	Infrastructure	
Remote Access Standards	N	Jan 2023	Programme & Risk Management	Programme & Risk Management	
Technical Standard for use on IT procurements	N	Nov 2022	Programme & Risk Management	Programme & Risk Management	
Digital Solutions Deployment Guide	N	Apr 2023	Programme & Risk Management	Programme & Risk Management	

4. Other known policies, procedures, and guidelines

The following is a list of University policies, procedures, and guidelines that impact IT but are not owned by IT Services.

Type of Documentation	Name	Date of last review	Document Owner

Policy	Payment Card Security Policy	Sept 2018	UCD Finance
Policy	Data Request Policy	Oct 2017	Data Protection Office
Policy	Research Data Management Policy	Jun 2022	UCD Research
Guidelines	Personal Data incident and Breach Management	Jun 2022	Data Protection Office
Guidelines	Leaving UCD	Oct 2022	UCD HR

5. Revision History

The Framework will be reviewed and updated on a regular basis or as required by Legal, Regulatory, technical, or administrational needs.

Version Number	Date	Summary of Changes	Approved By
3.0	12th May 2020	First edition for publication	ILTG
3.1	14th May 2020	Minor updates added	ILTG
3.2	2nd Mar 2021	Updates to AUP, Device Protection and other minor modifications	IT Security & circulated to ITLG
3.3	9th Sept 2022	Updates to Third Party Applications Integration Policy and other minor modifications	IT Security & circulated to ITLG
3.4	15th Feb 2023	Updates to Remote Access Standards and other minor modifications	IT Security & circulated to ITLG
4.0	03 Mar 2023	Digital Governance Policy and Major IT Incident Response Plan added	IT Security & circulated to ITLG
4.1	27th Sept 2023	New additions: ● Technical standard for use on IT procurements ● Added Digital Solutions Deployment Guide ● UCD IT Services Standards for generation of UCD Email addresses other minor modifications	IT Security & circulated to ITLG
4.2	27th Mar 2024	Minor modifications to links	IT Security & circulated to ITLG
4.3	22nd Oct 2024	Updates to Password Protection Policy and other minor modifications	IT Security & circulated to ITLG

Appendix – Best Practice Information Security Policies

Policy	Comment/Current Status
Acceptable Use Policy	Updated February 2021
Password Protection Policy	Updated September 2024
Device Protection Policy	Created January 2021
Remote Access Policy	No policy exist but there is a Remote Access Standards created January 2023
Firewall Policy	A technical firewall policy was implemented as part of the Enterprise Firewall Project.
Payment Card Security Policy	A policy exists created in 2018 and owned by UCD Finance.
Data Request Policy	Created in 2017 and is currently under review by UCD Data Protection Office.
Social Media Management	We are not aware that a policy exists. This falls outside of the remit of IT Services, possibly one for the Communications Office.
Data Governance	We are not aware that a policy exists. This falls outside of the remit of IT Services, possibly one for the Data Protection Office.
Third Party Outsourcing	We are not aware that a policy exists. This falls outside of the remit of IT Services.
Encryption Policy	No policy exists as IT Services does not manage encryption on users' devices. There are guidelines on the UCD IT Security website.
Anti-Virus Policy	Anti-virus is referred to in the Acceptable Use Policy and Device Protection Policy rather than a specific AV policy.
Data Retention Policy	This falls outside the remit of IT Services. The Data protection has a GDPR webpage There are also Data Storage and Retention Guidelines owned by UCD Research Ethics.
Change Control Policy / Change Management Policy	No policy exist but there is a Change Control Process
Information Security Policy	No such policy exists but from the IT perspective, the Acceptable Usage Policy is very far-reaching and is backed up by other procedures e.g. a IT Security Incident Response Procedure, Remote Access Standards
Incident Management Policy	No policy exists but currently there is a IT Security Incident Response Procedure
Cloud Security Policy	No policy exists. IT Services does not have any governance over the local use of cloud solutions but currently there is Cloud Computing Guidance and the IT Security Cloud Security Checklist document which is used for IT Services advisory purposes.
Vulnerability Management Policy	No policy exists. Currently the Acceptable Use Policy and the Device Protection Policy is used in the notification of scanning, owner's responsibility, and removal of device from the UCD Network.
Data Classification Policy	No policy exists and is out of the remit of IT Services. IT Services have File Storage & Sharing Guide

Data Protection Policy	Possibly this is now represented by GDPR. This falls under the UCD Data Protection Office.
Asset Management Policy	This is outside of the remit of IT Services. We are not aware of a policy.
Equipment and Media Disposal Policy -IT information Assets	No policy exists but there is Disposal of IT equipment Guidelines
Access Control Policy	No policy exits.
Physical Access / Environmental Security Policy	No policy exists.
Data Centre and Comms Room policy	No policy exists but there are Terms and Conditions of access and use. There is also a FAQ section that covers procedures/guidelines for hosting customers and their equipment.
Server Security Policy	No policy exists. Currently there is guidelines on Sever security
Email/ Communication Policy	No policy exists. Currently the Acceptable Use Policy is used to inform users of access rights.
Data Backup Policy	No policy exists but there is a Data Backup Procedure, but there is no central repository. Currently documentation is maintained locally per application requirements.
Vendor Management Policy	We are not aware that a policy exists. Possibly this would fall under the Procurement Office.
Leaver mover Policy	No policy exists. But there is a Leaving UCD Guidelines on the UCD HR website. Currently the Acceptable Use Policy is used to inform users of access rights. Users also sent an email to inform them that their email will be disabled a month after their leaving date.
BYOD Policy (Device Protection Policy)	Device Protection Policy created January 2021.
Vendor Remote Access Policy	No policy exist but there is a Remote Access Standards created January 2023
Vulnerability Management/ Patching Policy	No policy exists. Currently the Acceptable Use Policy and the Device Protection Policy is used to inform users that devices should have an up to date OS, application for users. IT Services systems documentation is maintained locally per system requirements.