IT SECURITY POLICY

Contents

1 Introduction

1.1 Purpose

UL recognises that information and IT assets are critical business assets of the University. These assets include, but are not limited to, all infrastructure, networks, hardware, and software, which are used to manipulate, process, transport or store Information owned or processed by UL.

UL is committed to preserving the confidentiality, integrity and availability of information used by the institution and maintained on behalf of students, researchers, employees, external stakeholders and government agencies.

1.2 Scope

1.2.1 To whom does the policy apply?

The IT Security Policy applies to all Staff and Students of the University of Limerick, visitors, contractors, third party agents and all other affiliate associates and users of UL IT and Information assets.

This policy should be read in conjunction with the University of Limerick's Acceptable Usage Policy and other supporting policies and procedures.

1.2.2 In what situations does the policy apply?

This Policy, along with relevant supporting policies, relate to use of all:

- UL networks connected to the UL Backbone
- UL-owned/leased/rented and on-loan facilities.
- Private or cloud systems (whether owned/leased/rented/on-loan) when connected to the UL network directly, or indirectly.
- UL-owned/licensed data/programs, on UL and on private systems.
- Data/programs provided to UL by sponsors or external agencies

1.2.3 Who is responsible for ensuring that the policy (and any associated procedure) is implemented and monitored?

Within UL, and under the direction of the CFPO, the Information Technology Division (ITD) has overall responsibility for leading the IT Security Management objectives of the institution.

In order to ensure that IT Security Risks are identified and managed In line with UL's Risk Management policy, ITD has implemented IT security controls and management reporting within the Quality Management System of the IT Division

1.3 Definitions

1.3.1 System or Information System

This is a group of related hardware units, software programs and/or business processes dedicated to a single application or business purpose

1.3.2 System Owner

This is the Head of the Faculty or Department that utilises the system to perform their day to day operations, this system owner is responsible for the confidentiality, integrity and availability of information in the asset in question

1.3.3 System Administrator

This is the person responsible for the upkeep, configuration, and reliable operation of a computer system or systems

1.3.4 System Users

These are students, employees, consultants, contractors, agents and authorized users accessing UL IT systems and applications.

1.3.5 Internet

The internet is a globally connected network system that uses a suite of communication protocols to transmit data via various types of media. The internet is a network of global exchanges – including private, public, business, academic and government networks – connected by guided, wireless and fiber-optic technologies.

1.3.6 Virus

This a piece of code which is capable of copying itself and typically has a detrimental effect, such as corrupting the system or destroying data

1.3.7 Malware

This is software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system

1.3.8 Phishing

This is the fraudulent practice of sending emails purporting to be from reputable companies or individuals in order to induce users to reveal sensitive information, such as passwords and credit card numbers

1.3.9 Multi-Factor Authentication (MFA)

Multi-Factor authentication (MFA) is a security technology that requires multiple methods of authentication from independent categories of credentials to verify a user's identity for a login or other transaction.

2 Context

2.1 Legal and Regulatory Context

2.1.1 Data Protection Laws and Legislation in the Jurisdiction

The University is committed to complying with all applicable Data Protection, privacy and information security laws and regulations in the locations in which it operates.

2.2 Other Context

2.2.1 UL IT Security Governance

The IT security governance model is the management system by which UL directs and controls IT security and provides oversight to ensure that identified IT Security risks are adequately mitigated. IT Security management ensures that controls are implemented to mitigate identified risks. Security of UL's IT and data assets requires a coherent governance model that ensures that all IT systems in the University are operated in accordance with approved policy and best practice.

IT Security Management
Within UL, the Information Technology Division (ITD) has overall responsibility for leading the IT Security Management objectives of the institution. In order to ensure that IT Security Risks are identified and managed In line with UL's Risk Management policy, ITD has implemented IT security controls and management reporting within the Quality Management System of the IT Division.

As part of ITD's monthly and quarterly Quality Management reviews, IT Security related incidents, events and security related KPIS are measured and reported on. Interventions and controls are implemented where incidents and risks are identified through this management review process. IT Security risks where identified are recorded and managed via ITD risk register. Where the risk rating requires, IT Security risks may be escalated to the fundamental risk register of the University and the University's Risk Management function notified, in accordance with UL's Risk Management Policy.

ITD periodically reports on IT related risks including security risks to the University's Audit and Risk Committee of the Governing Authority.

Enterprise Architecture Review Board
ITD's Enterprise Architecture (EA) Review Board meets periodically to review the non-functional aspects of business change and IT projects within UL's IT ecosystem. One of the guiding principles of the EA Review Board is to ensure that changes and IT systems are aligned with good practice from an IT Security and IT Architecture perspective. It is the role of the EA Review board to review new IT initiatives and make recommendations on design and implementation to ensure that IT security and IT architecture are considered from a design perspective and the UL's IT Systems and data are not compromised as a result of new initiatives and projects.

Cloud Governance Group

Cloud services provide significant benefits to individuals and organisations with increased solution choice, flexibility, scalability and faster time to solution. Challenges can arise without the appropriate checks and due diligence, which can lead to significant risks for the University:

- Data Security risks to University of Limerick Data with services that have not been assessed if fit for purpose
- Compliance issues with current UL Data Protection Policy and Regulations
- Contractual issues which may leave UL inadequately protected from a legal or 3rd party contract standpoint

UL has established a Cloud Governance Working Group with appropriate collective expertise to give guidance to UL stakeholders on the use of Cloud Services. The Cloud Governance Group's responsibilities include conducting reviews for approving Cloud solutions to ensure adopted cloud solutions:

- Are aligned with IT Security Best Practices
- Have appropriate data protection provisions
- The SLA's & contracts are fit for service purpose

The Cloud Governance Group meets monthly and proposals to adopt cloud can be submitted and the Group can be consulted for advice and guidance on the existing and proposed future use of industry cloud solutions to address business needs.

2.2.2 UL Risk Management Framework

The UL Risk Management Framework is an iterative process consisting of steps when taken in sequence, enable continual improvement in decision making. It constitutes a logical and systematic method of identifying, analysing, evaluating, treating, monitoring and communicating risks associated with any activity, function or process in a way that will enable the University to minimise losses and maximise opportunities.

The University of Limerick Risk Management Framework provides assurance from academic and administrative functions to the senior management team and, through the team, to the Audit & Risk Committee and Governing Authority. Effective risk management focuses on understanding and measuring risk rather than necessarily avoiding or totally eliminating it and comprises the following components:

- Risk Identification
- Risk Assessment
- Risk Monitoring and Reporting
- Risk Appetite
- Risk Management

With regard to Compliance, Regulation and Ethics matters, the University is committed to maintaining the highest standards of integrity, compliance, and ethics. As such the University has **no appetite** for any breaches in statute, regulation, professional standards, research ethics, bribery, or fraud.

2.2.3 UL Management Roles and Responsibilities

The UL Executive Committee
The UL Executive Committee is responsible for supporting the Director of ITD in the enforcement of the Policy where necessary.

Faculty Deans and Directors of Administrative Areas
Faculty Deans and Directors of administrative areas are required to familiarise themselves with the Policy. Where a breach of the Policy is highlighted, faculty Deans and Directors of administrative areas must co-operate in ensuring that appropriate action is taken. Faculty Deans and Directors of administrative areas are obliged to ensure that all IT systems under their remit are formally administered either by an administrator appointed by the head of an academic and administrative area or centrally by ITD.

The Director of the Information Technology Division
The Director of The Information Technology Division or his/her deputy is responsible for the management of the UL Network and for the provision of support and advice to all nominated individuals with responsibility for discharging these policies.

The Information Security Team
The Information Security Team is responsible for:

- Advising the University officers, Administrators, Director of ITD and other appropriate persons on compliance with this Policy and its associated supporting policies and procedures.
- Reviewing and updating the Policy and supporting policies and procedures.
- The promotion of the Policy throughout the University.
- Periodic assessments of security controls as outlined in the Policy and supporting policies and procedures.
- Investigating security incidents as they arise.
- Maintaining records of security incidents.
- Ensuring that IT Security awareness training is promoted and encouraged on an ongoing basis to staff and students of the University. This is to ensure that the necessary precautions are taken at an individual level by stakeholders to protect themselves and the University against the cyber-threat landscape.

Information Systems Users
It is the responsibility of each individual Information Systems user to ensure his/her understanding of and compliance with this Policy.

All individuals are responsible for the security of University Information Systems assigned to them. This includes but is not limited to infrastructure, networks, hardware, software and the handling of data. Users must ensure that any access to these assets, which they grant to others, is for University use only, is not excessive and is maintained in an appropriate manner.

3 Policy Statements

3.1 IT Security Principles

3.1.1 *UL will endeavour to ensure that information is created, used and maintained in a secure environment.*

3.1.2 *UL will endeavour to ensure that computing facilities, programs, data, networks and equipment are adequately protected against failure, loss, misuse or abuse.*

3.1.3 *UL will endeavour to ensure that all users are aware of and fully comply with the Policy and the relevant supporting policies and procedures.*

3.1.4 *UL will endeavour to ensure that all users are aware of and fully comply with the relevant Irish and European Community legislation.*

3.1.5 *UL will endeavour to create awareness that appropriate security measures must be implemented as part of the effective operation and support of Information Security.*

3.1.6 *UL will endeavour to ensure that all users understand their own responsibilities for protecting the confidentiality and integrity of the data they handle.*

3.1.7 *UL will endeavour to ensure that University owned assets have an identified owner /administrator.*

3.1.8 *UL will create awareness of the cyber security threat environment that exists for the institution and its users, in conjunction with the availability and delivery of mandatory cybersecurity awareness training to UL staff.*

4 Related Procedures for IT Security

4.1.1 Computing Resources

University computing resources are provided to facilitate a person's work as an employee or student of the University of Limerick and/or for educational, training, or research purposes. Computing or network resources must not be used for commercial or personal gain.

Users of the University Computing resources must maintain awareness of and comply with this Policy and related Policies. Users must also maintain awareness of and comply with related ITD procedures which include, but are not limited to, ITD User Access Control Procedures, ITD Network Security and Remote Access Procedures, ITD Mobile Device Management Procedures and ITD Disaster Recovery Procedures

While the University respects every individual's right to privacy, UL reserves the right to examine all information stored or transmitted on UL systems and networks, including Internet usage and Email, and will perform audits and inspections on a regular basis as required.

4.1.2 Software & Licensing

Software and/or information provided by the University of Limerick may only be used as part of the user's duties as an employee or student of the University or for educational purposes.

The user agrees to abide by all the licensing agreements for software entered into by the University.

4.1.3 User Accounts

Students and staff are allocated individual accounts to use University computing resources. Each account has a username and password. These are for the exclusive use of the person using computing resources. Unauthorised use must not be attempted to or made of computing or network resources allocated to another person.

The user is responsible and accountable for all activities carried out under his/her username. The password associated with a particular personal username must not be divulged to another person.

4.1.4 Security Awareness

Online IT Security Awareness training should be taken by all Users to develop an awareness of common cyber threats, such as phishing and other types of scamming, which can threaten the integrity of the university's computing infrastructure and compromise those that connect to it and their information.

4.1.5 Privacy

No user shall interfere or attempt to interfere in any way with information belonging to another user. Similarly, no user shall make unauthorised copies of information belonging to another user. The ability to undertake a particular action does not imply that it is acceptable.

Users must not use any of the University's computing or network resources to make use of, or publish material that is obscene, libellous or defamatory or in violation of any right of any third party.

Normal behaviours that apply to traditional, non electronic media apply similarly to computer based information.

4.1.6 Copyright

Any software, data or information which becomes available through the use of computing or communications resources shall not be copied or used without permission of the University, or any other owner of the software, data or information.

The user must not infringe any copyright residing in documentation of software.

The user must comply with all laws relating to the use of computers, use of computer networks and copyright (in particular the provisions of applicable data protection legislation).

The user must comply with the University's Ethical and Legal Use of Electronic Copyright Material policy.

4.1.7 Remote Access

The University recognises the need for users to be able to access IT systems and services off-campus.

Users may remotely access systems on the internal University network through approved solutions only. Users must ensure that any device used to remotely access University systems meets the minimum security requirements set out in the relevant ITD procedures.

In order to protect the University's systems & data, ITD provides remote access systems to Users on the principle of least privilege and Users will only be provided access to systems they are authorised to use.

Users must make themselves aware of the guidance provided by ITD in relation to remote access.

4.1.8 Mobile Devices

The University of Limerick recognises that Mobile Devices such as smartphones and tablet computers are important tools and supports their use to achieve business goals. University of Limerick owned Mobile Devices are issued to approved users and must be only be used for authorised purposes and in compliance with ITD Mobile Device Management Procedures. Users with Personal Mobile Devices must comply with the University of Limerick Personal Device Policy.

4.2 Responsibility and Authorisations for Systems

All UL Systems have a System Owner and a System Administrator designated in the Inventory of Assets. The “System Owner” is the Head of the Faculty or Department that utilises the system to perform their day to day operations. This System Owner is responsible for the confidentiality, integrity and availability of information in the asset in question. The “System Administrator” is the person responsible for the upkeep, configuration, and reliable operation of a computer system or systems.

Users may only access those IT systems for which they have been explicitly authorised by the System Owner. Users may use the IT system only for purposes for which they have been authorised, i.e. for which they have been granted access rights. Users must not take part in activities which may be used to bypass information system security controls.

4.3 Backup

All backups must conform to the following best practice procedures:

- All data, operating systems and utility files must be adequately and systematically backed up (Ensure this includes all patches, fixes and updates).
- Records of what is backed up and to where must be maintained.
- Records of software licensing should be backed up.
- Back-up media, together with the back-up record, should be stored safely in a remote location, at a sufficient distance away to escape any damage from a disaster at the main site.
- Regular tests of restoring data/software from the backup copies should be undertaken, to ensure that they can be relied upon for use in an emergency.

4.3.1 Responsibility

Critical systems, Network Shares and Sharepoint sites are routinely backed up by ITD. ITD backup all core systems such as SI, Agresso, Sharepoint, CoreHR, Sulis, staff email on a daily basis. System Owners are responsible for ensuring that their system is included in ITD backup plans or alternatively backed up.

The responsibility for backing up data held on the PCs and laptops of individuals, regardless of whether they are owned privately or by the University, falls entirely to the User. Any individuals that maintain local systems which are not backed up by ITD are responsible for putting adequate alternative arrangements in place.

4.4 Computer Virus, Malware and Phishing Protection

All users have a responsibility to protect any device, which they use which connects to the UL network by ensuring that they have not tampered with or changed the settings of the installed Kaspersky anti-virus product for their area and that it is up-to-date.

- Users must not install an unapproved anti-virus product or try to alter the configuration or disable the existing anti-virus product.
- Users must install when requested by ITD any software, which is for the prevention of or monitoring of malware infections.
- Users must ensure that all relevant software security updates are applied to their computer.
- Users should not open suspicious emails or attachments whether solicited or unsolicited from unknown or unusual sources.
- All users should be alert to the possibility of malware and report any suspicious behaviour to the ITD Service Desk immediately.
- Any user who suspects that they have fallen victim to a malicious attack and have had their UL username/password and/or their device compromised must immediately inform the ITD Service Desk, have their password changed and allow ITD to investigate.

4.5 Password Responsibilities

User must apply good security practices when selecting and using passwords. Users must set passwords in line with the requirements of the UL Password Standard.

4.6 Internet Use

Internet access is provided to staff and students to enable them to pursue their work as an employee or student of the University of Limerick. The Internet must not be used for commercial or personal gain.

4.6.1 Personal Use

Staff and students may use the Internet for personal use provided that it:

- does not incur additional cost to the University
- does not prevent the employee from attending to and completing work effectively and efficiently
- does not preclude others with work-related needs from using the resources
- does not result in any unauthorised personal profit to the individual
- does not expose the University to legal liability
- does not involve or constitute an illegal activity.

4.6.2 Confidentiality

Regardless of the level of protection provided for Internet communications, confidentiality cannot be assured. Confidentiality might be compromised, for example, by law or policy, including this Policy, by unintended redistribution, or by the inadequacy of current technologies to protect against unauthorised access. Therefore, users should exercise extreme caution in using Internet communications to transmit confidential or sensitive matters.

4.6.3 Logs

Users should also be aware that the University may retain logs of access to the Internet - including the identifier of the computer accessing the internet, the identification of the site being accessed and the amount of data transferred. These logs may need to be reviewed for information security or other purposes relating to efficient use of University resources.

4.6.4 Unavoidable Inspection

Users should be aware that, during the performance of their duties, personnel who operate and support internet communications facilities need from time to time to monitor transmissions or observe certain transactional information to ensure proper functioning of University internet communications facilities and services, and on these and other occasions might inadvertently observe the contents of internet communications

4.7 Email

Email is provided to staff and students to enable them to pursue their work as an employee or student of the University of Limerick. Email records are considered to be “General Correspondence” under the Records Management and Retention Policy. Where the content of an email and/or its attachment(s) fall under another specific class of record in the Records Retention Schedule, it should be handled, retained and disposed of appropriately as set out in the Schedule.

4.7.1 Limited Personal Use

Staff may use email for limited personal use provided that it:

- does not incur additional cost to the University
- does not prevent the employee from attending to and completing work effectively and efficiently
- does not preclude others with work-related needs from using the resources
- does not result in any unauthorised personal profit to the individual
- does not expose the University to legal liability
- does not involve or constitute an illegal activity
- does not expose the University to reputational damage

4.8 Removable Media

The use of removable media within the University is not prohibited, but should only be used in cases where no suitable alternative exists (e.g. sanctioned network shares/ sanctioned cloud storage facilities and services). Microsoft OneDrive for Business should be used as an alternative to the use of removable media whenever possible.

Users must apply the following best practice principles when using Removable Media:

- Managers and information asset owners must ensure that use of removable media is suitably controlled within their area of responsibility in line with the objectives of this policy.
- Managers and information asset owners reserve the right to request that technical controls be implemented to prevent the use of removable media in certain circumstances.
- Users electing to use removable media, shall be responsible for ensuring they are authorised to do so within their area.
- Removable Media used to transport or store University data must be purchased via approved channels. Personally owned removable media must not be used for the purposes of transporting or storing University data.
- Removable Media used to transport or store University data must be either hardware encrypted or employ the use of encrypted containers.
- Researchers are responsible for ensuring that use of removable media and the encryption of any such media meets the requirements imposed upon them by their research (e.g. by funders, or data sharing agreements).
- When the removable media has reached the end of its useful life it should be submitted for secure destruction via the corresponding ITD processes.
- Use of removable media by a third party or sub-contractor should be risk-assessed and authorised, and in accordance with University Data Protection Policy governing third-party access to data.

4.9 Incident Management

IT Security Events are those that may have significance to the security of systems or data. If the IT Security Event results in the compromise of a system such that action has to be taken by an IT administrator, the IT Security Event then escalates to become an IT Security Incident.

The IT Incident Response Team comprises of the IT Security Officer who is responsible for leading and coordinating the response, the Head of Enterprise Architecture, the Head of IT Service Delivery, the ITD QMS Manager and Quality Officer and the Deputy Director of ITD.

Incident response will follow recognised good practice guidelines for digital evidence:

- No action taken should change data that may later need to be relied on as evidence

- In circumstances where it is deemed necessary to access original data, the person doing so must be competent to do so and be in a position to explain the relevance and implication of their actions
- An audit trail of actions taken must be created and preserved; it should be sufficient for an independent 3rd party to replicate the actions and achieve the same result
- The person in charge of the incident response has responsibility for ensuring that the law and these principles are adhered to

If at any time during the investigation of an IT Security Incident it becomes apparent that there may be a Potential Personal Data Breach as defined by GDPR and Data Protection legislation, then the IT Security Officer will notify the Data Protection Officer (DPO) who will join the ITSIRT team for the remainder of the investigation of the incident, and will be fully involved in the ensuing decision making process.

4.10 Policy Breaches

The user must not undertake any actions that bring the University into disrepute. Persons in contravention of this Policy are subject to the University of Limerick's disciplinary and/or criminal procedures.

5 Related Documents

University of Limerick Password Standards
University of Limerick Ethical and Legal Use of Electronic Copyright Material
University of Limerick Acceptable Usage Policy
University of Limerick Data Management & Retention Policy
University of Limerick Data Protection Policy
University of Limerick Risk Management Policy
ITD Personal Device Procedure
ITD Email Management Procedure
ITD Data Encryption Procedure
ITD User Access Control Procedure
ITD Network Security and Remote Access Procedure
ITD Mobile Device Management Procedure
ITD Disaster Recovery Procedure

6 Document Control

Document Version	2.0
Document Owner	Director ITD
Approved by	Audit & Risk Committee
Date	15 June 2022
Approved by	Governing Authority
Date	30 June 2022
Effective Date:	30 June 2022
Scheduled Review Date:	30 June 2023