

University of Limerick

INFORMATION SECURITY POLICY

Version 1.00

TABLE OF CONTENTS

Page

1. Introduction 5
   - 1.1 Purpose 5
   - 1.2 Scope 5
     - 1.2.1 To whom does the policy apply? 5
     - 1.2.2 In what situations does the policy apply? 5
     - 1.2.3 Who is responsible for ensuring that the policy (and any associated 6
   - 1.3 Definitions 6
     - 1.3.1 Definitions of Policy Concepts 6
2. Context 9
   - 2.1 Legal and Regulatory Context 9
   - 2.2 Other Context 9
     - 2.2.1 Security Governance 9
     - 2.2.2 Risk Management Framework 10
3. Institutional Information Security Commitments 12
4. Policy Statements 13
   - 4.1 Governance and Strategic Management 13
     - 4.1.1 Security Strategy and Roadmap 13
     - 4.1.2 Policy, Standards and Procedures 13
     - 4.1.3 Risk Management 13
     - 4.1.4 Security Governance Forums 14
   - 4.2 Security Planning and Architecture 15
     - 4.2.1 Security Requirements Engineering 15
     - 4.2.2 Security Architecture 15
     - 4.2.3 Technical Security Configuration Management 15
   - 4.3 Identity and Access Management 16
     - 4.3.1 Identity Lifecycle Management 16
     - 4.3.2 Privileged Access Management 16
     - 4.3.3 Access Certification and Review 16
   - 4.4 Security Operations 16
     - 4.4.1 Monitoring and Detection 16
     - 4.4.2 Threat Intelligence 17
     - 4.4.3 Vulnerability Management 17
     - 4.4.4 Security Logging and Telemetry 17

4.5 Incident Management and Response 17
4.5.1 Triage and Initial Assessment 17
4.5.2 Incident Response 17
4.5.3 Communication and Escalation 18
4.5.4 Post-Incident Review 18
4.6 Data Security and Privacy 18
4.6.2 Encryption and Key Management 18
4.6.3 Privacy and GDPR Compliance 18
4.7 Business Continuity and Resilience 18
4.7.1 Business Impact Analysis 18
4.7.2 Disaster Recovery 19
4.7.3 Crisis Management 19
4.8 Audit, Assurance and Compliance 19
4.8.1 Internal Audit Support 19
4.8.2 Security Control Assurance 19
4.9 Issues, POA&M and Improvement Management 19
4.9.1 POA&M Administration 20
4.9.2 Continuous Improvement 20
4.10 Security Awareness and Training 20
4.10.1 Awareness Campaigns 20
4.10.2 Role-Based Training 20
4.11 Project and Change Security Integration 20
4.11.1 Project Security Assurance 20
4.11.2 Change and Release Security 20
4.12 Third-Party and Supply Chain Security 21
4.12.1 Vendor Risk Management 21
4.12.2 Contractual Security Controls 21
4.12.3 Ongoing Vendor Monitoring 21
4.13 Physical and Environmental Security 21
4.13.1 Physical Access Control 21
4.14 Network Security Management 21
4.14.1 Network Segmentation and Zoning 21
4.14.2 Perimeter Security and Firewalls 22
4.14.3 Network Intrusion Detection and Prevention 22
4.14.4 Network Access Control and Zero Trust Enforcement 22
4.15 Endpoint Security Management 22
4.15.1 Endpoint Protection 22
4.16 Cloud Security Management 23

4.16.1 Cloud Security Posture Management 23
4.16.2 Cloud Identity and Access Management 23

5. Information Security Plan 24

6. Related Documents 25

7. Document Control 33

Appendix A Roles and Responsibilities 26

A.1 Executive Committee 26
A.2 Director of Information Technology Division (ITD Director) 26
A.3 Chief Information Security Officer (CISO) 27
A.4 Head of IT Security 28
A.5 Data Protection Officer (DPO) 28
A.6 Human Resources (HR) 29
A.7 Audit & Risk Committee (IA) 29
A.8 Faculty Deans and Department Heads 30
A.9 Risk and Compliance 30
A.10 IT Operations and IT Services 30
A.11 Security Operations Centre (SOC) 30
A.12 IT Security 30
A.13 Information System Owners 31
A.14 Information Risk Owner 31
A.15 System Administrators 32
A.16 All System Users (Staff, Students, and Third Parties) 32

1. Introduction

1.1 Purpose

As required by the Information Security Charter, this Information Security Policy establishes the principles, governance framework, roles, responsibilities, and control requirements for the protection of information and information systems at the University of Limerick (UL). It provides the foundation for UL's system of information security management and supports the security objectives defined in the Charter. The policy statements in this document are the means by which Information, Cyber and Data Risk is minimised to within organisational risk appetite.

This Policy supports the University's compliance with the General Data Protection Regulation (GDPR) by contributing to the technical and organisational measures the University maintains to protect personal data. As the GDPR requires such measures to be in place, this Policy is one of the principal instruments through which the University gives effect to that requirement.

This Information Security Policy supports the University's broader due diligence obligations and its system of Internal Control — providing assurance to the Governing Authority, and Executive committee, and external regulators that information security risk is being managed by way of a disciplined, documented, and continuously reviewed system of information security management.

This policy is mandatory for all persons within its scope. This Information Security Policy replaces all previous versions of the IT Security Policy.

1.2 Scope

1.2.1 To whom does the policy apply?

This policy applies to:

- All staff, faculty, students, contractors, consultants, visiting researchers, and other persons authorised to access University information assets, in any capacity.
- All third parties processing University information on its behalf, regardless of contractual or jurisdictional location.
- All persons accessing University information from on-campus, remote, or third-party premises, including those accessing via personally owned devices.

1.2.2 In what situations does the policy apply?

This policy applies to:

- All information assets owned, processed, stored, or transmitted by or on behalf of the University, regardless of format (electronic or physical) or location (on-premises, cloud, or third-party).
- All information systems, networks, infrastructure, cloud services, and applications used to process University information.
- All circumstances in which University information is accessed, used, transmitted, stored, or disposed of.

This policy is read in conjunction with the University of Limerick's Acceptable Use Policy (AUP), with which compliance is mandatory for all persons within the scope of this policy. The

AUP forms an integral part of the University's information security framework, and breaches of the AUP and related procedures are treated as breaches of this policy.

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

The Executive Committee holds ultimate accountability for information security at the University. The Director of Information Technology Division (Director ITD) and the Chief Information Security Officer (CISO) hold operational responsibility for the implementation, monitoring, and continual improvement of this policy and its associated procedures, controls, and supporting documents. The detailed allocation of roles and responsibilities, including those of the Governing Authority, the Executive Committee, the Audit and Risk Committee, the Data Protection Officer, the Head of IT Security, the IT Security Team, the Security Operations Centre, IT Operations, Information System Owners, Risk Owners, System Administrators, and all System Users, is set out in the Appendix of this policy.

The **Information System Owners -** typically Heads of Faculty, Department, or Divisional Directors whose business or academic processes are delivered through the information system — distinct from the IT team responsible for technical operation - are accountable for ensuring the confidentiality, integrity, and availability of Information Systems and the information in that Information System, are protected to the appropriate level. Please see the Appendix for the full set of accountabilities and responsibilities relevant to this policy.

1.3 Definitions

1.3.1 Definitions of Policy Concepts

The following concepts and terms are central to the understanding, application, and review of this Information Security Policy at the University of Limerick.

Information Security	The protection of information assets from unauthorised access, use, disclosure, disruption, modification, or destruction, in order to preserve their confidentiality, integrity, and availability and to support the achievement of business objectives.
CIA	The core pillars of information security: Confidentiality, Integrity, and Availability.
Confidentiality	Preserving authorised restrictions on information access and disclosure.
Integrity	Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.
Availability	Ensuring timely and reliable access to and use of information by authorised users.
Information Asset	Any data, information, system, or service that has value to the University, including but not limited to databases, data sets, documents, intellectual property, research data, and the systems that process, store, or transmit them.

Information System	An organised combination of hardware, software, data, networks, processes, and people that collects, stores, processes, transmits, or presents information to support one or more University business or academic activities or business processes.
Information Asset Owner	The role accountable for the proper management, protection, and appropriate use of one or more information assets, including decisions on classification, access, retention, and acceptable use.
Information System Owner	The role accountable for the day-to-day operation, security configuration, and lifecycle of an information system, including authorising change, defining user access, and ensuring the system operates in accordance with University policy.
System User	Any individual who accesses or uses a University information system, network, device, or service, including staff, students, contractors, researchers, and other authorised persons.
Data Subject	An identified or identifiable natural person to whom personal data relates, as defined by Article 4(1) of the GDPR.
Third Party	Any external organisation, supplier, contractor, partner, or individual not directly employed by the University that processes, accesses, or interacts with University information assets or systems.
Data Classification	The process of categorising information assets based on their sensitivity and the impact of unauthorised disclosure, modification, or loss.
Confidential Information	Information classified at a level that requires protection from unauthorised disclosure, including personal data, financial data, research data, and legally privileged information.
Personal Data	Any information relating to an identified or identifiable natural person, as defined by GDPR Article 4(1).
Special Category Data	Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership; genetic data; biometric data processed for the purpose of uniquely identifying a natural person; data concerning health; and data concerning a natural person's sex life or sexual orientation, as defined by Article 9 of the GDPR.
Pseudonymisation	The processing of personal data in such a manner that it can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and subject to technical and organisational measures, as defined by Article 4(5) of the GDPR.

Anonymisation	The irreversible processing of personal data in such a way that the data subject is no longer identifiable, removing the data from the scope of data protection law.
Data Controller	The natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data, as defined by Article 4(7) of the GDPR.
Data Processor	A natural or legal person, public authority, agency, or other body which processes personal data on behalf of the data controller, as defined by Article 4(8) of the GDPR.
Data Protection Officer (DPO)	The role designated to inform and advise the University and its staff on data protection obligations, to monitor compliance with the GDPR and the Data Protection Acts, to provide advice on data protection impact assessments, and to act as the contact point for the supervisory authority.
Data Protection Commission (DPC)	The independent national supervisory authority in Ireland with responsibility for upholding the fundamental right of individuals to data privacy through the enforcement and monitoring of compliance with data protection law.
Threat	A potential cause of an unwanted incident that may result in harm to a system, organisation, or individual.
Vulnerability	A weakness in an information system, security procedures, internal controls, or implementation that could be exploited by a threat source.
Risk	The effect of uncertainty on objectives, expressed as a combination of the likelihood of an event occurring and the severity of its consequences.
Risk Appetite	The amount and type of risk that the University is willing to pursue, accept, or retain in pursuit of its strategic objectives, as defined and approved by senior governance.
Risk Tolerance	The acceptable level of variation in performance or outcome relative to the achievement of objectives, expressing how much deviation from risk appetite the University will tolerate before further action is required.
Risk Treatment	The process of selecting and implementing measures to modify risk, including avoiding, transferring, mitigating, or accepting the risk.
Risk Owner	The role accountable for the management of a specific risk, including authorising the chosen treatment, ensuring controls are implemented, and reporting on residual risk.

Control Owner	The role accountable for the design, implementation, operation, and ongoing effectiveness of a specific information security control or set of controls.
BIA	Business Impact Analysis — the process of identifying critical business functions and information assets and assessing the impact of their disruption.
Principle of Least Privilege	The security principle that users, processes, and systems should be granted only the minimum level of access necessary to perform their authorised functions.
Defence in Depth	A security strategy that employs multiple layers of controls so that if one layer fails, another is in place to provide protection.
Zero Trust	A security model that assumes no implicit trust is granted to any user, device, or network segment, and requires continuous verification.
Shared Responsibility Model	A framework, particularly relevant to cloud services, that defines and allocates information security responsibilities between the University and its service providers, distinguishing those responsibilities retained by the University from those operated by the provider.
Access Control	The selective restriction of access to information assets and systems, enforced through identification, authentication, and authorisation mechanisms to ensure that only entitled entities can perform permitted actions.
Authentication	The process of verifying that an entity — whether a user, device, or system — is who or what it claims to be, typically by validating one or more credentials.
Authorisation	The process of determining and enforcing what an authenticated entity is permitted to do or access within a system or resource, defining the boundaries of allowable actions based on assigned roles, rights, and privileges.
Multi-Factor Authentication (MFA)	A security mechanism requiring two or more independent methods of authentication from separate categories (knowledge, possession, inherence) to verify a user's identity.
Single Sign-On (SSO)	An authentication mechanism that allows a user to authenticate once against a centralised identity provider and thereby gain access to multiple applications and services without being required to present separate credentials for each.
Privileged Access	A level of access to systems, applications, or data that exceeds standard user permissions, typically granted to administrators, support personnel, or specific service accounts, and subject to enhanced controls and monitoring.

Endpoint	A network-connected device such as a laptop, desktop computer, workstation, smartphone, tablet, appliance, server, network device or network security device (whether on-premises or cloud-based), and virtual endpoints such as virtual machines (VMs) and cloud-based workstations.
Encryption	The process of transforming information using a cryptographic algorithm and key so that it cannot be read by unauthorised parties, applied to data at rest, in transit, and in use to preserve confidentiality and integrity.
Hardening	The process of configuring an information system, device, or application to reduce its attack surface by removing or disabling unnecessary services, applying secure configuration baselines, and tightening default settings.
Network Segmentation	The division of a computer network into smaller, isolated segments or zones to limit the lateral movement of threats, contain incidents, and apply differentiated security controls based on the sensitivity of the assets within each segment.
Patch Management	The process of identifying, acquiring, testing, deploying, and verifying security patches and updates for operating systems, applications, firmware, and other software components across the University's estate.
Vulnerability Management	The continuous cycle of identifying, classifying, prioritising, remediating, and verifying the closure of security vulnerabilities across information systems and assets.
Logging and Monitoring	The systematic generation, collection, retention, and analysis of records of activity on information systems for the purposes of detecting security events, supporting investigations, demonstrating compliance, and improving controls.
Audit Trail	A chronological, tamper-evident record of events and actions on an information system sufficient to reconstruct, review, and examine the sequence of activities surrounding a transaction, event, or incident.
Backup	A copy of data and configuration created and retained on separate media or systems, to permit the restoration of information following accidental loss, corruption, destruction, or compromise.
Cloud Service Models	The standard categorisation of cloud computing services, principally Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS), each defining a different allocation of

	responsibilities between the University and the cloud provider.
Security Event	An identified occurrence of a system, service, or network state indicating a possible breach of information security policy or failure of controls.
Security Incident	A security event that has been assessed as having an actual adverse effect on the confidentiality, integrity, or availability of information or information systems.
Personal Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed, as defined by Article 4(12) of the GDPR.
Notifiable Breach	A personal data breach that is likely to result in a risk to the rights and freedoms of natural persons and which must therefore be reported to the Data Protection Commission within 72 hours of the University becoming aware of it, in accordance with Article 33 of the GDPR.
ISMS	Information Security Management System — the policies, processes, procedures, and controls that collectively manage information security risk within the organisation.
Statement of Applicability (SoA)	A mandatory ISO/IEC 27001 document that lists the Annex A controls, identifies which are applicable to the ISMS, justifies inclusions and exclusions, and records the implementation status of each control.
PRM	Process Reference Model — a documented catalogue of information security processes, their inputs, outputs, and activities. The processes operate the controls which reduce risk.
RASCI	A table to document the persons or roles who are Responsible or Accountable for something, and who may Support it, be Consulted about it and be Informed about it.
POA&M	Plan of Action and Milestones — a structured register of identified security weaknesses, remediation actions, responsible owners, and target dates.
Compliance Register	A maintained record of the legal, regulatory, contractual, and other obligations applicable to the University, together with the controls and evidence demonstrating ongoing compliance.
IAR	Information Asset Register — a maintained inventory of all information assets, their owners, locations, classification, and value.
AUP	The Acceptable Use Policy is a policy that defines the rules and expected behaviours governing how staff, students, and other authorised users may access and

	use the University's information systems, networks, devices, and data.
GDPR	The General Data Protection Regulation (Regulation (EU) 2016/679), the European Union regulation governing the processing of personal data of individuals in the European Economic Area, transposed and supplemented in Ireland by the Data Protection Act 2018.
NIS2	Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union, setting harmonised obligations for risk management, incident reporting, and supervision applicable to essential and important entities; transposition into Irish law is pending.
ISO/IEC 27001:2022	The international standard specifying the requirements for establishing, implementing, maintaining, and continually improving an Information Security Management System, against which independent certification may be obtained.
ISO/IEC 27002:2022	The international standard providing a reference set of information security controls, together with implementation guidance, designed to support the application of ISO/IEC 27001 and other information security management frameworks.
NIST CSF 2.0	The National Institute of Standards and Technology Cybersecurity Framework, version 2.0; a voluntary, risk-based framework organised around six core functions (Govern, Identify, Protect, Detect, Respond, Recover) used to manage and reduce cybersecurity risk.

2. Context

2.1 Legal and Regulatory Context

The University is committed to complying with all applicable data protection, privacy, and information security laws and regulations. The following legislation and regulations are of particular relevance to this policy:

- General Data Protection Regulation (EU 2016/679) (GDPR)
- Data Protection Act 2018 (Ireland)
- NIS2 Directive (EU 2022/2555) — Network and Information Security
- European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011 (S.I. 336/2011)
- Payment Card Industry Data Security Standard (PCI-DSS) where applicable
- Freedom of Information Act 2014
- Criminal Justice (Offences Relating to Information Systems) Act 2017
- NIS1 (S.I. No. 360 2018)
- Public Service Cyber Security Baseline Standards (Revision 1, 2022)
- NCSC Draft Risk Management Measures (RMM) Guidance, Cyber Fundamentals Framework (CyFun®)
- Code of Practice for the Governance of State Bodies (2016), Higher Education Authority Act 2022, Universities Act 1997
- EU AI Act (Regulation 2024/1689)
- Specific requirements from Higher Education Authority (HEA) and DFHERIS (Department of Further and Higher Education Research Innovation & Science)

The CISO, in consultation with the Data Protection Officer (DPO) and the University's legal function, maintains awareness of changes to the legal and regulatory landscape and ensures that this policy and its supporting documents are updated accordingly.

2.2 Other Context

In addition to the legal and regulatory context, the following institutional and risk management frameworks shape the implementation of this policy.

2.2.1 Security Governance

Digital Governance Steering Committee

The Digital Governance Steering Committee (DGSC) is a subcommittee of the Executive Committee. The DGSC advises on the management of digital platforms, reviews IT and digital project initiatives and reports on progress to the Executive Committee. The DGSC provides ongoing recommendations for critical issues and risks related to cyber security and ensures current and future projects are aligned with UL's strategic goals.

As a subcommittee of the UL Executive Committee the DGSC approves the programme of work on an annual and/or longer-term basis, submitting it for noting to the Executive

Committee. One of the key roles of the DGSC is to provide the executive governance oversight for critical issues and risks related to IT and cyber security.

Enterprise Architecture Review Board

The 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. The EA Review Board reviews new IT initiatives and makes recommendations on design and implementation to ensure that IT security and architecture are considered from inception, and that 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 but can introduce significant risks where appropriate due diligence is not applied, including data security risks, compliance issues with UL's Data Protection Policy and applicable legislation, and contractual issues that may leave UL inadequately protected. UL has established a Cloud Governance Working Group with appropriate collective expertise to provide guidance on the adoption of cloud services. The Cloud Governance Group's responsibilities include conducting reviews to ensure that adopted cloud solutions are aligned with IT security best practice, have appropriate data protection provisions, and that service level agreements and contracts are fit for purpose. The Group meets monthly and can be consulted for advice and guidance on existing and proposed cloud solutions.

2.2.2 Risk Management Framework

Enterprise Risk Management

The University of Limerick's Enterprise Risk Management Policy (owned by the Corporate Secretary's Office and approved by the Executive Committee, Audit and Risk Committee, and Governing Authority) establishes the University's enterprise-wide framework for managing risk in pursuit of its strategic objectives. It is grounded in ISO 31000 (2018), ISO 31050 (2023), the Universities Act 1997 (as amended by the Higher Education Authority Act 2022), and the 2016 Code of Practice for the Governance of State Bodies, and applies to the University and all its subsidiary companies.

Operationally, the policy defines the University's Risk Management Process: how risks are categorised and assessed against impact criteria at both Faculty/Division and University levels (across strategic, operational, financial, and reputational dimensions), how they are scored on the University Risk Rating Matrix, and how they progress through the Risk Management Cycle of identification, analysis, inherent rating, control documentation, residual rating, evaluation, treatment, monitoring, and review. It articulates the University's risk appetite — higher tolerance for risk in academic enquiry, research, innovation, and international development, and very low tolerance for risks to life and safety, legal and regulatory compliance, financial stability, or lasting reputational damage — and embeds these arrangements within a Three Lines of Defence model covering management, the risk management function, and internal audit, supported by external assurance providers. In short, the document is both the University's governing policy on risk and the operating reference for how risk is to be identified, treated, escalated, and reported across the institution.

Information Security Risk Management

The University's Information Security Risk Management and Treatment Process provides a structured, repeatable approach to identifying, analysing, evaluating, treating, and monitoring information security risks across all University systems, information assets, and operations. The process is aligned with ISO/IEC 27001:2022 (Information Security Management Systems), ISO 27005 (Risk Management Guidelines), and the NIST Cybersecurity Framework 2.0, and draws on control guidance from the NIST Cybersecurity Framework 2.0, ISO/IEC 27002 and CIS Controls v8. Risk assessments are triggered by defined criteria — including ISMS implementation, significant organisational or system change, supplier evaluation, and legislative change — ensuring risk is assessed wherever exposure arises.

Treatment options — reduce, accept, transfer, or avoid — are documented in a Risk Treatment Plan with assigned owners, target dates, and selected controls drawn from the NIST CSF control sub-categories. Residual risks requiring acceptance above defined thresholds require approval consistent with the risk appetite set by the Executive Committee. The risk register is monitored on a defined cadence and reviewed at management review, ensuring that risk information flows continuously into the ISMS improvement cycle and into reporting to the Audit and Risk Committee.

3. Institutional Information Security Commitments

The following statements set out the University of Limerick's institutional commitments with respect to information security. These commitments underpin all policy statements in Section 4 and form part of the University's governance framework.

1. UL is committed to ensuring the confidentiality, integrity and availability of information and data according to the risk that their disclosure, alteration or destruction presents.
2. UL is committed to ensuring that information is created, used, and maintained in a secure environment.
3. UL is committed to ensuring that computing facilities, programmes, data, networks, and equipment are adequately protected against failure, loss, misuse, or abuse.
4. UL is committed to ensuring that all System Users are aware of and fully comply with this policy and the relevant supporting policies and procedures.
5. UL is committed to ensuring that all System Users are aware of and fully comply with relevant Irish and European legislation pertaining to information security and data protection.
6. UL is committed to creating awareness that appropriate security measures must be implemented as part of the effective operation and support of Information Security across the institution.

4. Policy Statements

The following policy statements establish the mandatory requirements for information security at the University of Limerick. Each statement is uniquely identified. Day-to-day obligations regarding the use of the University's Information and Communications Technology (ICT) facilities, systems, and services are set out in the Acceptable Use Policy (AUP), which all users of University ICT are required to comply with.

4.1 Governance and Strategic Management

4.1.1 Security Strategy and Roadmap

4.1.1.1: ITD develops and maintains an Information Security Strategy, aligned with the University's institutional strategy and risk appetite. The Executive Committee holds ultimate accountability for the implementation of the Strategy. The Information Security Strategy is a multi-year directional document, that sets out the strategic outcomes the Information Security Programme will deliver, and the priorities, capability investments, and dependencies required to achieve them.

4.1.2 Policy, Standards and Procedures

4.1.2.1: UL will ensure that all University-owned assets have an identified owner and/or administrator who is accountable for their security and lifecycle management.

4.1.2.2: The University protects the confidentiality, integrity, and availability of all information assets in its custody, proportionate to the value of the asset and the impact of its compromise.

4.1.2.3: The University establishes, implement, maintain, and continually improve an Information Security Management System (ISMS) aligned with ISO 27001.

4.1.2.4: The CISO maintains a Statement of Applicability identifying the controls selected and the justification for their inclusion or exclusion.

4.1.2.5: The CISO establishes and maintains an Information Security Process Reference Model (PRM). The PRM documents, at a high level, the key processes required to ensure effective information security management at the University. Each process within the PRM is decomposed into a defined set of sub-processes. The PRM is owned by the CISO and operationally maintained by ITD.

4.1.2.6: Each sub-process within the PRM is explicitly mapped to one or more NIST CSF 2.0 control sub-categories. This mapping ensures that the PRM serves as a clear, high-level lens through which the University's NIST CSF 2.0 control posture is understood, communicated, and managed. Changes to the NIST CSF 2.0 mapping is reviewed and updated whenever the PRM is reviewed.

4.1.2.7: The University maintains an Acceptable Use Policy (AUP) defining the acceptable and unacceptable behaviours of System Users in relation to University information and systems. The AUP is published as a separate document.

4.1.2.8: The CISO maintains records of policy breaches and enforcement actions, and report summary statistics to the Information Security Steering Group.

4.1.3 Risk Management

4.1.3.1: The CISO ensures that information security risk assessments are conducted for critical information systems, using a documented methodology consistent with ISO 27005 or equivalent.

4.1.3.2: Information security risks are recorded in a risk register, assigned to risk owners, and managed in accordance with the University's risk management framework. Risks exceeding defined thresholds are escalated to the University's fundamental risk register.

4.1.3.3: The University's risk appetite for information security is defined by the Governing Authority through the Audit and Risk Committee in it's published enterprise risk appetite statement.

4.1.3.4: Where remediation of a vulnerability within the defined timeframe is not technically or operationally feasible, a formal risk acceptance may be recorded as the treatment decision. Risk acceptance is not used as a default or convenience measure and requires documented justification, including the reason for non-remediation, any compensating controls in place, and approval by an appropriate authority. Risk acceptances are reviewed periodically and remains open and tracked until the vulnerability is remediated or formally re-accepted following review.

4.1.4 Security Governance Forums

4.1.4.1: The University establishes and maintains an Information Security Steering Group (ISSG), comprising cross-functional executive and senior management representation from ITD, Human Resources, Corporate Secretary's Office, Finance, chaired by the Director ITD, with the CISO as secretary. The ISSG provides strategic oversight of the University's information security programme, ensuring that the Information Security Strategy, risk appetite, and security investment decisions remain aligned with institutional objectives and the University's obligations to its students, staff, research partners, and regulators. The Group ensures that Information Security and Cyber related risks in the Fundamental Risk Register are correctly representative of the actual risks facing the University and are correctly understood. The Group ensures that identified risks, control deficiencies and emerging threats are managed or escalated appropriately and remediated within agreed timeframes.

4.1.4.2: Information security is a standing item on the Executive Committee Agenda. The CISO presents a formal Information Security Posture Report to the Information Security Steering Group annually, covering risk posture, incident summary, maturity assessment, strategy progress, and key metrics. If due to exceptional circumstance, an additional report is required again at a different time of year as an ad hoc necessity, it may be requested on an ad hoc basis, with one full working week's notice prior to presentation

4.1.4.3: The CISO provides regular reports to the Digital Governance Steering Committee covering security incidents, control status, risk register updates, POA&M progress, and metrics performance. ITD includes information security KPIs in its quality management reviews.

4.1.4.4: The ISMS are subject to management review at intervals not exceeding twelve months, conducted by the CISO with participation from senior ITD management.

4.1.4.5: A RASCI matrix is maintained cross-referencing each PRM (Information Security Process Reference Model) process's sub-process against the teams, roles, and functions across the University with a contribution to information security. The RASCI assigns clear

Responsible, Accountable, Support, Consulted, and Informed designations for each sub-process, ensuring that every relevant party understands the nature and extent of their required contribution to the University's information security programme.

4.1.4.6: The CISO produces integrated performance and control posture reports based on the PRM framework. These reports present: the performance rating of NIST CSF 2.0 control sub-categories; the derived performance of PRM (Information Security Process Reference Model) processes and sub-processes; and the attribution of that performance to the Responsible and Accountable parties identified in the RASCI.

4.1.4.7: A RACI matrix is maintained which cross-references the PRM (Information Security Process Reference Model) processes to establish clear accountability, responsibility, consultation, and information assignments for each sub-process.

4.2 Security Planning and Architecture

4.2.1 Security Requirements Engineering

4.2.1.1: Information systems are designed and configured to be Secure by Design and Secure by Default, with security considered from the earliest stages of procurement, development, and deployment.

4.2.2 Security Architecture

4.2.2.1: The following Security Design Principles as requirements be applied to all new systems, significant changes, and architectural decisions.

Least Privilege — Grant minimum necessary access.

Defence in Depth — Implement layered controls.

Secure by Design — Build security into systems from inception.

Secure by Default — Default configurations are restrictive.

Zero Trust — Verify explicitly; assume breach.

Separation of Duties — No single individual should control all aspects of a critical process.

Fail Secure — Systems default to a secure state on failure.

Complete Mediation — Every access to every object is checked for authority.

Economy of Mechanism — Keep security designs as simple as possible.

Open Design — Security should not depend on secrecy of design.

4.2.2.2: ITD establishes and maintains a current network architecture blueprint documenting the end-to-end logical and physical topology of the University’s network. The blueprint serves as the authoritative reference for network security design, zone enforcement, and access control decisions. It is maintained under version control, kept accurate following any significant network change, and access-controlled given the sensitivity of the information it contains.

4.2.3 Technical Security Configuration Management

4.2.3.1: ITD will ensure that agreed and approved baseline configurations are established for standard server, workstation, laptop, and network device builds.

4.2.3.2: ITD will ensure that systems deployed to production meet the approved baseline configuration standard.

4.2.3.3: ITD will ensure that change approvals for systems to be deployed to production confirm the approved baseline configuration standard is reached.

4.2.3.4: ITD will ensure that changes to the approved configuration baseline for the respective device and system platforms are approved through the change management and approval process.

4.2.3.5: Network infrastructure devices are managed securely, with administrative access restricted to authorised personnel and requiring strong authentication. Default vendor credentials are changed prior to deployment.

4.3 Identity and Access Management

4.3.1 Identity Lifecycle Management

4.3.1.1: All access to information and information systems are granted on the Principle of Least Privilege — users, processes, and systems receive only the minimum access necessary to perform their authorised functions.

4.3.1.2: Access to information and information systems are granted on the Principle of Least Privilege and on a need-to-know basis.

4.3.1.3: Multi-Factor Authentication (MFA) is required for all interactive users — staff, students, contractors, and third parties — accessing University systems.

4.3.1.4: In line with the ITD User Access Control Procedure, user access is promptly revoked or modified upon change of role, termination of employment, or conclusion of contractual relationship. Joiners, movers, and leavers processes incorporate access management.

4.3.2 Privileged Access Management

4.3.2.1: In line with the ITD Privileged Access Management Procedure, privileged access is restricted to the minimum number of individuals necessary, is separately controlled and logged, and requires enhanced authentication.

4.3.2.2: System and service accounts use certificate-based, token-based, or managed identity authentication where technically feasible. Shared credentials for system accounts are prohibited unless a documented exception is approved by the CISO.

4.3.3 Access Certification and Review

4.3.3.1: Separation of Duties are applied to critical processes and systems to reduce the risk of fraud, error, or unauthorised activity.

4.3.3.2: User access rights are formally authorised by System Owners and are reviewed at intervals not exceeding twelve months as per the ITD User Access Review Procedure. Privileged access is reviewed at intervals not exceeding six months.

4.4 Security Operations

4.4.1 Monitoring and Detection

4.4.1.1: The University maintains security monitoring and logging capabilities sufficient to detect, investigate, and respond to security events in a timely manner.

4.4.1.2: Backup infrastructure, backup jobs, and backup storage repositories are included within the scope of the University's security monitoring capability. Anomalous activity indicative of a ransomware precursor — including mass file modification events, unexpected deletion of shadow copies or backup catalogues, and unauthorised access to backup consoles — generate security alerts to the SOC for immediate triage.

4.4.2 Threat Intelligence

4.4.2.1: The University will participate in sectoral threat intelligence forums, including but not limited to those coordinated by NCSC-IE, Asiera, UCISA. The system of threat intelligence gathering and feeds will be documented and maintained by the Head of IT Security.

4.4.3 Vulnerability Management

4.4.3.1: The University establishes, maintain, and operate a documented ITD Vulnerability Management Procedure. The process defines roles and responsibilities, scope, severity classification, remediation timeframes, escalation, and reporting. It addresses software vulnerabilities, configuration weaknesses, and network-layer exposures across University systems.

4.4.3.2: Automated vulnerability scanning is conducted across University systems including internet facing systems to identify software vulnerabilities, configuration weaknesses, and network-layer exposures.

4.4.3.3: Vulnerability findings are severity-classified at the point of discovery and remediated within timeframes defined in the Vulnerability Management Process, proportionate to severity.

4.4.3.4: Critical and High severity security patches released by vendors are assessed for applicability and deployed within defined remediation timeframes.

4.4.3.5: Configuration weaknesses identified through vulnerability scanning or configuration assessment is evaluated against approved baselines. Material deviations that represent a security risk is treated as vulnerabilities and remediated or risk-accepted accordingly.

4.4.3.6: Vulnerability management performance is reported to the CISO on a regular basis, including trend data, remediation performance against defined timeframes, and open item status. Reports are presented to the Audit and Risk Committee as part of the periodic security posture report.

4.4.4 Security Logging and Telemetry

4.4.4.1: Security logs are retained for a minimum period defined in the UL Records Classification and Retention Schedule. Security logs are protected against unauthorised modification or deletion.

4.5 Incident Management and Response

4.5.1 Triage and Initial Assessment

4.5.1.1: All System Users report suspected security events to the ITD Service Desk immediately upon detection. A culture of reporting without fear of reprisal is maintained.

4.5.2 Incident Response

4.5.2.1: The University maintains and operates a Security Incident Management Procedure, defining procedures for the detection, triage, containment, eradication, recovery, and post-incident review of security incidents.

4.5.2.2: An Incident Management Framework is maintained describing how IT Incident Management, Security Incident Management, and Crisis Management plans interoperate, including escalation paths and communication protocols.

4.5.3 Communication and Escalation

4.5.3.1: Security incidents involving personal data are notified to the DPO immediately and assessed against GDPR breach notification requirements. Notification to the Data Protection Commission is made within 72 hours where required.

4.5.4 Post-Incident Review

4.5.4.1: Post-incident reviews are conducted for all significant security incidents. Lessons learned is documented and fed into the POA&M and risk assessment processes.

4.5.4.2: Following any security incident that results in data loss, data corruption, or activation of backup recovery procedures, a post-incident review assesses the adequacy of backup coverage, retention, recoverability, and recovery time. Findings are recorded in the POA&M and informs the next revision of the Backup and Recovery Policy. Where a ransomware or destructive attack reveals gaps in backup resilience, remediation actions are assigned an owner and a target completion date not exceeding ninety days.

4.6 Data Security and Privacy

4.6.2 Encryption and Key Management

4.6.2.1: Cryptographic controls are used to protect the confidentiality and integrity of sensitive information in transit and at rest, in accordance with standards defined in the Information Security Policy.

4.6.2.2: Cryptographic key management procedures are established and maintained.

4.6.2.3: A register of Cryptographic Certificates will be maintained, where those Certificates are CA signed or self-signed, and used in production systems.

4.6.2.4: Backup data are encrypted both in transit and at rest. Encryption keys for backup data are managed separately from the backup data itself and is recoverable in the event of a security incident affecting primary key stores.

4.6.3 Privacy and GDPR Compliance

4.6.3.1: Privacy by Design is applied in accordance with GDPR Article 25, embedding data protection into the design and operation of systems and processes.

4.7 Business Continuity and Resilience

4.7.1 Business Impact Analysis

4.7.1.1: A Business Impact Analysis (BIA) is performed and maintained to identify and prioritise critical information systems, business processes, and information assets according

to their value and the impact to the University in the event of their compromise, disruption, or loss. The BIA supports continuity management and planning.

4.7.1.2: Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) are defined for all critical systems based on the BIA and the MTD (Maximum Tolerable Downtime) as specified by the Information System Owner and tested within the schedule of recovery exercises.

4.7.2 Disaster Recovery

4.7.2.1: The University maintains a documented Backup and Recovery Procedure, approved by the CISO, defining backup scope, schedules, retention periods, storage locations, recovery procedures, and roles and responsibilities.

4.7.2.2: The University maintains a robust, tested, diverse and resilient backup and recovery capability for all critical and sensitive systems and data, ensuring that recovery remains possible even in the event of a widespread ransomware, destructive malware, or infrastructure compromise scenario. Full requirements governing backup scope, schedules, retention, storage, access controls, testing cadences, and recovery procedures are defined in the ITD Backup Management Procedure, which operationalises this statement and is read in conjunction with it.

4.7.3 Crisis Management

4.7.3.1: High impact, high urgency incidents are triaged to determine if they reach the threshold to invoke the crisis management process with dedicated coordination.

4.8 Audit, Assurance and Compliance

4.8.1 Internal Audit Support

4.8.1.1: An Audit and Security Testing Schedule is maintained and operated by the CISO. The schedule includes internal audits, external audits, penetration testing, vulnerability assessments, and compliance reviews, planned on a risk-proportionate basis.

4.8.1.2: The CISO establishes and maintains an Information Security Compliance Register that records all external legal, regulatory, contractual, and certification obligations, and all internal governance commitments, where an information security relationship or requirement exists. The Register is reviewed at least annually and following any material change to the University's legal environment or control framework.

4.8.2 Security Control Assurance

4.8.2.1: The University’s security controls are subject to periodic performance assessment. Performance ratings are reviewed at least biannually and provides a basis for assessing and reporting on the effectiveness of the security programme and the accountability of those responsible for its delivery.

4.8.2.2: A tabletop exercise is performed at least annually to test security and cyber incident management procedures, response capability, and decision-making.

4.8.2.3: A network security review is conducted at least annually to assess the University’s network security posture, evaluate the effectiveness of network controls, and identify gaps or

weaknesses not captured through routine vulnerability scanning. Findings are documented and tracked through the improvement management process.

4.9 Issues, POA&M, and Improvement Management

4.9.1 POA&M Administration

4.9.1.1: The CISO maintains and operates a Plan of Action and Milestones (POA&M) and POA&M process to track identified security issues, weaknesses, control gaps, and architectural vulnerabilities.

4.9.1.2: Each item in the POA&M has an assigned owner, a target remediation date, and defined milestones. The CISO uses the POA&M to hold assigned owners accountable for timely remediation.

4.9.2 Continuous Improvement

4.9.2.1: The PRM, its NIST CSF 2.0 control sub-category mappings, the RASCI, and the associated performance ratings are reviewed in their entirety at intervals not exceeding twelve months or following any significant change affecting the environment around it.

4.9.2.2: The maturity of the University's information security management is formally assessed at intervals not exceeding twelve months, using a recognised maturity model. Results are reported to the Governing Authority.

4.9.2.3: A target maturity level is agreed with the Governing Authority, and a maturity improvement plan is maintained to track progress towards the target.

4.10 Security Awareness and Training

4.10.1 Awareness Campaigns

4.10.1.1: All System Users complete mandatory information security awareness training upon joining the University and at intervals not exceeding twenty-four months thereafter. Completion of training is a condition of continued access to University systems.

4.10.1.2: UL will ensure that all System Users understand their own responsibilities for protecting the confidentiality and integrity of the data they handle.

4.10.1.3: UL will create and maintain awareness of the cyber security threat environment that exists for the institution and its System Users, through the delivery of mandatory cyber security awareness training to all UL staff and students.

4.10.2 Role-Based Training

4.10.2.1: Role-specific security training is provided to staff in elevated-risk roles, including System Administrators, developers, and staff handling Restricted or Confidential data.

4.11 Project and Change Security Integration

4.11.1 Project Security Assurance

4.11.1.1: The EA Review Board reviews significant IT initiatives and changes using the Security Design Principles defined in this policy (Section 6.2). No significant system change or new system deployment proceeds without EA Review Board consideration of its security implications.

4.11.2 Change and Release Security

4.11.2.1: All changes to information systems and infrastructure is managed through a formal change management process. Security impact is assessed as part of the change approval process.

4.11.2.2: Changes to network infrastructure is subject to the formal change management process and includes an explicit assessment of their security implications. Access rights arising from network changes does not exceed what is operationally necessary.

4.12 Third-Party and Supply Chain Security

4.12.1 Vendor Risk Management

4.12.1.1: Third-party suppliers are subject to security risk assessment prior to engagement and at least annually thereafter, proportionate to the sensitivity of the information and services involved.

4.12.1.2: Third-party suppliers have the Third Party and Vendor Risk Assessment applied to them and maintained on the Third Party and Vendor Risk Register.

4.12.2 Contractual Security Controls

4.12.2.1: Information security requirements are incorporated into all contracts with third-party service providers who access, process, use, or store University information, manage University systems or provide University services.

4.12.2.2: A right to audit is incorporated into all contracts with third-party service providers who access, process, use, or store University information, manage University systems or provide University services.

4.12.3 Ongoing Vendor Monitoring

4.12.3.1: According to the risk level determined by the Third Party and Vendor Risk Assessment, applicable controls will be applied to the Third Party Vendor, will have the status of the controls verified and reported on as part of annual questionnaire.

4.13 Physical and Environmental Security

4.13.1 Physical Access Control

4.13.1.1: Physical security controls are implemented to protect information processing facilities, server rooms, network infrastructure, and areas where sensitive information is stored or processed.

4.14 Network Security Management

4.14.1 Network Segmentation and Zoning

4.14.1.1: The University maintains an authoritative record of its network infrastructure, covering all defined networks and their assigned security zone classifications. This record is kept accurate, appropriately access-controlled, and subject to periodic review.

4.14.1.2: University networks are segmented into defined security zones based on the sensitivity of data carried and the criticality of connected systems. Security controls, access

permissions, and monitoring requirements are applied proportionately to each zone's classification.

4.14.1.3: Network zone classifications are reviewed whenever the purpose, data sensitivity, or usage of a network materially changes, and as part of any periodic review of network infrastructure records.

4.14.2 Perimeter Security and Firewalls

4.14.2.1: The University operates managed perimeter controls between its networks and all external or untrusted networks. Only traffic explicitly authorised in support of a legitimate University purpose is permitted to traverse network boundaries, and perimeter controls are subject to periodic review.

4.14.2.2: University-managed systems and devices are subject to DNS and web content filtering controls that limit exposure to known malicious destinations and categories of internet content presenting a material security risk to the University, whether operating on-campus or remotely.

4.14.2.3: DNS infrastructure operated on behalf of the University is secured against abuse and common attack techniques. Administrative access to DNS systems are appropriately restricted, and DNS activity is logged to support security investigation.

4.14.3 Network Intrusion Detection and Prevention

4.14.3.1: Network traffic is monitored at key internal and external network boundaries to detect anomalous behaviour, policy violations, and indicators of threat activity. Monitoring outputs feed into the University's security operations capability.

4.14.4 Network Access Control and Zero Trust Enforcement

4.14.4.1: The University adopts Zero Trust principles in its approach to network access, requiring continuous verification of identity and device posture regardless of network location. Access is granted only to the specific resources required for a user's or system's authorised purpose, and implicit trust is not assumed based on network position alone.

4.14.4.2: Remote access to University network resources are permitted only through approved, encrypted solutions requiring strong authentication. Access granted remotely is scoped to the minimum required for the user's authorised function.

4.14.4.3: Wireless network infrastructure is appropriately secured and segmented to separate University-managed users and devices from guest and unmanaged connections. Guest wireless access is isolated from internal University networks and systems.

4.15 Endpoint Security Management

4.15.1 Endpoint Protection

4.15.1.1: The University implements and maintains an active, risk-proportionate approach to endpoint protection across all University-owned and managed devices, whereby the security controls applied to any endpoint are determined by an assessed combination of the value of the device itself, the sensitivity and criticality of the information it holds or can access, the criticality of the role performed by its user, and the importance of the service or business process which that endpoint supports.

4.15.1.2: The University defines an appropriate baseline configuration and control state for endpoints, to ensure that all endpoints meet a defined standard. The baseline will ensure all endpoints conform to a hardened, consistent configuration, such that the uniformity of defence becomes a collective strength, reducing the attack surface across the herd by eliminating the opportunistic footholds that attackers rely on most — unpatched software, weak credentials, unnecessary services, and misconfigured permissions.

4.15.1.3: Endpoints assessed as high-value or high-risk — including those used in privileged administrative roles, those processing restricted or sensitive data, or those forming part of critical business or research processes — receive a commensurate level of protection beyond baseline controls. Full requirements governing endpoint protection and management are defined in the Device Management Procedure

4.16 Cloud Security Management

4.16.1 Cloud Security Posture Management

4.16.1.1: Cloud services should not be adopted without formal assessment and approval by the Cloud Governance Group.

4.16.1.2: Where backup or recovery services are delivered by or through a third-party cloud provider, the provider is assessed under the Cloud Governance Group process prior to adoption and at least annually thereafter. Contracts with cloud backup providers include explicit provisions for: data residency within the European Economic Area; recovery time guarantees aligned with UL RTOs; prohibition on provider access to unencrypted backup data; and the University's right to retrieve or delete all backup data upon termination of the contract.

4.16.2 Cloud Identity and Access Management

4.16.2.1: All cloud-based applications and services adopted or used by the University should where possible, be integrated with the University's centralised identity provider using Single Sign-On (SSO), ensuring that access to cloud resources is governed by the same identity lifecycle, authentication standards, and access control policies that apply to on-premises systems and are consistent and centrally managed and authenticated.

5. Information Security Plan

This Policy is operationalised through a suite of supporting procedures, standards, and guidelines (see Section 5: Related Documents) and the Information Security Plan as maintained by the CISO.

The Information Security Plan, is the operational instrument through which the principles and requirements set out in this Policy are translated into the structured day-to-day delivery of the University's information security programme.

The Plan explains the roles, responsibilities, and RACI assignments by which the programme is operated; the operating cadences and control assessment by which it is run and verified; the governance and reporting flows by which its performance is communicated. It is used by the University as the operational reference for delivering the programme, by Information System Owners, Risk Owners, and other accountable parties as the source of the operational expectations placed upon them.

The Plan is reviewed and updated by the CISO at least annually and is revised at any other time when a significant change to the operating environment, legal or regulatory landscape, risk appetite, control framework, or threat environment renders an existing element of the Plan no longer fit for purpose. Lessons learned from incidents, audit findings, control performance data, and exercise outcomes are incorporated into the Plan as part of its continual improvement.

A complete list of supporting documents is provided in Section 6 (Related Documents).

6. Related Documents

The following documents support or directly relate to this policy:

- Information Security Charter
- Acceptable Use Policy
- Enterprise Risk Management Policy
- Data Protection Policy
- Policy for the Disposal of Assets
- Records Management Policy
- Risk Appetite Statement
- Anti-Fraud Policy
- Intellectual Property Policy
- UL Password Standards
- ITD Vulnerability Management procedure
- ITD User Access Review procedure
- ITD User Access Control procedure
- ITD Privileged Access Management procedure
- ITD Network Security & Remote Access Procedure
- ITD Disaster Recovery Procedure
- ITD Device Management Procedure
- ITD Data Encryption Procedure
- ITD Cybersecurity Awareness & Compliance procedure
- ITD Authorising Access to User Data Procedure

Appendix A. Roles and Responsibilities

This Appendix sets out the roles and responsibilities for information security at the University of Limerick. The roles defined here give effect to the policy commitments in this document and are referenced throughout the policy statements in Section 3.

A.1 Executive Committee

The Executive Committee holds ultimate accountability for information security at the University. The Executive Committee shall:

- Approve this Information Security Policy and ensure it is reviewed at intervals not exceeding three years.
- Receive and consider a bi-annual Information Security Posture Report from the CISO.
- Ensure that information security is a standing item on the Executive Committee agenda (Board Forward).
- Set the University's risk appetite for information security risk through the Audit and Risk Committee.
- Hold the Director of ITD accountable for the development and execution of the Information Security Strategy.
- Support the Director ITD in the enforcement of this policy
- Ensure that information security considerations are integrated into institutional decision-making.

A.2 Director of Information Technology Division (Director ITD)

The Director ITD has responsibility for information security at the University of Limerick. While the Director ITD delegates responsibility for the development and execution of the Information Security Strategy to the Chief Information Security Officer (CISO), and holds the CISO accountable for its effective delivery, the Director ITD retains accountability to the Executive Committee and Governing Authority for the state of the University's information security programme and the adequacy of its controls.

- The Director ITD is responsible for:
- Strategic accountability and CISO oversight
- Holding the CISO accountable for the development, maintenance, and effective delivery of the Information Security Strategy, the Information Security Management System, and the policies, procedures, and controls that constitute the University's information security programme
- Ensuring that the CISO has the mandate, resources, organisational access, and executive support necessary to discharge their responsibilities effectively
- Escalating material information security risks, control failures, or programme deficiencies to the Executive Committee where the Director ITD considers that the risk profile requires executive visibility or intervention
- Internal control and compliance

- Ensuring that all IT systems, infrastructure, processes, and operating methods within the IT Division conform to the internal control framework established by this Policy and the Information Security Process Reference Model (PRM)
- Using the PRM RACI as the primary instrument for assigning and confirming that each PRM process and sub-process is owned and operated by the appropriate team or role within ITD, such that the controls those processes embody are consistently and correctly executed
- Ensuring that risk treatment actions within ITD — specifically, controls selected under a Remediate treatment decision recorded in the Information Security Risk Register — are implemented by the responsible individuals within the agreed timeframes, and that progress against those actions is tracked and reported through the POA&M process
- Ensuring that IT change management, incident management, and configuration management processes support the security requirements set out in this Policy and associated procedures
- Operational responsibilities
- Ensuring that IT services and infrastructure are operated in accordance with this Policy at all times
- Ensuring the security, integrity, and accurate maintenance of the IT Asset Register
- Ensuring the secure management and operation of the University's network infrastructure
- Providing the technical resources and cooperation necessary for the CISO and Head of IT Security to discharge their responsibilities
- Ensure that IT change management, incident management, and configuration management processes incorporate security requirements.
- Ensuring the provision of support and advice to all individuals with nominated responsibility for discharging obligations under this Policy or associated information security procedures

A.3 Chief Information Security Officer (CISO)

The CISO has responsibility for information security at the University and is accountable to the Director of ITD for the execution of the Information Security Strategy. The CISO shall:

- Develop and maintain the Information Security Strategy and be responsible for it’s execution.
- Establish and operate the Information Security Management System (ISMS).
- Report to the Digital Governance Steering Committee on information security risk posture, incidents, and programme performance.
- Maintain and operate the Plan of Action and Milestones (POA&M) process.
- Commission and oversee information security risk assessments, audits, and security testing.
- Develop and maintain the Information Security Process Reference Model and associated RACI matrix.

- Provide advice & guidance to the Information Security function, including to the Head of IT Security and to the Security Operations Centre (SOC).
- Ensure that information security awareness training is delivered and that completion is tracked.
- Maintain relationships with external bodies including An Garda Síochána, the Data Protection Commission, NCSC-IE, and sector peers.
- Collate control and process performance information and provide reporting on control performance to the Executive Committee
- Maintain the internal controls framework and define the control performance level necessary according to the risk appetite, desired residual risk level by Risk Owners and according to the desired assurance level of senior management
- The CISO retains oversight of all risks recorded in the Information Security Risk Register and is responsible for ensuring that each risk has an active, named Risk Owner at all times.
- Maintain and operate the Security Audit and Security Testing Schedule.

A.4 Head of IT Security

The Head of IT Security reports to the Office of the Director ITD and has responsibility for the day-to-day delivery of IT security operations. The Head of IT Security shall:

- Manage the IT Security Team and Security Operations.
- Manage vulnerability assessments, penetration testing, and security monitoring.
- Coordinate the technical response to security incidents.
- Advise the EA Review Board and Cloud Governance Group on security engineering and design.
- Maintain relationships with external bodies including An Garda Síochána, the Data Protection Commission, NCSC-IE, and sector peers.
- Maintain a documented system of threat intelligence gathering, feeds and method of review and usage.

A.5 Data Protection Officer (DPO)

The DPO is responsible for advising the University on its data protection obligations. In relation to information security, the DPO participates in the assessment of Personal Data breaches, advises on Data Protection Impact Assessments (DPIAs), and collaborates with the CISO on matters where data protection and information security intersect.

Information security governance

- In the context of information security governance, the DPO works in close collaboration with the CISO to ensure that technical and organisational security measures implemented under this Policy are adequate to meet the University's obligations under Articles 5(1)(f), 24, 25, and 32 GDPR.

Security Incidents

- Where a security incident involves or may involve the processing of personal data, the DPO and IT Security team coordinates to consider whether the incident constitutes a personal data breach and to assess whether a risk arises. Where relevant, the DPO decides whether a personal data breach notification obligation arises.

A.6 Human Resources (HR)

- HR ensures that the IT Division are informed on a timely basis of new employees joining the University and leaving the University.

A.7 Internal Audit

- Internal Audit provides independent assurance on the effectiveness of the University's information security controls.

A.8 Faculty Deans and Department Heads

- Faculty Deans and Department Heads are responsible for ensuring that information security requirements are observed within their areas, that System Owners are designated for all systems under their remit, that staff are aware of their security obligations, and that policy breaches are reported and addressed.
- Faculty Deans and Department Heads should familiarise themselves with this policy, cooperate in ensuring appropriate action is taken when a breach is identified, and ensure that all IT systems under their remit are formally administered either by an administrator appointed by the head of the relevant area or centrally by ITD.

A.9 Risk and Compliance

- The Risk and Compliance function should integrate information security risk into the University's enterprise risk management framework, support the CISO in risk assessment activities, and ensure that information security risks are reported to the Audit and Risk Committee in accordance with the University's risk management policy.

A.10 IT Operations and IT Services

- IT Operations and IT Services teams implement and operate security controls as directed by the Director of ITD and Head of IT Security, report security events promptly, and cooperate with security audits, assessments, and incident investigations.

A.11 Security Operations Centre (SOC)

- The SOC provides continuous security monitoring, alert triage, and management of detection and the central security logging system.

A.12 IT Security

The IT Security team shall –

- Provide security incident response and investigate incidents in accordance with the Security Incident Management Procedure.
- Advise University officers, administrators, and the Director of ITD on Technical Security Operations and Security Threats

- Assist with reviewing and updating the Information Security Policy
- Promote the policy throughout the University
- Conduct scheduled or periodic assessments of security controls
- Provide security awareness training is performed on an ongoing basis to all staff and students.
- Maintain records of security incidents, allowing retrospective reports to identify trends or emerging threats
- Contribute to continual improvement of security controls and posture
- Maintain a calendar of security testing, awareness training and audits & assessments which are arranged by ITD

A.13 Information System Owners

- The Information System Owner is a senior stakeholder who holds accountability for a specific information system or application from an organisational perspective - as distinct from the IT team or engineers responsible for its technical operation, hosting, or support, or from the person who is the primary consumer of the service the system provides.
- Information System Owners are often the Heads of Faculty, Department, or Divisional Directors, responsible for or deeply involved with or dependent on a business or academic process which is delivered by an Information System to provide a service to internal or external consumers.
- The Information System Owner is the person (or role) within the university who understands how the information system is used for the business: which business processes depend on it, who its primary user communities are, what data it holds or processes, and what would happen to the organisation if it became unavailable. They are the authoritative voice on the business impact of disruption, degradation, or loss of the system. They are often the 'business go-to' when the primary consumers of the service which it provides, find the system is unavailable, or would be the person who would stand to be under pressure, from a business perspective, in the event of loss or non-availability, and acutely aware of the impact it causes.
- Information System Owners are responsible for ensuring that the confidentiality, integrity, and availability of the systems and the information within the system, is protected to the correct level. The correct level is based on the value and criticality of the system - and the risk to the University in the event of Disclosure, Destruction, Alteration or Denial of the system or the information it uses.
- Information System Owners if consulted are capable of recommending the correct data classification is applied to the system or the information it holds or processes.~~,~~ Information System Owners are able to define the minimum amount of necessary access required by the Information system’s consumers and users. Information System Owners should be satisfied that access is authorised on the principle of least privilege, and that their systems are included in backup, recovery, and risk assessment processes.

A.14 Information Risk Owner

- A Risk Owner is an individual with the authority, accountability, and organisational knowledge to make decisions about how a specific information security risk should be managed and treated. Risk Owners are closely familiar with the asset which is at risk and may have accountability or ownership of that asset. Risk Owners are determined and assigned at the point of risk identification and are recorded in the Information Security Risk Register.
- The Information Risk Owner is responsible for:
- Understanding the nature, likelihood, and potential impact of the risk(s) assigned to them, including the assets or processes at risk and the University functions that could be affected
- Make or approve the risk treatment decision on behalf of the University in respect of the risk and the asset or assets which the risk is related to, where that treatment is to reduce, accept, transfer, or avoid the risk.
- Being satisfied that the risk treatment actions meet previously agreed deadlines or milestones.
- Notifying the CISO of any material change to the risk context — including changes to the relevant system, process, threat landscape, or organisational function — that may require the risk to be reassessed

A.15 System Administrators

System Administrators are responsible for the day-to-day technical management of the University's information systems, infrastructure, applications, and platforms. The role is collective rather than singular: it spans the staff who administer servers, networks, storage, identity systems, databases, cloud services, end-user computing, telephony, audio-visual systems, learning and research platforms, and the many specialist systems that support academic and administrative activity across the University.

- System Administrators are responsible for the technical delivery, upkeep, configuration, and reliable operation of information systems. System Administrators comply with the Information Security Policy, implement security configurations as directed, and report vulnerabilities and security events promptly.
- System Administrators perform changes to information systems, infrastructure, and network configurations only through the University's formal change management process. They participate in the security impact assessment of changes they propose or implement, ensuring that security implications are identified and recorded as part of change approval.
- System administrators do not implement changes that have not been assessed and approved through that process. Where changes give rise to new access rights, System Administrators ensure that the access required or granted does not exceed what is operationally necessary.

A.16 All System Users (Staff, Students, and Third Parties)

- All System Users are responsible for understanding and complying with this policy and the Acceptable Use Policy.
- System Users must complete mandatory security awareness training, protect their credentials, report security events, and use University systems only for authorised purposes.
- System Users are responsible for the security of University information systems assigned to them and must ensure that any access they grant to others is for University use only, is not excessive, and is maintained appropriately.

7. Document Control

Document Version	Version 1.00
Document Owner	Chief Information Security Officer
Approved by	Executive Committee
Date	20 May 2026
Approved by	Audit & Risk Committee
Date	29 May 2026
Approved by	Governing Authority
Date	16 June 2026
Effective Date:	16 June 2026
Scheduled Review Date:	3 years from approval date unless otherwise required