UNIVERSITY OF LIMERICK

Information Security Charter

Version 1.0

Issued by	Executive Committee, University of Limerick
Charged to	Director of Information Technology Division
Review Cycle	Every three years, or following material change to the University's governance, strategy, or risk profile

Statement from the President

The Executive Committee of the University of Limerick recognises that the integrity, confidentiality, and availability of the University's information assets are essential to the delivery of our academic mission, the protection of our research and institutional data, and the trust placed in us by our students, staff, partners, and the wider public. In discharging its statutory responsibilities under the Universities Act 1997 (as amended) and its obligations as a data controller under the General Data Protection Regulation, the Executive Committee hereby issues this Information Security Charter. This Charter establishes the mandate, governance structure, and strategic objectives for information security at the University of Limerick, and charges the Director of Information Technology Division to give effect to it.

Contents

1. Purpose and Authority of this Charter 2
2. Mandate 2
3. Charge to the ITD Director and CISO 5
4. Information Security Risk Appetite 7
5. Information Security Risk Ownership 7
6. Governance Framework and Standards 7
7. Alignment with the University's Guiding Digital Principles 8
8. Review and Renewal 8
9. Approval and Authorisation 9
10. Document Control 9

1. Purpose and Authority of this Charter

This Information Security Charter is issued by the Executive Committee of the University of Limerick in exercise of its governance and oversight responsibilities. It constitutes the highest-level expression of the University's commitment to information security and establishes the institutional mandate within which all information security activity is conducted.

The Charter has three primary purposes:

- **To mandate** the Information Security Policy (ISP), the Information Security Steering Group (ISSG), and the system of information security management that collectively give operational effect to the University's information security obligations;
- **To charge** the Director of Information Technology Division (ITD Director) with the accountability for, and the Chief Information Security Officer (CISO) with the responsibility for, implementing and sustaining an effective information security programme; and
- **To articulate** the University's information security objectives and reference the enterprise risk appetite statement, thereby aligning the information security programme with the University's strategic goals and enterprise risk management framework.

2. Mandate

2.1 Information Security Policy

The Executive Committee hereby mandates the existence and maintenance of a formal **Information Security Policy (ISP)** as the University's primary policy instrument for information security. The ISP shall establish mandatory requirements for the protection of all University information assets, define the obligations of all System Users, and give expression to the information security objectives set out in Section 3 of this Charter. The ISP shall be approved by the Executive Committee, maintained, reviewed and recommended by the CISO, and presented to the Executive Committee at intervals not exceeding three years. The current version shall be publicly accessible to all System Users.

2.2 Information Security Steering Group (ISSG)

The Executive Committee hereby mandates the establishment and continuous operation of an **Information Security Steering Group (ISSG) that will report to the Digital Governance Steering Committee (DGSC)**. The ISSG shall be the principal cross-functional governance forum for information security at the University of Limerick. It shall be chaired by the ITD Director, with the CISO serving as secretary, and shall comprise senior representation from IT, Human Resources, Corporate Secretary's Office, Finance & Research.

The ISSG shall:

- Provide strategic oversight of the information security programme and ensure its alignment with institutional objectives and risk appetite;
- Review and recommend the Information Security Policy and material changes to the information security control framework;
- Receive regular reports from the CISO on process & control performance, risk register status, incident trends, and Plan of Action and Milestones (POA&M) progress;
- Ensure that information security risks exceeding defined thresholds are escalated appropriately within the University's enterprise risk governance framework;
- Be made aware of significant emerging risks;

- Convene at a minimum quarterly, with provision for extraordinary sessions in response to significant security incidents or emerging risk.

2.3 System of Information Security Management

The Executive Committee hereby mandates the establishment and operation of a **system of information security management** aligned to ISO 27001 the international standard for management of Information security, cybersecurity and privacy protection which encompasses the policies, processes, procedures, controls, roles, and responsibilities through which the University identifies, assesses, treats, monitors, and reports on information security risks. This system shall be structured in accordance with the University's **Information Security Process Reference Model (PRM)**, which defines 16 process domains aligned to the NIST Cybersecurity Framework 2.0 and ISO/IEC 27001:2022. The system shall be subject to ongoing performance measurement, annual review, and continual improvement, and its effectiveness shall be reported to the ISSG.

2.4. Information Security Objectives

The following objectives define what the University's information security programme must achieve. They are given operational effect through the policy statements in the Information Security Policy and by the processes operating under the system of information security management.

#	Objective
1	Protect the confidentiality, integrity, and availability of all University information assets - including student, staff, research, financial, and operational data - commensurate with their classification and the sensitivity of the information they contain.
2	Implement a risk-based approach to information security in which threats are systematically identified, assessed, and treated through a documented risk management process aligned with ISO 31000, ISO/IEC 27005, and the University's Enterprise Risk Appetite Statement.
3	Ensure compliance with all applicable legal, regulatory, contractual, and sectoral obligations bearing on information security, including those arising from data protection law, cybersecurity legislation, sector-specific requirements, and research sponsor and contractual commitments.
4	Establish and maintain effective security governance through clear accountability structures, the ISSG, defined roles and responsibilities, and regular reporting to the Executive Committee, and Audit and Risk Committee.
5	Detect, respond to, and recover from security incidents in a structured, timely, and evidence-based manner that minimises impact, meets notification obligations, preserves forensic evidence, and incorporates lessons learned into continuous improvement.
6	Build and sustain a security-aware culture across all University communities - staff, students, researchers, and third parties - through mandatory awareness programmes, role-based training, and clear expectations of responsible behaviour.
7	Ensure that information security requirements are embedded in the design, procurement, deployment, and operation of all IT systems and services, and that supplier and third-party arrangements are subject to proportionate security due diligence and contractual obligations.

2.5 Information Security Plan

The Executive Committee hereby mandates the existence and maintenance of a formal **Information Security Plan** as the authoritative operational reference document for the University's information security programme. The Information Security Plan is distinct from the Information Security Policy,

which establishes mandatory requirements, and from the Information Security Strategy, which sets multi-year direction and priorities. The Plan answers a single operational question: *how, by whom, and at what cadence is information security actually run?* It is the document that an auditor, assessor, or regulator would examine to understand not what the University is required to do, but how the University delivers it in practice.

The Information Security Plan shall define and document all of the following:

Plan Component	Content Required
PRM Operational Coverage	For each of the 16 PRM process domains: the process objective, component sub-processes and activities, required inputs, produced outputs and artefacts, tools or systems used, and the operating cadence (continuous, daily, weekly, monthly, quarterly, annually, or event-triggered).
Roles and Responsibilities	The live RACI for each PRM process and sub-process, identifying which role is Responsible, Accountable, Consulted, and Informed. Operational relationships with functions outside the IT Division - including HR, Legal, the DPO, Faculty System Owners, and the Risk Management function - are defined where a process spans organisational boundaries.
Operating Cadence and Activity Calendar	The complete recurring activity schedule across the programme, including vulnerability scanning windows, patch assessment cycles, access review periods, risk register review cadences, backup restoration test schedules, tabletop exercise timing, compliance register reviews, ISSG meeting frequency, and management reporting dates.
Control Assessment and Performance Measurement	The control performance rating model applied to NIST CSF 2.0 sub-categories mapped to the PRM; criteria for assessing whether a control is operating, partially operating, or not operating; frequency of assessments; the mechanism for translating performance ratings into risk register and POA&M entries; and the reporting format for communicating control performance to the ISSG and Audit and Risk Committee.
Testing Programme	All testing activities providing assurance over the programme: vulnerability scanning scope and frequency; penetration testing commissioning criteria and cycle; tabletop exercise design and annual scheduling; backup and disaster recovery restoration testing; phishing simulation programme; and clean-room recovery exercise requirements. For each: who commissions it, who conducts it, who receives results, and how findings are tracked to resolution.
Governance and Reporting Flows	The complete information and reporting chain: what is produced, by whom, at what frequency, and to which governance body - including the monthly vulnerability management report, annual security posture report to the ISSG, annual programme review to the Executive Committee, and all event-triggered reporting obligations.
Interfaces with Related Processes	Operational interfaces between the information security programme and IT change management, IT incident management, data protection, enterprise risk management, supplier and procurement management, and the HR joiners-movers-leavers process.
Document and Artefact Register	A register of all operational artefacts produced and maintained by the programme - including the Risk Register, POA&M, Compliance Register, Statement of Applicability, Asset Register, and the suite of security procedures - recording owner, current version, review frequency, and the PRM process each artefact supports.

The Information Security Plan is owned by the CISO and maintained by the CISO. It is reviewed in its entirety on an annual basis, with the review outcome and any material changes reported to the ISSG. It is a living operational document, updated whenever a material change occurs to the programme's processes, tooling, roles, or cadences. It is classified as Protected and shall be made available to auditors, certification bodies, and the Audit and Risk Committee as required under the University's audit support and compliance obligations.

3. Charge to the ITD Director and CISO

The Executive Committee, which holds **accountability** for information security at the University, hereby charges the Director of Information Technology Division (Director ITD), and the Chief Information Security Officer (CISO) acting under the authority of the Director ITD and a part of the IT Division, with the following responsibilities in giving effect to this Charter.

3.1 Director of Information Technology Division

The Director ITD, who has **responsibility** for information security and the operational responsibility for the implementation, monitoring, and continual improvement of the Information Policy and its associated procedures, controls, and supporting documents, shall:

- Ensure that the information security programme receives the resources, authority, and executive support necessary for its effective delivery;
- Hold the CISO responsible for the development, implementation, and continuous improvement of the Information Security Strategy, the ISP, and all associated processes and controls;
- Ensure that all IT systems, infrastructure, and operational processes within the IT Division conform to the internal control framework established by the ISP and the PRM;
- Use the PRM RACI as the primary instrument for confirming that each information security process is owned and operated by the appropriate role within ITD;
- Ensure that risk treatment actions within ITD - specifically, controls selected under a Remediate treatment decision in the Information Security Risk Register - are implemented within agreed timeframes and tracked through the POA&M process;
- Report to the Executive Committee via the ISSG and DGSC on information security risk, control performance, and programme progress at the intervals defined in the ISSG terms of reference.

3.2 Chief Information Security Officer (CISO)

The CISO, who has **responsibility** for information security and the operational responsibility for the implementation, monitoring, and continual improvement of the Information Policy and its associated procedures, controls, and supporting documents, shall:

- Develop, maintain, and continuously improve the Information Security Strategy aligned to this Charter and the University's institutional strategy;
- Maintain and operate the ISP (Information Security Policy), the information security risk register and treatment plan, the POA&M, the Information Security Compliance Register, and the overall system of information security management;
- Serve as secretary to the ISSG and produce the periodic security posture reports provided to the ISSG, the Digital Governance Steering Committee, and the Director ITD;
- Ensure that the information security programme addresses the objectives set out in Section 3 of this Charter and that performance against those objectives is measurable and reported;

- Advise the University's leadership on emerging threats, regulatory developments, and the adequacy of the information security programme;
- Coordinate with the Data Protection Officer to ensure that technical and organisational security measures satisfy the University's GDPR obligations.
- Create the report for the Executive Committee via the ISSG and DGSC on information security risk, control performance, and programme progress at the intervals defined in the ISSG terms of reference.

4. Information Security Risk Appetite

The University's information security risk appetite is derived from, and is consistent with, the **Enterprise Risk Appetite Statement** approved by the Governing Authority (February 2026).

The discipline of Information Security crosses several of the risk categories defined in the University's Enterprise Risk Appetite Statement. In particular, information security failures bear on the University's appetite for risk in respect of Reputation, Compliance, Regulation and Ethics, Financial Performance and Sustainability, and Cybersecurity.

The University's risk appetite for each of these categories - including the appetite ratings, tolerance scores, and the risk acceptance criteria that apply to each - is set out in the University's Enterprise Risk Appetite Statement which is the authoritative source for that information and is referred to here in preference to restatement. Information security risks are assessed and treated in accordance with the appetite established in that Statement; where an information security risk crosses more than one category, the most restrictive applicable appetite governs.

5. Information Security Risk Ownership

The core governance principle for risk is the separation of two roles. Risk ownership sits with those best placed to understand the business impact of the risk. Control responsibility sits with those best placed to manage the risk to within the appetite and residual risk level agreed during Risk Treatment. This separation prevents conflicts of interest, supports audit transparency, and aligns with ISO/IEC 27001 and NIST CSF 2.0.

6. Governance Framework and Standards

The information security programme established by this Charter is structured in alignment with the following international standards and control frameworks:

- **ISO/IEC 27001:2022** - Information Security Management Systems: Requirements;
- **ISO/IEC 27002:2022** - Information Security Controls;
- **ISO/IEC 27005:2022** - Information Security Risk Management;
- **NIST Cybersecurity Framework 2.0** - Govern, Identify, Protect, Detect, Respond, and Recover;
- **ISO 31000:2018** - Risk Management - Guidelines;
- **AICPA Trust Services Criteria** - Security, Availability, and Confidentiality;
- **General Data Protection Regulation (EU) 2016/679** - Articles 5, 24, 25, and 32;
- **NIS2 Directive (EU) 2022/2555** - measures for a high common level of cybersecurity;
- **CyFun® (Belgium CCN)** - Cyber Fundamentals Framework, aligned to NIST CSF and ISO 27001.

Alignment with these frameworks does not imply certification unless otherwise stated. The University's information security programme is designed to be capable of satisfying the requirements of these frameworks and will be assessed against them through the annual Compliance Register review and periodic external assurance activities.

7. Alignment with the University's Guiding Digital Principles

The University of Limerick's IT Division operates under a set of Guiding Digital Principles that shape how technology is selected, designed, and delivered across the institution. Information security is not a constraint on those principles - it is an enabling condition for their safe and sustainable realisation. This Charter affirms that the information security programme will actively support each principle as set out below.

- **Start with the Business Problem:** Understand what the business problem is that we are trying to solve. Look at the different approaches that can be taken to achieve the solution.
- **Cloud First:** Cloud risks are identified, assessed, and managed before adoption and on an ongoing basis, with the Cloud Governance Group and CISO acting as the joint gateway for cloud commitments.
- **Security by Design:** Security requirements are considered from the earliest stages of every initiative, validated by the EA Review Board against the University's Security Design Principles before deployment.
- **Commercial Off the Shelf First:** Vendor risk assessment, supplier due diligence, and security clauses in procurement ensure that COTS adoption does not introduce unacceptable residual risk.
- **Limit Customisations:** A risk-informed view is provided on whether proposed customisations introduce new exposure or whether forgone customisations require compensating controls, with assurance confirmed before go-live.
- **Holistic Approach:** Consolidation and reuse are supported where they reduce attack surface, but reviewed to ensure they do not aggregate risk to unacceptable levels of concentration or compromise resilience.
- **Collaborate with the Business:** The ISSG is the primary forum through which information security and business leadership agree priorities, align investment with need, and address potential vulnerabilities in partnership rather than after the fact.
- **Universal Design:** Ensure that inclusivity is always considered and that our systems and solutions are accessible by as many of our staff and students as possible.
- **Digital sustainability:** Working across the University to streamline and digitally transform processes to deliver a positive impact on the University's environmental footprint.

8. Review and Renewal

This Charter shall be reviewed and reaffirmed at intervals not exceeding three years. It shall also be reviewed promptly on the occurrence of any of the following:

- Material change to the University's institutional strategy or governance structure;
- Significant change to the regulatory or legislative environment applicable to the University;
- Appointment of a new ITD Director or CISO;
- A significant security incident or series of incidents that calls into question the adequacy of the University's information security mandate or risk appetite;
- A material change to the University's Enterprise Risk Appetite Statement affecting the risk categories relevant to information security.

The review shall be conducted by the CISO, in consultation with the ITD Director and the ISSG, and the revised Charter shall be presented to the Executive Committee for approval.

9. Approval and Authorisation

This Charter has been approved by the Digital Governance Steering Committee (DGSC), Audit & Risk Committee, Executive Committee, and Governing Authority of the University of Limerick and is effective from the date of issue below.

10. Document Control

Document Owner	Chief Information Security Officer (CISO)
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
Next Review	16 June 2029