

Failte Ventures Group Information Security Policy

Document Version:	2.0
Policy Owner	Head of Compliance
Approved by	Chief Executive Officer
Approval Date	1 Nov 2025
Next Review Date	31 October 2025

1.1 Statement of Intent

The purpose of this policy is to ensure that all information created, received, processed, or stored by The Failte Ventures Group Limited and its group companies (collectively referred to as "*Failte Venture Group*") is managed securely, responsibly, and in accordance with applicable laws and regulatory requirements.

Information is one of the Company's most valuable assets. Protecting it is critical to maintaining business continuity, safeguarding stakeholder trust, and ensuring compliance with statutory and contractual obligations.

Failte Ventures Group is committed to maintaining the confidentiality, integrity, and availability of its information assets through the effective implementation of information security management practices, consistent with ISO 27001 standards and the Data Protection Acts 1988–2018 (as amended) and UK GDPR / EU GDPR where applicable.

1.2 Scope

This policy applies to:

- All employees, officers, directors, and group company personnel;
- All contractors, consultants, suppliers, and third-party service providers who have access to or process Company information; and
- All business systems, platforms, and devices (including mobile and cloud systems) used to access, process, store, or transmit information owned or managed by Failte Ventures Group.

This includes, but is not limited to:

- Any data, systems, or networks operated or managed by the Company;
- Electronic and physical records containing Company information;
- Email, messaging, and communication systems used for business purposes; and
- Personal devices used under a Bring Your Own Device (BYOD) policy that store or access Company data.

1.3 Objectives

The objectives of this Information Security Policy are to:

- Protect the confidentiality, integrity, and availability of information assets;
- Prevent unauthorised access, disclosure, alteration, or destruction of information;
- Ensure compliance with relevant legal, regulatory, and contractual requirements;
- Establish clear roles, responsibilities, and accountability for information security;

- Reduce the risk of financial, reputational, and operational losses arising from information breaches; and
- Promote a culture of security awareness and continuous improvement throughout the organisation.

Supporting policies, procedures, and standards—including the Company's Data Protection Policy, IT Usage Policy, and Incident Response Procedure—form part of this overall information security framework.

1.4 Information Security Principles

The following principles govern the management and protection of information across Failte Ventures Group:

1. Information Classification

- All information must be classified based on its sensitivity, criticality, and business value.
- Handling, storage, and transmission must align with the assigned classification level and any applicable legal or contractual requirements.

2. Access Control

- Access to information and systems shall be granted on the principles of least privilege and need-to-know.
- All access must be authorised, recorded, and regularly reviewed.

3. Confidentiality and Integrity

- Information must be protected against unauthorised access, modification, or disclosure.
- Encryption, password protection, and secure storage shall be applied where appropriate.

4. Availability

- Information must remain accessible to authorised users when required for legitimate business purposes.
- Backup, recovery, and business continuity measures shall be maintained.

5. Legal and Regulatory Compliance

- All information handling must comply with relevant data protection, intellectual property, and cybersecurity laws applicable in Ireland and other jurisdictions where the Company operates.

6. Incident Reporting and Response

- All information security incidents or suspected breaches must be reported immediately to the IT Security or Compliance Team.

- Incidents will be investigated promptly and, where required, reported to the Data Protection Commission or other authorities in accordance with legal obligations.

7. Continuous Improvement

- The Company will conduct regular internal audits, penetration tests, and policy reviews to evaluate and enhance its information security posture.
- Any formal Information Security Management Systems (ISMS) implemented within the Group will follow principles of continual improvement and alignment with ISO 27001 standards.

1.5 Legal and Regulatory Obligations

Faillte Ventures Group operates in compliance with all applicable Irish and European legislation governing information security, data protection, and privacy. Certain aspects of information management are subject to specific legal and regulatory requirements.

The following key laws and regulations are applicable:

- Data Protection Acts 1988–2018 (as amended)
- General Data Protection Regulation (EU) 2016/679 (GDPR)
- Safety, Health and Welfare at Work Act 2005
- Copyright and Related Rights Act 2000 (as amended)
- Criminal Damage Act 1991 and Criminal Justice (Theft and Fraud Offences) Act 2001
- Criminal Justice (Offences Relating to Information Systems) Act 2017
- The Irish Constitution (Article 40.3.1 – implicit right to privacy)
- European Convention on Human Rights (Article 8 – right to private and family life)
- Charter of Fundamental Rights of the European Union (Article 8 – protection of personal data)
- ePrivacy Regulations 2011 (S.I. 336 of 2011)
- Cybercrime Directive (Directive 2013/40/EU)

All employees, contractors, and third parties handling Company data are expected to act in accordance with these laws and any related internal policies, procedures, and contractual obligations.

Failure to comply with legal or regulatory requirements may expose the Company and individuals to criminal, civil, or regulatory penalties.

1.6 Information Classification

Faillte Ventures Group adopts a structured information classification framework to ensure appropriate handling, access, and protection of all information assets.

Classification Level	Description	Examples

Public	Information that can be freely accessed and shared without restriction. Disclosure poses no risk to the Company or its stakeholders.	Website content, marketing materials, published reports, public announcements
Internal (Restricted)	Information intended for internal use within Failte Ventures Group and its subsidiaries. Access is limited to authorised personnel. Unauthorised disclosure could cause reputational or operational harm.	Internal emails, business data, standard operating procedures, supplier and customer correspondence
Confidential	Information restricted to designated employees, management, or board members. Unauthorised disclosure may cause significant financial, legal, or reputational damage.	Personal data, employee records, payroll information, financial reports, contracts, technical documentation, supplier pricing
Highly Confidential / Classified	Information critical to the Company's business operations, intellectual property, or commercial interests. Access is strictly limited to authorised individuals.	Strategic plans, merger and acquisition documents, proprietary designs, trade secrets, cybersecurity credentials

1.7 Supplier and Third-Party Security

All suppliers, service providers, and contractors who process or access Failte Ventures Group's information or systems must comply with this Information Security Policy or demonstrate equivalent corporate security standards.

This includes:

- Ensuring secure handling, processing, and storage of Company data both on-site and remotely;
- Adhering to the Company's confidentiality and data protection requirements;
- Implementing appropriate technical and organisational measures to protect information; and
- Ensuring that any subcontractors or downstream suppliers also comply with equivalent security obligations.

Failure to meet these standards may result in suspension or termination of contract, and, where applicable, legal action for breach of data security obligations.

1.8 Compliance, Policy Awareness, and Disciplinary Procedures

- All personnel accessing or managing Company information must comply with this Policy and supporting IT and data protection policies.

- Any breach of this Policy may result in the loss of confidentiality, integrity, or availability of personal, financial, or commercially sensitive data, potentially leading to legal, financial, and reputational harm.
- Unauthorised disclosure or mishandling of data may constitute a breach under the GDPR, the Data Protection Acts, or other applicable laws, and may expose the Company and responsible individuals to penalties.
- All employees, contractors, and authorised users will be informed of the existence and requirements of this Policy and related documents through the induction and training process.
- Any confirmed or suspected security breach will be handled in accordance with the Information Security Incident Response Procedure, the Data Protection Policy, and the Company's disciplinary framework.
- Breaches of this Policy by employees may lead to disciplinary action, up to and including termination of employment, in accordance with Company policy and Irish employment law.

1.9 Incident Handling

- Any employee or contractor who becomes aware of an information security incident or data breach must immediately report it to the Information Security Officer (ISO) or Data Protection Officer (DPO).
- All incidents will be promptly logged, investigated, and remediated according to the Company's Incident Response Procedure.
- Where a breach involves personal data, the DPO will assess the risk and, if necessary, report it to the Data Protection Commission within the statutory timeframe under the GDPR.
- The Company will notify affected individuals and stakeholders where legally required.
- Post-incident reviews will be conducted to identify root causes and prevent recurrence.

1.10 Supporting Policies, Procedures, and Guidelines

Information security at Fáilte Ventures Group is guided by three key principles:

- **Confidentiality:** Information is accessible only to those authorised to have access.
- **Integrity:** Information and systems remain accurate, complete, and reliable.
- **Availability:** Information and systems are accessible to authorised users when required for legitimate business purposes.

This Policy must be read alongside related IT and compliance policies, including:

- Acceptable Use of IT Policy
- Access Control and Password Policy
- Data Protection and Privacy Policy
- Remote Working Policy
- Email and Communication Policy
- Clear Desk / Clear Screen Policy



- Cybersecurity and Network Security Policy

All employees, contractors, and authorised third parties are required to familiarise themselves with and adhere to these supporting policies.

Non-compliance may result in disciplinary action, contract termination, or other action deemed appropriate by management and in accordance with applicable law.

A handwritten signature in black ink, appearing to read "Mark Shinnars", with a horizontal line underneath.

Mark Shinnars

CEO

The Failte Ventures Group Limited