Information Security Policy - External

Date	Name	Role	Change	Version
Fri Jan 16 2026	Tim Murnaghan	CTO	Approved	V1.0

General

This Information Security Policy defines Integrum ESG's information security practices and serves as the overarching framework for safeguarding our organisation's information assets. While this document outlines our commitment to maintaining resilient security measures, detailed procedural and operational requirements are defined within specific policies available upon request.

Purpose and Scope

This policy aims to provide a framework for the implementation of Integrum ESG's security controls to protect its information systems, assets, and data and to establish procedures for identifying, mitigating, and managing information security risks.

Information Security Objectives

Integrum ESG is committed to the below security objectives;

- Safeguarding the confidentiality, integrity, and availability of all physical and electronic information and personal data;
- To ensure that regulatory, operational, and contractual requirements are fulfilled;
- To develop and implement information security controls;
- Provide guidance, support, and communication in the implementation of information security controls within the organisation's business operations;

- To carry out regular risk assessments and identify potential threats that could harm business operations;
- Regularly review and update the information security controls to ensure they remain current and implement any new improvements;
- Educate employees about information security controls and encourage them to take responsibility, ownership, and stay informed to help reduce the risk of security incidents;
- Ensure the organisation is capable of continuing its operations in the event of a security breach;
- Comply with international standards, frameworks, laws, and regulations governing information security and the protection of personal data; and
- Ensure that external service providers comply with this policy.

Roles and Responsibilities

All employees and external contractors of Integrum ESG have a responsibility to comply with this policy.

The Chief Information Security Officer (CISO) is responsible for developing, maintaining, and implementing this policy. The CISO'S duties also include:

- Defining and implementing the organisation's information security controls and procedures;
- Updating and reviewing this policy and the organisation's information security controls and procedures;
- Defining and managing information security auditing and testing processes; and
- Managing information security incident responses.

Further information regarding the roles and responsibilities can be found in the "Roles and Responsibilities Policy"

Information Classification and Sensitivity

We are not in a heavily regulated environment so the types of information that we handle have few legal definitions, but there are three main levels of data for which Integrum ESG draws useful

distinctions:

- **Commercially Sensitive**

This is data which would compromise our commercial position and could include supplier contracts, business and product plans.

- **Customer Sensitive**

This is data which identifies customers including names and contact details of customers and potential customers.

- **Customer Private**

Example of this kind of data would be customer portfolios. This is one of our most sensitive types of data as this is commercially sensitive to our customers and would seriously limit our ability to service customers if they were not confident in our ability to handle this data properly.

In the Office environment, all of these types of data should be stored in folders with suitable permissions.

Some customer sensitive data is only stored within the CRM system – and only permissioned users can access it.

In the Integrum ESG dashboard, customer private data is stored with an identifying organisation ID. All access from the dashboard or API will have the organisation checked before access is allowed.

Access Control

Access to Integrum ESG's information security assets are restricted and will be granted to the organisation's employees and external contractors to fulfil their duties on a need-to-use basis. Each employee and external contractor is personally accountable for their actions regarding Integrum ESG's information assets and devices and must comply with this policy in their use of information assets. Further information regarding access control can be found in the "Access Control Policy"

User Account Management and Authentication

Each employee will receive and have access to a personal account. Employees will not allow another individual access to their account or access a user account of other employees. Access to this account will require users to authenticate themselves.

Third-Party Management

Integrum ESG will ensure its partners, suppliers, and contractors maintain adequate security measures to secure Integrum ESG's information as well as the information of its customers through contracts and periodic audits as necessary. Further information regarding third-party management can be found in the "Third Party Risk Management Policy".

Security Awareness and Training

Managers must ensure that employees and external parties working with the organisation's information systems are informed and trained on the required security and privacy policies and procedures. Further information on security awareness and training can be found in the "Security Awareness and Training Policy".

Risk Assessment and Risk Treatment

Risk Assessment

Integrum ESG will conduct regular risk assessments on its information systems and will be based on relevant international standards and frameworks. The Risk Assessments will identify potential risks that may disrupt business operations.

Risk Treatment/Mitigation

A Risk Treatment Plan will be implemented which sets out the resources, responsibilities, and actions taken towards mitigating and managing the identified risks. Further information on risk assessment and treatment can be found in the "Risk Assessment and Treatment Policy".

Audit logging & Tracking

The use and activity of Integrum ESG's information assets will be recorded for auditing purposes to ensure compliance with this policy. Further information on audit logging and tracking can be found in the "Audit Logging and Monitoring Policy".

Document Ownership

The CISO is the owner of this document and is responsible for ensuring that this policy is reviewed in line with Integrum ESG's review requirements. A current version of this document is available to all employees of Integrum ESG.

CISO contact details: tim.murnaghan@integrumesg.com