Date	Name	Role	Change	Version
Fri Jul 25 2025	Tim Murnaghan	CTO	Approved	V1.0

Data Classification Policy

General

The Integrum ESG Data Classification Policy covers all data relevant to and used by Integrum ESG. Integrum ESG's data refers to any type of data that is prepared, managed, used, or retained by an operating unit or employee of Integrum ESG and is related to the activities or operations of the company.

Integrum ESG data does not include individually-owned data, which is defined as an individual's personal information and is not related to the business specifically.

Purpose and Scope

This document outlines Integrum ESG's procedure for information classification, and the proper ways to handle confidential information, according to the various sensitivity levels.

Functional Responsibilities

Information Owners/System Owners

- Identifying information assets that require to be controlled, and managing these documents according to the processes listed within this document.
- Ensuring that information media items, (e.g. USB devices or flash drives, hard drives, magnetic tapes, memory cards, etc.) that have been used to store sensitive information are destroyed or are not used for other purposes without being erased per established industry best practices.
- Ensuring that methods for exchanging information with third parties are consistent with the requirements within this document and ensuring that confidentiality of information is maintained.

Authors

- Determining if a specific paper-based or electronic document has security or privacy implications.
- Processing the document according to practices listed within this procedure.

Department Managers

- Ensuring that each of their employees follows these guidelines.

CISO

- Maintaining the classification and handling of information assets process, as part of the Company's Information Security and Privacy Management framework.
- Providing advice about the classification of specific information assets.

Users/Employees

- Ensuring that the classification applied to an information item is not changed when that item is transferred to another location or between information systems.

Classification

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 HubSpot 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.

Information Asset Inventory

All information assets shall be registered in an Asset Inventory by the Asset Owner. The inventory will include, for each applicable asset:

- Asset name.
- Asset owner.
- Asset classification.
- Type of data.
- Asset criticality.
- Access Control mechanism used (password, SSO).

Customer access to private information

- Integrum ESG customers can access their data, defined as private information, via Integrum ESG's system using a username and password or other authentication methods. A Integrum ESG customer can access **only its data and does not have access to other customers' data**.
- All-access to sensitive customer information is encrypted, using AES-256.
- The security and privacy of customer access to their private information are tested and verified periodically by performing penetration tests and vulnerability scans.
- The Penalty for deliberate or inadvertent disclosure of Integrum ESG Confidential information is up to and including termination, and possible civil and/or criminal prosecution to the full extent of the law.

Responsibilities

Responsibility to follow this policy applies to all Integrum ESG employees. The CISO is responsible for developing, maintaining, and implementing the Data Classification Policy.

The roles and responsibilities of the respective employees at Integrum ESG are set out in the Roles and Responsibility Policy.

Document Ownership

The CISO is the owner of this document and is responsible for ensuring that this procedure is reviewed in line with Integrum ESG’s review requirements. A current version of this document is available to all members of staff in the company's share platform (Sharepoint).