INTEGER WEALTH GLOBAL

POLICY DOCUMENT

Data Classification

Issue: September 2024

1. Purpose

This policy establishes a standardized approach to classifying, handling, storing, and disposing of all data processed by Integer Wealth Global (IWG). Its goals are to:

1.1 Safeguard investor, project client, employee, and company information.
1.2 Ensure compliance with the EU General Data Protection Regulation (GDPR) and other applicable financial regulations.
1.3 Support secure and efficient information management across IWG entities in Luxembourg, Liechtenstein, Gibraltar, and Cyprus.

2. Scope

This policy applies to:

- All IWG employees, contractors, consultants, and third parties who create, access, store, or transmit IWG data.
- All forms of information: electronic, paper, verbal, and media.
- All IWG systems, including the Accelero Investment Platform and data rooms.

3. Data Classification Levels

All IWG data must be assigned one of the following classifications:

Classification	Description	Examples	Handling Requirements
Confidential	Information whose unauthorized disclosure could cause significant harm to IWG, investors, or clients, or is protected by GDPR or financial regulations.	Investor personal data, financial records, legal agreements, trade secrets.	Strong encryption in transit and at rest; access strictly role-based; logging and monitoring; secure disposal (shredding or secure wipe).

Classification	Description	Examples	Handling Requirements
Internal	Non-public information required for internal operations but not as sensitive as Confidential.	Internal policies, staff directories, internal project notes.	Access restricted to IWG staff or approved vendors; encryption recommended; secure disposal.
Public	Information approved for public release.	Marketing materials, publicly filed financial statements.	No special restrictions, but integrity must be maintained.

4. Roles & Responsibilities

4.1 Data Owners: Senior managers accountable for data sets within their domain; responsible for classification and authorization decisions.

4.2 Data Stewards: Operational managers ensuring correct handling and periodic reviews of data classification.

4.3 All Employees and Contractors: Required to protect data in accordance with this policy and report suspected breaches.

4.4 Compliance Department: Ensures GDPR compliance and conducts periodic audits.

4.5 Information Security Team: Implements technical controls, encryption standards, and monitoring tools.

5. Data Handling & Management Requirements

5.1 Collection & Creation

- Collect only data necessary for legitimate business purposes.
- Document lawful basis for personal data under GDPR.

5.2 Storage

- Use IWG-approved storage systems with encryption for Confidential data.
- Maintain geographic controls to ensure EU/EEA data residency when required.

5.3 Access Control

- Enforce least-privilege and role-based access.
- Require multi-factor authentication for systems storing Confidential data.
- Log and regularly review all access activities.

5.4 Transmission

- Encrypt all Confidential and Internal data during transmission (TLS 1.2 or higher).
- Public data may be transmitted without encryption but must be validated for integrity.

5.5 Retention & Disposal

- Retain data only for the period defined by regulatory or business requirements.
- Securely destroy data at end of retention period (digital wiping or certified shredding).

6. Data Breach & Incident Response

6.1 All suspected or actual data breaches must be reported immediately to the Information Security and Compliance teams.

6.2 Breaches involving personal data will be handled in accordance with GDPR requirements, including notifying supervisory authorities within 72 hours when applicable.

7. Training & Awareness

7.1 All employees and relevant contractors must complete annual data protection and classification training.

7.2 Specialized training required for roles handling large volumes of Confidential data.

8. Policy Compliance & Enforcement

8.1 Violations may result in disciplinary action, contract termination, or legal penalties.

8.2 Compliance audits will be conducted at least annually.

9. Policy Review

This policy will be reviewed annually or upon significant regulatory, technological, or operational changes.