INTEGER WEALTH GLOBAL

POLICY DOCUMENT

System Access Control Policy

Issue: July 2024

1. Purpose

This policy establishes monitored access control for IWG's secure data environments, including the IWG Data Rooms and the Accelero Investment Platform to protect the confidentiality, integrity, and availability of data belonging to investors and project clients, in full compliance with the EU General Data Protection Regulation (GDPR).

2. Scope

Applies to all IWG employees, contractors, investors, project clients, and third parties who request or obtain access to:

- IWG Data Rooms (physical and virtual)
- Accelero Investment Platform and associated repositories

3. Governance

- **Legal Department:** Oversees adherence to contractual obligations and regulatory requirements.
- **Compliance Department:** Ensures GDPR and other regulatory compliance, including ongoing monitoring and reporting.
- **Information Security Team:** Implements technical safeguards and continuous monitoring.

4. Access Principles

- **Least Privilege:** Access granted only to the minimum data required for the stated purpose.
- **Role-Based Controls:** Permissions aligned with defined user roles.
- **Auditability:** All access and modifications are logged and regularly reviewed.
- **Time-Bound:** Access rights expire automatically at the end of the approved period.

5. Access Request Sequence

To obtain access to IWG Data Rooms or the Accelero Investment Platform, the following steps apply:

5.1 **Formal Request Submission:**

- The requester submits an access request form, specifying the dataset, purpose, and duration of access.

- The request must be emailed simultaneously to:
  - IWG Legal Department: **legal@integerwealth.global**
  - IWG Compliance Department: **compliance@integerwealth.global**

5.2 **Legal Review:**
The Legal Department verifies contractual rights, data processing agreements, and jurisdictional considerations.

5.3 **Compliance Review:**
The Compliance Department ensures GDPR alignment, including data minimization and lawful basis for processing.

5.4 **Information Security Authorization:**
Upon dual approval (Legal + Compliance), the Information Security Team configures access permissions and enables multi-factor authentication.

5.5 **Notification & Credentials:**
Approved users receive encrypted access credentials and instructions.

5.6 **Monitoring & Logging:**
All user activity is logged and retained for a minimum of [insert retention period] in accordance with GDPR Article 30 records.

5.7 **Periodic Review & Revocation:**
Access rights are reviewed every [insert frequency] and revoked when no longer required.

6. Data Protection Measures

- Encrypted data transfer (TLS 1.2 or higher)
- Multi-factor authentication
- Regular penetration testing and vulnerability assessments
- Immediate revocation upon termination of relationship or detection of unauthorized activity

7. Enforcement & Breach Handling

Non-compliance may result in disciplinary action, contract termination, or legal penalties. Any data breach will be reported within the GDPR-mandated timeframe (72 hours) to the relevant supervisory authority and affected parties.

8. Review Cycle

This policy is reviewed annually or upon significant changes to technology, regulations, or business operations.