INTEGER WEALTH GLOBAL

Policy Document

Encryption Policy

Issue: May 2024

1. Purpose

The purpose of this Encryption Policy is to define requirements for the use of encryption technologies to protect sensitive data handled by Integer Wealth Global (IWG), a European-based financial services and investment management company registered in **Luxembourg, Liechtenstein, Gibraltar, and Cyprus**. This policy ensures that all personal, financial, and corporate data is safeguarded against unauthorized access, in compliance with the **General Data Protection Regulation (GDPR)**, financial sector regulations, and industry best practices.

2. Scope

This policy applies to:

- All employees, contractors, and third-party service providers who process or manage IWG's data.
- All systems, networks, applications, mobile devices, storage media, and communication channels that handle sensitive information.
- All data classified as confidential, personal, financial, or regulatory.

3. Policy Statement

IWG mandates the use of strong encryption methods for the protection of data at rest, data in transit, and data stored or processed by third parties. Encryption must be implemented to ensure confidentiality, integrity, and authenticity of sensitive information.

4. Data Protection Requirements

- **Data at Rest:**
  - All sensitive client and financial data stored on servers, databases, laptops, and removable media must be encrypted using **AES-256** or equivalent.
  - Mobile devices must be protected with full-disk encryption.
- **Data in Transit:**
  - Data transmitted over public or untrusted networks must use **TLS 1.2 or higher**.
  - Secure email transmission must be implemented via encryption standards such as S/MIME or PGP.

- **Backups:**
  - All backup data must be encrypted both in storage and during transmission to secondary/offsite locations.
- **Cloud Services:**
  - Cloud storage providers must support strong encryption and comply with GDPR and EU financial data protection regulations.

5. Key Management

- Encryption keys must be generated, stored, distributed, and retired securely.
- Keys must never be hard-coded into applications or transmitted in plain text.
- Access to encryption keys is restricted to authorized personnel only.
- Key rotation and renewal must occur at least every **12 months** or sooner if compromise is suspected.
- A secure key escrow system must be maintained for disaster recovery purposes.

6. Authentication & Access Control

- Multi-factor authentication (MFA) is required for access to encrypted systems.
- Strong password policies must be enforced alongside encryption practices.
- Access to encrypted data must follow the principle of **least privilege**.

7. Third-Party and Vendor Compliance

- Third-party service providers handling IWG data must comply with this policy.
- Data-sharing agreements must specify encryption requirements.
- Vendors must undergo due diligence and periodic security reviews.

8. Exceptions

Exceptions to encryption requirements may only be granted by the **Data Protection Officer (DPO)** in consultation with the **Chief Information Security Officer (CISO)** and must be documented with clear justification.

9. Incident Response

- Any suspected or confirmed compromise of encryption systems must be reported immediately to the Information Security Team.
- IWG will investigate and remediate incidents in line with its **Data Breach Response Policy**.

10. Compliance & Enforcement

- Failure to comply with this policy may result in disciplinary action, termination of contracts, and regulatory penalties.
- Regular audits will be conducted to ensure compliance with encryption requirements.

11. Policy Review

This Encryption Policy will be reviewed **annually**, or sooner if regulatory requirements, business operations, or threat environments change.