INTEGER WEALTH GLOBAL

Policy Document

Information Security

Issue: February 2024

1. Purpose

This Information Security Policy establishes the framework for protecting the confidentiality, integrity, and availability of Integer Wealth Global's (IWG) information assets. As a European-based financial services and investment management company registered in **Luxembourg, Liechtenstein, Gibraltar, and Cyprus**, IWG is committed to safeguarding client data, financial records, and business systems in compliance with the **General Data Protection Regulation (GDPR)**, financial sector regulatory requirements, and industry best practices.

2. Scope

This policy applies to:

- All IWG employees, contractors, and third-party service providers.
- All systems, networks, applications, mobile devices, and storage media.
- All information assets, including client data, financial data, intellectual property, and operational records.

3. Information Security Objectives

IWG's objectives are to:

- Protect sensitive client and business data from unauthorized access, disclosure, alteration, or destruction.
- Ensure availability of critical financial and investment management services.
- Maintain compliance with GDPR and applicable financial regulators in each jurisdiction.
- Establish accountability and awareness among staff and partners.

4. Information Security Principles

IWG adheres to the following principles:

- **Confidentiality** – Sensitive data is only accessible to authorized personnel.
- **Integrity** – Data must remain accurate, complete, and safeguarded from unauthorized modification.

- **Availability** – Information and systems must be accessible when required by authorized users.
- **Accountability** – Users are responsible for following security protocols and reporting incidents.

5. Roles and Responsibilities

- **Board of Directors** – Provides governance and oversight of information security.
- **Chief Information Security Officer (CISO)** – Responsible for policy enforcement, risk management, and oversight of security controls.
- **Data Protection Officer (DPO)** – Ensures compliance with GDPR and manages data subject rights.
- **Employees and Contractors** – Must adhere to security practices, complete training, and report incidents.
- **Third-Party Vendors** – Must comply with contractual information security obligations.

6. Security Controls

6.1 Access Control

- Access is granted on a **least privilege** basis.
- Multi-factor authentication (MFA) is required for critical systems.
- User accounts must be unique, regularly reviewed, and promptly revoked upon termination.

6.2 Data Protection

- Sensitive data must be encrypted at rest (**AES-256**) and in transit (**TLS 1.2+**).
- Backups must be encrypted, tested regularly, and stored securely offsite.
- Data retention and deletion must follow the **Data Deletion Policy**.

6.3 Network & Systems Security

- Firewalls, intrusion detection/prevention systems (IDS/IPS), and antivirus protections must be in place.
- Systems must be patched and updated in a timely manner.
- Segregation of networks must be applied between critical financial systems and general office IT.

6.4 Physical Security

- Office premises must be secured with access controls, CCTV monitoring, and visitor management systems.
- Sensitive documents must be stored in locked cabinets or secure rooms.
- Disposal of physical records must use certified shredding services.

6.5 Incident Management

- All suspected or confirmed information security incidents must be reported immediately to the CISO.
- The **Incident Response Plan** will be activated to contain, investigate, and remediate breaches.
- Regulators and affected clients will be notified in compliance with GDPR and financial laws.

6.6 Business Continuity & Disaster Recovery

- Critical systems and data must have documented recovery procedures as defined in the **Disaster Recovery Plan (DRP)**.
- Annual testing of recovery processes is mandatory.

7. Employee Awareness & Training

- All employees must undergo **annual information security and GDPR training**.
- Employees must acknowledge and agree to this policy as part of onboarding.
- Regular awareness campaigns will be conducted to reinforce secure practices.

8. Third-Party Security

- Vendors and partners with access to IWG systems or data must sign data processing and confidentiality agreements.
- Security audits and due diligence will be conducted before engaging third parties.
- Ongoing monitoring will ensure continued compliance with IWG security standards.

9. Monitoring and Auditing

- IWG's IT systems are subject to continuous monitoring for suspicious activities.
- Security audits and penetration tests will be conducted annually.
- Compliance with this policy will be reviewed during internal and external audits.

10. Policy Compliance & Enforcement

- Non-compliance with this policy may result in disciplinary action, contract termination, or regulatory reporting.
- Employees, contractors, and partners are required to report violations immediately.

11. Policy Review

This Information Security Policy will be reviewed **annually**, or sooner if significant changes occur in business operations, regulatory requirements, or threat environments.