INTEGER WEALTH GLOBAL

Policy Document

Cyber Security

Issue: March 2025

1. Purpose

The purpose of this Cybersecurity Policy is to protect the confidentiality, integrity, and availability of IWG's information assets, financial data, and client information. This policy establishes the framework for managing cybersecurity risks across all IWG member companies, ensuring compliance with applicable laws and regulations in Luxembourg, Liechtenstein, Gibraltar, Cyprus, and the European Union.

2. Scope

This policy applies to:

- All IWG employees, contractors, consultants, temporary staff, and third-party service providers.
- All information systems, applications, networks, cloud services, and data assets owned, leased, or managed by IWG.
- All physical and digital information processed, stored, or transmitted within the IWG Group.

3. Governance & Compliance

- IWG's Group Chief Information Security Officer (CISO) is responsible for policy oversight and enforcement.
- Each subsidiary must appoint a Local Information Security Officer (LISO).
- The policy aligns with:
  - EU General Data Protection Regulation (GDPR)
  - Luxembourg CSSF requirements
  - Liechtenstein FMA regulations
  - Gibraltar Financial Services Commission guidelines
  - Cyprus Securities and Exchange Commission (CySEC) standards
- Annual cybersecurity audits will be conducted across all jurisdictions.

4. Cybersecurity Principles

4.1 Data Protection & Privacy

- Personal and financial data must be processed in compliance with GDPR and relevant local data protection laws.
- Data must be encrypted in transit (TLS 1.2 or higher) and at rest (AES-256).

- Access to client and financial data must follow the principle of least privilege.

4.2 Access Control & Identity Management

- Multi-Factor Authentication (MFA) is mandatory for all remote and privileged access.
- User accounts must be reviewed quarterly, with immediate revocation of access upon termination of employment.
- Privileged accounts must be monitored and logged continuously.

4.3 Network & System Security

- Firewalls, intrusion detection/prevention systems, and endpoint protection must be implemented across all IWG networks.
- All servers, applications, and endpoints must be patched within 30 days of security updates being released.
- Cloud services must comply with ISO/IEC 27001 and EBA outsourcing guidelines.

4.4 Incident Response & Reporting

- A Group Incident Response Plan (IRP) must be maintained and tested annually.
- All cybersecurity incidents must be reported immediately to the Group CISO and relevant Local Information Security Officer.
- Incidents involving personal data breaches must be reported to regulators within 72 hours (GDPR Article 33).

4.5 Business Continuity & Disaster Recovery

- Each subsidiary must maintain a Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) aligned with group standards.
- Backup data must be stored securely and tested for recovery at least twice annually.

4.6 Vendor & Third-Party Security

- All third-party vendors must undergo cybersecurity due diligence prior to engagement.
- Contracts with service providers must include cybersecurity and data protection obligations.
- Vendors must notify IWG of any breaches within 24 hours.

4.7 Employee Awareness & Training

- All staff must undergo annual cybersecurity awareness training.
- Phishing simulations will be conducted at least twice per year.
- Specialized training is required for employees handling sensitive financial or client data.

5. Prohibited Activities

Employees and contractors are prohibited from:

- Circumventing security controls.
- Using unauthorized software, devices, or cloud services (“shadow IT”).

- Sharing corporate credentials with unauthorized persons.
- Storing client or company data on personal devices without encryption and approval.

6. Enforcement

- Violations of this policy may result in disciplinary action, up to and including termination of employment, contractual penalties, and legal prosecution where applicable.
- Subsidiaries failing to comply may face financial and operational sanctions within the Group.

7. Review & Updates

- This policy will be reviewed annually by the Group CISO and updated in response to regulatory changes, emerging threats, or business requirements.
- Subsidiaries may introduce stricter local measures but must remain aligned with group standards.

8. Approval

This Cybersecurity Policy has been approved by the Board of Directors of Integer Wealth Global (IWG) and is effective as of the date indicated above.