INTEGER WEALTH GLOBAL

POLICY DOCUMENT

Vendor Management

Issue: August 2024

1. Purpose

This policy establishes a standardized framework for selecting, onboarding, monitoring, and offboarding all vendors and service providers who process or have access to Integer Wealth Global (IWG) data, systems, or facilities. The aim is to safeguard IWG's operations and meet applicable regulatory requirements, including the EU General Data Protection Regulation (GDPR).

2. Scope

Applies to:

2.1 All third-party vendors, consultants, and contractors providing goods or services to IWG.
2.2 Any engagement involving personal data of investors, project clients, or employees.
2.3 All IWG subsidiaries and branches in Luxembourg, Liechtenstein, Gibraltar, and Cyprus.

3. Governance

3.1 Legal Department:

Reviews and approves contractual terms, ensuring inclusion of data protection and confidentiality clauses.

3.2 Compliance Department:

Verifies GDPR and other regulatory obligations are met.

3.3 Procurement & Vendor Management Team:

Oversees vendor evaluation, risk assessment, and performance monitoring.

3.4 Information Security Team:

Assesses cybersecurity posture and ongoing security controls.

4. Vendor Selection & Due Diligence

4.1 Pre-Qualification Screening:

- Financial stability and reputation check.
- Regulatory compliance verification, including licenses where required.

4.2 Risk Assessment

- Identify data sensitivity and potential impact to IWG operations.
- Evaluate cybersecurity maturity (e.g., ISO 27001 certification, SOC reports).

4.3 Data Protection Review

- Assess data flows and ensure GDPR-compliant processing agreements (Data Processing Addendum).

5. Contracting

All vendor agreements must include:

4.2 Confidentiality and non-disclosure obligations.
4.3 GDPR-compliant Data Processing Agreements (where personal data is processed).
4.4 Right-to-audit and inspection clauses.
4.5 Incident reporting obligations within defined timeframes (e.g., 24 hours for suspected data breaches).
4.6 Termination rights for security or compliance breaches.

6. Onboarding

6.1 Assign an IWG relationship owner.
6.2 Provide vendors with IWG's Code of Conduct, security requirements, and privacy expectations.
6.3 Require training for vendors handling personal or sensitive data.

7. Ongoing Monitoring

7.1 **Performance Reviews:**
At least annually, measuring service levels and key performance indicators.
7.2 **Security Assessments:**
Periodic verification of cybersecurity controls, including penetration testing or attestations.
7.3 **Compliance Audits:**
Ensure adherence to contractual and regulatory requirements.

8. Incident Management

Vendors must:

8.1 Report any security or privacy incidents within 24 hours of discovery.
8.2 Cooperate fully with IWG investigations and regulatory notifications.

9. Offboarding & Termination

Upon contract completion or termination:

9.1 Access credentials to IWG systems must be revoked immediately.
9.2 All IWG data must be returned or securely destroyed, with written confirmation.
9.3 Final performance and compliance review documented.

10. Recordkeeping

IWG will maintain records of vendor assessments, contracts, audits, and incident reports for the duration of the engagement plus a minimum of [insert retention period], in accordance with GDPR Article 30.

11. Policy Review

This policy will be reviewed annually or sooner if there are significant regulatory or operational changes.