INTEGER WEALTH GLOBAL

PROCEDURE DOCUMENT

Backup Policy & Procedure

Issue: January 2024

1. Purpose

To ensure the confidentiality, integrity, and availability of IWG's data and systems by defining a consistent approach to the backup, retention, and restoration of critical information across all offices and data centres.

2. Scope

This policy applies to:

- All IWG entities registered in Luxembourg, Liechtenstein, Gibraltar, and Cyprus.
- All employees, contractors, and third-party service providers who manage or store IWG data.
- All information systems, including on-premise servers, cloud platforms, end-user devices, and SaaS applications.

3. Policy Statement

IWG shall maintain reliable, encrypted, and verifiable backups of all critical data and systems to protect against data loss caused by hardware failure, cyberattack, accidental deletion, or natural disaster. Backups must comply with EU GDPR, local financial supervisory requirements, and industry best practices (ISO/IEC 27001).

4. Roles & Responsibilities

Role	Responsibility
Board of Directors	Approves the policy and reviews annual compliance reports.
CISO	Oversees backup strategy, risk assessments, and vendor selection.
IT Operations Team	Implements and monitors backup schedules, encryption, and restoration tests.
Business Unit Heads	Identify critical data and applications requiring backup.
Third-Party Providers	Must meet IWG's security, encryption, and retention standards.

5. Backup Requirements

5.1 Data Classification

- Tier 1 (Critical): Financial records, client portfolios, regulatory filings, KYC/AML data.
- Tier 2 (Important): Internal reports, HR records, operational documentation.
- Tier 3 (General): Publicly available or non-sensitive materials.

5.2 Frequency

Data Tier	Backup Frequency	Retention
Tier 1	Real-time replication + nightly full backup	7 years minimum (or as per regulatory requirement)
Tier 2	Nightly incremental + weekly full	3 years
Tier 3	Weekly full	1 year

5.3 Storage & Location

- Primary Site: Encrypted network-attached storage within the EU.
- Secondary Site: Geographically separate EU-based data center (Luxembourg or Frankfurt) for disaster recovery.
- Cloud Backups: Only GDPR-compliant providers (ISO 27001 certified).

5.4 Encryption

- Data must be encrypted in transit and at rest using AES-256 or stronger.
- Keys stored in a dedicated Hardware Security Module (HSM).

6. Backup Procedure

6.1 Preparation

- Identify critical systems and assign data tiers.
- Verify sufficient storage and network capacity.

6.2 Execution

6.2.1 Run automated backups according to frequency table.

6.2.2 Log all backup jobs with timestamp, size, and status.

6.3 Verification

6.3.1 Automated checksum validation after each backup.

6.3.2 Daily review of backup logs by IT Operations.

6.4 Testing

6.4.1 Perform quarterly restore drills for each data tier.

6.4.2 Document results and report to CISO.

6.5 Retention & Disposal

6.5.1 Retain data per schedule and applicable law (e.g., CSSF in Luxembourg, CySEC in Cyprus).

6.5.2 Securely delete or shred expired backups.

7. Incident Response

If backup failure or data loss occurs:

7.1 Notify CISO within 1 hour.

7.2 Initiate emergency restore procedures from the latest verified backup.

7.3 Escalate to regulatory bodies if a reportable data breach is suspected (within 72 hours per GDPR).

8. Compliance & Audit

- Annual independent audit of backup and restoration process.
- Evidence retained for minimum of 7 years.
- Non-compliance may result in disciplinary action and regulatory reporting.

9. Review & Update

This policy shall be reviewed annually or upon significant changes in technology, regulation, or company structure.

10. Approval Signatures

- Chief Information Security Officer
- Chief Executive Officer