INTEGER WEALTH GLOBAL

POLICY DOCUMENT - 20231104/01

Document Retention

04 November 2023

Purpose

This policy outlines the guidelines for secure document storage, access, and retention within Integer Wealth Global. It ensures compliance with ISO 27001 standards and protects sensitive information.

Scope

This policy applies to all employees, contractors, and third parties handling company documents.

Key Elements of the Policy

1. Purpose:
    - The purpose of this policy is to define how data is managed throughout its lifecycle, including storage and disposal.
    - It ensures compliance with ISO 27001 requirements.

2. Data Classification:
    - All documents must be classified based on sensitivity (e.g., confidential, internal use, public).
    - Classification determines access controls and retention periods.

3. Access Controls:
    - Access to documents is restricted to authorized personnel.
    - Role-based access controls (RBAC) are implemented.

4. Storage Locations:
    - Electronic documents:
        - Stored on secure servers or encrypted cloud platforms.
        - Regular backups prevent data loss.
    - Physical documents:
        - Kept in locked cabinets or restricted-access rooms.

5. Retention Periods:
    - Documents are retained based on legal, regulatory, and business requirements.
    - Refer to the **Data Retention Policy** for specific guidelines.

6. Document Destruction:
    - Obsolete or expired documents are securely destroyed (e.g., shredding, digital wiping).
    - Regular testing of backup systems ensures data restoration.

7. Version Control:
    - Maintain clear version histories for documents.
    - Consistent naming conventions prevent confusion.

8. Audit Trails:
    - Document access and modifications are logged.
    - Regular review of audit logs detects unauthorized activities.

Responsibilities

1. Document Owners:
    - Classify, label, and maintain documents.
    - Monitor versions and updates.

2. IT and Security Teams:
    - Implement technical controls.
    - Monitor access logs and enforce security policies.

Review and Compliance

- This policy is reviewed annually by the Information Security Officer (ISO).
- Non-compliance may result in disciplinary action