INTEGER WEALTH GLOBAL

Policy Document

Disaster Recovery Plan

Issue: May 2024

1. Purpose

The purpose of this Disaster Recovery Plan (DRP) Policy is to establish a structured framework for restoring critical business operations, IT systems, and data in the event of a disruptive incident. Integer Wealth Global (IWG), a European-based financial services and investment management company registered in Luxembourg, Liechtenstein, Gibraltar, and Cyprus, is committed to ensuring operational resilience, safeguarding client interests, and maintaining compliance with applicable financial and data protection regulations.

2. Scope

This policy applies to:

- All IWG offices, operations, IT systems, and infrastructure across Luxembourg, Liechtenstein, Gibraltar, and Cyprus.
- All employees, contractors, and third-party service providers with roles in business continuity and disaster recovery.
- Critical business functions, including financial transactions, client data management, compliance reporting, and investment services.

3. Objectives

The DRP aims to:

- Minimise the impact of disasters on business operations and clients.
- Restore critical IT systems and data within defined recovery objectives.
- Protect sensitive financial and personal data in compliance with GDPR and regulatory obligations.
- Provide clear roles, responsibilities, and communication channels during recovery.
- Ensure business continuity in line with regulatory and client expectations.

4. Risk Scenarios

The DRP covers potential disasters, including but not limited to:

- Cyberattacks, data breaches, or ransomware incidents.
- Hardware or software failures.

- Natural disasters (flood, fire, earthquake).
- Power or network outages.
- Pandemic or health-related disruptions.
- Human error or insider threats.

5. Recovery Objectives

- Recovery Time Objective (RTO): Critical systems must be restored within 24 hours of disruption.
- Recovery Point Objective (RPO): Data loss must not exceed 4 hours from the point of last backup.
- Business Continuity Objective: Essential financial and client services must remain operational through alternate methods where possible.

6. Roles and Responsibilities

- Board of Directors: Provides oversight and ensures resources for disaster recovery planning.
- Disaster Recovery Committee (DRC): Oversees implementation and activation of the DRP.
- IT Department: Responsible for backup, restoration, and system resilience.
- Data Protection Officer (DPO): Ensures compliance with GDPR and oversees protection of client data during recovery.
- Employees: Must follow disaster recovery procedures and report incidents promptly.

7. Data Backup and Storage

- Daily backups of critical data are performed and stored securely in both primary and secondary (offsite/cloud) locations.
- Backup integrity is tested on a monthly basis.
- Encrypted backups are maintained in compliance with GDPR and financial regulatory requirements.

8. Disaster Response and Recovery Procedures

- Incident Detection & Reporting – Any disaster or disruption is reported immediately to the DRC.
- Impact Assessment – Evaluate the scope, severity, and potential consequences of the incident.
- Activation of DRP – The DRC decides whether to activate the recovery plan.
- Communication – Notify employees, regulators, clients, and stakeholders as required.
- System Restoration – Restore IT systems and data from backups in priority order.
- Business Resumption – Resume critical services and monitor system stability.
- Post-Incident Review – Document lessons learned and update the DRP.

9. Communication Plan

1. Internal communications are coordinated by the DRC.
2. Clients and partners are informed of service disruptions and recovery timelines transparently.
3. Regulators in Luxembourg, Liechtenstein, Gibraltar, and Cyprus are notified where required by law.

10. Testing and Maintenance

- The DRP will be tested at least annually through simulated disaster scenarios.
- Testing will cover IT recovery, data restoration, and business process continuity.
- The DRP will be updated following major system changes, regulatory updates, or post-incident reviews.

11. Compliance

This policy aligns with:

- General Data Protection Regulation (GDPR).
- Financial regulatory requirements applicable in Luxembourg, Liechtenstein, Gibraltar, and Cyprus.
- Industry best practices for business continuity and disaster recovery.

12. Policy Review

This DRP Policy will be reviewed annually and updated as necessary to reflect evolving risks, regulatory requirements, and business priorities.