INTEGER WEALTH GLOBAL

Procedure Document

Business Continuity

Issue: March 2025

1. Purpose

This Business Continuity Procedure ensures that IWG can continue critical operations with minimal disruption in the event of a crisis or disaster. It provides a standardized framework for response, recovery, and resumption of services across all member companies.

2. Scope

This procedure applies to:

- All employees, contractors, and third-party service providers engaged with IWG operations.
- All critical business functions, including investment management, client advisory, trading, finance, compliance, IT services, and communications.
- All physical offices and digital systems used by IWG Group companies in Luxembourg, Liechtenstein, Gibraltar, and Cyprus.

3. Objectives

- Protect the safety and well-being of employees, clients, and stakeholders.
- Maintain continuity of critical financial services to clients.
- Minimize operational, financial, legal, and reputational impact.
- Ensure regulatory compliance with local financial authorities (CSSF, FMA, GFSC, CySEC) and EU requirements.
- Restore full business operations within agreed Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO).

4. Definitions

- Critical Business Function (CBF): Any process essential to financial stability, regulatory compliance, and client service.
- RTO (Recovery Time Objective): Maximum acceptable downtime for a business function (target: 4 hours for core services).
- RPO (Recovery Point Objective): Maximum acceptable data loss in time (target: 1 hour for critical systems).
- DRP (Disaster Recovery Plan): IT-specific procedures for restoring systems and data.

5. Roles & Responsibilities

Role	Responsibility
Board of Directors	Approves and oversees the BCP framework.
Group CEO	Ensures business recovery aligns with strategic objectives.
Group CISO & CIO	Lead technical recovery (cyber, IT infrastructure, communications).
Local Information Security Officer (LISO)	Country-level coordination and execution.
Crisis Management Team (CMT)	Activated in case of disruption; coordinates response across jurisdictions.
Employees	Follow instructions, report incidents, support recovery actions.

6. Business Continuity Activation

The BCP is activated when any disruption significantly affects IWG's ability to deliver critical services, such as:

- Cyberattack or ransomware incident
- IT system outage or cloud service failure
- Natural disaster (flood, earthquake, fire)
- Geopolitical or regulatory disruption
- Pandemic or health emergency
- Major third-party service provider failure

Activation Steps:

1. Incident detected and reported to Local ISO.
2. Local ISO notifies Group CISO & CMT within 30 minutes.
3. CMT evaluates severity and declares Business Continuity Activation if disruption > 1 hour or affects critical services.
4. Communication sent to employees, regulators, and clients (as required).

7. Recovery Priorities

Tier 1 – Critical (Immediate, RTO 4 hours)

- Core trading and investment platforms
- Client account access and fund transfer services
- Regulatory reporting systems
- Cybersecurity monitoring & communication channels

Tier 2 – Important (RTO 24 hours)

- Internal finance and accounting systems
- Risk management & compliance monitoring tools
- HR and payroll systems

Tier 3 – Non-Critical (RTO 72 hours)

- Marketing systems, corporate website, non-essential applications

8. Business Continuity Procedures

8.1 Incident Response & Escalation

- Employees report disruptions immediately to IT Helpdesk / Local ISO.
- Local ISO escalates to Group CISO & CMT.
- CMT assesses severity and activates continuity measures.

8.2 Communication Protocols

- Internal: Updates provided via secure email/SMS every 60 minutes until resolution.
- Clients: Transparent communication within 4 hours of disruption if client services are impacted.
- Regulators: Notify within required timelines (e.g., CSSF, FMA, GFSC, CySEC, GDPR breach notification within 72 hours).

8.3 Alternate Work Arrangements

- Remote working enabled via secure VPN with MFA.
- Relocation to alternate office sites if physical premises unavailable.
- Cross-border support: teams in unaffected jurisdictions provide operational backup.

8.4 IT & Data Recovery

- Activate Disaster Recovery Plan (DRP).
- Critical systems restored from secondary data centres or cloud backup.
- Daily encrypted backups stored off-site and tested quarterly.
- For ransomware incidents, forensic analysis conducted before restoration.

8.5 Vendor & Third-Party Dependencies

- Pre-identified alternate providers for critical services (e.g., telecoms, cloud).
- Vendors contractually obligated to meet RTO/RPO commitments.
- Continuous monitoring of service provider disruptions.

9. Post-Incident Review

- After recovery, CMT conducts post-mortem analysis within 7 business days.
- Identify root cause, evaluate response effectiveness, and implement improvements.
- Report submitted to the Board and regulators (if required).

10. Testing & Maintenance

- Full BCP simulation annually in each jurisdiction.
- Quarterly tabletop exercises with Crisis Management Team.
- IT recovery tests at least twice per year.
- Policy reviewed annually and updated based on lessons learned, regulatory updates, or business changes.

11. Enforcement

Failure to comply with this procedure may result in disciplinary action, contractual penalties for vendors, or regulatory sanctions.

12. Approval

This Business Continuity Procedure is approved by the Board of Directors of Integer Wealth Global (IWG) and applies to all group companies effective **11 March 2025**.