INTEGER WEALTH GLOBAL

Procedure Document

Incident Response Plan

Issue: April 2025

1. Purpose

The purpose of this Incident Response Plan (IRP) is to provide a structured approach for detecting, managing, and recovering from cybersecurity and operational incidents that could affect the confidentiality, integrity, or availability of IWG's financial services, client data, and IT systems.

2. Scope

This plan applies to:

- All IWG employees, contractors, and third-party service providers.
- All systems, networks, applications, and data owned, operated, or managed by IWG.
- All jurisdictions in which IWG operates: Luxembourg, Liechtenstein, Gibraltar, and Cyprus.

3. Objectives

- Detect and respond to incidents quickly and effectively.
- Minimize business, financial, reputational, and regulatory impact.
- Ensure continuity of critical financial operations.
- Comply with regulatory obligations (including GDPR's 72-hour breach reporting).
- Capture lessons learned for continuous improvement.

4. Definitions

- Incident: Any event that compromises, or has the potential to compromise, IWG's IT systems, data, or operations.
- Security Incident: Unauthorized access, malware infection, data breach, ransomware, insider threat, or denial-of-service attack.
- Major Incident: Any incident that impacts client services, financial transactions, or regulatory compliance obligations.
- Data Breach: Unauthorized disclosure, loss, or theft of personal or financial data.

5. Incident Categories

1. Cybersecurity Incidents – Phishing, ransomware, malware, unauthorized access, data breach.
2. Operational Incidents – System outage, application failure, human error, vendor failure.
3. Physical Security Incidents – Theft, unauthorized entry, disaster affecting premises.

4. Regulatory/Compliance Incidents – Breaches of GDPR, DORA, AML/CFT obligations.

6. Roles & Responsibilities

Role	Responsibility
Board of Directors	Oversight, ensuring IRP effectiveness and compliance.
Group CEO	Strategic decision-making during major incidents.
Group CISO (Chief Information Security Officer)	Leads the Incident Response Team (IRT), overall coordination, reporting to Board.
Local Information Security Officer (LISO)	Country-level incident management and escalation.
Incident Response Team (IRT)	Cross-functional team (IT, Compliance, Legal, Risk, Communications, HR).
IT Security Team	Technical containment, eradication, recovery.
Compliance Officer	Ensures regulatory notifications are made (GDPR, CSSF, FMA, GFSC, CySEC).
All Employees	Report incidents immediately via designated reporting channels.

7. Incident Response Lifecycle

IWG follows a 6-phase approach, aligned with NIST Cybersecurity Framework and EU DORA guidelines:

7.1. Preparation:

- Ensure monitoring tools (SIEM, IDS/IPS, anti-malware, logging) are active.
- Maintain updated contact lists for Incident Response Team.
- Conduct annual training and simulations.
- Ensure contracts with vendors include incident notification requirements.

7.2. Identification

- Incidents may be detected via monitoring tools, user reports, vendor alerts, or regulatory notifications.
- All employees must report suspected incidents immediately to:
  - Local ISO
  - security@iwg.global (central mailbox)
- Initial triage determines severity:
  - Low – Minor, no business impact
  - Medium – Localized disruption, potential client impact
  - High – Major service disruption, regulatory breach, reputational risk

7.3. Containment

- Short-Term Containment: Isolate affected systems, accounts, or networks.
- Long-Term Containment: Apply security patches, firewall rules, or alternate routes.

- Preserve forensic evidence (logs, memory dumps, system images).

7.4. Eradication

- Remove malware, disable compromised accounts, block malicious IPs.
- Conduct forensic analysis to identify root cause.
- Verify complete removal before restoring systems.

7.5. Recovery

- Restore systems from clean backups (verified and tested).
- Monitor systems for signs of re-infection or persistence.
- Gradually return services to normal operation while monitoring stability.

7.6. Lessons Learned & Reporting

- Conduct a post-incident review within 7 business days.
- Document timeline, root cause, impact, and corrective measures.
- Update IRP and security controls as required.
- Submit final incident report to Board and regulators (if required).

8. Communication Protocols

Internal

- Notify Group CISO and Local ISO immediately.
- CISO informs Group CEO for major incidents.
- Employees receive regular status updates via secure channels.

External

- Regulators: Notify within regulatory timelines (GDPR – 72h; CSSF, FMA, GFSC, CySEC – per local rules).
- Clients: If client data or services are impacted, notify within 24 hours of confirmed incident.
- Vendors: Engage if third-party systems are affected.
- Law Enforcement: Engage in cases of fraud, theft, or major cybercrime.

9. Incident Severity Levels & Response Times

Level	Description	Response Requirement
Low	Localized, no client impact	Resolve within 24 hours
Medium	Potential client impact, localized system outage	Escalate to Local ISO, resolve within 12 hours
High	Major disruption, client impact, regulatory breach	Immediate escalation to Group CISO & Board, containment within 4 hours

10. Testing & Maintenance

- Tabletop exercises: Quarterly
- Full incident simulations: Annually (including cross-border scenarios)
- Incident Response Team refresher training: Annual
- Plan review and update: Annual or after any major incident

11. Enforcement

Non-compliance with this IRP may result in disciplinary action, contractual penalties for vendors, or regulatory sanctions for the group.

12. Approval

This Incident Response Plan is approved by the Board of Directors of Integer Wealth Global (IWG) and is effective as of **16 April 2025.**