Policy Document

Cyber Security - Incident Response Plan

Issue: March 2025

INCIDENT RESPONSE PLAN (IRP)

Purpose.

To ensure IWG can detect, respond to, and recover from cybersecurity incidents quickly and effectively.

Key Sections:

1. **Incident Categories**
   - Data Breach (client or employee personal data)
   - System Outage / Ransomware Attack
   - Unauthorized Access (internal/external)
   - Financial Fraud Attempt (phishing, BEC, etc.)
   - Insider Threat

2. **Incident Response Lifecycle (aligned with NIST framework):**
   - Preparation – Train staff, maintain contacts, deploy monitoring tools.
   - Detection & Reporting – Employees must report incidents to security@iwg.global within 1 hour.
   - Triage & Containment – Group CISO + Local ISO decide scope and immediate actions.
   - Eradication & Recovery – Remove malicious access, restore systems from backups.
   - Post-Incident Review – Lessons learned, report to Board, regulator notifications (72h for GDPR).

3. **Roles & Responsibilities**
   - Group CISO – Overall coordination.
   - Local ISO – Country-level execution.
   - IT Teams – Technical containment & recovery.
   - Communications Officer – Regulator & client notifications.

4. **Communication Protocol**
   - Internal escalation (within 1 hour).
   - External reporting to regulators (within 72 hours for GDPR-related breaches).
   - Law enforcement engagement if fraud/financial crime suspected.

1. ACCEPTABLE USE POLICY (AUP)

Purpose.

To define responsible use of IWG's IT systems, networks, and data.

Key Rules:

- Use of IWG devices is for business purposes only.
- No installation of unauthorized software or use of shadow IT.
- Personal email, messaging apps, or cloud storage must not be used for company data.
- Passwords must not be shared or reused.
- Employees must lock devices when unattended.
- Remote work must use company-approved VPN with MFA.

Prohibited Activities:

- Accessing offensive, illegal, or malicious content.
- Bypassing or disabling security controls.
- Using personal USB devices without encryption/approval.

---

2. DATA CLASSIFICATION & HANDLING STANDARD

Purpose:

To ensure sensitive information is handled with appropriate protection.

Classification Levels:

1. Confidential – Client financial data, personal data, investment strategies. (Encryption mandatory).
2. Internal Use Only – Internal reports, financial results before publication.
3. Public – Marketing materials, published financial statements.

Handling Rules:

- Confidential data must only be accessed on secured, monitored systems.
- Confidential data must be encrypted (AES-256 at rest, TLS 1.2+ in transit).
- Paper documents with confidential information must be shredded when no longer needed.
- Data transfers outside the EU require GDPR-compliant safeguards (e.g., SCCs).

3. VENDOR & THIRD-PARTY RISK MANAGEMENT POLICY

Purpose.

To ensure all vendors meet IWG cybersecurity and regulatory requirements.

Requirements:

- Cybersecurity due diligence before onboarding.
- Contracts must include:
  - Data protection clauses (GDPR compliant).
  - Breach notification within 24 hours.
  - Right to audit vendor's security.
- Critical service providers must provide annual SOC 2 / ISO 27001 reports.

---

4. BUSINESS CONTINUITY & DISASTER RECOVERY (BCP/DRP)

Purpose:

To ensure IWG operations remain resilient in case of disruptions.

Key Provisions:

- Backups of critical data must be taken daily and tested twice annually.
- Recovery Time Objective (RTO): 4 hours for core trading/investment systems.
- Recovery Point Objective (RPO): 1 hour maximum data loss tolerance.
- Alternate work sites must be available in each jurisdiction (or cloud failover).

---

5. SECURITY AWARENESS & TRAINING POLICY

Purpose:

To build a culture of security across IWG.

Requirements:

- Annual cybersecurity training for all employees.
- Quarterly phishing tests with follow-up training for those who fail.
- Specialized training for IT admins, compliance staff, and executives.
- New hire onboarding must include cybersecurity awareness.

COLLECTIVELY, THESE DOCUMENTS FORM A COMPLETE GOVERNANCE FRAMEWORK:

- Cybersecurity Policy (umbrella)
- Incident Response Plan (IRP)
- Acceptable Use Policy (AUP)
- Data Classification Standard
- Vendor & Third-Party Risk Management Policy
- Business Continuity & Disaster Recovery Plan (BCP/DRP)
- Security Awareness & Training Policy