INTEGER WEALTH GLOBAL

Procedure Document

Physical Security Plan

Issue: May 2025

1. Purpose

The purpose of this Physical Security Plan is to protect IWG's people, facilities, information assets, and physical infrastructure from unauthorized access, damage, or disruption. This plan defines the standards, procedures, and responsibilities for implementing and maintaining effective physical security across all IWG sites.

2. Scope

This plan applies to:

- All IWG offices, data centres, and operational facilities in Luxembourg, Liechtenstein, Gibraltar, and Cyprus.
- All employees, contractors, visitors, and third parties who require access to IWG premises.
- All physical assets, including IT equipment, client records, financial documents, and communication systems.

3. Objectives

- Safeguard personnel, clients, and visitors.
- Prevent unauthorized access to IWG premises and sensitive areas.
- Protect confidential information and client assets from theft, tampering, or destruction.
- Ensure business resilience in the event of physical disruptions (fire, flood, vandalism, natural disaster).
- Comply with applicable EU, local laws, and financial services regulations.

4. Roles & Responsibilities

Role	Responsibility
Board of Directors	Approves security strategy and ensures compliance across the group.
Group Facilities Security Officer (FSO)	Oversees physical security framework across IWG.
Local Security Officer (LSO)	Manages physical security operations at local offices.
IT & Security Teams	Manage security technology (CCTV, access control, alarm systems).

Role	Responsibility
Employees	Comply with all physical security procedures and report breaches.
Reception & Security Personnel	Control access, manage visitors, enforce entry/exit protocols.

5. Physical Security Controls

5.1 Access Control

- Offices and sensitive areas must use electronic access cards, biometric systems, or keypads.
- Access rights must follow the Principle of Least Privilege.
- Visitor access must be pre-approved, logged, and escorted at all times.
- Lost or stolen access cards must be reported immediately and deactivated.

5.2 Surveillance & Monitoring

- All IWG offices must deploy CCTV monitoring in entry/exit points, data rooms, and sensitive areas.
- CCTV recordings must be retained for a minimum of 90 days, in line with local law.
- Alarm systems must be integrated with monitoring services or law enforcement response.

5.3 Facility Protection

- Critical areas (server rooms, archives) must be locked and accessible only to authorized staff.
- Environmental controls (fire suppression, smoke detectors, temperature/humidity sensors) must be installed.
- Backup power supplies (UPS, generators) must be available for critical infrastructure.
- Offices must have fire evacuation plans posted and tested annually.

5.4 Data & Asset Protection

- Confidential documents must be stored in locked cabinets or secure archives.
- Shredding or secure disposal must be used for sensitive physical records.
- Portable IT equipment (laptops, mobile devices) must be secured with cable locks or stored in secure cabinets after hours.
- Equipment disposal must follow secure destruction methods (e.g., degaussing or certified shredding for hard drives).

5.5 Perimeter Security

- Office buildings must have secure entry points (locked doors, staffed reception).
- Visitor parking areas must be monitored.
- Emergency exits must be alarmed but compliant with safety regulations.

6. Physical Security Procedures

6.1 Employee Access Procedures

- Employees are issued personalized access cards/badges.
- Access rights are role-based and reviewed quarterly.
- Upon termination, access credentials must be deactivated immediately.

6.2 Visitor Access Procedures

- Visitors must:
  - Be registered at reception.
  - Present valid identification.
  - Wear visible visitor badges.
  - Be escorted at all times.
- Visitor logs must be retained for at least 12 months.

6.3 Deliveries & Contractors

- Deliveries must be inspected before entry.
- Contractors must sign Non-Disclosure Agreements (NDAs) and comply with IWG security policies.
- Temporary access credentials must expire at the end of each day.

6.4 Incident Response – Physical Security

In the event of a physical security incident (e.g., unauthorized entry, theft, vandalism, fire, natural disaster):

1. Detection – Incident identified via alarms, CCTV, or staff report.
2. Containment – Secure the affected area and restrict access.
3. Notification – LSO notifies Group FSO, CISO, and senior management.
4. Escalation – Engage law enforcement or emergency services if required.
5. Recovery – Repair damage, restore operations, secure evidence.
6. Post-Incident Review – Conduct analysis, update procedures, and submit incident report within 7 business days.

7. Training & Awareness

- Employees must complete annual physical security training (covering access control, visitor management, and emergency procedures).
- Fire evacuation drills must be conducted at least once annually in each jurisdiction.
- Security personnel must receive enhanced training in incident handling and conflict management.

8. Auditing & Compliance

- Local offices must conduct quarterly physical security audits.
- Group FSO conducts an annual review across all jurisdictions.
- Non-compliance will result in corrective action plans and possible disciplinary measures.

9. Plan Testing & Maintenance

- Evacuation and emergency response tests – annually.
- Security system tests (alarms, CCTV, access controls) – semi-annually.
- Review and update this plan – annually or after a major incident.

10. Enforcement

Any violation of this plan may result in disciplinary action, up to and including termination of employment, contractual penalties for vendors, or legal prosecution.

11. Approval

This Physical Security Plan & Procedure is approved by the Board of Directors of Integer Wealth Global (IWG) and is effective as of **11 May 2025**.