INTEGER WEALTH GLOBAL

Policy Document

Vulnerability Management (Update from 2021)

Issue: February 2025

1. Purpose

This policy defines the principles, responsibilities, and procedures for identifying, assessing, mitigating, and reporting vulnerabilities within IWG's technology environment. It aims to protect client data, financial assets, and operational integrity by ensuring timely and effective vulnerability management across all platforms and services.

2. Scope

This policy applies to:

- All IWG-owned and managed IT systems, including cloud and on-premises infrastructure
- All software applications, databases, and network components
- All third-party services and integrations, including those provided by Integer Wealth Professional Services Ltd (IWPS)
- All jurisdictions: Luxembourg, Liechtenstein, Gibraltar, and Cyprus

3. Governance and Roles

Role	Responsibility
Chief Information Security Officer (CISO	Overall accountability for vulnerability management strategy and compliance
IT Security Team	Execution of scanning, assessment, remediation, and reporting activities
IWPS (External Provider)	Conducting vulnerability assessments for client-facing platforms and investment fund systems
System Owners	Ensuring remediation actions are implemented within defined timeline
Compliance Officer	Monitoring regulatory alignment and audit readiness

4. Vulnerability Management Lifecycle

IWG follows a structured lifecycle for vulnerability management:

4.1 Identification

- Automated vulnerability scans using industry-standard tools (e.g., Nessus, Qualys)
- Manual assessments for high-risk systems and bespoke applications
- Threat intelligence feeds and vendor advisories

4.2 Classification

Vulnerabilities are classified based on CVSS (Common Vulnerability Scoring System)

Severity	CVSS Score	Response Time
Critical	9.0–10.0	Immediate (within 24 hours)
High	7.0–8.9	Within 3 business days
Medium	4.0–6.9	Within 10 business days
Low	0.1–3.9	Within 30 business days

4.3 Assessment

- Risk impact analysis conducted by IT Security and IWPS
- Evaluation of exploitability, asset criticality, and exposure
- Prioritization based on business risk and regulatory implications

4.4 Remediation

- Patch deployment, configuration changes, or system upgrades
- Temporary controls (e.g., firewall rules, access restrictions) if immediate remediation is not feasible
- Verification of remediation through re-scanning and testing

4.5 Reporting and Documentation

- Monthly vulnerability status reports submitted to the Risk Committee
- Incident reports for critical vulnerabilities
- Audit logs maintained for all remediation actions

5. Continuous Monitoring

- Scheduled scans: Weekly for critical systems, monthly for standard infrastructure
- Real-time alerts for zero-day vulnerabilities and active exploits
- Integration with SIEM (Security Information and Event Management) for correlation and escalation

6. Third-Party and IWPS Integration

- IWPS conducts vulnerability assessments on behalf of IWG for client investment platforms
- All third-party providers must adhere to IWG's vulnerability disclosure and remediation timelines
- Contracts must include clauses for vulnerability reporting, patching obligations, and audit rights

7. Regulatory Compliance

This policy aligns with:

- EU GDPR for data protection
- MiFID II and AIFMD for financial services security
- Local cybersecurity regulations in Luxembourg, Liechtenstein, Gibraltar, and Cyprus
- ISO/IEC 27001 and NIST SP 800-40 guidelines

8. Documentation and Recordkeeping

- Vulnerability logs retained for a minimum of 5 years
- Remediation evidence archived for audit and compliance purposes
- Reports encrypted and stored in secure repositories

9. Policy Review and Updates

- Reviewed annually by the CISO and Risk Committee
- Updates approved by the Board of Directors
- All stakeholders notified of changes impacting operational procedures