INTEGER WEALTH GLOBAL

Policy Document

Password and Access

Issue: November 2024

1. Purpose

This policy establishes the standards for password creation, management, and system access control at Integer Wealth Global (IWG), ensuring the confidentiality, integrity, and availability of sensitive financial and client data across all jurisdictions in which IWG operates—Luxemburg, Liechtenstein, Gibraltar, and Cyprus.

2. Scope

This policy applies to all employees, contractors, consultants, and third-party service providers who access IWG systems, applications, networks, or data.

3. Password Requirements

3.1 Complexity Standards

- All passwords must meet the following criteria:
- Minimum length: 12 characters
- Must include at least one uppercase letter, one lowercase letter, one number, and one special character
- Must not contain the user's name, username, or easily guessable terms (e.g., "password123")

3.2 Expiration and Rotation

- Passwords must be changed every 90 days
- Users will be notified 10 days prior to expiration
- Reuse of the last 5 passwords is prohibited

3.3 Storage and Transmission

- Passwords must never be stored in plain text
- Passwords must not be shared via email, messaging apps, or written notes
- All password transmission must occur over encrypted channels (e.g., HTTPS, VPN)

4. Access Control

4.1 Role-Based Access

- Access to systems and data is granted based on job role and business need
- Access rights are reviewed quarterly and adjusted upon role changes or termination

4.2 Multi-Factor Authentication (MFA)

- MFA is mandatory for all remote access, privileged accounts, and access to financial systems
- MFA must include at least two of the following: password, biometric verification, hardware token, or mobile authenticator

4.3 Account Lockout

- Accounts will be locked after 5 consecutive failed login attempts
- Locked accounts require IT administrator intervention to reset

5. Privileged Accounts

- Admin and superuser accounts must use unique, complex passwords and MFA
- Activities performed using privileged accounts must be logged and monitored
- Privileged access must be reviewed monthly

6. Auditing and Monitoring

- All access attempts (successful and failed) are logged and retained for a minimum of 12 months
- Logs are reviewed regularly for anomalies and unauthorized access attempts

7. Training and Awareness

- All users must complete annual cybersecurity training, including password hygiene and access protocols
- New hires must complete training within 30 days of onboarding

8. Compliance

This policy supports compliance with:

- GDPR (EU General Data Protection Regulation)
- CSSF (Luxembourg), FMA (Liechtenstein), GFSC (Gibraltar), and CySEC (Cyprus) regulatory frameworks
- ISO/IEC 27001 and 27002 standards for information security

9. Violations

Violations of this policy may result in disciplinary action, including termination of access, employment sanctions, or legal proceedings.

10. Policy Review

This policy will be reviewed annually or upon significant changes to regulatory requirements, business operations, or technology infrastructure.