Cybersecurity and Physical Security Policy

Adviser: Rob Toyer

Firm: Toyer Investment Advisors

Effective Date: January 2023

Reviewed/Updated: October 14, 2025

1. Purpose

This policy establishes procedures to safeguard client records and information, protect against unauthorized access, and ensure the physical and digital security of all data handled by the firm. It fulfills the requirements of WAC 460-24A-200(1)(bb), which requires investment advisers to adopt and implement written policies and procedures reasonably designed to protect the security, confidentiality, and integrity of client information.

2. Scope

This policy applies to all:
- Client data (electronic and physical);
- Computers, mobile devices, and storage media used for business;
- Office locations or areas where confidential information is stored;
- Third-party systems or vendors with access to client data.

3. Roles and Responsibilities

Rob Toyer serves as the Chief Compliance and Security Officer. He is solely responsible for:
- Implementing and maintaining cybersecurity safeguards.
- Ensuring the physical security of records and equipment.
- Conducting periodic reviews and incident response drills.
- Training and enforcing compliance with this policy.

4. Cybersecurity Policy

4.1 Data Protection and Access Controls

Client data is stored on encrypted, password-protected systems. Strong, unique passwords and multi-factor authentication (MFA) are required for all accounts accessing sensitive data. Access to client information is limited to authorized devices under Rob Toyer's direct control. Regular backups are performed and stored securely, with encryption applied to both local and cloud-based copies.

4.2 Device Security

All computers and mobile devices are configured with current antivirus and anti-malware software, automatic system updates, and screen-lock time-outs. Lost or stolen devices must be reported immediately, and remote wipe procedures will be executed if necessary.

4.3 Email and Communication Security

Confidential client information shall only be transmitted via secure, encrypted email or client portals. Public Wi-Fi is not to be used for accessing client data unless a secure VPN is employed.

4.4 Incident Detection and Response

Suspicious emails, unauthorized logins, or data anomalies are to be reported to and investigated by Rob Toyer immediately. Incident logs will be maintained for at least five years. If a data breach occurs, affected clients and the Washington State Securities Division will be notified in compliance with state law.

4.5 Vendor and Third-Party Management

Third-party vendors with access to client data must provide written assurance of their cybersecurity and data protection measures. Vendor access is reviewed annually.

5. Physical Security Policy

5.1 Office and Records Security

Physical client files are kept in a locked cabinet or secure office area accessible only to Rob Toyer. The office is locked during non-business hours, and keys or access codes are not shared with unauthorized individuals. Shredding or certified document destruction is required before disposing of any physical client records.

5.2 Equipment and Media Handling

Computers and external drives are stored in secure locations when not in use. Backup drives (if applicable) are kept in a locked, fire-resistant safe. Old hardware and media are securely wiped or destroyed prior to disposal.

6. Business Continuity and Data Recovery

Regular encrypted backups ensure data can be restored promptly in case of system failure, theft, or disaster. A written recovery plan outlines procedures for restoring operations and client communication following an incident.

7. Annual Review and Testing

Rob Toyer reviews this policy annually to ensure ongoing compliance with WAC 460-24A-200 and evolving cybersecurity standards. The review includes testing backup restoration, confirming encryption and password compliance, updating software and vendor records, and documenting any incidents and responses.

8. Client Confidentiality Statement

All client information, whether oral, written, or electronic, shall remain confidential. Disclosure is only permitted when authorized by the client or required by law.

9. Acknowledgment

By implementing and following this policy, Rob Toyer affirms that the firm maintains reasonable procedures to protect client information and comply with Washington Administrative Code WAC 460-24A-200(1)(bb).