GA PINCUS FUNDS

CYBERSECURITY RISK MANAGEMENT POLICY

Effective Date: October 15, 2022
Approved By: Chief Compliance Officer
Last Reviewed: February 17, 2026
Next Review: Annual (or upon material change)

1. Purpose

This Cybersecurity Risk Management Policy ("Policy") establishes a comprehensive framework for identifying, assessing, mitigating, detecting, responding to, and recovering from cybersecurity threats that may impact GA Pincus Funds ("Firm"), its clients, vendors, systems, or confidential information.

The Firm recognizes cybersecurity as a fiduciary and regulatory obligation.

2. Scope

This Policy applies to:

- All employees, officers, contractors, and supervised persons
- All Firm-owned and personal devices used for Firm business
- All information systems, cloud platforms, vendors, and data
- All client non-public personal information (NPI)

3. Governance & Oversight

3.1 Chief Compliance Officer (CCO)

The CCO is responsible for:

- Administering this Policy
- Overseeing cybersecurity risk management
- Maintaining documentation and incident logs
- Reporting material events to regulators and clients
- Coordinating with vendors and legal counsel

3.2 Annual Review

The Firm will review this Policy at least annually and upon any material cybersecurity event.

4. Risk Assessment Program

The Firm shall conduct a documented cybersecurity risk assessment at least annually, including:

- Inventory of systems and data
- Identification of reasonably foreseeable internal and external threats
- Evaluation of likelihood and impact of threats
- Review of existing safeguards
- Gap analysis and remediation plan

Risk assessments will be documented and retained in accordance with SEC recordkeeping rules.

5. Access Controls

5.1 Authentication

- Unique user IDs required for all systems
- Multi-factor authentication (MFA) required for:
    - Email
    - VPN
    - Cloud platforms
    - Custodian portals
- Password complexity requirements enforced
- Password manager required for secure credential storage

5.2 Least Privilege

Users are granted only the access necessary to perform their duties.

5.3 Termination Procedures

Upon termination or role change:

- Access revoked immediately
- Credentials disabled
- Devices returned and reviewed

6. Endpoint & Device Security

6.1 Firm Devices

All Firm devices must:

- Use enterprise-grade anti-malware
- Have automatic OS and software updates enabled
- Use full disk encryption
- Be protected by firewall
- Lock automatically after 15 minutes of inactivity

6.2 Personal Devices (BYOD)

If used for Firm business:

- Must comply with Firm security standards
- Must use MFA
- Must permit remote wipe capability

7. Network Security

- Firewall configured to block unauthorized inbound traffic
- Encrypted VPN required for remote access
- Secure Wi-Fi (WPA3 or equivalent)
- Public Wi-Fi access requires VPN
- Periodic penetration testing (at least annually)
- Log monitoring performed regularly

8. Email & Electronic Communications

- All Firm communications must use official Firm email domain
- Email archiving required
- Secure email encryption required for client NPI
- Advanced phishing protection enabled
- DMARC, DKIM, SPF configured and monitored

Employees must immediately report suspected phishing attempts.

9. Data Protection & Storage

9.1 Sensitive Data Handling

Client NPI must:

- Be stored on secure network or approved cloud storage
- Not be saved to unsecured local drives
- Be encrypted in transit and at rest

9.2 Data Minimization

The Firm collects and retains only necessary client information.

9.3 Backups

- Daily encrypted backups
- Offsite storage of backup data
- Periodic restore testing

10. Vendor Risk Management

Prior to onboarding vendors that access client data or systems, the Firm shall:

- Conduct due diligence (SOC 2, security questionnaire, certifications)
- Evaluate data protection practices
- Review contractual confidentiality provisions
- Assess incident notification obligations

Vendor reviews conducted annually.

11. Incident Response Plan

11.1 Definition

A cybersecurity incident includes any unauthorized access, disruption, misuse, ransomware, phishing compromise, data breach, or system compromise.

11.2 Response Steps

1. Immediate containment

2. Preserve evidence
3. Assess scope and impact
4. Engage IT/security professionals
5. Notify insurance carrier
6. Determine regulatory and client notification obligations
7. Document incident thoroughly

11.3 Notification

If client NPI is compromised:

- Notify affected clients promptly
- Notify regulators if required
- Comply with state breach laws
- Consult legal counsel

12. Business Continuity During Cyber Events

The Firm maintains a Business Continuity Plan (BCP) addressing:

- System outages
- Ransomware events
- Custodian access disruptions
- Remote operations
- Communication continuity

Critical functions must be restored as soon as practicable.

13. Secure Disposal

When disposing of hardware or media:

- Use certified data destruction services
- Wipe devices using NIST-compliant standards
- Retain destruction certificates

Paper records containing NPI must be shredded.

14. Monitoring & Logging

The Firm maintains:

- System log monitoring
- Firewall log reviews
- Email security monitoring
- Incident log documentation
- Penetration testing results

Monitoring logs retained per SEC recordkeeping requirements.

15. Training & Awareness

All personnel must:

- Attend annual cybersecurity training
- Complete phishing awareness training
- Review Acceptable Use Policy annually
- Report suspicious activity immediately

Training completion documented.

16. Cyber Insurance

The Firm maintains cybersecurity insurance and shall notify carriers promptly upon potential claim-triggering events.

17. Testing & Continuous Improvement

The Firm will:

- Conduct periodic phishing simulations
- Perform tabletop incident response exercises
- Review threat intelligence updates
- Update safeguards as threats evolve

18. Documentation & Recordkeeping

The Firm retains:

- Risk assessments
- Incident reports
- Training records
- Vendor due diligence files
- Monitoring logs

Records maintained in accordance with SEC Rule 204-2.

Certification

I certify that GA Pincus Funds has adopted and implemented this Cybersecurity Risk Management Policy.

Chief Compliance Officer
Date: October 15, 2022