Cybersecurity Policy and Procedures Manual

Table of Contents

1. Purpose and Regulatory Basis

This Cybersecurity Policy and Procedures Manual establishes the framework through which Kingswood US("the Firm") maintains the confidentiality, integrity, and availability of its information systems and client data. The Firm's cybersecurity program is designed to comply with the applicable requirements of FINRA Rules 3110 (Supervision), 4370 (Business Continuity), 4511 (Books and Records), Regulation S-P (Privacy of Consumer Financial Information), and Regulation S-ID (Identity Theft Red Flags Rule), as well as the guidance set forth in FINRA's 2024–2025 Cybersecurity and Technology Governance priorities.

2. Governance and Oversight Structure

The Chief Compliance Officer (CCO) has primary responsibility for oversight of the Firm's cybersecurity program, with operational implementation delegated to the designated Information Security Officer (ISO). The ISO may be an independent contractor. The ISO is responsible for developing, implementing, and maintaining policies, controls, and monitoring systems. The CCO ensures periodic testing, regulatory alignment, and management reporting. Cybersecurity responsibilities are defined within the Firm's Written Supervisory Procedures (WSPs) to ensure accountability at all levels.

3. Cybersecurity Risk Management Program

The Firm maintains a documented risk management program designed to identify, assess, and mitigate cybersecurity risks. Risk assessments are conducted at least annually and upon material changes in technology, business operations, or regulatory obligations. The Firm's risk assessment process incorporates elements of the NIST Cybersecurity Framework (CSF), focusing on identification, protection, detection, response, and recovery. Findings and remediation actions are tracked and reported to senior management.

4. Access Control and Identity Management

The Firm implements strict access control procedures consistent with the principle of least privilege. Multi-factor authentication (MFA) is required for all systems containing nonpublic personal information. Access rights are reviewed quarterly and promptly revoked upon employee or contractor termination. Passwords must meet complexity standards, be unique per system. Privileged accounts are subject to enhanced monitoring and approval protocols.

5. Information Security and Data Protection

All client and confidential Firm data must be protected through encryption both in transit and at rest. Systems used for data storage and transmission (e.g., Microsoft 365, Global Relay, Box) must be firm-approved and configured for compliance with SEC Rule 17a-4 requirements. Data classification procedures must be maintained to ensure appropriate handling and disposal of sensitive information. The Firm prohibits the use of unauthorized removable media and enforces data loss prevention controls.

6. Network and Systems Security

The Firm maintains layered network defenses including firewalls, intrusion detection and prevention systems (IDPS), endpoint protection, and patch management protocols. Security patches and software updates must be applied in a timely manner consistent with vendor recommendations. The ISO or designated vendor conducts vulnerability scanning and penetration testing at least annually to evaluate system integrity.

7. Incident Response and Notification Protocols

The Firm maintains a written Incident Response Plan ("IRP") outlining the procedures for identifying, containing, and remediating cybersecurity events. All personnel are required to report suspected or confirmed incidents immediately to the ISO and CCO. The ISO coordinates the investigation, remediation, and notification process in accordance with SEC and FINRA reporting obligations. All incidents are documented, and post-incident reviews are conducted to identify process improvements.

8. Third-Party Vendor Oversight

Vendors and service providers with access to Firm systems or data must undergo a cybersecurity due diligence review prior to engagement. This review evaluates the vendor's data protection practices, incident response capabilities, and regulatory compliance posture. Contracts must include confidentiality, breach notification, and data retention provisions consistent with SEC and FINRA expectations. Vendor reviews are renewed annually to confirm ongoing compliance and risk management adequacy.

9. Business Continuity and Disaster Recovery Integration

Cybersecurity controls are integrated into the Firm's Business Continuity Plan (BCP) pursuant to FINRA Rule 4370. The BCP ensures data availability and system recoverability in the event of a cyber-related disruption. Regular backup testing and disaster recovery exercises are conducted to validate recovery time objectives (RTO) and data integrity.

10. Employee Training and Awareness

All registered representatives, receive cybersecurity training at least annually. Training includes secure handling of data, phishing awareness, password management, and incident reporting obligations. Periodic phishing simulations and refresher courses are used to assess effectiveness and reinforce best practices.

11. Ongoing Monitoring, Testing, and Auditing

The Firm continuously monitors network and user activity to detect unauthorized access or data exfiltration. The ISO ensures that log retention and audit trail preservation meet SEC Rule 17a-4 standards. Independent cybersecurity audits or third-party assessments are performed at least annually, with results reviewed by the CCO and executive management.

12. Annual Review, Certification, and Recordkeeping

The CCO and ISO conduct an annual review of the Firm's cybersecurity program to assess effectiveness and regulatory alignment. The results of this review are presented to senior management and incorporated into the Firm's annual FINRA Rule 3130 certification process. Records of all cybersecurity activities, including incident logs, training records, and testing results, are retained for not less than five years in accordance with SEC Rule 17a-4(f).

13. Cyber Incident Reporting and IC3.gov Filing Procedures

Purpose

To establish the Firm's process for identifying, escalating, and reporting cybersecurity incidents, fraud attempts, or electronic crimes through the Internet Crime Complaint Center (IC3.gov), consistent with SEC and FINRA expectations and applicable recordkeeping requirements under Exchange Act Rules 17a-3 and 17a-4.

Scope

This procedure applies to all officers, registered representatives, employees, and contractors of the Firm who become aware of any of the following events:
- Suspected or confirmed data breaches or unauthorized system intrusions
- Business Email Compromise (BEC) or spoofed wire instructions
- Phishing or credential-harvesting attempts
- Malware or ransomware attacks
- Fraudulent transactions or wire requests involving client or firm assets

Responsibility

- Designated Officer: The Chief Compliance Officer (CCO) or Chief Information Security Officer (CISO), if applicable, is responsible for submitting IC3.gov filings on behalf of the Firm.
- Escalation Contacts: In the absence of the CCO/CISO, the AML Compliance Officer or a designated Principal shall assume responsibility.
- Supervisory Oversight: The CCO will ensure that all filings and supporting documentation are reviewed, retained, and cross-referenced to any related FINRA Rule 4530 or FinCEN filings.

Procedures

Step 1 – Incident Identification

When a potential cyber incident is discovered, the discovering party must:
1. Immediately notify the CCO or CISO.
2. Preserve relevant evidence (e.g., emails, logs, messages).
3. Avoid interacting with or deleting suspicious communications.

Step 2 – Internal Documentation

The CCO or designee will complete a Cyber Incident Report Form containing:
- Description of the event and date/time detected
- Affected systems or accounts
- Estimated or actual financial loss
- Actions taken to mitigate risk
- Notification to affected clients, if applicable

This report will be maintained under Rule 17a-4(e) for not less than six years.

Step 3 – Filing on IC3.gov

The CCO or designee shall:
1. Access www.IC3.gov
2. Select “File a Complaint” and choose “Business/Organization.”
3. Provide the following:
   - Firm’s legal name, CRD number, and address
   - CCO contact information
   - Type of incident (e.g., Business Email Compromise, Wire Fraud, Phishing, Ransomware)
   - Narrative description of the event
   - Monetary loss amount or attempted amount
   - Relevant IP addresses, domains, or email accounts involved
4. Upload supporting documents or screenshots, if available.
5. Submit the report and retain the IC3 Confirmation Number.

Step 4 – Notification to Regulatory and Law Enforcement Agencies

Following submission:
- Email FINRA's Cybersecurity Reporting mailbox at cybersecurity@finra.org if the event involves client data, system compromise, or potential investor harm.
- Evaluate whether the event triggers reporting under FINRA Rule 4530(b) (significant events) or (f) (statistical reporting).
- Review for possible Suspicious Activity Report (SAR) obligations under the Bank Secrecy Act / FinCEN requirements.
- Notify the clearing firm and/or FBI local field office as appropriate.

Step 5 – Recordkeeping and Follow-Up

- Retain a copy of the IC3 filing confirmation and all related materials in the Cyber Incident File.
- Document remedial actions (e.g., password resets, security patching, employee retraining).
- Include a summary in the next annual 3120/3130 compliance review.

Training and Awareness

All personnel shall receive annual cybersecurity awareness training addressing phishing, password security, and incident reporting channels. Periodic reminders shall reference the IC3.gov reporting option and internal escalation contacts.

Review and Testing

This procedure shall be reviewed annually by Compliance and IT Security as part of the Annual Supervisory Controls Test (Rule 3120) to confirm:
- Awareness of IC3.gov reporting
- Timely escalation and documentation
- Proper cross-reporting to FINRA and FinCEN

Record Retention

All IC3.gov reports, confirmations, and supporting materials shall be retained for not less than six years and shall be readily accessible for the first two years, in accordance with SEC Rule 17a-4(e)(5).