Buckler

Risk & Insurance Associates

Cyber Program

Policy Title & Content
10/16/2023

Cyber Program

Table of Contents

1. Program Controls

1.1 Governance

Cyber Program Management

16321
The Firm must establish, maintain, and share a Cyber Program for the definition, implementation, monitoring, revision, tracking, and improvement of security policies, procedures, and controls to ensure the confidentiality, integrity, and availability of Nonpublic Information (NPI).

Policy Ownership

40591
Every Cyber Program Policy must be assigned an Owner who holds responsibility for its formulation. The Owner or one of its Delegates must also oversee the enforcement of the Policy and the tracking of supporting evidence.

Nonpublic Information (NPI) Definition

90285
Nonpublic Information (NPI) means all information that is not publicly available information such as:
. Firm Confidential Information.
. Personal Financial Information (PFI).
. Personally Identifiable Information (PII).
. Protected Health Information (PHI).

Senior Governing Body & Senior Leadership Involvement

18177
The Firm's Senior Governing Body and Senior Leadership must be involved and committed to overseeing the Firm's Cyber Program implementation and adoption.

Cyber Program Approval

43891
Periodically, the Firm's Cyber Program must be approved by the Firm's Senior Governing Body.

Task Recurrency: Annually

Reporting to Senior Governing Body

45812
Periodically and when required, the Firm must provide its Senior Governing Body with briefing materials on cyber-related risks, cybersecurity incident response planning, actual cybersecurity incidents and breaches, and cybersecurity-related matters involving vendors.

Task Recurrency: Annually

Senior Leadership & Management Personal Compliance

85483
The Firm's Senior Leadership and Management must demonstrate commitment to the Firm's Cyber Program by personal compliance with its requirements.

Chief Information Security Officer (CISO) Nomination

53658
The Firm must name a Chief Information Security Officer (CISO).

Evidence of Compliance

63022
The Firm must document and store evidence of all activities, events, assessments, reports, contracts, and agreements related to its Cyber Program for future demonstration to:
. Authorities and Regulators (during an Audit or a Breach).
. The Firm's cyber insurer and their cyber experts during the analysis of a claim after a breach.

1.2 Cybersecurity Compliance

Cybersecurity Laws, Regulations, Framework & Standards

78722
The Firm's Cyber Program must meet applicable cybersecurity laws and regulations.

It must also be based on cybersecurity risk management and framework standards.

Compliance Notice to NYDFS Superintendent

50153
Annually, the Firm must submit to the NYDFS Superintendent a written statement covering the prior calendar year.

Unless otherwise announced by NYDFS, this statement shall be submitted by February 15 in the form set forth as Appendix A of the NYDFS Regulation, certifying that the Firm complies with the NYDFS requirements.

Task Recurrency: Annually

5-Year Retention of Annual Attestation Records, Schedules & Data

93744
The Firm must maintain for examination by the New York DFS all records, schedules, and data supporting the annual attestation for 5 years after submission of the attestation.

6-Year Retention of Cyber Program

59905

The Firm must maintain its Cyber Program documentation and records of any action, activity, or assessment for a minimum period of 6 years.

Privacy Notice

16480
The Firm must provide Clients with a Privacy Notice about its privacy policies and practices and describe the conditions under which it may disclose Client NPI to nonaffiliated third parties.

In the event the Firm discloses Client NPI to nonaffiliated third parties, the Firm's Privacy Notice must provide a method for the Firm's Clients to prevent the Firm from disclosing that information to nonaffiliated third parties by opting out of that disclosure.

Privacy Notice Change & Delivery

84681
Initially to new Clients, periodically, and upon changes, the Firm must deliver its Privacy Notice to Clients using at least one of these delivery methods:
. Hand-deliver a printed copy of its Privacy Notice to each Client.
. Mail a printed copy of its Privacy Notice to each Client's last known address.
. Publish its Privacy Notice on a website after getting a signed acceptance of such delivery method from each Client.

Task Recurrency: Annually

Privacy Policy

94967
The Firm must publish a Privacy Policy on its website that describes how the Firm websites or applications collect, use, maintain, and shares information collected from or about its users.

1.3 Risk Management

Cyber Insurance

96682
The Firm must have Cyber Insurance and ensure that coverage related to cybersecurity risk is appropriate.

Cyber Insurance Review

60467
Periodically, the Firm must conduct an analysis of the adequacy of the coverage provided in connection with the Firm’s risk assessment process to determine if the policy and its coverage align with the Firm’s risk assessment and ability to bear losses.

Task Recurrency: Annually

Change Management

14908

The Firm must identify, document, and manage change requests related to its Cyber Program and corrective efforts provided during security audits and Risk Assessments.

Data Classification, Nature, Risk & Location

49172
The Firm must document the nature, risk, and location of information that the Firm accesses, collects, processes, and/or stores.

Business Risks Associated with Cybersecurity

41476
The Firm must identify, manage, and mitigate cyber risks relevant to the Firm’s business.

KPI, Metric & Threshold Review

49119
Periodically, the Firm must review and update its KPIs, metrics, and thresholds.

Task Recurrency: Annually

Verbal Confirmation with Clients for Account Changes & Transfer of Funds & Assets

67877
Account setting changes, wire transfers, and any other banking information to transfer or receive funds and assets from and to Clients must be confirmed verbally with Clients to authenticate their validity.

Verbal Confirmation with Members of Senior Leadership for Account Changes & Transfer of Funds & Assets

68255
Account setting changes, wire transfers, and any other banking information to transfer or receive funds and assets from and to a member of the Firm's Senior Leadership must be confirmed verbally with such a member of Senior Leadership to authenticate their validity.

Exceptions

92121
The Firm must identify, document, and risk rank exceptions and Compensating Controls to its Cyber Program.

Task Recurrency: Annually

Exceptions Review

71584
Periodically, the Firm must review the Exception Evidence Event Log to ensure current exceptions are still justified, and outdated exceptions were revoked.

Task Recurrency: Annually

1.4 Risk Assessments & Security Audits

Risk Assessment Policy

70070
Periodically, the Firm must perform risk assessments of its Cyber Program, Technical Controls, Data Classification, Business and Cyber Risks, Systems, and, if applicable, Applications and Databases.

Cyber Program Risk Assessment

41462
Periodically, a Cyber Program Risk Assessment must be performed to assess the Firm's policies, procedures, processes, plans, tasks, and events and the risks associated with them.

Task Recurrency: Annually

Business Risk Assessment

32187
Periodically, the Firm must review its business risks associated with Cybersecurity.

Task Recurrency: Annually

Governance Structure Assessment

58097
Periodically, the Firm must assess the governance structure's effectiveness in managing cybersecurity risk.

Task Recurrency: Annually

Technical Controls Security Risk Assessment

81862
Periodically, the Firm must audit the Firm's Network and Endpoint Cyber Posture, including Network Penetration Testing and Vulnerability Scans.

The Firm must also assess any Compensating Controls.

The Assessor must provide the Firm with Technical Controls Security Risk Assessment Report & Recommendations.

In the event the Firm accesses shared common networks, these must also be assessed.

Task Recurrency: Annually

Data Classification Assessment

58378
Periodically, the Firm must assess the nature, risk, and location of information that the Firm collects, processes, or stores.

Task Recurrency: Annually

Logging Assessment

47638

Periodically, the Firm must assess logging capabilities and practices for adequacy, appropriate retention, and secure maintenance.

Task Recurrency: Annually

Physical Security Assessment

96310
Periodically, the Firm must perform a Physical Security Assessment to ensure the Firm follows its Cyber Program Physical Security Policies.

Task Recurrency: Annually

Field Offices Review

45454
Periodically, the Firm must review its Field Offices to evaluate their compliance with the Firm's Cyber Program.

Task Recurrency: Annually

1.5 Security Team

Security Team Organizational Structure, Committees & Members

18017
The Firm must document information regarding the committees, positions, and departments responsible for cybersecurity-related matters and where they fit within the Firm’s organizational structure.

Security Incident Response Plan (SIRP) Lead Nomination

33992
The Firm must name a SIRP Lead who must lead the execution of the Firm's SIRP in the event of a Security Incident or Breach.

Security Incident Response Team (SIRT) Member Nomination

42903
The Firm must name its SIRT Members and keep an updated list of their contact information.

Business Continuity & Disaster Recovery Plan (BCDRP) Lead Nomination

40768
The Firm must name a BCDRP Lead who must lead the execution of the Firm’s BCDRP in the event of a Significant Business Disruption (SBD).

Insider Threat Controls Lead Nomination

73257
The Firm must name an Insider Threat Controls Lead.

Field Office Cybersecurity Supervisor Nomination

28874
The Firm's Field Offices must name a Field Office Cybersecurity Supervisor whose responsibility is to enforce the Firm's Cyber Program.

Cybersecurity Personnel & Intelligence

29896
The Firm must utilize internal or external qualified cybersecurity personnel sufficient to manage the Firm's cybersecurity risks and to perform or oversee the performance of the core cybersecurity functions specified in the Firm's Cyber Program.

Cybersecurity Personnel Training

89748
The Firm must provide cybersecurity personnel with cybersecurity updates and training sufficient to address relevant cybersecurity risks.

Intelligence-Sharing Opportunities

35722
The Firm must take advantage of intelligence-sharing opportunities and engage in collaborative self-defense to protect itself from cyber threats.

CISA Security Alerts

67623
The Firm must sign up for alerts published by the Cyber Infrastructure Security Agency (CISA).

Business Continuity & Disaster Recovery Plan (BCDRP) Committee Member Nomination

49986
The Firm must name its BCDRP Committee Members and keep an updated list of their contact information.

2. Process Controls

2.1 Business Continuity & Disaster Recovery Plan (BCDRP)

BCDRP Policy

32791
The Business Continuity & Disaster Recovery Plan (BCDRP) must allow the Firm to respond to Significant Business Disruptions (SBDs) by, whenever possible:
. Safeguarding the property of the Firm, its Employees, and Affiliates.
. Making a financial and operational assessment.
. Recovering and resuming operations.
. Protecting all of the Firm's NPI and Books & Records.
. Allowing Clients to transact business.

Significant Business Disruption (SBD) Definition

16261
A Significant Business Disruption (SBD) is either:
1. Affect the Firm's Employees & Affiliates' ability to reach their work location, such as a fire in the office.
2. Prevent the Firm from delivering services to clients, such as a pandemic, a city flood, a terrorist attack, or a wide-scale, regional disruption.

Disaster Recovery of Systems & Data

11252
The Firm must ensure its Systems and Data can be restored or, if possible, that an alternate solution can be provided to conduct business.

Backup of Systems & Data

11708
The Firm must back up its computing systems (Servers, Computers, etc.) and NPI.

Backup Retention

12648
Backups must be kept for 5 years to allow for the reconstruction of material financial transactions sufficient to support normal operations and obligations of the Firm.

Backup Recovery Test

20512
Periodically, a Backup Recovery Test must be performed.

Task Recurrency: Annually

Communications with Clients Before Anticipated SBDs

97044
Before an anticipated SBD, the Firm must contact Clients to validate if they have any transactions they want to execute before such SBD occurs.

Communications with Employees, Affiliates, Clients, and Vendors During & After SBDs

18064
During and after an SBD, the Firm must communicate the status of its operations with impacted Employees, Affiliates, Clients, and Vendors.

Centralized SBD Communications

41545
The Firm must establish a centralized process to communicate with its Employees and Affiliates during and after an SBD.

Uninterrupted Battery Power Supply

92733
The Firm must maintain an uninterrupted battery power supply to keep essential operations running until the backup generator is turned on during power outages.

Alternative Office Location in the event of an SBD

13806
In the event of an SBD where Employees or Affiliates are not able to work at their assigned Firm's Location, they must work from an Alternate Location or home.

Data Service Provider Redundancy

40791
The Firm must have its data at multiple service providers and test the connectivity to such providers to ensure that the data is accessible from remote locations.

Elevated Electronic Equipment

50050
The Firm must elevate electronic equipment in ground-level facilities to mitigate the risk of damage in the event of flooding.

Internet Connectivity Redundancy

68828
The Firm must have internet connectivity redundancy.

Emergency Contact Lists

84566
The Firm must maintain and update emergency contact lists as Employees and Affiliates are added or removed so they can be contacted with Firm updates.

Alternate Contact Information

98975
The Firm must provide Employees, Affiliates, Clients, Vendors and Regulators with updated contact information should alternate telephone numbers be used.

In the event of a Significant Business Disruption, an alternative telephone number will be posted on the Firm's Website.

BCDRP Test & Review

84044
Periodically, and when required, the BCDRP must be tested and reviewed.

Task Recurrency: Annually

2.2 Security Incident Response Plan (SIRP)

SIRP Policy

90168
The Firm must implement a Security Incident Response Plan (SIRP) to identify, document, respond, limit, and counteract Security Incidents and Breaches.

Security Incident & Breach Definitions

19575
A Security Incident is an act or attempt, successful or unsuccessful, by an unauthorized person or system to access, store, control, disrupt, or misuse NPI.

A Security Breach is either:
1. There is evidence that NPI was accessed, stored, controlled, disrupted, or misused by an unauthorized person or system.
2. A Security Incident occurred, and there is no evidence to prove NPI was not accessed, stored, controlled, disrupted, or misused by an unauthorized person or system.

Most Common Attack Response Plan

62165
The Firm must document response plans to prepare for the most common attacks to which the Firm may be subjected.

Phishing Email Deletion

19143
The Firm's Employees and Affiliates must delete phishing emails.

Phishing Attack Impact Reduction

48911
The Firm must reduce the impact of a successful phishing attack by segmenting Clients and other critical assets.

Locking or Wiping Lost or Stolen Devices

83700
The Firm must be able to remotely lock a lost or stolen device or wipe its data.

Security Incident Reporting at the Time of Discovery

21525
The Firm Employees & Affiliates must report a Security Incident to the Firm CISO as soon as they are aware of it.

Security Incident Response Process

90023
In the event of a Security Incident or Breach, the Security Team, led by the SIRP Lead, must follow the Firm Security Incident Response process.

Security Incident & Breach Event Tracking

52378
Security Incident and Breach Events must be documented with details about the type of incident or the breach, the discovery, the data that may have been compromised, the associated risk, and the potential impacts.

Unauthorized User Access & Cyber Program Violation

56038
The Firm must document information related to the identification and remediation of instances in which system users, including Employees, Affiliates, Clients, and Vendors, access Firm data and systems without required authorization or are in contravention of the Firm's Cyber Program.

Compromised Endpoint Disconnection from Network & Internet Access

24181
The Firm, Employees, and Affiliates must immediately remove, disconnect, and stop using devices suspected of being compromised by malicious software (virus, malware) from the Firm's Network and the Internet until remediated.

Decision & Communication Approval

61598
Decisions and communications regarding a Security Incident or Breach, internal or external, must be pre-approved by the Firm's Senior Leadership.

Breach Notifications

95443
The Firm must comply with all Breach Notification Requirements from Regulators, States, Authorities, Insurance, Enterprises, and other Stakeholders.

In the event of a security event or a breach, the Firms' Security Team and Senior Leadership must determine if notifications must be sent and, if yes, when and to whom.

Depending on the situation, Clients, Employees, Affiliates, Vendors, Authorities, Regulators, Cyber Insurers, and other Stakeholders may be notified.

Local Federal Bureau of Investigation (FBI) Office

15771
For each location, the Firm must list the contact information of the Local Federal Bureau of Investigation (FBI) Office to report security incidents.

Incident Reporting to Local Police

13153
In the event of a robbery or burglary, the Firm or affected Employee or Affiliate must immediately report the event to the local police department.

Remediation Documentation & Tracking

49442
The Firm must document and track remediation identified during a SIRP Review, a Security Incident, or a Breach.

SIRP Review with Senior Leadership

76188
SIRP Reviews must include Senior Leadership.

2.3 Vendor Risk Management

Vendor Risk Management Policy

33340
Periodically and when adding new vendors, the Firm must evaluate and document the security risk of Vendors.

As a general principle, the Firm must avoid using vendors whose security standards do not at least meet those of the Firm.

Vendors must provide the Firm with a Vendor Cybersecurity Package detailing how they protect their Endpoints, Networks, and, if applicable, the Firm's NPI they access, store, or control.

The Vendor Cybersecurity Package must confirm that minimum cybersecurity standards, security policies, and procedures are in place and enforced.

Vendors must notify the Firm if a cybersecurity event directly impacts the Firm's NPI.

Vendor Contract Management

48197
The Firm must ensure contracts are in place with third parties with access to Nonpublic Information (NPI). These contracts

must contain requirements relating to cybersecurity as defined in the Vendor Risk Management Policy and address technical issues and related responsibilities in the case of a cyber-attack.

Pre-Contract Vendor Due Diligence

49197
The Firm must perform pre-contract due diligence on prospective service providers.

Vendor Contract Provisions

88663
The Firm must ensure that provisions of the contract with Vendors govern the Vendor's obligation to the Firm, as well as identify the Firm's prerogatives with Vendors.

This includes how the Firm can conduct its ongoing oversight of the Vendor, the conditions for terminating the relationship, and the Vendor's obligations to protect Firm information if the relationship terminates.

Vendor Contingency Plan & Change Notices

69657
The Firm must ensure its contracts with vendors include contingency sections related to conflict of interests, bankruptcy, and other issues that might put the vendor out of business or in financial difficulty.

The Firm must ensure that its contracts with vendors include the requirements for documentation or notices from such vendors, required before any significant changes to the third-party vendors' cyber program, systems, components, or services that could potentially have security impacts on the Firm and the Firm's data containing NPI.

Vendor Termination & Replacement

53020
When terminating or replacing a Vendor, the Firm must follow the Firm's Vendor Termination & Replacement process.

Vendor Privacy Notice

10865
The Firm must ensure its Vendors that are accessing, controlling, or storing the Firm's Client NPI are providing a Privacy Notice.

Such Vendor's Privacy Notice must describe the conditions under which the Vendor may disclose the Firm's Client NPI to nonaffiliated third parties.

Initially to new Clients, annually, and if there is any change to it, the Vendor must deliver its Privacy Notice to the Firm's Clients with at least one of these delivery methods:

. Hand-deliver a printed copy of its Privacy Notice to each Firm's Client.

. Mail a printed copy of its Privacy Notice to each Firm Client's last known address.

. Publish its Privacy Notice on a Website after getting a signed acceptance of such delivery method from each Firm's Client. In

this case, if there is any change and annually, the Vendor must advise the Firm's Clients via email or mail.

In the event a Vendor discloses the Firm's Client NPI to non-affiliated third parties, the Vendor's Privacy Notice must provide a method for the Firm's Clients to prevent the Vendor from disclosing that information to nonaffiliated third parties by opting out of that disclosure.

Technology System Impact Assessment

89668
When adding or reviewing Vendors, the Firm must conduct an assessment of the Vendor systems the Firm uses, the impact should the information or technology systems become compromised, and potential alternatives if the system fails.

Approved Vendors

85947
The Firm must maintain a list of approved Vendors and make it available to Employees & Affiliates.

Approved Vendors for Secure Disposal of Hard Copy & Computer Hardware

75196
The Firm must provide its Employees, Affiliates, Field Offices, and Vendors responsible for the secure disposal of hard copies and computer hardware that may contain NPI a list of approved Vendors to perform such disposal.

2.4 Physical Security

Physical Security Policy

34778
The Firm must ensure that its Physical Security Policies are enforced at each of its Locations.

Location List

86637
The Firm's office Locations must be managed and updated with information about their main contacts, network infrastructure, and alternate location in the event of an SBD.

Access to Physical Locations

53617
Access to the Firm's physical Locations and offices where NPI is stored or used must be controlled and restricted to authorized persons with a legitimate business need.

Access to Printers, Copiers & Fax Machines

84271
Access to printers, copiers, and fax machines must be controlled and limited to only those with a business need. These devices must not be located where they are accessible to unsupervised visitors and non-authorized personnel.

Clean Desk

75469
The Firm's Employees and Affiliates must ensure that NPI in hardcopy or electronic form is secure in their work area at the end of the day and when they are expected to be gone for an extended period.

Cabinet & Drawer Locks

38156
Cabinets and Drawers containing the Firm's NPI must be locked when not used.

Paper Shredding

71016
To dispose of printed documents containing NPI, the Firm must shred them.

Labeling & Storage of NPI

40272
All documents, files, disks, and other media containing NPI must be labeled as such, securely stored, and only shared with authorized parties.

Periodic Walk-Throughs & Examinations of Workspaces

60127
The Firm must perform periodic walk-throughs and examinations of workspaces to ensure Employees and Affiliates comply with the Clean Desk Policy.

Task Recurrency: Annually

Removal of Confidential Information from Printers, Scanners & Copiers

45387
Confidential Information must be promptly retrieved from printers, scanners, and copiers and secured at the end of the business day.

Movement of Hardware & Electronic Media Containing NPI

92824
Movement of Hardware & Electronic Media Containing NPI must be pre-authorized by the Firm.

Physical Security of Personal & Firm Devices

90890
The Firm's Employees and Affiliates must ensure the physical security of personal and Firm devices.

Physical Environment Monitoring

24446
The Firm must monitor its physical environments to detect potential security events.

Protection of Documents with NPI Removed from Office Locations

28020
Documents containing NPI removed from the Firm's office locations must be protected from being accessed, viewed, taken, copied, lost, or stolen.

2.5 Employees & Affiliates

Criminal & Credit Background Checks

61233
Clear and satisfactory results of criminal and credit background checks must be obtained for all new Employees and Affiliates before employment and before they can access NPI.

Acceptable Use Policy (AUP) Agreement & Consent

70419
Periodically, the Firm's Employees and Affiliates must sign the Firm's Acceptable Use Policy (AUP).

Task Recurrency: Annually

Violation of Cyber Program Requirements

19450
Firm's Employees or Affiliates, regardless of their position or status in the Firm, found to be in violation of the Firm's Cyber Program may be subject to disciplinary action.

Cybersecurity Awareness Training

25275
When they join the Firm, and then periodically, the Firm's Employees and Affiliates must follow Cybersecurity Awareness Training.

Task Recurrency: Annually

Cybersecurity Awareness Training Evaluation & Update

17669
Periodically, the Firm must re-evaluate and update Cybersecurity Awareness Training programs based on their effectiveness and cyber-threat intelligence.

Task Recurrency: Annually

Assessment of Cybersecurity Awareness Training Participation

79574
Periodically, the Firm must assess that Employees and Affiliates attend Cybersecurity Awareness Training.

Task Recurrency: Annually

Mobile Device Training

83689
The Firm must train Employees & Affiliates on mobile device policies and effective practices to protect mobile devices.

BCDRP Training to Employees & Affiliates

78588
Periodically, the Firm must conduct BCDRP training for Employees and Affiliates to familiarize them with the plan.

Task Recurrency: Annually

Social Media Usage Training

12141
When they join the Firm, and then periodically, the Firm must provide Employees and Affiliates with training about the Firm's Social Media usage policies.

Task Recurrency: Annually

Security Updates to Employees & Affiliates

13901
Periodically, the Firm must provide security updates to its Employees and Affiliates.

Task Recurrency: Annually

Phishing Simulations

62980
Periodically, a Phishing simulation email message must be sent to Employees & Affiliates to test their awareness of potential threats.

Task Recurrency: Quarterly

Internet Searches for Policy Violation

26029
Periodically, the Firm must run internet searches on Employees and Affiliates to identify potentially unauthorized advisory business being conducted online.

Task Recurrency: Annually

Identification of Potentially Malicious Insiders

26922
The Firm must monitor Employees and Affiliates behavior indicators to identify potentially malicious insiders.

Such behavior may include changes in working patterns, unexcused or unauthorized absences, performance decline, and work conflicts.

Confidential Reporting of Potentially Suspicious Activity

89013
The Firm must allow Employees and Affiliates to report concerns about a colleague's electronic messaging, website, use of social media for business communications, and any potentially suspicious activities.

The Firm must protect the identification of Employees and Affiliates who report such activities.

3. Data Controls

3.1 Software & Systems

General Password Rules

74689
The Firm's Employees and Affiliates must follow these password rules:
. Passwords, secret or challenge questions, images, and any other authentication information must be kept confidential and must not be shared with anyone.
. Passwords cannot be written on paper or in electronic form (except in Password Management Software).
. OS and Browser "Auto Complete" and "Remember Password" features are not allowed and must not be used.
. Password reuse for multiple access is not permitted (passwords must be unique).
. Passwords must not contain the Username.

Temporary & Default Account Username & Password Change

68961
Temporary and default account usernames and passwords must be changed immediately upon first use.

Regular User Password

42737
Regular User passwords to access a Firm's System and Software containing or providing access to NPI must follow the Firm's Minimum Standards.

Administrator & Privileged Account Password

80311
Administrator & Privileged Account passwords to access the Firm's System and Software containing or providing access to NPI must follow the Firm's Minimum Standards.

Software MFA Configuration

96100
When available, the Multi-Factor Authentication (MFA) capability of Software used by the Firm Employees or Affiliates must be enabled.

Software Updates & Security Patches

23792
Software must be configured to automatically download and install software updates and security patches.

This should be done manually when this configuration is not available.

Operating System Major Version Upgrade

22770
Upon the Firm's approval, upgrades to the latest Operating System major versions (6, 7, etc.) must be installed.

Operating System Version & Security Updates

31488
Unless not approved by the Firm, operating system security patches and updates must be automatically installed.

Software Access Logs

64973
The Firm must turn on all available log features for Software and Systems used to access, store and control NPI.

Failed Login Attempts

99024
The Firm must prevent, monitor, and track failed login attempts and lockouts.

Email Security Information & Event Management (SIEM)

72087
The Firm must implement an email Security Information & Event Management (SIEM) system that centralizes logging and security event alerting. Off-site logs must be kept for 3 years.

Dark Web Monitoring for Leaked Credentials

20554
The Firm must monitor the dark web for lists of leaked usernames and passwords.

Task Recurrency: Annually

System Notifications to Users

82964
The Firm must document and notify all users of appropriate usage obligations when logging into the Firm's systems. (e.g., log-on banners, warning messages, or acceptable use notifications).

Authorized Communication Channels

54455
The Firm must establish and share with its Employees & Affiliates a list of Authorized Communication Channels.

Prohibited Communication Channel

67368
When a communication is received outside of authorized channels, the Firm's Employees and Affiliates are not allowed to continue the communication and must transition to an Authorized Communication Channel.

Software & System Hardening

89890
The Firm must ensure the secure configuration of its systems and software using Vendor guidance or industry standards, such as those published by the Center for Internet Security (“CIS”). (https://www.cisecurity.org/)

Account & Trading Application Session Time-Out

25612
The Firm must set account and trading session time-out following the Firm's Minimum Standards.

Application Control Capability

65516
The Firm must use an application control capability that ensures only the Firm's approved software can be executed.

SIEM Configuration Change Approval

88497
Changes to SIEM configuration must be pre-approved by the Firm before being implemented.

3.2 Data & File Management

File Synchronization & Sharing

38202
The Firm's Employees and Affiliates must store and synchronize files containing NPI to an encrypted Cloud File Service selected by the Firm.

The Firm's Employees and Affiliates must not use personal Cloud File Service to store or synchronize NPI.

Email, File & Network Trafic Encryption

75373
Email messages, files, and Network traffic that include NPI must be encrypted in transit and at rest.

Communication Archiving

11024
All communication content distributed to Authorized Communication Channels must be archived for not less than 5 years.

NPI Storage Outside the United States

48516
NPI must not be stored outside the United States.

Email Filtering

50147

The Firm must filter email to block phishing, spam, and malicious attachments/links from reaching users.

Electronic Storage Media Decommissioning

61773
Before decommissioning Electronic Storage Media (Hard Disk, USB Drive, etc.), the Firm must document evidence that NPI has been destroyed or erased from the device.

3.3 User Management

Identity Access Management (IAM)

95436
The Firm must implement effective Identity Access Management (IAM) and user entitlements processes to ensure Employees and Affiliates are assigned proper access to systems, applications, files, and databases.

User Responsibility

22921
To ensure accountability and responsibility, activities performed using a Username must be the responsibility of the Employee or Affiliate to whom that Username was assigned.

Access Rights & Controls

11013
Access to and viewing of NPI must be limited to authorized persons on a need-to-know basis.

The concept of Least Privilege must be applied to ensure users only get privileges essential to perform their intended duties.

The allocation and use of privileged and administrative access rights (Software administration, Servers, Active Directory, etc.) must be restricted to only those requiring it and pre-approved by the Firm's Senior Leadership, the CISO, or one of their representatives.

Privileged & Service Accounts

71613
Privileged and service accounts must require MFA, be used only for tasks requiring elevated privileges, and cannot be shared unless there is an alternate control to log who is using the accounts.

Privileged and service accounts must be given the minimum level of access necessary to perform their associated tasks.

Access Rights & Controls Review

41516
Periodically or upon onboarding, the Firm must review changes in responsibilities, transfers, and terminations of Employees,

Affiliates, or Contractors, Access Rights & Controls.

Ex-Employees, Affiliates, or Contractors' access must be immediately canceled when no longer necessary.

Task Recurrency: Annually

Clients' Credential Request Handling

62158
The Firm must properly handle Clients' username and password change requests and authenticate anomalous or unusual Client requests.

Access to Systems from Personally Owned Devices

74670
Firm Employees and Affiliates must get approval from the Firm before they can access Firm email servers, systems, and other business applications from personally owned devices.

Client Access Complaints Tracking & Remediation

55005
Client complaints received by the Firm related to Client access, resolution of the complaints, and any remediation efforts undertaken in response must be documented.

3.4 Social Media

Approved Social Media Sites

93489
The Firm must document social media sites approved for use, including the continuing obligation to address any upgrades or modifications to the functionality that affect the risk exposure for the Firm or its clients.

Social Media Content Pre-Approval

63446
The Firm's Employees and Affiliates must have the content of their intended social media posts validated and approved by the Firm before posting.

NPI on Social Media Sites

95378
The Firm's Employees and Affiliates must not post, comment, or discuss on social media sites any information related to NPI and investment recommendations, information on specific investment services, or investment performance.

Firm Social Media Site Disclaimer

55788

The Firm must post disclaimers directly on its sites stating that they do not approve or endorse any third-party communications posted on such sites in an attempt to avoid having a third-party posting attributed to the Firm.

Participation on Social Media Sites

38601
The Firm's Employees and Affiliates must not like, approve, upvote, or comment on a Client's or Client's experience with Employees and Affiliates on social media sites.

Social Media Sites & Content Monitoring

86351
Periodically, the Firm must monitor and verify the Firm’s social media sites and Firm's Employees and Affiliates' use of third-party sites.

Task Recurrency: Annually

4. Technical Controls

4.1 Endpoint Security

Endpoint Security Policy

82214
Endpoints (Computers, Smartphones, and Tablets) used to access, store or control NPI must have their Cybersecurity Settings and Software adequately installed, configured, and managed to allow for the following:
. Identification and protection of such Endpoints.
. Detection, response, remediation, and recovery from Cybersecurity Events.

Endpoint Hardware

62421
The Firm must provide its Employees and Affiliates with a list of Endpoint hardware Minimum Standards.

Endpoint Asset Inventory Report Production

33584
Periodically, an Asset Inventory Report must be produced with the list of Endpoints accessing, controlling, or storing NPI.

The Report must include Endpoint information as well as Cybersecurity Settings and Software.

Periodical Asset Inventory Reports must be saved in the Cyber Folder or accessible in a system.

Complex & Unique Endpoint Name

97594
The Endpoint names must be complex and unique.

Endpoint Asset Inventory Report Review

84434
Periodically, the Firm must review the Endpoint Asset Inventory Report to assess the Endpoint Cyber Posture and identify Endpoints that are no longer in use and should be decommissioned.

Task Recurrency: Monthly

Working Remotely and/or From Home

85578
In the event that the Firm's Employees or Affiliates must work remotely or from home, Endpoints must have the same Security Protection as office Endpoints.

Data Controls on Personally Owned Devices

60369

The Firm must block NPI from being printed, copied, pasted, or saved to and from personally owned Computers, Smartphones, or Tablets.

Printers, Copiers & Scanners Configuration

11925
Printers, copiers, and scanners must have encryption. If such capability is unavailable, they must be set to overwrite.

4.2 Computer Security

Computer Definition

30382
Computer refers to Desktops, Laptops, Virtual Machines, Physical Servers, and Virtual Servers.

Computer Remote Monitoring Software

89996
The Firm must implement a Computer Remote Monitoring Software.

Computer Security Monitoring

93843
Computers must be monitored 24x7 in order to detect and respond to Cybersecurity Events.

Computer Antivirus, Anti-Malware, and Ransomware

45667
An Antivirus, Anti-Malware, and Anti-Ransomware must be installed on all Computers following the Firm's Minimum Standards.

Endpoint Detection & Response (EDR)

35536
The Firm must implement an Endpoint Detection and Response (EDR) solution.

Computer Full-Disk Encryption

76582
Full-Disk Encryption (FDE) must be configured on all Computers following the Firm's Minimum Standards.

Computer Screen Saver

77422
Screen Saver Settings must be configured following the Firm's Minimum Standards.

Computer Password Settings

83800
Computer Password Settings must be configured following the Firm's Minimum Standards.

Computer Firewall

36038
Computer Firewall must be enabled.

Computer Logs

69762
Computer Log Settings must be configured following the Firm's Minimum Standards.

Computer Security Information and Event Management (SIEM)

96811
The Firm must use a Computer Security Information and Event Management (SIEM) system that centralizes logging and security event alerting. Off-Site Logs must be kept for 3 years.

External & Mobile Data Drive Encryption

60916
External and mobile data drives such as flash drives, thumb drives, memory sticks, USB hard drives, and backup drives must be encrypted before NPI can be stored on them.

Session Fingerprinting

18496
The Firm must implement session and device fingerprinting to detect a brute force or credential stuffing attack rapidly.

User and Entity Behavioral Analytic (UEBA)

63062
The Firm must implement behavioral analytics and other artificial intelligence systems to identify emerging trends and suspicious activities in a timely manner.

4.3 Smartphone/Tablet Security

Mobile Device Management (MDM)

39559
Smartphones and Tablets must be managed by a Mobile Device Management (MDM) solution selected by the Firm.

Only mobile devices managed by the approved Mobile Device Management solution may be used to access and store NPI.

Smartphone/Tablet Password/Biometrics

20403
Password/Biometrics (Face ID, Pattern, or Fingerprint) Settings must be enabled and configured following the Firm's Minimum Standards.

Smartphone/Tablet Screen Saver

75488
Screen Saver Settings must be configured following the Firm's Minimum Standards.

Smartphone/Tablet Full-Disk Encryption

68164
Smartphones and Tablets storing NPI must be encrypted.

Smartphone Multi-Factor Authentication

56769
The Firm's Employees and Affiliates must be able to receive Multi-Factor Authentication requests on their Smartphone (MFA App), Key Fob, or phone call and confirm such requests to authenticate themselves.

Smartphone/Tablet OS Version & Security Updates

10054
The Firm must ensure that the latest supported OS versions are installed. Jailbroken devices are not allowed.

Smartphone/Tablet Security Information and Event Management (SIEM)

76490
The Firm must use a Smartphone/Tablet Security Information and Event Management (SIEM) system that centralizes logging and security event alerting. Off-Site Logs must be kept for 3 years.

4.4 Network Security

Network Security Policy

61289
The Firm's Network Systems (Firewalls, Wireless Access Points, Switches, Routers, etc.) must have their Cybersecurity Settings and Software adequately installed, configured, and managed to allow for the following:
. Identification and protection of such Network Systems.
. Detection, response, remediation, and recovery from Cybersecurity Events.

Network Monitoring

27041
Networks must be monitored 24x7 in order to detect and respond to Cybersecurity Events.

Network Design & Diagrams

73721
The Firm must create and update maps of network resources, connections, data flows and NPI locations.

Firewall Configuration

19778
Firewall Configuration must follow the Firm's Minimum Standards.

Firewall Firmware/Software Functionality & Security Updates

49502
Firewall firmware/software must be kept up-to-date, ensuring the manufacturer’s functionality and security updates are applied.

Firewall Logs

76971
Firewall Log Settings must meet the Firm's Firewall Logs Minimum Standards.

Network Security Information and Event Management (SIEM)

55887
The Firm must use a Network Security Information and Event Management (SIEM) system that centralizes network logging and security event alerting. Off-Site Logs must be kept for 3 years.

Encrypted Private Hidden WiFi

46887
A Private Hidden WiFi must be configured to be used by anyone accessing, storing, or controlling NPI following the Firm's Minimum Standards.

Public WiFi

52245
A Public WiFi must be segmented from the Private Hidden WiFi to ensure users of Public WiFi cannot access data or services from the Private Hidden WiFi.

Network Hardware Asset Inventory Report

17379
The Firm must maintain a list of its Network Hardware Assets.

Secure Remote Access to Firm Networks, Systems & Computers

68919
The Firm must configure remote access to the Firm's Networks, Systems & Computers following the Firm's Minimum Standards.

VoIP Network Security

16539
The Firm must protect Voice Over IP (VoIP) networks to protect the confidentiality and integrity of NPI.