ClientGen

Cyber Program

Buckler-Generated Report

Cyber Program

Table of Contents

1. Program Controls 3
   - 1.1 Governance 3
   - 1.2 Cybersecurity Compliance 4
   - 1.3 Risk Management 5
   - 1.4 Risk Assessments & Security Audits 6
   - 1.5 Security Team 8

2. Process Controls 11
   - 2.1 Business Continuity & Disaster Recovery Plan (BCDRP) 11
   - 2.2 Security Incident Response Plan (SIRP) 14
   - 2.3 Vendor Risk Management 18
   - 2.4 Physical Security 21
   - 2.5 Employees & Affiliates 22

3. Data Controls 26
   - 3.1 Software & Systems 26
   - 3.2 Data & File Management 28
   - 3.3 User Management 29
   - 3.4 Social Media 30

4. Technical Controls 32
   - 4.1 Endpoint Security 32
   - 4.2 Computer Security 33
   - 4.3 Smartphone/Tablet Security 34
   - 4.4 Network Security 35

1. Program Controls

1.1 Governance

Cyber Program Management

16321
The Firm must establish, maintain, and share a Cyber Program to define, implement, monitor, revise, track, and improve security policies, procedures, and controls to ensure the confidentiality, integrity, and availability of Information Systems and Nonpublic Information (NPI).

Policy Ownership, Implementation, Enforcement, and Evidencing

40591
Each Cyber Program Policy must be assigned an Owner responsible for its formulation. The Owner, or an appointed Delegate, must also oversee the policy's implementation, enforcement, and, where applicable, the tracking of supporting evidence.

Information System Definition

57864
An Information System is a discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of electronic information.

Nonpublic Information (NPI) Definition

90285
Nonpublic Information (NPI) means all information that is not publicly available information such as:
. Business Confidential Information (BCI).
. 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 CISO must provide its Senior Governing Body with written reports and updates on the Firm's Cyber Program effectiveness, cyber-related risks, cybersecurity incidents and breaches, cybersecurity-related matters involving vendors, and corrective efforts.

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) responsible for overseeing and implementing the Firm's Cyber Program and enforcing its Policies.

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.

5-Year Retention of Compliance Records, Schedules & Data

93744
The Firm must retain records, schedules, documentation, and data for 5 years for examination and inspection purposes. This includes identifying areas, systems, and processes needing improvement, efforts made to address these issues, and the timeline for implementing remediation plans.

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.

Privacy Complaints Tracking & Remediation

46477
The Firm must document, manage, and resolve Privacy Complaints following the Firm's Privacy Complaint Management process.

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

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.

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.

Change Management Approval

67170
The Firm must approve change requests.

Exception & Compensating Control Management

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

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.

Risk Assessment Process Review

30009
Periodically, and whenever a change in the business or technology causes a material change to the Firm’s cyber risk, the Firm must review, assess, and update as necessary the risk assessment process of its Cyber Program, Technical Controls, Data Classification, Business and Cyber Risks, Systems, and, if applicable, Applications and Databases.

Task Recurrency: Annually

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 assess 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

System, Application & Database Assessment

75525
Periodically, to ensure the quality and security of developed systems and applications by or for the Firm, the Firm must perform Software Penetration Testing and review secure development practices and quality assurance processes.

The Assessor must provide the Firm with a System & Application Security Risk Assessment Report & Recommendations.

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

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

1.5 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) Committee & Member Nomination

42903
The Firm must establish a SIRT Committee, name its 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).

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

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

Change Management Committee & Member Nomination

94354
The Firm must establish a Change Management Committee, name its Members, and keep an updated list of their contact information.

Insider Threat Controls Lead Nomination

73257
The Firm must name an Insider Threat Controls Lead.

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).

Cyber Program Committee Responsibilities

41196
The Firm's Cyber Program Committee must exercise oversight of the Firm's Cyber Program by:

. Progress Monitoring: Ensuring that cybersecurity initiatives are progressing according to established timelines and objectives.

. Gap Identification: Identifying and addressing gaps in the Firm's Cyber Program to ensure continuous improvement.

. Violation: Exercising appropriate actions when Employees or Affiliates fail to adhere to Cyber Program Requirements.

. Review and Approval: Reviewing and approving updates to the Cyber Program to maintain its relevance and effectiveness in managing risks.

. Receiving Reports: Reviewing reports from each Cybersecurity Committee to ensure comprehensive oversight of cybersecurity activities.

. Reporting: Assembling and coordinating the delivery of reports and information to the Senior Leadership and SGB (Senior Governing Body) in a timely and effective manner.

2. Process Controls

2.1 Business Continuity & Disaster Recovery Plan (BCDRP)

Business Continuity & Disaster Recovery Plan (BCDRP) Policy

32791
The 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 an information system downtime, a pandemic, a city flood, a terrorist attack, or a wide-scale, regional disruption.

Significant Business Disruption (SBD) Response Process

59799
In the event of an SBD, the Firm must follow its SBD Response Process.

1. Document date/time of all activities and updates.
2. Request that the person who discovered the SBD send a report describing the findings.
4. Collect and review the BCDRP Committee.
5. Organize the initial Security Team conference call.
6. Assess the extent of the disruption, focusing on critical systems and services. Document the damage and begin planning for continuity.
7. Execute the steps outlined in the BCDRP to continue essential operations
8. Alert appropriate external and internal contacts.
9. If required, consult legal counsel.
10. Review cyber insurance coverage and process.
11. If a Vendor is involved, review and follow the Vendor incident response process.
12. Conduct a thorough review of the SBD response, identifying what worked well and what needs improvement.
13. Update the BCDRP based on lessons learned to improve readiness for future SBDs.
14. Communicate recovery status to all stakeholders and provide a full report on the SBD.

Significant Business Disruption (SBD) Event Tracking

48159
The Firm must document Significant Business Disruption (SBD) events.

Disaster Recovery of Systems & Data

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

Backup of Systems & Data

11708
The Firm must back up its Information Systems 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

Business Continuity Plan and Disaster Recovery (BCPDR) Notice

42377
At account opening and upon request, the Firm must disclose to its customers how its business continuity plan addresses the possibility of a future significant business disruption (SBD) and how the Firm plans to respond to events of varying scope following the Firm's selected means.

Centralized SBD Communications

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

Communications During & After SBDs

18064
During and after an SBD, the Firm must communicate the status of its operations with Senior Leadership and, as appropriate, Regulatory Authorities and Law Enforcement.

The Firm must also communicate the status of its operations with impacted Employees, Affiliates, Clients, and Vendors.

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.

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.

BCDRP Test & Review

84044
Periodically, and when required, the the Firm must test and review its BCDRP.

Task Recurrency: Annually

BCDRP Test Scenarios

77712
When testing its Business Continuity and Disaster Recovery Plan (BCDRP), the firm must incorporate a variety of scenarios from the list below or other relevant sources, ensuring that different scenarios are alternated to achieve preparedness across multiple potential disruptions.

1. Natural Disaster: Natural disasters can disrupt operations, damage physical assets (like data centers), and impact customer service.

2. Pandemic Outbreak: The financial services sector must maintain operations even during pandemics, as these impact workforce availability and customer interaction methods.

3. Supply Chain Disruption: While not as critical as in manufacturing, financial services rely on third-party vendors (e.g., cloud services, data providers). A disruption here can impact service delivery.

4. Power Outage: Power outages can disrupt operations, especially if backup systems fail, affecting transaction processing and customer access.

5. Data Loss: Critical in financial services, as loss or corruption of financial data can lead to severe regulatory penalties and loss of customer trust.

6. Terrorism or Active Shooter Incident: Physical security threats can disrupt operations, especially in large financial hubs or headquarters.

7. Telecommunications Failure: Financial services rely heavily on communication networks for trading, customer service, and internal coordination. Failure here can halt operations.

8. Regulatory Action: Sudden changes in regulations or unexpected legal actions can require immediate changes to operations or halt certain activities, especially in trading or lending.

9. Critical Payment Systems Failure: In financial services, a failure in payment processing systems, such as SWIFT or internal payment networks, could lead to significant disruptions in service.

10. Market Volatility Crisis: Sudden, extreme market fluctuations can lead to liquidity issues, margin calls, or mass withdrawals, impacting financial stability.

11. Internal Fraud: A significant case of fraud or embezzlement by employees, undermining trust and potentially leading to financial losses and regulatory scrutiny.

12. Technology Upgrade Failure: A major failure during the upgrade or migration of core banking systems or trading platforms, leading to service interruptions.

13. Currency Devaluation: Rapid devaluation of a key currency affecting international transactions, hedging strategies, and cross-border payments.

14. Regulatory Compliance Failure: A significant failure to meet compliance requirements, leading to fines, legal action, and operational disruptions.

15. High-Profile Litigation: Involvement in a major lawsuit, either from customers, regulators, or partners, that can result in financial losses and damage to the firm's reputation.

16. Loss of Key Personnel: Sudden loss of critical staff, such as top executives or key traders, which could disrupt operations and decision-making processes.

BCDRP Approval by Senior Leadership

79788
Periodically, as part of the Cyber Program approval, the Firm's Senior Leadership must approve its Business Continuity and Disaster Recovery Plan (BCDRP).

Critical Vendors

42845
The Firm must identify Vendors necessary for the continued operations of its Information Systems.

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 Event, Incident & Breach Definition

19575
Security Event
An act or attempt, successful or unsuccessful, by an unauthorized person or system to access, disrupt, or misuse Information Systems or NPI.

Security Incident
A Security Event that impacts the Firm and has a reasonable likelihood of materially harming any material part of the normal operations of the Firm.

Security Breach
A successful access, disruption, or misuse of an Information System or NPI 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.

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 Response Process:

1. Document date/time of all activities and updates.
2. Request that the person who discovered the incident send a report describing the findings.
3. Do not modify or erase any system, software, configuration, data, etc.
4. Collect and review the SIRP.
5. Alert and activate the Security Team.
6. Organize the initial Security Team conference call.
7. Alert appropriate external and internal contacts.
8. Consult legal counsel.
9. Review cyber insurance coverage and process.
10. If a Vendor is involved, review and follow the Vendor incident response process.
11. Conduct forensic analysis, evidence gathering, and preservation.
12. Restrict information sharing until a communication plan is in place, legal counsel is involved, and Senior Leadership approves the information to be shared.
13. For each Security Incident or Breach, fill out the Security Incident & Breach Event Tracking Evidence Log.
14. If this is a Security Breach, or you cannot evidence that this is a Security Incident, contact the authorities and the regulators (follow Notifications Policies).

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, the potential impacts, and a plan to avoid future similar incidents or breaches.

Phishing Email Deletion

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

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.

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.

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 Firm's 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.

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.

SIRP Review & Update

33180
Periodically and following a Security Incident or a Breach, the Firm must perform a SIRP Review and, as necessary, update its SIRP.

Task Recurrency: Annually

Remediation Documentation & Tracking

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

SIRP Test

32693
Periodically, the Firm must test its SIRP using various methods, including Tabletop Exercises (TTX).

TTX is a discussion-based simulation of an emergency situation in a stress-free environment. During a TTX, the Security Incident Response Team (SIRT) must walk through the steps they would take during an incident to evaluate the effectiveness of their response strategies, identify gaps, and enhance their preparedness for actual incidents.

TTX Purpose
. Validate the Security Incident Response Plan: Ensure that the IRP is up-to-date, practical, and effective in managing different types of incidents.
. Enhance coordination: Improve communication and coordination among the SIRT, management, and external stakeholders.
. Identify gaps and weaknesses: Uncover any gaps or weaknesses in the plan, such as unclear roles, missing resources, or unanticipated challenges.
. Increase familiarity: Allow the SIRT to familiarize themselves with their roles and responsibilities during an incident.
. Test decision-making: Evaluate the decision-making process under simulated stress to ensure that Senior Leadership can make informed and timely decisions.

Task Recurrency: Annually

SIRP Test Process

93000
During a SIRP Test, the Firm must follow its SIRP Test Process.

1. Scenario selection: Choose a relevant SIRP Test scenario that aligns with the Firm's risk profile.
2. Participant identification: Involve key personnel, including the SIRT, Senior Leadership, and other stakeholders as needed.
3. Facilitation: A facilitator guides the exercise, presenting the scenario, asking probing questions, and encouraging discussion.
4. Discussion: Participants discuss their actions, decision-making processes, and communication strategies based on the scenario presented.
5. Debriefing: After the exercise, a debriefing session is held to discuss what was learned, identify areas for improvement, and refine the SIRP if needed.

SIRP Table Top Exercise Scenarios

20724
When testing its Security Incident Response Plan (SIRP), the firm must incorporate a variety of scenarios from the list below or other relevant sources, ensuring that different scenarios are alternated to achieve preparedness across multiple potential incidents.

1. Phishing Attack: Lead to compromised employee credentials and unauthorized access to sensitive systems.
2. Ransomware Attack: Encrypt critical business data, demanding a ransom for the decryption key.
3. Insider Threat: A disgruntled employee begins exfiltrating NPI to a third party.
4. Denial of Service (DoS) Attack: Attack the Firm's Website or Servers, causing an outage of online services.
5. Data Breach: Expose clients' personal and financial information, triggering regulatory reporting requirements.

6. Business Email Compromise (BEC): With Senior Officer email access, hackers attempt to authorize fraudulent wire transfers.
7. Malware Outbreak: Spread rapidly through the network, impacting multiple systems and disrupting operations.
8. Physical Security Breach: Unauthorized individuals gain physical access to a location with NPI or a data center.
9. Supply Chain Attack: A vendor is compromised, introducing malicious code into the Firm's systems.
10. Social Engineering Attack: Trick employees into divulging NPI or bypassing security controls.
11. Financial Fraud Incident: Discovery of a significant internal or external financial fraud.
12. Mobile Device Compromise: An employee's mobile device, with access to corporate data, is lost or stolen, and the data is at risk of exposure.
13. Zero-Day Exploit: A zero-day vulnerability in widely-used software is exploited, leading to unauthorized access to the Firm's systems.
14. Cyber Espionage: A nation-state actor is conducting espionage activities against the Firm, targeting sensitive data.

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.

SIRP Review with Senior Leadership

76188
SIRP Reviews must include Senior Leadership.

SIRP Approval by Senior Leadership

16280
Periodically, as part of the Cyber Program approval, the Firm's Senior Leadership must approve its Security Incident Response Plan (SIRP).

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.

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.

Task Recurrency: Annually

Vendor Definition

58896
A Vendor is a third party that maintains, processes, stores, or otherwise is permitted access to NPI by providing services to the Firm.

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.

Security Risk Assessments of Vendors

78979
Periodically, the Firm must require Technical Controls Security Risk Assessment reports from Vendors, including Vendors with access to the Firm's networks and systems.

Such Assessments must include routine vulnerability scans of networks, endpoints, and, when application, software code, web applications, databases, and servers.

Approved Vendors

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

Vendor NDA

73490
The Firm must sign a Non-Disclosure Agreement with all Vendors.

Subscription to Vendor Notifications

50528

The Firm must subscribe to Vendor notifications in order to be informed of Vendor service changes that could affect the Firm.

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.

CD & DVD Disposal

30520
To dispose of CDs/DVDs containing NPI, the Firm must destroy them to ensure they are unreadable and unrecoverable.

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.

Computer Equipment & Facilities Protection

32023
The Firm must implement measures to protect Informations Systems and NPI against destruction, loss, or damage due to fire, water damage or other environmental hazards.

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.

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

Acceptable Use Policy Review

48423
Periodically, the Firm must review security policies, procedures, and processes included in the Acceptable Use Policy with Employees and Affiliates.

NPI Collection

67559
The Firm Employees and Affiliates must collect only the essential NPI necessary for conducting business and utilize such NPI exclusively for business purposes.

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.

NPI Access & Sharing

74186
Firm Employees and Affiliates are prohibited from accessing, disclosing, or discussing NPI with unauthorized individuals unless their identity is validated and a legitimate business need to know.

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.

Compliance and Ethical Responsibility

83315
The Firm's SGB (Senior Governing Body), Officers, Senior Leadership, Employees, and Affiliates must:

1. Act with integrity, honesty, and fairness in all business dealings.
2. Comply with laws, regulations, and internal policies.
3. Treat all individuals fairly with mutual respect, fostering a collaborative team environment while avoiding any intent or appearance of unethical or compromising practices.
4. Apply diligent effort and intelligence to uphold ethical values, and actively contribute to enhancing customer and vendor satisfaction through the delivery of high-quality products, services, and timely responses to inquiries.
5. Report unethical conduct to Senior Leadership.

Conflict of Interest Divulgation

24408
Employees and Affiliates must disclose any conflict of interest related to the Firm in writing to the Senior Leadership.

3. Data Controls

3.1 Software & Systems

Password Management Software

82852
The Firm must select Password Management Software in which User credentials are encrypted and saved.

Employees & Affiliates must use such Password Management Software for accessing the Firm's software and 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.

Tracking of Software & Systems Without MFA

81689
The Firm must document information about Software and Systems for which the Firm does not use Multi-Factor Authentication (MFA).

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.

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/)

Software Development & Testing Environment

59107
The Firm must maintain an environment for testing and developing software and applications separate from its business environment.

Software Development Life Cycle (SDLC)

10466
The Firm must define and follow its Software Development Life Cycle (SDLC) procedures.

Software Development Life Cycle (SDLC) Assessment

69829
Periodically, the Firm's CISO must review, assess, and update as necessary its Software Development Life Cycle (SDLC) procedures.

Task Recurrency: Annually

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 Traffic 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.

Credit Card Processing Outsourcing

37804
The Firm must not store, process, or transmit credit card information.

The Firm must outsource credit card processing to ensure credit card information is only processed and validated by a selected PCI-Compliant Vendor.

Email Filtering

50147
The Firm must filter email to block phishing, spam, and malicious attachments/links from reaching users.

NPI Printing Controls

94828
The Firm's Employees and Affiliates must request approval from Senior Leadership before printing documents with NPI.

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

Unique User Identification

78636
Firm Employees and Affiliates must each have their unique username and password to access the Firm's systems.

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.

Segregation of Duties

70252
The Firm must implement Segregation of Duties for User access approvals.

Non-Privileged Accounts for Administrators

99890

For each Firm system they access, and in addition to their Privileged Accounts, Administrators must have a non-privileged account for other tasks not related to their Administrator roles.

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

Termination Checklist

61619
The Firm must follow its Employee & Affiliate Termination Checklist when offboarding an Employee or Affiliate.

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.

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.

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.

Complex & Unique Endpoint Name

97594
The Endpoint names must be complex and unique.

Endpoint Asset Inventory Report

33584
Periodically, the Firm produce and must maintain a list of Endpoints accessing, controlling, or storing NPI.

The Report must include Endpoint technical information and Cybersecurity Settings and Software.

Reports must be kept for future evidence.

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.

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 Password/Biometric

15204
To use Biometrics (Face ID, Pattern, or Fingerprint), the associated device password or PIN must meet or exceed the Firm's Computer Password Minimum Standards.

Computer's Workgroup Name

75309
The default Computer's Workgroup Name ("Workgroup") must be changed to a unique and complex Workgroup Name.

Computer Security Software Enforcement

88042
Computer Security Settings & Software must be automatically installed, configured, and updated without End-User involvement.

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.

Device Locking When Non-Attended

28568
When left unattended, Employees and Affiliates must lock their Computer, Smartphone, and Tablet.

Computer Firewall

36038
Computer Firewall must be enabled.

Computer Logs

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

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.

4.3 Smartphone/Tablet Security

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.

. Screen Saver Status enabled
. Screen Saver Timeout 1 minute (60 seconds) or less

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.

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.

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.

Private WiFi

46887
A Private 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

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

Reports must be kept for future evidence.

Network Hardware Asset Inventory Review

42306
Periodically, the Firm must review the Network Hardware Asset Inventory Report to assess hardware cyber posture and lifecycle.

Task Recurrency: Monthly

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.

Forbidden Internet Connections

60056
The Firm prohibits Split Tunneling and Bridged Internet Connections to its network.