Triad Securities Corp.
Cyber Security Policies and Procedures

CONTENTS

OVERVIEW 2

ACCESS MANAGEMENT 3

END-USER: MOBILE DEVICE AND APPLICATION SECURITY 5

COLLABORATION SITES AND END-USER DATA STORAGE 5

SECURITY RISK ASSESSMENT 7

EMPLOYEE SECURITY AWARENESS TRAINING 8

VENDOR SELECTION AND MANAGEMENT 8

TECHNOLOGY ASSET INVENTORY, CLASSIFICATION AND TRACKING 9

TECHNOLOGY END-OF-LIFE PROCESS 9

EMPLOYEE TERMINATION 10

DISASTER RECOVERY AND BACKUP TESTING 10

CYBERSECURITY INSURANCE 10

CYBERSECURITY BREACH FRAMEWORK 10

Overview

Triad Securities Corp. has a holistic, systematic and risk-based approach to technology and information security. At a high level, the goal of this program is to:

- Provide that the business takes action relevant to the firm's technology assets and related events
- Provide for the safety and protection of information
- Prevent inappropriate use or access to data that can lead to an information security incident, where any firm computer, device or data is lost, stolen, misused or left unsecured

Nilabja Bhattacharya has been designated as the Chief Information Security Officer ("CISO") and has primary oversight, maintenance, and execution of this Technology and Information Security Program (the "Program"). The CISO is authorized to delegate physical, technical, and administrative components of this program to qualified third parties as and whenever appropriate.

The Triad Securities Corp. CEO bears overall responsibility for Business Continuity Plan ("BCP") / Disaster Recovery ("DR") planning, information protection, and creating agile security processes and procedures. The CEO has identified the following core functions to guide the Program. These functions will be evaluated and updated by the CISO as indicated below to adjust to technological, business and/or operational changes at the firm that may have a material impact on the Program. The CISO will also be reporting any exceptions to the CEO or other management as appropriate.

Functions	Designated Person	Frequency of Document Review	Frequency of Execution
Access management: password and technology access	CISO	Quarterly	As needed
Access management: physical access	CISO	Quarterly	As needed
End-user: desktop, web, network and server security	CISO	Quarterly	As needed
End-user: mobile devices and application security	CISO	Quarterly	As needed
Collaboration sites and storage	CISO	Quarterly	Quarterly with 3rd Party

networks			
Security risk assessment	CISO	Annually	Annually with RSI Technologies
Cyber security testing and audit	CISO	Annually or as needed	Annually or as needed with RSI Technologies
Network vulnerability scan	CISO	Annually	Ongoing with 3rd Party
Employee security awareness training	CISO	Annually	Annually (CCO during ACM)
Vendor selection and maintenance	CEO	As needed	Ongoing with 3rd Party
Technology asset inventory	CISO	Annually	Annually
Technology end-of-life process	CISO	Annually	As needed with 3rd Party
Employee termination	CEO	Annually	As needed with CCO
Disaster recovery and backup testing	CEO	See BCP/DR Manual	See BCP/DR Manual
Cybersecurity insurance	CISO	Upon renewal	N/A at this time

Access Management

We have a rigorous approach to entitlement management that helps establish controls around access activities. The goal of this program is focused on the following:

- Protect remote, mobile, cloud and social access
- Provide transparency and up-to-date information on entitlements
- Provide centralized administration for permissions
- Ensure that employees have access only relevant to their job functions
- Protect against insider threats and unauthorized escalation of user privileges

Each employee's profile will be managed in a central directory that will be used to create, delete and modify employee access data. The President is the primary owner of the central directory.

Authorization: We will manage authorization information that defines what functions an employee can perform in the context of a specific application. Please consult the President for the complete directory of employees and associated applications.

Passwords: For accessing any firm desktop, employees will use unique passwords, requiring the following characteristics:

- Contains at least 8 characters
- Uses a combination of lower and uppercase letters
- Expires every 90 days (the reuse of 24 previous passwords is disallowed)
- After 10 failed login attempts within 15 minutes, the user account will be locked until released by the CISO or Sysadmin.

Each administrator will have a unique login account and password

3rd Party's employees, on an as needed basis, will each have a unique login and password to access the firm's password management list.

Physical access: We will secure the firm's physical premises with locks and inventory keys issued to authorized persons on an ongoing basis.

End-user: desktop, web, network and server security
We have developed practices in our firm to protect the sensitivity of all information by implementing the following processes:

• Implement the use of password protection for all sensitive data, applications, and collaboration tools

• Reconcile the inventory of hardware, software and devices with 3rd Party

• Educate end-users on appropriate use of desktops and web browsing for business purposes

• Track and log USB portable flash drive uses that access the firm's desktop to detect any unauthorized use

• Maintain white-list of desktop approved applications and blacklist policy for websites (i.e. adult content, social media, gambling, etc.)

As needed, any 3rd Party will work closely with the CISO to proactively manage the following items:

• Maintain inventory of hardware, software and devices

• Closely monitor application and systems log activity (i.e. control the execution of code with an application white-listing policy)

• Deploy critical operating system security patches within 48 hours of release

• Non-critical patches are delivered monthly

• Implement appropriate protections for electronic systems, including anti-virus software and firewalls

• Anti-virus software is set to auto-update and firewalls are updated at least quarterly by 3rd Party

• To combat social engineering, the 3rd Party will do the following:

– Employ up-to-date anti-malware systems (continuously updated by auto-update plus quarterly reviews)

– Employ spam filters and other email gateways (continuously updated by auto-update and periodically reviewed by 3rd Party)

End-user: mobile device and application security

Firm-owned devices include, but are not limited to, laptops, tablets, cellular phones, and smartphones. Personal devices may utilize mobile access as long as they are password-encrypted and firm-approved.

Employees are advised to report any lost, stolen, or compromised electronic device to the CISO or CCO immediately. The CISO or CCO will update the firm inventory and shut off inbound and outbound access to the device as necessary. Firm personnel will receive training on the secure use of mobile devices and removable media on an as-needed basis including during the annual compliance meeting.

Collaboration sites and end-user data storage

The CISO will be primarily responsible for vetting any collaboration site and data storage along with the CCO. Each site must have identified “data owners,” who manage, control, and review access. Only firm approved collaboration sites listed below will be utilized:
Global Relay (http://www.globalrelay.com)
Vonage (http://www.vonage.com)

Protecting firm data includes the proper use of collaboration sites and data storage sites. The following are requirements for collaboration sites and storing data:

Desktop, laptop, remote desktop and tablets

• Ensure storage only in an approved, sandboxed or otherwise encrypted location instead of the desktop

• Save information to be shared to an access-controlled network location such as a network shared drive

• Store data and information with retention requirements in a records management repository

• Only use applications obtained through firm-approved channels

Mobile devices (smart phones and tablets)

• Only store data within firm-approved applications

• Triad Securities Corp. will continue to review options to implement remote-wipe capability for all employee devices

Records retention

- Certain types of data have retention periods
- All records including digital should be stored in an approved records repository
- Employees are responsible for preventing inappropriate use of or access to data by:
  - Only accessing information needed for your job function
  - Preparing, handling, using and releasing data
  - Using correct storage locations
  - Following appropriate use or restrictions of electronic communications, including but not limited to email, instant messaging, text, chat, audio/video conferencing and social media

Security risk assessment threats to identify potential risks and business impacts. The following items under review include, but are not limited to:

Category	Subcategory
Network Security	Network Infrastructure Firewalls Network Diagram Frequency of Documentation Wireless
Data Security	Data Classification Backup and Restoration Encryption Mobile Security Disposal Protection of Transmission
Access Control	Active Directory Authentication Network Access Control Account/Password Management Application Access
System Development	Systems Installation Software Development Maintenance and Patching Decommissioning Change Control Management
Protection	Antivirus software Updates and patches Web Filter and traffic
Testing and Monitoring	Server Monitoring Network Monitoring Penetration Testing Vulnerability Testing Alerting
Vendors	Vendor Assessment Client Data
Employees	Termination / Role Transfer
Physical Premise Security	Data Center Building Security and Staff Building and Office Access Server Room
Information Security Program	Info Security Policy

Employee security awareness training

To assist firm employees in understanding their obligations regarding sensitive firm information, the CISO will provide or make available to each employee a copy of this Program upon commencement of employment and whenever changes are made. In addition, the CISO and/or CCO will implement programs to perform training functions on an as-needed basis.

Employee security awareness training will include, but is not limited to:

• Instruct employees to take basic steps to maintain the security, confidentiality and integrity of client and investor information, including:

– Secure all files, notes, and correspondence

– Change passwords periodically and do not post passwords near computers

– Avoid the use of speaker phones and discourage discussions in public areas

– Recognize any fraudulent attempts to obtain client or investor information and report to appropriate management personnel

– Access firm, client, or investor information on removable and mobile devices with care and on an as-needed basis using firm protocols (passwords, etc.)

• Instruct employees to close out of files that hold protected client and investor information, investments, investment strategies, and other confidential information when they are not at their desks

• Educate employees about the types of cybersecurity attacks and appropriate responses

Vendor selection and management

For vendors interacting with our systems, network and data, the firm will perform the following activities to protect sensitive information:

• Assess vendors before working with them including a cyber-security risk assessment

• Review third-party vendor contract language to establish each party's responsibility with respect to cyber-security procedures

• Segregate sensitive firm systems from third-party vendor access and monitor remote maintenance performed by third-party contractors

Technology asset inventory, classification and tracking

Triad Securities Corp. has a process in place to identify, classify, and track all technology assets ("assets"):

• We will maintain an inventory of all assets as well as an identified owner

• Asset identification and classification process will be scalable to accommodate growth and acquisition

• We will track assets and their attributes throughout their lifecycle

• Automated processes will be used periodically to perform discovery of unknown assets

• We will create a map of network resources, including data flows, internal connections and external connections

• We will establish and enforce a process of assessing and classifying assets based on their sensitivity to attack and business value.

Technology end-of-life process

We have developed and will follow processes for securely disposing of assets once they are no longer being used by the firm or have reached the end of their usable life (the "end-of-life process").

Notification: The end-of-life process will notify all necessary and relevant parties to initiate a coordinated execution:

• CISO

• Asset owner

• End user(s)

• Relevant vendor(s)

Hard Drives: Any decommissioned hard drive will be securely stored for a minimum of 6 years since decommission date. When disposing the hard drive, the EMV will do the following:

• Erase all data on the drive

• Physically destroy the hard drive

• Produce documentation of proper disposal

Employee termination

The firm is highly focused on protecting the network and proprietary data at risk upon termination of employees. To prevent any issues of former employees leaking information, we have a strict approach towards access controls and entitlement management.
Please refer to the 3rd Party checklist for employee on/off-boarding. We will continuously maintain this list as new applications, drives, systems, and vendors are incorporated. The following items will be monitored:

• Network access

• Desktop access

• Mobile device access

• Internal and external applications

• Vendors, such as prime brokers, executing brokers, etc.

Disaster recovery and backup testing

Please see the original Business Continuity Procedures / Disaster Recovery Plan ("BCP") for detailed documentation. Any changes can be represented in that BCP / DR plan.

The CEO in connection with the CISO will update the firm's BCP on an as-needed basis to ensure that it is consistent with the Program.

Cybersecurity insurance

On an annual basis the CISO will review the possibility of the firm acquiring insurance coverage related to cybersecurity threats and make a determination as to its relevancy.

Cybersecurity breach framework

The firm has implemented a framework to identify, prepare, prevent, detect, respond, and recover from cybersecurity incidents.

In the event of a cybersecurity incident, the firm's information technology personnel (or anyone detecting the incident) will immediately notify the CISO who will work with appropriate personnel to:

• Assess the nature and scope of any such incident and maintain a written record of the systems and information involved

• Take appropriate steps to contain and control the incident to prevent further unauthorized access, disclosure or use, and maintain a written record of steps taken

• Promptly conduct a reasonable investigation, determine the likelihood that personal information has or will be misused, and maintain a written record of such determination

• Discuss the issue with in-house counsel and make a determination regarding disclosing the issue to regulatory authorities, law enforcement and/or individuals whose information may have been affected

• Evaluate the need for changes to the firm's policies and procedures in light of the breach

The undersigned CEO has consulted with the CISO, and other officers as applicable (referenced above), and such other employees to the extent appropriate, in order to attest to the statements made in this document.

_____ _____

Arthur Linden, CEO Date