



TRITON
INVESTMENTS

*Triton Investments, LLC
Written Information Security Policy
Effective Date: August 23rd, 2023*

Cybersecurity & Information Security Policy

Non-Public Information (NPI)

In the course of conducting its investment advisory business, TIL has access to clients' personally identifiable financial information, which constitutes *non-public personal information* ("NPI"). NPI generally includes any:

- Information that a consumer provides in order to obtain a financial service or product from TIL;
- Information about a consumer resulting from transactions involving a financial service or product; or
- Information TIL otherwise may obtain about a consumer in connection with providing a financial service or product to that consumer.

This encompasses a broad range of data when it comes to TIL's clients, who are generally considered to be "consumers" under Regulation S-P. As a registered investment adviser, TIL is generally required to adopt written policies and procedures reasonably designed to protect the security and confidentiality of client information and records.

Safeguarding clients' confidential information is a primary focus of TIL's cybersecurity program. TIL appreciates that a cybersecurity data breach involving NPI can lead not only to regulatory issues, but also to loss of client trust and significant reputational damage to TIL.

National Institute of Technology (NIST) Framework

TIL has appointed Charles Mark Coleman as the firm's Chief Information Security Officer ("CISO"). The CISO is responsible for managing TIL's information security program. To help establish and implement TIL's information security program, the CISO utilizes the National Institute of Technology ("NIST") cybersecurity framework. NIST is a government agency within the U.S. Department of Commerce that fosters cybersecurity research, education, and collaboration.

As such, TIL's information security policy is modeled on the **NIST cybersecurity framework** which includes five functions:

1. Identify
2. Protect
3. Detect
4. Respond
5. Recover

These five NIST functions serve as the primary pillars of the TIL information security program. These five functions also help TIL to address particular areas of current regulatory focus, which include:

- Governance and Risk Assessment
- Access Rights and Controls

- Data Loss Prevention
- Vendor Management
- Training
- Incident Response

MyRIACompliance Cybersecurity Platform

TIL utilizes the MyRIACompliance cybersecurity program to help implement and maintain its information security program. Cybersecurity awareness training, testing, and documentation for TIL staff is delivered via the MyRIACompliance platform.

Role of Each Staff Member

TIL recognizes that many investment adviser cybersecurity events resulting in the exposure of NPI begin with the inadvertent action of a staff member. While TIL has implemented an information security policy designed to protect against the exposure of sensitive client information, each staff member of TIL must take a proactive approach to helping TIL and the CISO implement the information security program.

To help educate and train each staff member, all TIL staff members will be required to do the following via the MyRIACompliance platform:

- Carefully review and attest to understanding this information security policy;
- Complete information security awareness training and testing; and
- Report any potential suspicious activity or conduct.

Any staff member who has discovered or experienced a *potential* cybersecurity incident should immediately inform TIL's CISO via MyRIACompliance in order to properly investigate the incident. TIL's personnel are the firm's first and best line of defense when it comes to cybersecurity.

IDENTIFY

The **identify** function helps TIL to identify relevant human, technology system, and third party vendor risks.

Inventory of Technology Infrastructure

On an annual basis, the CISO of TIL will utilize MyRIACompliance to make an inventory of the following:

- Physical devices and systems (computers, servers, etc.);
- Software platforms and applications (email applications, file management, etc.);
- Systems that house client data; and
- Third-party contractors that have access to these systems, platforms, etc.

TIL utilizes cloud-based technology systems, which it believes provide increased information security capabilities including:

- Ability to leverage the established infrastructure of trusted technology industry leaders; and
- Improved system alert capabilities, including better user activity logging and alerts related to unusual user activity.

TIL also recognizes that cloud-based technology creates a greater reliance on passwords and user login security. In particular, TIL understands that certain users with administrative access to the firm's cloud-based technology systems may pose even greater risk given their expanded access to sensitive client data. As such, TIL has designed and will continue to further develop information security policies with this increased risk as a focus.

Inventory of Staff Devices and System Access Levels

On an annual basis, the CISO of TIL will utilize MyRIACompliance to make an inventory of the following:

- Each staff member's physical devices (computers, mobile devices, etc.);
- Each staff member's access level to internal systems; and
- Each staff member's access level to third-party systems.

The CISO will regularly review the system access levels for personnel to ensure that each TIL staff member only has the necessary level of access to each system in order to perform that individual's job.

PROTECT

The **protect** function helps TIL create safeguards to help prevent, limit, or contain the impact of a cybersecurity incident or attack.

Security of Technology Infrastructure

TIL has implemented the following firm-wide information security policies to help prevent unauthorized access to sensitive client data:

- All computers used to access client data will have antivirus software installed. In addition, the antivirus software will have an active subscription and all updates will be scheduled to automatically install.
- All staff will utilize devices with up to date operating system software with all security patch and other software updates set to automatically install
- All staff workstations (e.g. desktop, laptop, mobile device) will be locked when the device is not in use
- All staff workstations (e.g. desktop, laptop, mobile device) will be shut down completely at the end of each work day
- All staff workstations (e.g. desktop, laptop, mobile device) will use proper data encryption when possible

- All staff mobile devices used to access work email and files will be password protected and will have the capability to be remotely wiped if lost or stolen
- All staff members are prohibited from accessing TIL systems from unsecured internet connections

All staff should immediately alert the CISO of any suspicious behavior or potential incidents.

User Access Rights and Controls

TIL has implemented the following firm-wide user access privilege policies to help prevent unauthorized access to sensitive client data:

- Staff members will only have access to systems deemed necessary by the CISO;
- Each new staff member's login credentials will be created by the CISO;
- Staff members, besides the CISO or other designated personnel, will not have administrative privileges on systems unless deemed necessary and approved by the CISO; and
- Upon a staff member's departure or termination, the CISO will immediately remove the former staff member's access to all firm systems.
- The CISO will use MyRIACompliance to keep a record of former staff members and the date that access to each firm system was terminated for such former staff member.

Staff members may request additional access to systems by contacting the CISO.

Prevention of Unauthorized Funds Transfers

TIL recognizes the risk of client impersonation attacks and the need to validate the identity of its clients before transmitting funds. For example, after gaining unauthorized access to a client's email or financial account, a bad actor may then target TIL by impersonating the client in order to access the client's funds. Client impersonation campaigns are particularly dangerous to TIL because, given their financial profile, clients of TIL may be more likely targets for bad actors.

TIL has implemented the following firm-wide security policies to help prevent unauthorized funds transfers:

- Wire requests should be reviewed for suspicious behavior (e.g. time of request, atypical amount of request, etc.); and
- Clients must confirm all third party wire requests verbally or utilizing DocuSign's "Knowledge Based" authentication. Wire requests may not be authorized solely via email

TIL is particularly aware of the risk caused by fraudulent emails, purportedly from clients, seeking to direct transfers of customer funds or securities and will train staff members to properly identify such fraudulent emails.

User Login Security

TIL has implemented the following firm-wide user login security policies to help prevent unauthorized access to sensitive client data:

- All staff passwords are required to meet or exceed the following guidelines. Each password must:
 - Contain both upper and lower case letters
 - Contain at least one number
 - Contain at least one special character
 - Be at least 10 characters in length
 - Not contain words that can be found in a dictionary (exception for LastPass and personal computer)
 - Not contain personal information such as pet names, birthdates, or phone numbers
 - Not contain sequenced or repeated characters (e.g., 123456, abc123, etc.)
 - Not be similar to the username
- All staff are required to have unique passwords to access each technology system (e.g., desktop computer, CRM system, etc.)
- All staff are required to update passwords on a quarterly basis
- No passwords are allowed to be stored in writing on paper or on any system
- Staff members should not use the “remember password” feature of any application (excluding LastPass), including on web browsers
- Staff members should never share passwords with any other staff member or third party whether via email, phone, or text message
- When available, staff is required to utilize two-factor authentication

Password Management

TIL is aware of the risks and challenges in managing multiple, unique passwords to access technology systems. As such, TIL has implemented the following password manager tool to help safeguard and organize staff member login credentials: LastPass. All staff members are required to:

- manage all user login credentials via the password manager
- utilize the password manager’s two-factor authentication capabilities (as mentioned above)
- follow all user login security password policies as outlined above when establishing their “master password” for the password manager

Social Engineering Protection

Sophisticated bad actors looking to gain access to TIL’s sensitive information may target particular staff members personally via a cyber attack method called social engineering. In such an attack, cyber criminals will research the individual staff member online, looking for publicly available information that may help them answer the staff member’s personal security questions, decipher a username and password, or launch an email phishing attack specifically targeted at what they know about the individual.

As such, all staff members are instructed not to disclose personal information on social media websites. Such information includes but is not limited to:

- Birthdate
- Place of birth
- Place of wedding
- Name of high school
- Name of elementary school
- Best friend's name
- Name of favorite pet
- Name of favorite drink
- Name of favorite song
- Mother's maiden name
- Make and model of first car
- Favorite color
- Name of favorite teacher

In addition, staff member should be aware of these best practices:

- Do not make personal social media profiles accessible to the public
- Be cautious when accepting social media friend or connection requests
- Utilize less common online security questions
- Use different online security questions for different systems
- Be wary before providing personal information to any third party

Secure Communications

TIL is aware of the limitations and security concerns that email communication entails. As such, TIL has implemented the following secure communication system: Norton Secure VPN. All staff members are required to utilize this method of communication when sending NPI or other sensitive information to clients.

Email Phishing

Email poses one of the greatest cybersecurity risks to TIL. Bad actors look to exploit this vulnerability using fake emails designed to look like legitimate correspondence or offers. Often, the "phishing" email directs TIL personnel to click on an attachment or link with the goal of either installing dangerous software (malware) on the individual's computer or stealing sensitive access information from the staff member, such as an email username or login credentials to one of TIL's software platforms.

TIL has implemented the following firm-wide email security polices to help prevent unauthorized access to sensitive client data:

- Staff should never open or download any email attachments from unknown senders;
- Staff should never open or download any email attachments from known senders that look suspicious or out of the ordinary;
- Staff should never directly click on or open any links sent in emails;
- Staff should not send sensitive client or NPI via unsecured email to clients;

- Staff should be acutely aware of how to identify attempted “phishing” emails seeking to obtain the staff member’s user login credentials. Warning signs to look for include:
 - Bad spelling or poor grammar in the email subject or body text;
 - A company or website with which the staff member is not familiar;
 - The sender’s email address does not match the display name;
 - The sender’s email address is valid, but something looks suspicious;
 - An “urgent” or “action required” subject line; and
 - A suspicious sender email domain.

TIL understands the risks that email phishing poses to an investment adviser. A successful phishing attack is particularly dangerous for TIL because if hackers gain access to one of TIL’s technology systems, they may also gain unauthorized access to sensitive, non-public client and company information. In addition, as discussed above, email phishing can lead to fraudulent wires or other unauthorized transfers of funds.

When a staff member receives a suspicious email, the CISO should be immediately alerted. The CISO will then determine next steps and communicate to other staff members if deemed appropriate.

Ransomware Attack Protection

In a ransomware attack, hackers look to access TIL data or even personal information, block access to that information, and hold the information “hostage” until a ransom is paid to unlock the data. Ransomware is a specific type of malware that, when installed on staff member’s computer, encrypts the data on the computer or company network, preventing TIL from accessing the data without the requisite decryption key. Ransomware is often circulated via phishing emails and most commonly installed when an individual downloads a malicious file via an email attachment, email link, or web link.

As such, all TIL personnel should take the following precautions to help protect against a potential ransomware attack:

- Follow TIL’s email use security and guidelines including:
 - Never open or download any email attachments from unknown senders
 - Never open or download any suspicious email attachments from known senders
 - Never directly click on or open any links sent in emails
- Never provide remote computer access to a third party unless the CISO approves the request

Safe Internet Browsing

TIL recognizes that with the prevalence of web-based applications and the need to consistently access the internet in personal and professional life, proper vigilance while browsing the internet is essential. Malware, spyware, and other viruses can be unknowingly distributed to TIL staff members while browsing the internet if proper safeguards are not in place.

As such, all staff members should take the following steps:

- Only use a modern web browser, such as Google Chrome, Mozilla Firefox, or Microsoft Edge
- Disable the browser's autofill form completion feature
- Do not use the browser's "save password" feature
- Utilize the browser's pop-up window blocking feature
- Only browse on secure websites (look for *https://*)
- Be highly cautious before downloading files or applications online
- Keep all device operating system software updated
- Do not access file sharing websites unless authorized by CISO
- Do not use unsecured wireless internet connections

Clean Desk Policy

TIL recognizes that third parties, such as visitors or service providers, may have access to a staff member's office area during or after normal business hours.

As such, all TIL personnel should take the following steps throughout the day and before departing for the day to help secure their respective office areas:

- Securely store any physical client files
- Avoid the use of flash drives
- Shred sensitive client and firm documents when appropriate
- Promptly gather any documents that have been printed
- Never write down passwords
- Erase any white board or similar displays containing sensitive or confidential information

Preventing Unauthorized Office Access

TIL recognizes that sensitive client information may be accessible in the firm's office. Staff members should always exercise great caution before letting an unknown or unauthorized third party, such as unexpected vendor or former staff member, into the office.

In particular, staff should be mindful of "tailgating" - a classic type of physical security breach. In a tailgating incident, an individual is exploited when trying to extend a common courtesy by opening or holding the door for a visitor or uniformed vendor when entering the office. Unfortunately, this gesture can be exploited by potential bad actor attempting to gain unauthorized office access. As such, TIL staff should be cognizant of this possibility when entering and leaving the office.

Mobile Device Usage Guidelines

In order to help prevent unauthorized access to sensitive client and firm data, TIL permits the limited use of personal mobile devices only under the following firm-wide mobile device usage guidelines:

- Before utilizing a personal mobile device to access company systems, such as company email or CRM system, the device must be inspected and approved by the CISO to ensure proper security features are activated on the device.

- The mobile device's built-in password / passcode security feature must be activated at all times. If the staff member's mobile device does not offer a built-in password / passcode security feature, then the device is not permitted to be used to access company systems.
- Sensitive client or firm information should never be downloaded directly onto a personal mobile device, since that bypasses the additional password protection that cloud-based systems offer.
- If available, the mobile device's local or remote wipe security features(s) should be activated.
- In the event a mobile device used to access company systems is lost or stolen, the staff member should immediately alert the CISO.
- Before disposing of any mobile device used to access company systems, all data must be wiped from the mobile device.

Cybersecurity Travel Policy

TIL recognizes that staff members may need to travel as part of their job responsibilities, but that the risk of a cybersecurity incident is higher when traveling.

As such, all staff members should take the following steps before traveling:

- Any mobile device being used for travel to conduct TIL business should first be approved by the CISO
- Avoid bringing unnecessary mobile, tablet, or laptop devices
- Ensure the latest operating system updated and patches are installed on any mobile device that will be used
- Make sure all necessary file back-ups have been conducted

While traveling, staff member should take the following precautions:

- Make sure auto connectivity and Bluetooth features are disabled on all devices
- Do not use devices in a public manner that could expose sensitive information
- Never leave a device unattended in a public area
- Properly secure all devices before leaving a hotel room
- Avoid publicly accessible and shared computers
- Never connect to unsecured wireless networks
- Use a virtual private network (VPN) connection to access the internet before conducting business on behalf of TIL

Third Party Vendor Security and Diligence

TIL has implemented the following firm-wide third party vendor security and diligence policies and guidelines to help prevent unauthorized access to sensitive client data:

- All third party vendors that have physical access to the office and/or the firm's systems are reviewed for confidentiality before establishing a business relationship in order to protect sensitive client information; and

- Proper due diligence will be performed on all relevant technology vendors prior to establishing a business relationship and then again on at least an annual basis. This will include review of the vendor's:
 - information security policies (or equivalents);
 - disaster recovery policies (or equivalents); and
 - broader capabilities to ensure the vendor meets TIL's business and security needs.

All of this information will be stored and maintained in TIL's vendor diligence file.

Staff Training

All TIL personnel are required to complete mandatory cybersecurity awareness training and testing, delivered via the MyRIACompliance platform. Mandatory training topics include:

- Non-Public Information
- Preventing Identity Theft
- Email Phishing
- Social Engineering
- Ransomware Attacks
- Client Impersonation
- Safe Internet Browsing
- Password Best Practices
- Physical Security
- Cybersecurity while Traveling

The MyRIACompliance platform will provide training videos and quizzes that are required to be completed by all TIL staff.

New staff members will receive training, led by the CISO, within one (1) month of their initial hire date. The training conducted by the CISO will include the following topics:

- Review of the current Cybersecurity & Information Security Policy, including a note of any changes to the policy since the last training session;
- Review of any relevant information security incidents or suspicious activity;
- Review of how to identify potential "phishing" or fraudulent emails;
- Review of how to identify potential "ransomware" or similar attacks;
- Review of any relevant regulatory compliance issues; and
- Review of general information security best practices.

On an annual basis, TIL's CISO will conduct a firm-wide training session to ensure that all staff members are properly trained and equipped to implement the Cybersecurity & Information Security Policy.

DETECT

The detect function helps TIL to establish the framework to identify a potential cybersecurity vulnerability or event in a timely manner.

Testing

On a quarterly basis, TIL will test its current Cybersecurity & Information Security Policy and capabilities. The test conducted by the CISO will include the following activities:

- Ensure all staff members have proper system access privileges;
- Ensure all relevant software patches designed to address security vulnerabilities have been implemented on TIL's server; and
- Make a physical inspection of the office to ensure that all workstations have the proper security measures including:
 - Attempt to access a random sample of firm devices to ensure that proper passwords are in place to prevent access;
 - Observe staff members access systems to ensure that two-factor authentication has been activated;
 - Ensure staff members are not using the "remember password" feature of any application (excluding LastPass);
 - Ensure computers used to access client data have an antivirus software subscription; and
 - Ensure passwords are not visibly stored in writing on paper or on any system.
- For its remote offices, the CISO will either perform directly or assign a delegate to perform the above-referenced physical inspection.

Risk Assessment

On an annual basis, TIL will further test and evaluate its current Cybersecurity & Information Security Policy and capabilities. The test conducted by the CISO will include the following activities:

- Conduct a risk assessment to determine if any changes need to be made to information security policies and procedures;
- Attempt to access users' accounts with the proper password to ensure that two-factor authentication prevents system access;
- Perform any relevant third party penetration tests or vulnerability scans and remediate any relevant discoveries; and
- Attempt to restore a sample of files and records from the systems documented in *TIL's Inventory of Technology Infrastructure* to ensure that the restoration process is sufficient and properly configured.

The results from the annual testing program and risk assessment will be documented and utilized as an opportunity to update the Cybersecurity & Information Security Policy.

Detection of Unauthorized Activity or Security Breaches

The CISO is responsible for monitoring on-site and cloud-based systems for suspicious activity and security breaches. Such activity may include:

- Logins to company systems after traditional business hours
- Logins to company systems from non-local regions (e.g., outside of the local region, outside the United States, etc.)

- Large transfers of files or data

When suspicious activity or a potential security breach is discovered, the CISO will restrict access to the systems, assess what information may have been accessed, and determine what actions need to be taken to remediate the event.

Regardless of the severity, the CISO will keep a log on MyRIACompliance of all incidents and note the action taken. This log will include the following information about each incident:

- Date and time of the incident
- How the incident was detected
- The nature and severity of the incident
- The response taken to address the incident
- Any changes made to the Cybersecurity & Information Security Policy as a result of the incident

All TIL staff are required to immediately alert the CISO of any suspicious behavior or other information security concerns.

RESPOND

The respond function helps TIL to establish the framework to respond to a potential cybersecurity incident once detected, and also how to mitigate the impact of such an incident.

Responding to Unauthorized Activity or Security Breaches

If a cybersecurity incident is deemed by the CISO to have led to unauthorized release or use of sensitive client information, then the CISO will take the following steps:

- Communicate the details of the event to the relevant principals of the firm
- Determine if any staff disciplinary action needs to be taken
- Determine if any third party vendors were involved in the incident
- Contact proper law enforcement and/or regulatory agencies as required by law (if necessary)
- Communicate the details of the event and steps being taken to rectify the incident to impacted clients of the firm (if necessary)
- Follow all relevant state data breach notification laws (if necessary)

Improvements to Cybersecurity Policies and Procedures

Following the proper mitigation and response to a cybersecurity incident, TIL's CISO will review the details of the incident to determine if any changes to be made to the Cybersecurity & Information Security Policy or other related procedures.

Any changes made to the Cybersecurity & Information Security Policy will be communicated to all TIL staff members and all staff members will be required to review and attest to the updated policy via the MyRIACompliance platform.

RECOVER

The recover function helps TIL to plan for and recover to normal operations in a timely manner in the event of a cybersecurity breach.

Significant Technology System Disruption Plan

In the event of a significant business disruption that results in a significant interruption in access to the firm's technology systems; TIL will implement its business continuity plan as detailed in its policies and procedures manual.

Client Information

In the event of the theft, loss, unauthorized release, or unauthorized use or of access of client information due to a technology system breach, the incident will be investigated and documented by the CISO and the CCO. If client information is involved, then TIL will follow its separate procedures concerning such exposure client information. The non-exhaustive list of possible follow-up actions includes notification of the parties involved, notification of appropriate regulatory officials if required, taking remedial actions to assist in the recovery of the stolen information, and possible sanctions of firm personnel if deemed necessary.

Data Back-Up Policies

TIL stores sensitive firm and client data on local and third party systems as documented in *TIL's Inventory of Technology Infrastructure*. This data is backed up in accordance with TIL's data back-up and recovery procedures.

Chief Compliance Officer Appointment (Exhibit 1)

The person herein named "Chief Compliance Officer" is stated to be competent and knowledgeable regarding the Advisers Act or applicable state rule or regulation and is empowered with full responsibility and authority to develop and enforce appropriate policies and procedures for the firm. The compliance officer has a position of sufficient seniority and authority within the organization to compel others to adhere to the Information and Security Policy.

Chief Compliance Officer	Date Responsibility Assumed	Annual Review Completed	Employee Training	Information and Security Updates:	Updates Notes:	
Charles M Coleman	6/20/2018	06/27/2019	12/13/2018	05/23/2019		
		04/23/2020	Completed on MyRIACompliance (See Example Log)	12/31/2019		
				03/31/2020		
				04/15/2020		
				05/07/2020	Blackout period was updated Samples Can be found in MyRIACompliance	
				05/20/2020	Added Chief Compliance Officer Appointment and table MyRIACompliance Log Attached for Reference	
				08/25/2020	Vendors are reviewed for confidentiality, NDA not required	
				09/11/2021	Removed references to Global Relay	
				12/22/2022		
		08/23/2023	Annual Review, no changes besides date			

DocuSigned by:
Signature of Chief Compliance Officer:

Charles Coleman
Name
6D307AE33CD3495...

08-23-2023
Date

MyRIACompliance Example Log

5/18/2020

MyRIACompliance Compliance Log

Triton Investments, LLC

MyRIACompliance Compliance Log on 05/18/2020

Q3 2020 Compliance Activities

Registration Changes

FIRM REGISTRATIONS

There are no Firm Registration Status updates to show for this period.

INDIVIDUAL REGISTRATIONS

There are no Individual Registration Status updates to show for this period.

ADV CHANGES

There are no closed Change Requests to show for this period.

* Date Case Closed

Risk Assessment

2020 Risk Assessment

Not Complete

Compliance Calendar

DEADLINE ACTIVITIES

There are no completed Deadline Activities to show for this period.

EXPECTED ACTIVITIES

There are no completed Expected Activities to show for this period.

RIA EDUCATION

There are no completed RIA Education activities to show for this period.

CUSTOM ACTIVITIES

There are no completed Custom Activities to show for this period.

Marketing & Document Review

There are no completed Marketing & Document Reviews to show for this period.

* Date Review Initiated

Attestation Documents

There are no uploaded Attestation Documents to show for this period.

* Date Archived

Reviews & Submissions

There are no completed Attestation Activities to show for this period.

Dismissed Reviews & Submissions

There are no dismissed activities to show for this period.

Activity Requests

There are no completed activities to show for this period.

Employee Reports

There are no reports to show for this period.

Trade Monitoring

HOLDINGS

There are no Holdings Reports to show for this period.

TRANSACTIONS

There are no Transactions for this period.

ACCOUNTS

There are no Accounts Reports to show for this period.

Custom Checklists

There are no archived checklists to display for this period.

Cybersecurity - Vendor Due Diligence

Subscribed Vendor Document Reviews

There are no reviewed subscribed vendor documents to show for this period.

Other Vendor Document Reviews

There are no reviewed other vendor documents to show for this period.

Cybersecurity - Employee & Systems Inventory Confirmations

Cyber Employees Confirmation

There are no cyber employee confirmations for this period.

Technology NPI/Users Confirmation

There are no vendor user confirmations for this period.

Vendor Access Removals

There are no vendor access removal confirmations for this period.

Vendor Removals

There are no vendor removals for this period.

Cybersecurity - Device Inventory

Device Submissions

There are no device submissions for this period.

Periodic Device Reviews

There are no periodic device reviews for this period.

Device Removals

There are no device removals for this period.

Cybersecurity - Email Phishing Testing

There are no email phishing testing campaigns to show for this period.

Certificate Of Completion

Envelope Id: 571C1310C1114B5289B67629E5E7A254	Status: Completed
Subject: Complete with DocuSign: Complete I&C (August 23rd, 2023).pdf	
Source Envelope:	
Document Pages: 18	Signatures: 1
Certificate Pages: 1	Initials: 0
AutoNav: Disabled	Envelope Originator:
Envelope Stamping: Disabled	Charles Coleman
Time Zone: (UTC-06:00) Central Time (US & Canada)	200 S 108th Ave
	Omaha, NE 68154-2631
	charlescoleman@TritonInvestments.net
	IP Address: 69.84.71.190


Record Tracking

Status: Original	Holder: Charles Coleman	Location: DocuSign
8/23/2023 2:07:49 AM	charlescoleman@TritonInvestments.net	

Signer Events

Charles Coleman
charlescoleman@TritonInvestments.net
Managing Partner
Triton Investments, LLC
Security Level: Email, Account Authentication (None)

Signature

DocuSigned by:

6D307AE33CD3495...
Signature Adoption: Pre-selected Style
Using IP Address: 69.84.71.190

Timestamp

Sent: 8/23/2023 2:08:02 AM
Viewed: 8/23/2023 2:08:08 AM
Signed: 8/23/2023 2:08:30 AM
Freeform Signing

Electronic Record and Signature Disclosure:
Not Offered via DocuSign

In Person Signer Events

Signature

Timestamp

Editor Delivery Events

Status

Timestamp

Agent Delivery Events

Status

Timestamp

Intermediary Delivery Events

Status

Timestamp

Certified Delivery Events

Status

Timestamp

Carbon Copy Events

Status

Timestamp

Witness Events

Signature

Timestamp

Notary Events

Signature

Timestamp

Envelope Summary Events

Status

Timestamps

Envelope Sent	Hashed/Encrypted	8/23/2023 2:08:02 AM
Certified Delivered	Security Checked	8/23/2023 2:08:08 AM
Signing Complete	Security Checked	8/23/2023 2:08:30 AM
Completed	Security Checked	8/23/2023 2:08:30 AM

Payment Events

Status

Timestamps