INVESTMENT SERVICES

2024

CYBERSECURITY PROGRAM OVERVIEW

As part of our Cybersecurity Program, **STP Investment Services** (STP) publishes this CYBERSECURITY PROGRAM OVERVIEW. This document covers how we preserve the security of our data and technology infrastructure, and how we proactively put in place comprehensive controls for cybersecurity.

Purpose & Audience

This document is for review by the *Public*. It provides an overview of the company's CYBERSECURITY PROGRAM, which is based on the Center for Internet Security Critical Security Controls (CIS Controls®) and official guides such as the United States Department of Labor (DOL) Cybersecurity Program Best Practices. For each of the 18 POLICY PROVISIONS in this document, STP maintains corresponding policies and procedures in its internal INFORMATION SECURITY POLICY. This overview is made available to the public to allow interested parties to understand the program without disclosing any of the sensitive details of the internal policy.

Scope

The POLICY PROVISIONS mentioned in this document apply to all *Employees*, *Third-Party Service Providers* and *Vendors*, our *Contractors*, and *anyone who has permanent or temporary access* to STP' systems and hardware.

Objective

The objective of this cybersecurity program is to align the organization to best practices in cybersecurity management.

Document Distribution

Copies of this plan are available from the Security Coordinator and on the company website: https://stpis.com/security-policy/

Document Maintenance History

The table below tracks the most recent update to the plan, the type of change and the current version.

PLAN MAINTENANCE DATE	TYPE OF MAINTENANCE	VERSION	REVIEWED AND APPROVED
09/06/2024	new plan format	3.0	STP General Counsel

Table of Contents

Policy Provisions

1. Data Governance and Classification

As a custodian of sensitive information for its clients, the confidentiality of data is one of STP's most important cybersecurity objectives. To meet its goal, STP has implemented a DATA GOVERNANCE AND CLASSIFICATION program which assigns data to classes according to its level of sensitivity. STP seeks to always exceed all requirements for protecting regulated information under state and federal privacy laws.

Some Key Policy Provisions:

- data is assigned a classification of *Confidential*, *Internal* or *Public*
- data which is protected by privacy regulations is assigned to the *Confidential* class and governed according to the provisions of the *Data Privacy Policy* and the *Data Retention Schedule* (see section 7, DATA DISPOSAL and section 14, DATA PRIVACY)
- access to data by employees is granted on a need-to-know basis
- data classified as *Confidential* is never shared with third parties except where required by law
- the procedures for handling data according to classification are linked with the policies and code of conduct for *Employees* depending on their location and context (see section 13, PHYSICAL SECURITY AND ENVIRONMENTAL CONTROLS)
- the company provides its employees with periodic reminders, training and guidelines for best practices for handling data

At all times employees' highest priority is to protect the confidentiality of data and err on the side of caution by applying the highest applicable classification and using their own good judgment and training.

2. Access Controls and Identity Management

STP intentionally limits ACCESS to its systems through various CONTROLS including IDENTITY MANAGEMENT. Prior to accessing company systems and data, *Authorized Individuals* must provide authentication by username, password and/or other means (*). Each *Authorized Individual* has a unique set of credentials to track activities and limit access according to the *Principle of Least Privilege*. Various steps of Identity Management include account provisioning, deprovisioning, and auditing of access logs.

Some Key Policy Provisions:

- individuals each have unique credentials
- activities by credentials are tracked and audited
- individuals are granted access based on their role and only to the least data and lowest level of access necessary to perform their job function
- access is reviewed and revised periodically
- systems access is restricted to compliant devices
- computer system access requires a username and password and/or biometric authentication or pin code

Accounts with higher privileges, administrative or service accounts require additional factors of authentication according to their level of access to systems and/or according to the sensitivity of data.

(*) also see section 16, Consistent Use of Multi-Factor Authentication

3. Business Continuity and Disaster Recovery

STP is dedicated to maintaining business continuity in the face of unexpected disruptions and disasters. A comprehensive plan for BUSINESS CONTINUITY AND DISASTER RECOVERY (BCDR) has been established to ensure the prompt resumption of critical business operations. The BCDR defines roles, responsibilities, and procedures for disaster preparedness, recovery, and testing.

Some Key Policy Provisions:

- employees in roles which are primarily computer-based are provided access to company systems through a secure remote connection method in cases where the office must be closed or cannot be reached due to weather, pandemic, terrorist or other emergencies and disasters
- communication and enterprise resource systems are cloud-based services for which the respective *Third-Party Service Providers* maintain redundancy and contractually guarantee uptime/availability
- data backups are maintained and tested regularly and *Third-Party Service Providers* are contractually guaranteeing the backup's functionality and availability from across their redundant infrastructure
- data backups are distributed and layered across multiple systems and different *Third-Party Service Providers* which are geographically separated from each other and redundant
- to further protect against any compounding or catastrophic losses, the company maintains general liability and specific cyber liability insurance coverages

The BUSINESS CONTINUITY AND DISASTER RECOVERY plan is subject to regular updates and testing. On an annual basis, STP reassesses the *Third-Party Service Providers* and coordinates between them for any changes in the roles, responsibilities, infrastructure, technology, or business continuity objectives.

4. Configuration Management

To maintain the security and stability of its systems, STP applies best practices to its CONFIGURATION MANAGEMENT. Policies and procedures ensure that current inventories of all hardware assets and software configurations are maintained *(also see section 5,* ASSET MANAGEMENT*)*. Configurations for the same or similar devices are managed to the same baseline and according to the *Principle of Least Functionality*. All configurations and software versions are regularly audited.

Some Key Policy Provisions:

- the company standardizes on manufacturers and vendors as much as possible so to maintain the same or similar configurations across workstations, firewalls, network equipment and other devices
- all assets use currently supported versions of operating systems and/or firmware
- devices with the same version operating system are provisioned with a baseline configuration which ensures the same security settings are applied uniformly and consistently (such as enabling Bitlocker disk encryption on all devices with Windows 11)
- employee workstations are setup with a *Core Group of Approved Applications* according to the *Principle of Least Functionality*
- the configurations of all critical devices (firewalls, other) are audited on a regular schedule

Employees and *Third-Party Service Providers* are prohibited from making any changes without authorization. Any changes and exceptions (as needed for valid business reasons) are subject to risk assessments, testing, approval and documentation.

5. Asset Management

STP prioritizes ASSET MANAGEMENT as vital to safeguarding resources and data. The company actively manages its inventory of data processing assets with physical tags. Assets are assigned to an employee or group which are responsible for their asset's safety and condition.

Some Key Policy Provisions:

- assets are assigned to employees based on need and according to the *Principle of Least Functionality*
- any assets with hardware or software that reach end-of-life (as defined by vendors and manufacturers) are upgraded or replaced in accordance with the company's *Asset Lifecycle Policy*
- mobile devices are tracked & inventoried by status and location, can be wiped remotely in case of loss or theft
- retired assets are securely decommissioned and disposed through a *Third-Party Service Provider*
- for any leased equipment containing company data (such as copy machines), vendors are under contract to securely erase any data left on devices prior to re-possession and/or disposal

Employees are prohibited from acquiring, using, or disposing of data processing assets without specific authorization. STP prohibits the use of any USB removable media. A *Third-Party Services Provider* is retained to securely and certifiably dispose of assets containing any class of data and in accordance with the company's Data Disposal policy *(also see section 7,* DATA DISPOSAL*)*.

6. Risk Assessment

Effective risk management is fundamental to STP's cybersecurity program. The company conducts regular RISK ASSESSMENTS to identify, evaluate, and prioritize cybersecurity risks. The company's cyber risk program is based on the Center for Internet Security Critical Security Controls (CIS Controls®).

Some Key Policy Provisions:

- members of the Risk Management Team continuously evaluate risks and actively shape the company's risk management strategy
- the company periodically conducts risk assessments with internal and external parties including *Vendors*, *Third-Party Service Providers*, partners and independent consultants

Additional RISK ASSESSMENTS are conducted for use by leadership to inform decision-making for strategic cybersecurity improvements, for evaluating the outsourcing of processes, for selecting *Vendors,* for anticipating the impact from regulatory changes, and for many other reasons.

7. Data Disposal

Clients entrust STP to keep their personal, financial, and proprietary data confidential and protected at all times. STP takes this responsibility very seriously. In accordance with its DATA DISPOSAL policy, the company only collects and maintains records and files containing *Personally Identifiable Information* and *Personal Financial Information* of the type, and for the length of time as reasonably necessary for legitimate business purposes. The company periodically reviews its records, files, forms, and documents to ensure that it is not unnecessarily gathering and retaining data unless there is a valid and compelling (business or regulatory) need to do so.

Some Key Policy Provisions:

- the company does not keep any *Client* data indefinitely
- any data collected by the organization, regardless of type and classification, has a formally defined retention period and disposal event
- records are securely destroyed according to their applicable retention period
- to securely dispose of *Confidential* and *Internal* data, the company uses paper shredders and/or *Third-Party Service Providers* for paper shredding and secure media disposal
- where *Third-Party Service Providers* dispose of data assets, disposal events are documented, including paper shredding, hard drive destruction and secure digital erasure

As a custodian of sensitive information of *Clients*, *Partners* and *Employees*, STP is committed to the concept of DATA DISPOSAL over indefinite retention of data.

8. Incident Response

An effective plan is critical to minimize the impact of cybersecurity incidents. STP has established INCIDENT RESPONSE procedures for detecting, reporting, and responding to security incidents promptly. An *INCIDENT RESPONSE TEAM* has been designated and trained to handle incidents effectively. The *INCIDENT RESPONSE PLAN* outlines the steps for incident identification, containment, mitigation, recovery, and recording the lessons learned.

Some Key Policy Provisions:

- all business-critical functions are identified with their Recovery Time Objectives (RTOs)
- tolerance for downtime is aligned to maximum time-to-recovery goals and the provisions are in place to achieve them
- recovery levels (and the triggers for them) are defined so to enable a dynamic response to any incident based on incident severity and its affected function's recovery time objectives
- the organization put in place key recovery strategies to reduce impact from downtime (for example detailed process documentation, workforce cross-training, etc.)
- the organization put in place key recovery provisions to enable an expedited response (for example maintaining active warranties and support contracts, investing in a uniform technology stack, etc.)
- a designated Security Coordinator receives and evaluates all reported incidents for meeting response thresholds and for triggering mitigation actions
- a cyber liability insurance policy makes available further response capacities as needed

Copies of the *INCIDENT RESPONSE PLAN* are located with stakeholders and in strategic locations to ensure its availability under most circumstances. The plan is regularly tested, reviewed and updated to ensure it is still covering critical functions and that includes new types of incidents.

9. Systems Operations

One of the primary goals of STP's cybersecurity program is the continuity of operations and maintaining availability of all critical systems. The company's SYSTEMS OPERATIONS policies define responsibilities for system administrators, including system backups, log monitoring, and performance tuning. Many of these responsibilities are shared by the internal IT department and external vendors. Where responsibilities are delegated to *Third-Party Service Providers* they are tied to guarantees for performance and uptime through service level agreements (SLAs).

Some Key Policy Provisions:

- the IT department continuously monitors the performance of workstations and servers with several autonomously running tools (see section 11, SYSTEM, APPLICATION, AND NETWORK SECURITY AND MONITORING)
- monitoring systems create alerts for the IT department to take action and/or pro-actively notify of any potential concerns (hard drives filling up, systems running hot, frequent errors, loss of monitoring capability, missing updates, etc.)
- workstations and servers are deployed with a remote support tool for more efficient support service
- the IT department performs proactive maintenance for stable operations of systems and applies performance and security patches (see section 10, VULNERABILITY AND PATCH MANAGEMENT)
- the company's network architecture is strategically designed to eliminate single points of failure from service interruptions or broken technology (power, connectivity, network switches)
- independent data backup and recovery systems ensure data integrity and availability and that a failure or corruption in one system does not affect the other
- for STP's cloud-hosted infrastructure-as-a-service, accessibility and availability are the responsibility of the respective provider according to the contractual obligations and their SLAs (in most cases guaranteeing more than 99% uptime)

STP also maintains active collaboration with all supporting providers impacting system operations (building management, utilities, telco) to ensure systems' availability, integrity, and confidentiality.

10. Vulnerability and Patch Management

STP maintains a rigorous VULNERABILITY AND PATCH MANAGEMENT program. Various tools are deployed to identify, assess, patch and mitigate vulnerabilities in systems, applications, and network devices. In addition, STP uses independent external auditors to periodically verify the effectiveness of the program and its adherence to internal goals and standards.

Some Key Policy Provisions:

- workstations and servers are scanned daily for new vulnerabilities
- the IT department schedules all updates for operating systems and productivity software according to severity and with priority given to critical and high severity vulnerabilities[1]
- the company reserves maintenance windows outside regular business hours for system maintenance
- periodically, STP hires independent auditors to conduct additional vulnerability scans on all systems

STP recognizes that patching success requires active participation by workforce members (keeping systems turned on and connected to the Internet, allowing system reboots, etc.) and has integrated the necessary provisions in its policies and training.

[1] *based on CVSS scores published by the National Institute of Standards and Technology*

11. System, Application and Network Security and Monitoring

STP has put in place various tools to perform continuous SYSTEM, APPLICATION, AND NETWORK SECURITY AND MONITORING. Network devices, computers, and security programs send events to a central repository where

logs are aggregated, parsed, and evaluated. For any issues detected which are beyond the automated mitigation capabilities of the system, it generates alerts for escalation to the security and IT teams.

Some Key Policy Provisions:

- networks and systems are continuously monitored for abnormal performance and security events
- all computers are setup with remote monitoring and management (RMM) agents to track:
    - anti-virus software status and definition updates
    - system stability (free space on hard drive, memory usage, component status)
    - current software inventory and any changes
- a Security Information and Event Management (SIEM) system provides several layers of autonomous detection through Endpoint Detection and Response (EDR) and User and Entity Behavior Analytics (UEBA), all of which are orchestrated in an Extended Detection and Response (XDR) system
- the XDR continuously works to:
    - collect events, monitor, parse, intervene, and generate alerts from the EDR agents, firewalls and network devices, and from Internet activity logs
    - evaluate, process and escalate any incidents as necessary
- common types of issues are mitigated automatically according to pre-established playbooks and using process automation
- unmitigated incidents are escalated to human inspection

The Extended Detection and Response system is first in line for evaluating events for meeting any security incident threshold. Upon human inspection and where an incident is confirmed, the INCIDENT RESPONSE process will be triggered (see section 8, INCIDENT RESPONSE) for further investigation and resolution.

12. Systems and Application Development and Performance

As a software development company, STP takes seriously its responsibility for secure SYSTEMS AND APPLICATION DEVELOPMENT AND PERFORMANCE, including safe coding practices. The company has implemented a rigorous Software Development Life Cycle (SDLC) process to ensure that security assurance activities such as penetration testing, code review, and architecture analysis are an integral part of the system development effort.

Some Key Policy Provisions:

- the company has adopted secure design principles in application architecture such as the concept of *Least Privilege*, explicit error checking and minimizing the application attack surface
- upon hire and periodically thereafter, development personnel receive training in writing secure code for their specific development environment and responsibilities
- members of the public can submit reports of software bugs and vulnerabilities through an established intake process which assigns severity according to the company's internal rating system and which submits issues to the appropriate team for root cause analysis
- newly developed code is subject to vulnerability scanning by static and dynamic analysis tools and to a code review process by peers
- any third-party software components for use in the company's applications are reviewed to come from trusted sources and proven frameworks and libraries
- the company conducts periodic penetration testing against its applications

Developers use standard, industry-recommended hardening configuration templates for application infrastructure components. Wherever possible, the application development process leverages vetted modules or services for application security components, such as identity management, encryption, and auditing and logging. It is STP's imperative that its software shall never purposefully bypass or weaken any security configuration of the systems on which it is run.

13. Physical Security and Environmental Controls

PHYSICAL SECURITY AND ENVIRONMENTAL CONTROLS are essential to protecting STP's people, as well as its property including equipment, materials, and data. The company defines several different security zones. These are applicable to all spaces, including the company's offices, employee's home offices as well as public spaces. Depending on the security zone in which they are located, employees must follow a code of conduct and may have to take precautions or work under certain restrictions.

Some Key Policy Provisions:

- the company has implemented the principle of security zones, and employees are aware of the need to protect themselves and company property and have clear guidance on how to act depending on their location and context
- the company leases office space located in multi-tenant buildings which are protected by the private security services hired by property management
- depending on location, physical security includes fencing, gatekeepers, cameras, access badge terminals, reception desks, motion sensors, glass break alerts, building alarms and other measures
- the company has co-located some critical infrastructure into high security data centers which are in isolated, reinforced buildings with dedicated security personnel, and with sophisticated environmental controls for climate control and fire suppression, among many other provisions
- certain zones are only accessible by authorized company personnel and through audited and logged access methods and only for valid business purposes, which cannot be simple day-to-day operations

The company recognizes that physical controls alone can never be sufficient and therefore has many additional policies and procedures in place to use employee's wherewithal to enhance overall security. This includes awareness for common security concerns such as someone attempting to tailgate personnel through security barriers, challenging unescorted visitors encountered on company premises, reporting unusual observations such as open doors, and many more.

14. Data Privacy

Protecting the privacy of *Client* data as well as its own data is one of STP's top priorities. STP publishes a DATA PRIVACY policy on its website for review by the public. Where *Third-Party Providers* handle sensitive data on its behalf, STP only works providers which are committed to the same or a higher standard of care as its own.

Some Key Policy Provisions:

- the *Data Protection Officer* (DPO) conducts periodic *Data Privacy Impact Assessments* to uphold compliance with applicable privacy regulations and STP's obligations for the *Client* data it manages on behalf of other stakeholders
- the organization periodically audits data records to ensure the purpose for maintaining the data is still valid and in compliance with the DATA PRIVACY policy and applicable regulations
- where valid reasons have expired, data is disposed of in accordance with the DATA DISPOSAL policy (see section 7)

Beyond training *Employees* to be aware of their data protection obligations, STP also seeks to foster an active DATA PRIVACY culture by making available shredding bins, lockable cabinets, folder covers, pin-code protected printers, and various other provisions.

15. Vendor and Third-Party Service Provider Management

STP recognizes that prudent VENDOR AND THIRD-PARTY SERVICE PROVIDER MANAGEMENT is a key factor in controlling organizational risk. *Third-Party Service Providers* pose a greater risk for having exposure to sensitive data, locations, and for maintaining vital business infrastructure. In this context, a *Third-Party Service Provider* is any entity under contract which integrates with STP's operations. A *Vendor* is a contracted entity which supports STP holistically but does not integrate with its operations. STP has policies for evaluating, selecting, and monitoring both *Third-Party Services Providers* and *Vendors*.

Some Key Policy Provisions:

- the organization actively maintains an updated inventory of *Third-Party Services Providers* and *Vendors*
- providers which are sufficiently integrated to pose a risk to STP's viability are required to make contractual guarantees, such as SLAs
- prospective *Third-Party Services Providers* and *Vendors* are vetted against a set of security and other suitability requirements

At its own discretion and if deemed necessary, STP reserves the right to conduct audits of *Third-Party Services Providers* and *Vendors* to ensure compliance with contractual obligations and cybersecurity standards.

16. Consistent Use of Multi-factor Authentication

STP has adopted the CONSISTENT USE OF MULTI-FACTOR AUTHENTICATION to ensure that technology and data access is limited to authorized individuals. The Consistent Use of Multi-factor Authentication (MFA) is a required security standard under all common security frameworks and a key component of trust services criteria. STP consistently enforces secure authentication and MFA for systems holding *Confidential* data.

Some Key Policy Provisions:

- the company has a policy defining MFA as using at least two authentication factors but excluding any deprecated methods
- MFA is implemented and required for all types of remote access to company systems (VPN, remote support tools, directory services, mobile device management, and firewall management portals)
- MFA is implemented and required for access to email systems and spam filters
- MFA is implemented for access to source code repositories and key storage
- MFA is implemented for physical access to areas with sensitive information and critical equipment
- where it is offered for vendor systems, the company mandates the implementation and use of MFA
- STP periodically surveys sensitive systems (banking portals, SaaS portals, regulatory agencies, local/state/federal agencies) for the availability of MFA where it has not been offered previously

Where MFA is not offered on providers' systems containing STP's sensitive information, STP will request from the provider to implement MFA or evaluate alternative options if the provider cannot offer it.

17. Cybersecurity Awareness Training

A well-informed workforce is a critical defense against cyber threats. STP recognizes this and provides all *Employees* with CYBERSECURITY AWARENESS TRAINING through a provider of training services as well as through in-house training. The program allows *Employees* to test themselves and track their own progress. STP has internal performance goals and closely tracks progress against these goals.

Some Key Policy Provisions:

- all personnel must participate in and receive regular Cybersecurity Awareness Training
- aside from structured training, from time to time personnel is tested for resilience to phishing and other forms of social engineering
- training topics are amended as the threat landscape evolves and have previously included
    - phishing awareness
    - password hygiene
    - recognizing and reporting security incidents
- personnel working in trusted roles receive additional training specific to their responsibilities

STP's senior leadership stands behind the training program and has made fostering a culture of cyber safety a strategic objective, with Cybersecurity Awareness Training, auditable controls, and accountability being critical components of this effort.

18. Encryption to protect all Sensitive Information Transmitted and at Rest

The use of ENCRYPTION TO PROTECT ALL SENSITIVE INFORMATION TRANSMITTED AND AT REST is fundamental to safeguarding sensitive information. STP mandates the use of strong encryption algorithms and protocols to protect sensitive data. STP also recognizes the importance of key management in this context and makes use of the *Third-Party Service Providers*' and/or hardware *Vendors'* provisions, for example Microsoft Azure Key Vault and TPM chip technology.

Some Key Policy Provisions:

- all enterprise assets with physical and virtual storage media are configured to automatically encrypt all data at rest
- data stored locally on computers is encrypted through the use of whole disk encryption
- data stored on mobile devices is encrypted through biometric lock and encryption
- encryption is used for data transmissions between the computers and *Third-Party Service Providers* hosting sensitive information (use of HTTPS over HTTP, VPN and other technology)
- email containing *Confidential* data must be sent encrypted or the data must be shared by other means

For selecting cipher strength and algorithms, STP adheres to and applies cryptographic standards in line with recommendations of the National Institute of Standards and Technology (NIST) Cryptographic Standards and Guidelines (CSRC).

Appendix

Privacy Policy

https://stpis.com/privacy-policy

Thank you for choosing to leverage the STP Investment Service, LLC Portal for your data aggregation and reporting needs. We are committed to protecting your personal information and your right to privacy. If you have any questions or concerns about our policy, or our practices with regards to your personal information, please contact us at info@stpis.com.

When you visit our STP Portal (https://stpis.com), and use our services, you trust us with your personal information. We take your privacy very seriously. In this privacy notice, we describe our privacy policy. We seek to explain to you in the clearest way possible what information we collect, how we use it and what rights you have in relation to it. We hope you take some time to read through it carefully, as it is important. If there are any terms in this privacy policy that you do not agree with, please contact us using the provided contact information below.

This privacy policy applies to all information collected through our production and UAT portals (https://stpis.com, https://portaltest.stpis.com), and/or any related services, sales, marketing or events (we refer to them collectively in this privacy policy as the "Portal").

Please read this privacy policy carefully as it will help you make informed decisions about sharing your personal information with us.

TABLE OF CONTENTS

1. WHAT INFORMATION DO WE COLLECT?

Personal information you disclose to us

Summary: We collect personal information that you provide to us such as name, phone number and password information. Please note all data housed in STP data centers is encrypted at rest in the storage array.

We collect personal information that you or a representative at your firm provides to us in the new user setup process.

Name and Contact Data. We collect your first and last name, email address, username and phone number information.

Credentials. We collect username and passwords for authentication and account access. The STP Portal monitors all login activity to ensure a secure environment.

Payment Data.The STP Portal does not collect or store any payment or credit card information.

All personal information that you provide to us must be true, complete and accurate, and you must notify us of any changes to such personal information.

Information collected from other sources

Summary: We do not collect any data from public databases, marketing partners, and other outside sources.

The only information stored about an individual is referenced above in the “personal information we disclose” section.

2. HOW DO WE USE YOUR INFORMATION?

Summary: We process your information for purposes based on legitimate business interests, the fulfillment of our contract with you, compliance with our legal obligations, and/or your consent.

We use personal information collected via our Portal for a variety of business purposes described below. We process your personal information for these purposes in reliance on our legitimate business interests (“Business Purposes”), in order to enter into or perform a contract with you (“Contractual”), with your consent (“Consent”), and/or for compliance with our legal obligations (“Legal Reasons”). We indicate the specific processing grounds we rely on next to each purpose listed below.

We use the information we collect or receive:

To facilitate account creation and logon process The logon information associated to your account drives the logic for the Portal's security framework and enforces entity and feature level permissioning.

To protect our Portal for Business Purposes and/or for Legal Reasons . We may use your information as part of our efforts to keep our Portal safe and secure (for example, for fraud monitoring and prevention).

3. WILL YOUR INFORMATION BE SHARED WITH 3RD PARTIES?

Summary: We only share information with your consent, to comply with laws, to protect your rights, or to fulfill business obligations.

We only share and disclose your information in the following situations:

Compliance with Laws. We may disclose your information where we are legally required to do so in order to comply with applicable law, governmental requests, a judicial proceeding, court order, or legal process, such as in response to a court order or a subpoena (including in response to public authorities to meet national security or law enforcement requirements).

Vital Interests and Legal Rights. We may disclose your information where we believe it is necessary to investigate, prevent, or take action regarding potential violations of our policies, suspected fraud, situations involving potential threats to the safety of any person and illegal activities, or as evidence in litigation in which we are involved.

Business Transfers. We may share or transfer your information in connection with, or during negotiations of, any merger, sale of company assets, financing, or acquisition of all or a portion of our business to another company.

With your Consent. We may disclose your personal information for any other purpose with your consent.

4. DO WE USE COOKIES AND OTHER TRACKING TECHNOLOGIES?

Summary: We do not use cookies and other tracking technologies to collect and store your information.

We do not use cookies to access or store your personal information. The only cookie the Portal stores is a unique id to track a user's session. This cookie does not contain any private and/or personal information about the logged in user.

5. WHAT IS THE STP RETENTION PERIOD FOR YOUR DATA?

Summary: We keep your information for as long as necessary to fulfill the purposes outlined in this privacy policy unless otherwise required by law.

We will only keep your personal information for as long as it is necessary for the purposes set out in this privacy policy, unless a longer retention period is required or permitted by law (such as tax, accounting or

other legal requirements). No purpose in this policy will require us keeping your personal information for longer than 2 years past the termination of the user's account .

When we have no ongoing legitimate business need to process your personal information, we will either delete or anonymize it, or, if this is not possible (for example, because your personal information has been stored in backup archives), then we will securely store your personal information and isolate it from any further processing until deletion is possible.

6. HOW DO WE KEEP YOUR INFORMATION SAFE?

Summary: We aim to protect your personal information through a system of organizational and technical security measures.

We have implemented appropriate technical and organizational security measures designed to protect the security of any personal information we process. However, please also remember that we cannot guarantee that the internet itself is 100% secure. Although we will do our best to protect your personal information, transmission of personal information to and from our Portal is at your own risk. You should only access the services within a secure environment.

7. DO WE COLLECT INFORMATION FROM MINORS?

Summary: We do not knowingly collect data from or market to children under 18 years of age.

We do not knowingly solicit data from or market to children under 18 years of age. By using the Portal, you represent that you are at least 18 or that you are the parent or guardian of such a minor and consent to such minor dependent's use of the Portal. If we learn that personal information from users less than 18 years of age has been collected, we will deactivate the account and take reasonable measures to promptly delete such data from our records. If you become aware of any data we have collected from children under age 18, please contact us at info@stpis.com.

8. WHAT ARE YOUR PRIVACY RIGHTS?

Summary: You may review, change, or terminate your account at any time.

If you are resident in the European Economic Area and you believe we are unlawfully processing your personal information, you also have the right to complain to your local data protection supervisory authority. You can find their contact details here: http://ec.europa.eu/justice/data-protection/bodies/authorities/index_en.htm
Account Information

If you would at any time like to review or change the information in your account or terminate your account, you can:

■ Log into your account settings and update your user account.

■ Contact us using the contact information provided.

Upon your request to terminate your account, we will deactivate or delete your account and information from our active databases. However, some information may be retained in our files to prevent fraud, troubleshoot problems, assist with any investigations, enforce our Terms of Use and/or comply with legal requirements.

Cookies and similar technologies: Most Web browsers are set to accept cookies by default. If you prefer, you can usually choose to set your browser to remove cookies and to reject cookies. If you choose to remove cookies or reject cookies, this could affect certain features or services of our Portal.

Opting out of email marketing: You can unsubscribe from our marketing email list at any time by clicking on the unsubscribe link in the emails that we send or by contacting us using the details provided below. You will then be removed from the marketing email list – however, we will still need to send you service-related emails that are necessary for the administration and use of your account. To otherwise opt-out, you may:

■ Contact us using the contact information provided.

9. DO CALIFORNIA RESIDENTS HAVE SPECIFIC PRIVACY RIGHTS?

Summary: Yes, if you are a resident of California, you are granted specific rights regarding access to your personal information.

California Civil Code Section 1798.83, also known as the “Shine The Light” law, permits our users who are California residents to request and obtain from us, once a year and free of charge, information about categories of personal information (if any) we disclosed to third parties for direct marketing purposes and the names and addresses of all third parties with which we shared personal information in the immediately preceding calendar year. If you are a California resident and would like to make such a request, please submit your request in writing to us using the contact information provided below.

If you are under 18 years of age, reside in California, and have a registered account with the Portal, you have the right to request removal of unwanted data that you publicly post on the Portal. To request removal of such data, please contact us using the contact information provided below, and include the email address associated with your account and a statement that you reside in California. We will make sure the data is not publicly displayed on the Portal, but please be aware that the data may not be completely or comprehensively removed from our systems.

10. DO WE MAKE UPDATES TO THIS POLICY?

Summary: Yes, we will update this policy as necessary to stay compliant with relevant laws.

We may update this privacy policy from time to time. The updated version will be indicated by an updated "Revised" date and the updated version will be effective as soon as it is accessible. If we make material changes to this privacy policy, we may notify you either by prominently posting a notice of such changes or by directly sending you a notification. We encourage you to review this privacy policy frequently to be informed of how we are protecting your information.

11. HOW CAN YOU CONTACT US ABOUT THIS POLICY?

If you have questions or comments about this policy, you may email us at info@stpis.com or by post to:
STP Investment Service, LLC
158 W. Gay St.
STE 300
West Chester, PA 19380
United States