FONDA-FULTONVILLE CENTRAL SCHOOL DISTRICT
DATA PRIVACY AGREEMENT

Fonda-Fultonville Central School District

and

Stock-Trak Inc.

This Data Privacy Agreement ("DPA") is by and between Fonda-Fultonville Central School District ("EA"), an Educational Agency, and Stock-Trak Inc. ("Contractor"), collectively, the “Parties”.

ARTICLE I: DEFINITIONS

As used in this DPA, the following terms shall have the following meanings:

1. **Breach:** The unauthorized acquisition, access, use, or disclosure of Personally Identifiable Information in a manner not permitted by State and federal laws, rules and regulations, or in a manner which compromises its security or privacy, or by or to a person not authorized to acquire, access, use, or receive it, or a Breach of Contractor’s security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personally Identifiable Information.
2. **Commercial or Marketing Purpose:** means the sale, use or disclosure of Personally Identifiable Information for purposes of receiving remuneration, whether directly or indirectly; the sale, use or disclosure of Personally Identifiable Information for advertising purposes; or the sale, use or disclosure of Personally Identifiable Information to develop, improve or market products or services to students.
3. **Disclose**: To permit access to, or the release, transfer, or other communication of personally identifiable information by any means, including oral, written or electronic, whether intended or unintended.
4. **Education Record:** An education record as defined in the Family Educational Rights and Privacy Act and its implementing regulations, 20 U.S.C. 1232g and 34 C.F.R. Part 99, respectively.
5. **Educational Agency**: As defined in Education Law 2-d, a school district, board of cooperative educational services, school, charter school, or the New York State Education Department.
6. **Eligible Student:** A student who is eighteen years of age or older.
7. **Encrypt or Encryption**: As defined in the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule at 45 CFR 164.304, means the use of an algorithmic process to transform Personally Identifiable Information into an unusable, unreadable, or indecipherable form in which there is a low probability of assigning meaning without use of a confidential process or key.

8. **NIST Cybersecurity Framework**: The U.S. Department of Commerce National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1.
9. **Parent:** A parent, legal guardian or person in parental relation to the Student.
10. **Personally Identifiable Information (PII):** Means personally identifiable information as defined in section 99.3 of Title 34 of the Code of Federal Regulations implementing the Family Educational Rights and Privacy Act, 20 U.S.C 1232g , and Teacher or Principal APPR Data, as defined below.
11. **Release:** Shall have the same meaning as Disclose.
12. **School:** Any public elementary or secondary school including a charter school, universal pre-kindergarten program authorized pursuant to Education Law § 3602-e, an approved provider of preschool special education, any other publicly funded pre-kindergarten program, a school serving children in a special act school district as defined in Education Law § 4001, an approved private school for the education of students with disabilities, a State-supported school subject to the provisions of Article 85 of the Education Law, or a State-operated school subject to the provisions of Articles 87 or 88 of the Education Law.
13. **Student:** Any person attending or seeking to enroll in an Educational Agency.
14. **Student Data:** Personally identifiable information as defined in section 99.3 of Title 34 of the Code of Federal Regulations implementing the Family Educational Rights and Privacy Act, 20 U.S.C 1232g.
15. **Subcontractor:** Contractor's non-employee agents, consultants and/or subcontractors engaged in the provision of services pursuant to the Service Agreement.
16. **Teacher or Principal APPR Data**: Personally Identifiable Information from the records of an Educational Agency relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of Education Law §§ 3012-c and 3012-d.

ARTICLE II: PRIVACY AND SECURITY OF PII

1. **Compliance with Law.**

   In order for Contractor to provide certain services ("Services") to the EA pursuant to a contract dated [December 16, 2022] ("Service Agreement"); Contractor may receive PII regulated by several New York and federal laws and regulations, among them, the Family Educational Rights and Privacy Act ("FERPA") at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); New York Education Law Section 2-d; and the Commissioner of Education's Regulations at 8 NYCRR Part 121. The Parties enter this DPA to address the requirements of New York

law. Contractor agrees to maintain the confidentiality and security of PII in accordance with applicable New York, federal and local laws, rules and regulations.

2. **Authorized Use.**
   Contractor has no property or licensing rights or claims of ownership to PII, and Contractor must not use PII for any purpose other than to provide the Services set forth in the Service Agreement. Neither the Services provided nor the manner in which such Services are provided shall violate New York law.

3. **Data Security and Privacy Plan**.
   Contractor shall adopt and maintain administrative, technical and physical safeguards, measures and controls to manage privacy and security risks and protect PII in a manner that complies with New York State, federal and local laws and regulations and the EA's policies. Education Law Section 2-d requires that Contractor provide the EA with a Data Privacy and Security Plan that outlines such safeguards, measures and controls including how the Contractor will implement all applicable state, federal and local data security and privacy requirements. Contractor's Data Security and Privacy Plan is attached to this DPA as Exhibit C.

4. **EA's Data Security and Privacy Policy**
   State law and regulation requires the EA to adopt a data security and privacy policy that complies with Part 121 of the Regulations of the Commissioner of Education and aligns with the NIST Cyber Security Framework. Contractor shall comply with the EA's data security and privacy policy and other applicable policies.

5. **Right of Review and Audit.**
   Upon request by the EA, Contractor shall provide the EA with copies of its policies and related procedures that pertain to the protection of PII. It may be made available in a form that does not violate Contractor's own information security policies, confidentiality obligations, and applicable laws. In addition, Contractor may be required to undergo an audit of its privacy and security safeguards, measures and controls as it pertains to alignment with the requirements of New York State laws and regulations, the EA's policies applicable to Contractor, and alignment with the NIST Cybersecurity Framework performed by an independent third party at Contractor's expense, and provide the audit report to the EA. Contractor may provide the EA with a recent industry standard independent audit report on Contractor's privacy and security practices as an alternative to undergoing an audit.

6. **Contractor's Employees and Subcontractors**.

(a) Contractor shall only disclose PII to Contractor's employees and subcontractors who need to know the PII in order to provide the Services and the disclosure of PII shall be limited to the extent necessary to provide such Services. Contractor shall ensure that all such employees and subcontractors comply with the terms of this DPA.

(b) Contractor must ensure that each subcontractor performing functions pursuant to the Service Agreement where the subcontractor will receive or have access to PII is contractually bound by a written agreement that includes confidentiality and data security obligations equivalent to, consistent with, and no less protective than, those found in this DPA.

(c) Contractor shall examine the data security and privacy measures of its subcontractors prior to utilizing the subcontractor. If at any point a subcontractor fails to materially comply with the requirements of this DPA, Contractor shall: notify the EA and remove such subcontractor's access to PII; and, as applicable, retrieve all PII received or stored by such subcontractor and/or ensure that PII has been securely deleted and destroyed in accordance with this DPA. In the event there is an incident in which the subcontractor compromises PII, Contractor shall follow the Data Breach reporting requirements set forth herein.

(d) Contractor shall take full responsibility for the acts and omissions of its employees and subcontractors.

(e) Contractor must not disclose PII to any other party unless such disclosure is required by statute, court order or subpoena, and the Contractor makes a reasonable effort to notify the EA of the court order or subpoena in advance of compliance but in any case, provides notice to the EA no later than the time the PII is disclosed, unless such disclosure to the EA is expressly prohibited by the statute, court order or subpoena.

7. **Training**.

Contactor shall ensure that all its employees and Subcontractors who have access to PII have received or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access.

8. **Termination**

The obligations of this DPA shall continue and shall not terminate for as long as the Contractor or its sub-contractors retain PII or retain access to PII.

9. **Data Return and Destruction of Data**.

(a) Protecting PII from unauthorized access and disclosure is of the utmost importance to the EA, and Contractor agrees that it is prohibited from retaining PII or continued access to PII or any copy, summary or extract of PII, on any storage medium (including, without limitation, in secure data centers and/or cloud-based facilities) whatsoever beyond the period of providing Services to the EA, unless such retention is either expressly authorized for a prescribed period by the Service Agreement or other written agreement between the Parties, or expressly requested by the EA for purposes of facilitating the transfer of PII to the EA or expressly required by law. ~~As applicable, upon expiration or termination of the Service Agreement, Contractor shall transfer PII, in a format agreed to by the Parties to the EA.~~ PII will be deleted upon teacher/administrator request, or automatically after 12 months of user inactivity.

(b) If applicable, once the transfer of PII has been accomplished in accordance with the EA's written election to do so, Contractor agrees to return or destroy all PII when the purpose that necessitated its receipt by Contractor has been completed. Thereafter, with regard to all PII (including without limitation, all hard copies, archived copies, electronic versions, electronic imaging of hard copies) as well as any and all PII maintained on behalf of Contractor in a secure data center and/or cloud-based facilities that remain in the possession of Contractor or its Subcontractors, Contractor shall ensure that PII is securely deleted and/or destroyed in a manner that does not allow it to be retrieved or retrievable, read or reconstructed. Hard copy media must be shredded or destroyed such that PII cannot be read or otherwise reconstructed, and electronic media must be cleared, purged, or destroyed such that the PII cannot be retrieved. Only the destruction of paper PII, and not redaction, will satisfy the requirements for data destruction. Redaction is specifically excluded as a means of data destruction.

(c) Contractor shall provide the EA with a written certification of the secure deletion and/or destruction of PII held by the Contractor or Subcontractors within 30 days of a written request to delete student data, by providing the Contractor with a list of student usernames by email to privacy@stocktrak.com. PII will automatically be deleted after 12 months of user inactivity.

(d) To the extent that Contractor and/or its subcontractors continue to be in possession of any de-identified data (i.e., data that has had all direct and indirect identifiers removed), they agree not to attempt to re-identify de-identified data and not to transfer de-identified data to any party.

10. **Commercial or Marketing Use Prohibition.**
Contractor agrees that it will not sell PII or use or disclose PII for a Commercial or Marketing Purpose.

11. **Encryption.**
Contractor shall use industry standard security measures including encryption protocols that comply with New York law and regulations to preserve and protect PII. Contractor must encrypt PII at rest and in transit in accordance with applicable New York laws and regulations.

12. **Breach**.
(a) Contractor shall promptly notify the EA of any Breach of PII without unreasonable delay no later than seven (7) calendar days after discovery of the Breach.
(b) Notifications required pursuant to this section must be in writing, given by personal delivery, e-mail transmission (if contact information is provided for the specific mode of delivery), or by registered or certified, and must to the extent available, include a description of the Breach which includes the date of the incident and the date of discovery; the types of PII affected and the number of records affected; a description of Contractor's investigation; and the contact information for representatives who can assist the EA. Notifications required by this section must be sent to the EA's District Superintendent or other head administrator with a copy to the Data Protection Office. Violations of the requirement to notify the EA shall be subject to a civil penalty pursuant to Education Law Section 2-d. The Breach of certain PII protected by Education Law Section 2-d may subject the Contractor to additional penalties.
(c) The EA shall notify the Contractor by email to privacy@stocktrak.com either a list of all teachers and/or class administrators or the email extensions used by all teachers and/or class administrators, to the extent applicable, whose respective accounts form part of the EA, for the purposes of the Contractor notifying the EA in the event of a breach.
(d) Notifications required under this paragraph must be provided to the EA at the following address:
[Name: Jarrod Baker
Title: Data Privacy Officer
Address: 112 Old Johnstown Rd
City, State, Zip: Fonda, NY 12068
Email: jbaker@ffcsd.org]

13. **Cooperation with Investigations.**
Contractor agrees that it will cooperate with the EA and law enforcement, where necessary, in any investigations into a Breach. Any costs incidental to the required cooperation or participation of the Contractor or its' Authorized Users, as related to such investigations, will

be the sole responsibility of the Contractor if such Breach is attributable to Contractor or its Subcontractors.

14. **Notification to Individuals.**
    Where a Breach of PII occurs that is attributable to Contractor, Contractor shall pay for or promptly reimburse the EA for the full cost of the EA's notification to Parents, Eligible Students, teachers, and/or principals, in accordance with Education Law Section 2-d and 8 NYCRR Part 121.

15. **Termination**.
    The confidentiality and data security obligations of the Contractor under this DPA shall survive any termination of this DPA but shall terminate upon Contractor's certifying that it has destroyed all PII.

ARTICLE III: PARENT AND ELIGIBLE STUDENT PROVISIONS

1. **Parent and Eligible Student Access**.
   Education Law Section 2-d and FERPA provide Parents and Eligible Students the right to inspect and review their child's or the Eligible Student's Student Data stored or maintained by the EA. To the extent Student Data is held by Contractor pursuant to the Service Agreement, Contractor shall respond within thirty (30) calendar days to the EA's requests for access to Student Data so the EA can facilitate such review by a Parent or Eligible Student, and facilitate corrections, as necessary. If a Parent or Eligible Student contacts Contractor directly to review any of the Student Data held by Contractor pursuant to the Service Agreement, Contractor shall promptly notify the EA and refer the Parent or Eligible Student to the EA.

2. **Bill of Rights for Data Privacy and Security**.
   As required by Education Law Section 2-d, the Parents Bill of Rights for Data Privacy and Security and the supplemental information for the Service Agreement are included as Exhibit A and Exhibit B, respectively, and incorporated into this DPA. Contractor shall complete and sign Exhibit B and append it to this DPA. Pursuant to Education Law Section 2-d, the EA is required to post the completed Exhibit B on its website.

ARTICLE IV: MISCELLANEOUS

1. **Priority of Agreements and Precedence.**

In the event of a conflict between and among the terms and conditions of this DPA, including all Exhibits attached hereto and incorporated herein and the Service Agreement, the terms and conditions of this DPA shall govern and prevail, shall survive the termination of the Service Agreement in the manner set forth herein, and shall supersede all prior communications, representations, or agreements, oral or written, by the Parties relating thereto.

2. **Execution.**

This DPA may be executed in one or more counterparts, all of which shall be considered one and the same document, as if all parties had executed a single original document, and may be executed utilizing an electronic signature and/ or electronic transmittal, and each signature thereto shall be and constitute an original signature, as if all parties had executed a single original document.

EDUCATIONAL AGENCY	**CONTRACTOR**
BY: ***[Signature]***	Andrew Zeidel Digitally signed by Andrew Zeidel DN: cn=Andrew Zeidel, o=Stock-Trak Inc., ou, email=azeidel@stocktrak.com, c=CA Date: 2022.12.16 14:01:44 -05'00'
[*Printed Name*]	Andrew Zeidel
[Title]	COO
Date:	Date: December 16, 2022

EXHIBIT A - Education Law §2-d Bill of Rights for Data Privacy and Security

Parents (including legal guardians or persons in parental relationships) and Eligible Students (students 18 years and older) can expect the following:

1. A student's personally identifiable information (PII) cannot be sold or released for any Commercial or Marketing purpose. PII, as defined by Education Law § 2-d and the Family Educational Rights and Privacy Act ("FERPA"), includes direct identifiers such as a student's name or identification number, parent's name, or address; and indirect identifiers such as a student's date of birth, which when linked to or combined with other information can be used to distinguish or trace a student's identity. Please see FERPA's regulations at 34 CFR 99.3 for a more complete definition.

2. The right to inspect and review the complete contents of the student's education record stored or maintained by an educational agency. This right may not apply to Parents of an Eligible Student.

3. State and federal laws such as Education Law § 2-d; the Commissioner of Education's Regulations at 8 NYCRR Part 121, FERPA at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); and the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); protect the confidentiality of a student's identifiable information.

4. Safeguards associated with industry standards and best practices including, but not limited to, encryption, firewalls and password protection must be in place when student PII is stored or transferred.

5. A complete list of all student data elements collected by NYSED is available at www.nysed.gov/data-privacy-security/student-data-inventory and by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234.

6. The right to have complaints about possible breaches and unauthorized disclosures of PII addressed. (i) Complaints should be submitted to the EA at: [Insert EA's contact information for complaints]. (ii) Complaints may also be submitted to the NYS Education Department at www.nysed.gov/data-privacy-security/report-improper-disclosure, by mail to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234; by email to privacy@nysed.gov; or by telephone at 518-474-0937.

7. To be notified in accordance with applicable laws and regulations if a breach or unauthorized release of PII occurs.

8. Educational agency workers that handle PII will receive training on applicable state and federal laws, policies, and safeguards associated with industry standards and best practices that protect PII.

9. Educational agency contracts with vendors that receive PII will address statutory and regulatory data privacy and security requirements.

CONTRACTOR	
[Signature]	Andrew Zeidel Digitally signed by Andrew Zeidel DN: cn=Andrew Zeidel, o=Stock-Trak Inc., ou, email=azeidel@stocktrak.com, c=CA Date: 2022.12.16 14:02:21 -05'00'
[Printed Name]	**Andrew Zeidel**
[Title]	**COO**

Date:	December 16, 2022

EXHIBIT B

BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY - SUPPLEMENTAL INFORMATION FOR CONTRACTS THAT UTILIZE PERSONALLY IDENTIFIABLE INFORMATION

Pursuant to Education Law § 2-d and Section 121.3 of the Commissioner's Regulations, the Educational Agency (EA) is required to post information to its website about its contracts with third-party contractors that will receive Personally Identifiable Information (PII).

Name of Contractor	Stock-Trak Inc.
Description of the purpose(s) for which Contractor will receive/access PII	PII that is collected during user registration will be used for no purpose other than for the service listed below: PersonalFinanceLab.com, a portfolio simulation tool to help students get familiar with real market data, buying and selling securities, and managing a portfolio in a controlled environment. It also includes a personal budget game to help students learn how to budget their expenses, and to manage cash and credit cards. Please note that teachers can create student accounts with auto-generated usernames where no PII is collected.
Type of PII that Contractor will receive/access	Check all that apply: ☒ Student PII ☐ APPR Data
Contract Term	Contract Start Date: January 1, 2023 Contract End Date: December 31, 2025
Subcontractor Written Agreement Requirement	Contractor will not utilize subcontractors without a written contract that requires the subcontractors to adhere to, at a minimum, materially similar data protection obligations imposed on the contractor by state and federal laws and regulations, and the Contract. (check applicable option) ☐ Contractor will not utilize subcontractors. ☒ Contractor will utilize subcontractors.

Data Transition and Secure Destruction	Upon expiration or termination of the Contract, Contractor shall: • Securely transfer data to EA, or a successor contractor at the EA's option and written discretion, in a format agreed to by the parties. • Securely delete and destroy data.
Challenges to Data Accuracy	Parents, teachers or principals who seek to challenge the accuracy of PII will do so by contacting the EA. If a correction to data is deemed necessary, the EA will notify Contractor. Contractor agrees to facilitate such corrections within 21 days of receiving the EA's written request.
Secure Storage and Data Security	Please describe where PII will be stored and the protections taken to ensure PII will be protected: (check all that apply) ☒ Using a cloud or infrastructure owned and hosted by a third party. ☐ Using Contractor owned and hosted solution ☐ Other: Please describe how data security and privacy risks will be mitigated in a manner that does not compromise the security of the data: We use Imperva & TierPoint for vulnerability management. TierPoint manages our operating systems and applies patches. We conduct yearly security awareness training.
Encryption	Data will be encrypted while in motion and at rest.

CONTRACTOR	
[Signature]	Andrew Zeidel Digitally signed by Andrew Zeidel DN: cn=Andrew Zeidel, o=Stock-Trak Inc., ou, email=azeidel@stocktrak.com, c=CA Date: 2022.12.16 14:02:54 -05'00'
[Printed Name]	**Andrew Zeidel**
[Title]	**COO**
Date:	**December 16, 2022**

EXHIBIT C - CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

The Educational Agency (EA) is required to ensure that all contracts with a third-party contractor include a Data Security and Privacy Plan, pursuant to **Education Law § 2-d and Section 121.6 of the Commissioner's Regulations**. For every contract, the Contractor must complete the following or provide a plan that materially addresses its requirements, including alignment with the NIST Cybersecurity Framework, which is the standard for educational agency data privacy and security policies in New York state**. While this plan is not required to be posted to the EA's website, contractors should nevertheless ensure that they do not include information that could compromise the security of their data and data systems.**

1	Outline how you will implement applicable data security and privacy contract requirements over the life of the Contract.	Stock-Trak's data is stored in a secure Type 2, SOC 2, professionally managed hosting facility. Student PII is automatically deleted after 1 year of user inactivity. Stock-Trak has appointed specific personnel who are responsible for ensuring compliance with its data privacy and security agreements as well as striving to adhere to national data privacy and security standards. Stock-Trak's management team has allocated the necessary resources to making sure these objectives are carried out and achieved on an ongoing basis.
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	Stock-Trak has implemented procedures to ensure minimal student PII is collected. Data is protected via a firewall and also encrypted in transit and at rest. All its staff are trained in data security and privacy procedures and have signed confidentiality agreements in place. Stock-Trak regularly undergoes security audits conducted by independent 3rd parties and then follows up to remediate any vulnerabilities that may be discovered.
3	Address the training received by your employees and any subcontractors engaged in the provision of services under the Contract on the federal and state laws that govern the confidentiality of PII.	We require that all employees complete a security awareness training program as well as attend ad-hoc training sessions covering specific, security related topics.

4	Outline contracting processes that ensure that your employees and any subcontractors are bound by written agreement to the requirements of the Contract, at a minimum.	All employees are required to sign confidentiality agreements as well as an acknowledgement that they have completed the security training. Stock-Trak also has agreements in place with any 3rd party contractors that may have access to PII.
5	Specify how you will manage any data security and privacy incidents that implicate PII and describe any specific plans you have in place to identify breaches and/or unauthorized disclosures, and to meet your obligations to report incidents to the EA.	Stock-Trak has created a formal incident response plan to provide a well-defined, organized approach for handling security breaches.
6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.	PII is deleted after 1 year of inactivity or within 30 days upon written request by an EA.
7	Describe your secure destruction practices and how certification will be provided to the EA.	PII is deleted after 1 year of inactivity. Stock-Trak will provide written certification that PII has been deleted upon request from an EA.
8	Outline how your data security and privacy program/practices align with the EA's applicable policies.	PII data is protected within a secure SOC Type II facility. All PII data is encrypted and only accessible to authorized personnel who are properly trained and under confidentiality agreements. Stock-Trak does not share or disclose PII data to 3rd parties and deletes PII data after 12 months of inactivity or upon written request from an EA. Stock-Trak has a team responsible for data security and privacy and also conducts security audits on a regular basis to ensure that appropriate standards are being adhered to.
9	Outline how your data security and privacy program/practices materially align with the NIST CSF v1.1 using the Framework chart below.	PLEASE USE TEMPLATE BELOW.

EXHIBIT C.1 – NIST CSF TABLE

The table below will aid the review of a Contractor's Data Privacy and Security Plan. Contractors should complete the Contractor Response sections in the table below to describe how their policies and practices align with each category in the Data Privacy and Security Plan template. To complete these 23 sections, a Contractor may: (i) Demonstrate alignment using the National Cybersecurity Review (NCSR) Maturity Scale of 1-7 ; (ii) Use a narrative to explain alignment (may reference its applicable policies); and/or (iii) Explain why a certain category may not apply to the transaction contemplated. Further informational references for each category can be found on the NIST website at Vk. Please use additional pages if needed.

Function	Category	Contractor Response
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	Stock-Trak utilizes the services of a fully managed, hosting service provider. Servers and databases are located in a SOC 2 type facility, which undergoes regular security audits. All servers are behind a firewall and incoming traffic must also pass through Imperva's DDOS protective firewall. Only authorized staff will have access to PII data via a secure VPN connection (requires multi-factor authentication and secure passwords). All PII is encrypted at rest and in transit. All staff and contractors who have access to PII are under signed confidentiality agreements and are trained to adhere to industry standard security policies and procedures. Servers are fully monitored, and Operating systems are patched regularly as required. All data is backed up daily, offsite.
	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	Stock-Trak establishes organizational goals, objectives, and priorities on a regular basis. A team is in place to manage all aspects of maintaining industry standards for data privacy and security. The team can be reached by sending an email to privacy@stocktrak.com. The team also utilizes 3rd party cyber security specialists on an ad-hoc basis if needed.
	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	Stock-Trak has measures in place (including policies and procedures) to protect PII from loss, misuse and unauthorized access, disclosure, alteration, and destruction. We have security policies in place that all employees must adhere to along with clearly defined information systems roles in place both internally and with our external contractors.
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	Stock-Trak engages with a Cyber Security firm on a regular basis to perform an internal audit, and remediates identified vulnerabilities based on a risk assessment. We receive communication from various sources on threat and vulnerabilities, and we remediate vulnerabilities based on

Function	Category	Contractor Response
		determined levels of risk to the business. All new data privacy agreements are vetted with senior management prior to being executed.
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	Stock-Trak engages with a Cyber Security firm for a regular audit to determine vulnerabilities. We assess the risks associated with the vulnerabilities to determine our risk tolerance levels and remediate issues accordingly.
	Supply Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.	Stock-Trak's senior leadership are aware of all supply chain risks and have contractual agreements with all external vendors. Suppliers and third-party partners are reassessed regularly to confirm they are meeting their contractual obligations.
PROTECT (PR)	**Identity Management, Authentication and Access Control (PR.AC):** Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	Stock-Trak's data center requires badge access to limit entry to those who require access for their job function. Visitors must be identified and escorted into the facility. Remote access requires two-factor authentication and is limited to those who require it. Those restricted staff members have access to the database via a secure VPN connection. Processes are in place to give and remove access to designated staff and contractors.
	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.	All Stock-Trak employees are required to complete an initial and on-going data privacy and security training program to handle personal information. All employees have unique login credentials to access personal information through a secure VPN connection (which includes MFA) and access is limited to those employees who require access for the normal course of business. Members of the executive team, IT team, and Development team are part of the Incident Response Team and are aware of the necessary actions to take in the event of a cyber security breach.
	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	Stock-Trak's database is hosted within TierPoint's facilities, and both data at rest and data in transit are encrypted. These secure servers are patched and secured with managed endpoints. Processes are in place to automatically delete PII after 1 year of user inactivity. All data access requires unique login credentials. The IT specialist maintains an up-to-date inventory of hardware and software assets as well as monitors capacity and investigates alerts generated by the system.
	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among	Stock-Trak secures access to its data center through requiring badge access, and guests and visitors are required to be identified and escorted on premise. The IT Specialist ensures that hard drives and other retired storage assets are destroyed, to prevent

Function	Category	Contractor Response
	organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	data recovery from these assets by unauthorized individuals. We have processes in place to destroy PII after 1 year of user inactivity. Stock-Trak has backup config of firewall appliance settings. We have a firewall appliance that scans all incoming traffic. We perform testing on our staging sites prior to migration into production and automatic backups are done daily by our hosting service provider. Both Stock-Trak and its Managed hosting service provider (currently TierPoint) engage with Cyber Security firms to perform security audits on a regular basis and the results of the security tests are shared with appropriate stakeholders. The Incident Response team will test recovery plans and review results annually, to ensure that the plan meets organization requirements. When employees and nonemployees leave the organization, HR provides notification to disable network and e-mail accounts.
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	Stock-Trak's IT specialist ensures that all system components are regularly maintained and observed for quality control. Other standard maintenance (such as operating system patches and upgrades) are performed by our hosting service provider whenever required.
	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	The technical security solutions are managed both by Stock-Trak's IT and security personnel as well as its professionally managed hosting service provider (currently TierPoint). TierPoint is responsible for maintaining the firewall, conducting the daily backups, monitoring the servers, applying regular patches and updates, etc. The system also uses Imperva firewall to protect against DDOS attacks and filter out non-human traffic.
DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected and the potential impact of events is understood.	Stock-Trak's IT specialists review logs and monitor network traffic and are alerted in the event of abnormal traffic patterns and other network anomalies. The IT specialist and Development team investigate alerts, escalating events as appropriate to senior management, who may invoke the incident response plan. We can see real time connections from our resources, where incidents are investigated, based on the sensitivity of data involved. We have thresholds set to alert the team of incidents, and guidelines on when to escalate issues accordingly.
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	All key network components are monitored 24/7/365. Monitoring is performed by Stock-Trak's professionally managed, hosting service provider within a secure, Soc 2, Type 2 datacenter facility. The Imperva firewall and DDOS protection is an added layer of

Function	Category	Contractor Response
		monitoring and security. Thresholds are established which generate automatic alerts. Logs are checked regularly for anomalies.
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	Stock-Trak has a dedicated IT specialist who is responsible for the identification of anomalous activity. We perform penetration tests through a Cyber Security firm to assess the company's ability to detect attacks. Senior management is responsible for selecting remediation actions to be performed. The incident response plan includes steps for escalating incidents to the Incident Response team, which determines the appropriate stakeholders and when to communicate details of the incident to affected parties. We incorporate back into our security practices all lessons learned from testing and documented incidents.
RESPOND (RS)	**Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	Stock-Trak has an Incident Response Plan in place to be enacted in the event of a cybersecurity breach. Stock-Trak has a close working relationship with its managed hosting service provider as well as a 3rd party specializing in security and data privacy.
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	Stock-Trak maintains an incident response plan, which outlines the roles and responsibilities of key team members and external parties. The incident response plan details steps to escalate incidents depending on the severity. It includes a list of contact information for all individuals that we have contractual agreements with, should a breach occur.
	Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	Stock-Trak has designated employees (including management). IT Specialist receives alerts and determines if an event or incident must be investigated. If escalation is not required, the alert is closed. Events and incidents are investigated and triaged, based on the sensitivity of data and assets involved. The executive team will engage a Cyber Security firm for incidents requiring forensic investigation.
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	The members of the incident response team will maintain an incident response plan that includes steps necessary to contain and mitigate incidents. Stock-Trak already greatly mitigates risk by allowing its customer user base to register accounts without requiring any personal information.
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	Stock-Trak's Incident Response Team will meet to discuss all lessons learned after an incident and update the incident response plan based on the results of a security related incident and the associated activities and results thereof.
RECOVER (RC)	**Recovery Planning (RC.RP):** Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.	Stock-Trak has a well-defined plan in place, outlining key roles and responsibilities in the event of a cybersecurity breach. Our environment is hosted with TierPoint where we perform daily, offsite backups. In the event of a disaster, TierPoint will bring up

Function	Category	Contractor Response
		our environment in one of their secondary data centers where we can restore data from the last daily backup.
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	Stock-Trak's incident response team will discuss all lessons learned after an incident response. The team will review the Incident Response plan on an annual basis to ensure any necessary changes are incorporated.
	Communications (RC.CO): Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).	Stock-Trak's Incident Response Team is responsible for coordinating and managing the communication to all external and internal parties during an incident. In addition, the members of the Incident Response Team will determine next steps for repairing reputational damage and communicate with external stakeholders. Throughout the response and recovery process, the development team and/or the contracted Cyber Security firm will provide timely updates to the team.