Information Security Policy

August 1, 2023

Version	Author	Date	Information Security Policy
1.0	Michael F Frey	8-01-2023	Reviewed by: Michael F Frey
1.1	Michael F Frey	8-01-2024	Reviewed by: Michael F Frey

Table of Contents

Overview

This document outlines the ***Information Security Policy*** and corresponding procedures for True Trade Pro LTD. (the "Company"). This document provides all necessary information for information security governance and management.

1 Information Security Policy

1.1 Security Goals

Information security has been identified by regulators as a very significant and current threat. Information security intrusion and malware infection can be perpetrated by vendors, consultants or our employees or by outsiders that gain access to our computer systems. The Company can also be threatened by information security intrusions and malware infections that take place at our vendors, as well as intrusions and malware infections experienced by the IT systems of our own customers. This supply chain threat has emerged as a critical vulnerability.

Our *Information Security Policy* is intended to prevent and detect intrusions and malware infections, protect the confidential information of our customers, protect the Company's confidential and proprietary information, and provide a response guide should an information security intrusion or malware infection occur. Every employee and consultant must be familiar with and follow the ***Information Security Policy*****.** This Information Security Policy should be read in conjunction with the **Company's *Disaster Recovery and Business Continuity Plan*****.** The policies, procedures and processes that are explained in this document are to help manage and monitor our organization's regulatory, legal, risk environment and operationalize the requirements to inform the management of information security risk.

1.2 Security Strategy

The Company's current business strategy and framework are the basic guidelines for identifying and evaluating information related risks.

To secure business operations at the Company following serious and unexpected incidents, the firm shall ensure the availability of business continuity plans, backup procedures, protection against malicious activities, proper access controls, incident management and regular reporting.

Key goal of this security strategy is to ensure confidentiality, integrity, and availability of the Company information systems. Every employee of the Company is required to comply with the firm's ***Information Security Policy*****.**

2 Roles and Areas of Responsibility

2.1 Information Security Governance

The IT and Operations Committee that reports directly to the Company Board of Directors governs information security protocols for the Company. Information security management is included in the standing agenda for this committee and reviewed on a regular basis. The governance structure supports immediate elevation of potential security threats or availability disruptions to the IT and Operations Committee and the Board of Directors.

2.2 Key Roles and Responsibilities

Board of Directors: The Company Board of Directors provides oversight for the IT and Operations Committee, ensuring proper information security policies and procedures are set forth for the Company.

IT and Operations Committee: The IT and Operations Committee sets information security standards and protocols to minimize risk and vulnerabilities to Company systems, data, and business continuity.

Chief Technology Officer ("CTO"): The CTO provides technical oversight and management of the *Information Security Policy* and corresponding procedures.

Chief Security Officer ("CSO"): The CSO operates as an independent role to the technology organization providing oversight and review of information security policies and procedures.

2.3 Organizational Responsibility

Effective information security is the responsibility of all employees. The Company recognizes that trusted systems are essential to our business and will impart that understanding to all employees.

While it is the responsibility of all employees to follow the information security policies defined herein, we have defined specific responsibilities in the Company to ensure adequate definition, verification, implementation, and assessment of our policies.

3 Principles for Information Security

3.1 Risk Assessment

The Company continuously engages in assessing the risk and evaluating the need for protective measures. Risk assessments identify, quantify, and prioritize risks according to relevant criterion for acceptable risk. The Head of Infrastructure is responsible for ensuring that the risk management processes are coordinated in accordance with the policy. Risk assessments must be approved by the management and/or system owners.

3.2 Risk Management

The Head of Infrastructure shall be responsible for periodically, but no less than semi-annually reviewing the private and public devices we use, the nature of our data, risks identified through cyber intelligence gathering. The IT and Operations Committee will review the current cybersecurity risks and determine the Company's plan to mitigate those risks. The IT and Operations Committee will review semi-annually whether cyber insurance coverage should be obtained or maintained, and the breadth of coverage required. The IT and Operations Committee is also responsible for ensuring that the Company utilizes an intrusion detection process.

3.3 Information Security Policy

The Head of Infrastructure is responsible for distributing documentation about *the Information Security Policy* to the employees. The Head of Infrastructure is also responsible for providing sufficient training for all users and to ensure that all the guidelines and standards are met. The *Information Security Policy* shall be reviewed and updated quarterly or as needed. Detailed technical manuals are developed for infrastructure technology staff for implementation of the policies set forth in this document.

3.4 Classification and Control of Assets

Laptops, thumb drives, and PDAs can easily be lost or stolen. All Company data stored on any such devices must therefore be secured or encrypted. Employees and consultants must immediately report to the Head of Infrastructure upon any such device being lost or stolen for passwords to be disabled, and/or remotely wipe all devices.

The Head of Infrastructure shall be responsible for assuring that all information retained on the Company desktops, laptops, thumb drives, and PDAs are secure or encrypted.

Employees and consultants may not conduct Company business on computers or PDAs that do not secure or encrypt data pursuant to Company requirements and that are not captured by the Company.

Each employee and consultant are responsible for the security of any device on which s/he conducts Company business. If any such device is lost or stolen, the employee or consultant must immediately notify the Head of Infrastructure or member of the Infrastructure Team, who shall take appropriate steps to disable the device. The Head of Infrastructure shall make an electronic log of all such incidents, noting the date, name of the employee or consultant, a brief description of the circumstances, and corrective action taken.

3.5 Information Security for Employees

Employees are expected to understand, and as appropriate, provide signed acknowledgement of relevant security policies. Certain roles may have higher levels of access for both systems and data. In such cases, the employees will be expected to adhere to the policies that are required of their role. Employees believed by the Company to have willfully compromised its information security will be subject to termination. Any employee who interferes with or refuses to cooperate in the investigation of violation of this policy will be subject to discipline, up to and including termination of employment.

Independent reviews will be conducted for all personnel both during the hiring process and periodically throughout a person's employment. Before hiring, all personnel will undergo appropriate background investigations by the Company's human resource department, including driving records, computer crimes, criminal records, employment verification, and education verification. Personnel that are assigned to a sensitive role will have a more rigorous background investigation - including a more detailed financial investigation (e.g., bankruptcy, review, credit reports). The Company will internally handle such investigations yearly as deemed necessary.

Access privileges, both logical and physical, are reviewed when personnel are reassigned or terminated. Working with the Infrastructure Team, the Company will remove all privileges for any terminated employees. As part of the termination process for all staff, the Infrastructure Team will review the access privileges for the terminated employee, and as needed, reassign the privileges to current personnel.

In addition, at the time of an employee transfer, the Company will review the existing access privileges for the employee, changing responsibilities and the required access privileges for the employee's new role. The employees' access privileges will be adjusted accordingly and will be reviewed with the employee.

Periodically the Infrastructure Team will review staff roles and corresponding privileges. This review confirms that all employees are in their defined roles and that their privileges are relevant to that role. Any staff that has changed roles will be handled as above. Furthermore, infrastructure staff will amend access for any personnel privileges that are no longer needed.

3.6 Information Security for Physical Conditions

The Company leverages industry best practices providing the highest level of security available for technology and platforms to protect platform access and confidential data. Included in the Company's security strategy are the following mechanisms for protection:

Penetration Testing - The Company regularly engages independent external vendors to conduct penetration testing with the purpose of identifying technology vulnerabilities. All findings from such tests are properly addressed minimizing susceptibility to external threats.

Network Security - The Company trading platform network is secured through a sophisticated three-tier design with firewalls, intrusion detection monitoring, and IP permissions. The network has been properly hardened at each layer to prevent unauthorized access.

Encryption - The highest levels of encryption are deployed at various layers of the trading platform including network, application, and database.

3.7 IT Communications and Operations Management

Technology operations are managed through specific processes and structures ensuring governance including:

Change Control - Change control policies and procedures are set forth to ensure software is released in a controlled fashion, and properly documented for accountability.

Segregation of Responsibilities - Roles and responsibilities are suitably segregated providing proper oversight for development and testing processes preventing unauthorized code deployment.

Independent External Audits - Independent external audits are regularly conducted with findings thoroughly reviewed and recommended changes incorporated into technology processes to mitigate risk.

Audit Trails - Audit trails exist to track all technology and platform changes providing accountabilities for all changes.

3.8 Access Control

All users, internal and external, must be authenticated before they access any system. Written guidelines are established for access controls and passwords based on business and security requirements. These guidelines shall have connectivity information and restrictions on username and password requirements (frequency of change, minimum length, character types etc.) Where necessary, dual authentication shall be considered. Physical access to information security equipment is strictly monitored and recorded.

External users can access the platform via two entry points, either via a secure website or via an API. Regardless of the entry point, the access is controlled by IP restriction, username, and encrypted password. Connection type includes VPN, SSL based web connection, and a secure private leased line.

Users shall only have access to the services that they are authorized to access and as required by their role in the organization. Access to privileged accounts and sensitive information is heavily restricted. Only personnel who have a specific need to be logged into the system will have system credentials that enable them to login.

3.9 Information Systems Acquisition, Development, and Maintenance

Security is embedded throughout all phases of the system development life cycle, assessed during system acquisition processes, and monitored during system maintenance, including disposal.

As a provider of systems for our clients, Company relies on effective and secure software development process to integrate security controls into the design process and ensure delivery of efficient and secure services to our clients. The Company leverages an Agile Methodology for iterative development. New functionality is fully tested before release into production including unit testing, new functionality testing, and full regression testing. The Company utilizes extensive automated testing to supplement the standardized quality assurance effort. All new software that is released to the production environment is approved through the change control process and deployed by staff segregated from the development staff to ensure proper controls and accountability.
All information systems are maintained and monitored after implementation.

3.10 Information Security Incident Management

Information security incident management for the Company is managed through a structured Incident Management process. The Incident Management process is fully outlined with staff roles and responsibilities, and a defined response and resolution process in the *Incident Management Policy and Procedures* document.

3.11 Continuity Planning

The Company regularly maintains the *Business Continuity and Disaster Recovery Plan* ("BC-DR") documentation that outlines the policies and procedures necessary to allow for continuous and uninterrupted business operations in the event of primary business disruption. The BC-DR is tested company-wide on a quarterly basis, and industry-wide on an annual basis.

3.12 Compliance

The Company shall comply with current laws as well as guidelines from regulators. Clients and employees' personal information shall be safeguarded.

All employees must comply with the *Information Security Policy* and guidelines and IT regulations. Independent audits are regularly planned and arranged with the parties involved.

3.13 Vendor Management

All vendor relationships and engagements are reviewed pre-contract with necessary due diligence on vendor capability and accountability. Vendors are reviewed on a risk-based assessment to ensure that the vendor's cybersecurity procedures are acceptable to the Company.

3.14 Staff Training

All personnel are aware of, receive appropriate training for, and formally acknowledge their security responsibilities. Each member of the Company staff will have their security responsibilities explicitly defined. The staff will be required to formally sign off on their responsibilities prior to assuming them. In addition, Company will define specific training requirements for each role, and any staff placed in that role must complete the training prior to taking on any responsibility.

The following groups will be subject to basic security awareness training before Company authorizes access to its system:

1. Technical staff, including developers and QA team
2. All management level positions
3. Senior executives

High-Security Training for Information System Security Personnel

All positions that demand significant system security responsibilities will complete a more thorough information system security training instead of the basic awareness training. High-security training will cover prevention and procedure for these areas:

1. Logical security for every software component and entry point
2. Information security response protocol
3. Data center infrastructure and security
4. BC-DR plan

Refresher Training

Refresher training, both for the basic and high-level security levels, will be required for all applicable positions once a year.

4 Governing Documents

4.1 Business Continuity and Disaster Recovery Plan

True Trade Pro LTD. regularly maintains the *"**Business Continuity and Disaster Recovery Plan Procedures"*** (available upon request).

4.2 Incident Management Policy and Procedures

True Trade Pro LTD. regularly maintains the Company "***Incident Management Policy and Procedures"*** *(available upon request).*