INFORMATION SECURITY STRATEGY
(INTERNATIONAL TRADING SYSTEM LIMITED)

At the current stage of the technological society development, expansion of the scope of application of the latest information technologies and processes, information security is facing both unprecedented challenges and exceptional opportunities. Continuous attacks are putting the limits of existing capabilities to a test as they become more sophisticated and widespread.

This document of the Company is an Information Security Strategy (the "Strategy"), which defines the system of approaches the Company's management has on the company's information security.

The Company's Strategy's goal is to develop a systemic risk-oriented approach to information security. It involves implementing a set of measures, including studying information security threats, assessing the risk of realisation of the identified threats, developing an information security system from the perspective of a comprehensive application of technical and organisational measures aimed at ensuring the completeness and quality of information protection intended for planning, implementation, control and improvement of information protection system processes.

The Company's information security means the security of the Company's technological and business processes, including its employees, hardware and software for information processing, information, including restricted information not containing classified data, including personal data (the "Information"), the Company's partners' and client' information under conditions of threats in the information sphere.

The Company's strategy serves as the basis for the development of a set of organisational and technical measures to ensure information security, as well as regulatory and methodological documents that ensure its implementation.

The Company's Strategy is the methodological basis for:

- creating and implementing a unified policy related to the Company's information security;
- making managerial decisions and developing practical measures to implement the information security policy and developing a set of coordinated measures of a regulatory, technological, organisational and technical nature aimed at identifying, reflecting and handling the consequences of the realisation of various types of threats;
- coordinating the activities of business units during the work on the development and operation of information systems in compliance with information security requirements;
- developing proposals for improving legal, regulatory, methodological, technical and organisational security in information systems.

The Company's Strategy in terms of countering InSec threats consists in the balanced implementation of complementary information security measures, from organisational measures at the level of the Company's management to specialised InSec measures applicable to each identified information security threat.

The following forms the legal basis for the development of this Company's Strategy:

- legislation governing security, information technology security and information protection, personal data security, trade secrets and other legal acts;
- regulatory acts of the bodies authorised to govern physical security and technical protection of information, countering technical intelligence and ensuring information security and privacy;
- requirements applicable to information security and information protection.

The Company's management is aware of the importance and necessity of developing and improving information security measures and tools in the context of development of legislation and regulations governing financial activities as well as development of implemented technologies and expectations of the Company's clients, as well as other stakeholders.

The Company's management encourages the development of a culture of safe behaviour by their own attitude to compliance with information security principles, which allows the Company to create competitive advantages, ensures its financial stability, profitability and compliance with legal, regulatory and contractual requirements.

The Company develops and controls the information security system in accordance with the following basic principles:

- legality;
- systematicity;
- integrity;
- continuity;
- timeliness;
- continuous and uninterrupted improvement;

- personal responsibility;
- minimisation of authority;
- engagement and cooperation;
- protection system flexibility;
- ease of use of protection tools;
- validity and technical feasibility;
- specialisation and professionalism;
- mandatory control.

Legality

Implementation of protective measures in accordance with the applicable law governing information protection and other regulatory acts on information security approved by state authorities within their competence.

Information systems users and maintenance personnel are aware of the procedure for working with protected information and of the responsibility for violating information security.

Systematicity

Taking into account all the interrelated, interacting and time-varying elements, conditions and factors that are essential for understanding and tackling the issue of information security.

When creating an information protection system, all the weak and most vulnerable points of information systems are taken into account, as well as the nature, possible objects and directions of attacks on systems by violators, ways of breaching distributed systems and gaining unauthorised access to information. The information protection system is built taking into account not only all known channels for breach and unauthorised access to information, but also taking into account the possibility of fundamentally new ways of security threats realisation.

Integrity

Coordinated use of heterogeneous means when constructing an integral protection system that covers all essential (significant) channels of threat realisation and does not contain weaknesses at the "seams" between individual components.

Several protective lines are provided for each channel of information leak and for each security threat. These protective lines are created in a way that requires a potential violator to have professional skills in several unrelated areas in order to breach the protection.

Continuity of Information Protection

Information protection is a continuous, target-driven process involving the adoption of appropriate measures at all stages of an information system's life cycle.

The information system must be in a protected state throughout the entire period of its operation. In accordance with this principle, measures are taken to prevent the transition of the information system to an unprotected state.

Most physical means and hardware used for protection require constant technical and organisational (administrative) support (timely change and ensuring the correct storage and use of logins, passwords, encryption keys, reassignment of authority, etc.) for efficient performance of their functions. Interruptions in the operation of security tools may be used by violators to analyse the protection methods and tools used, to introduce special software and hardware "backdoors" and other means of breaching the security after it will resume its functions.

Timeliness

The proactive nature of information security measures, which means the formulation of tasks related to comprehensive protection of information systems and the implementation of information security measures at early stages of information system development.

Continuity and improvement

Continuous improvement of information protection tools and measures based on the continuity of organisational and technical solutions, personnel, analysis of information systems' functioning taking into account changes in information interception tools and methods, regulatory requirements applicable to protection and experience gained in this area.

Personal Responsibility

Assigning responsibility for ensuring security of information and the information processing system it to each employee within their authority. In accordance with this principle, the rights and duties of the Company's employees are distributed in a way that minimises the circle of alleged violators and makes this circle clearly known in case of any illegal action.

The Principle of Authority Minimisation

Providing information system users with minimal access rights in accordance with the business necessity in accordance with the "everything that is not allowed is prohibited" principle.

Access to information is provided only in the case and to the extent necessary for the employee to perform their job duties.

Engagement and Cooperation

Creating a favourable atmosphere within the Company's units that ensure information systems operate to reduce the likelihood of negative actions related to the human factor.

In such an environment, employees must consciously comply with the established rules and assist the activities of units that ensure technical protection of information.

Information Protection System Flexibility

The measures taken and the established information protection tools (systems), especially in the initial period of their operation, can provide both an excessive and insufficient level of protection. To ensure the possibility of varying the level of protection, information protection tools (systems) must have certain flexibility. This is especially important in cases when the information protection tools (systems) must be installed for a working system without disrupting its normal functioning.

Validity and Technical Feasibility

Information technologies, hardware and software, information protection measures in information security systems are implemented at the current level of development of science and technology; they are justified from the point of view of achieving a given level of information security and the accepted risk appetite, and they must comply with the established information security standards and requirements.

Specialisation and Professionalism

Involvement in the development of tools and implementation of information protection measures of specialised organisations that are most prepared for a specific type of information security activity, have practical experience and a state license to provide services in this area. Implementation of administrative measures and the operation of information protection tools (systems) is carried out by trained professionals.

Mandatory Control

The obligatory nature and timeliness of identifying and suppressing attempts to violate the established rules for ensuring information security on the basis of information protection tools and systems used while improving the criteria and methods for evaluating the efficiency of these systems and tools.

Control over the activities of any user, each information protection tool (system) and in relation to any object of protection is carried out on the basis of prompt control and registration tools and covers both unauthorised and authorised user actions.

Implementation of the Company's Strategy will allow to:

– assess the state of information security in information systems and business processes, identify sources of internal and external threats to information security, identify priority areas for preventing, warding off and neutralising these threats;

– develop administrative, regulatory and methodological documents in relation to processes and information systems;

– carry out organisational, mode-setting and technical measures to ensure the security of information in information systems;

– ensure the necessary level of security for protection objects.

The implementation of these measures will ensure the creation of a unified and coordinated protection system and create conditions for its further improvement.