TurnKey Lender

INFORMATION SECURITY POLICY

Produced by the TurnKey Lender Working Group on Security

REVISION HISTORY

Date	Version	Description	Author
19.11.2019	V1	Initial document creation	Olena Tkachova
17.11.2020	V2	Policy improvements and detailing	Kseniia Nazarenko
15.11.2021	V3	Policy improvements and revision	Kseniia Nazarenko
22.06.2022	V4	Policy improvements	Kseniia Nazarenko
19.06.2023	V5	Update section Regulation compliance	Kseniia Nazarenko
29.09.2023	V5	Redesign according to new brand guidelines	Kseniia Nazarenko

DOCUMENT REVIEWERS AND APPROVAL

Approval Date	Position/Email	Reviewer Name	Version Approved
19.11.2019	CEO	Dmitry Voronenko	V1
18.11.2020	CEO	Dmitry Voronenko	V2
19.11.2021	CEO	Dmitry Voronenko	V3
24.06.2022	CEO	Dmitry Voronenko	V4
28.06.2023	CEO	Dmitry Voronenko	V5

CONTENT

INTRODUCTION

The document provides a security framework that ensure the protection of information from unauthorized access, loss or damage while supporting the open, information-sharing and storing needs of business demands and providing by the Turnkey Lender LLC (hereinafter - the Company).

A systematic presentation of high-level goals and objectives of the protections guided in their activities, as well as basic principles of building an information security management system (hereinafter - ISMS) are drown in the document.

SCOPE

The Policy applies to all employees of the Company, as well as other individuals and entities granted use of the Company information, including, but not limited to, contractors, temporary employees, and third-party vendors.

To meet legal and professional requirements and satisfy obligations of all the Company clients. The Policy of the practice is to accept willingly all obligations in respect of information security and to protect its information resources by implementing recognized best practices that will achieve a balance between cost and risk.

The Information Security Policy applies to all forms of information including:

- Speech, spoken face to face, or communicated by phone or radio;
- Hard copy data printed or written on paper;
- Information stored in manual filing systems;
- Communications sent by post / courier, fax, electronic mail;
- Stored and processed via servers, PCs, laptops, mobile devices,
- Stored on any type of removable media, CDs, DVDs, USB memory sticks, digital cameras.

MAIN GOAL

The main goal is to ensure the uninterrupted functioning of the software and hardware environments crucial to business operations, to stop unauthorized use of information and information systems, to prevent intentional or unintentional destruction or distortion of information, and to minimize the caused damage.

OBJECTIVES

Resource protection

- To protect the providing information. The availability of complete and accurate information is essential for providing products and services to customers.
- To hold and process confidential and personal information on private individuals, employees, partners and suppliers and information relating to its own operations.
- To safeguard sensitive information and prevent its misuse while receiving, holding and processing client customer and staff data.
- To assure that sensitive information remains private and is not visible to an eavesdropper.

Authentication and Authorization

- To assure that attendees (human or machine) are clear about their roles in using the information and to verify that the resource (human or machine) at the other end of the session really is what it claims to be.
- To assure that attendees (human or machine) at the other end of the session has permission to carry out the request.
- To work with trusted/certified software vendors and maintainers to prevent vulnerabilities in third party open and closed source software.

Data integrity maintain

- To assure that arriving information is the same as what has been sent out and data is protected from unauthorized changes or tampering.
- To assure that consistent and expected results with expected performance are provided.

Auditing security activities

- To monitor security-relevant events to provide a log of both successful and unsuccessful (denied) access.
- To ensure business continuity and minimize business damage. The Company has a responsibility to suspicious activity on networks, systems, applications and follows formal incident response processes to recognize, analyze, and remediate information security threats.

Regulation compliance

- ISO/IEC 27001:2022 and risk management
- ISO/IEC 27002:2022 clauses and controls
- ISO/IEC 27017:2015
- ISO/IEC 27018:2019
- GDPR 2016

Organization of Information Security

- The CEO reviews and makes recommendations on the security policy, policy standards, directives, procedures, Incident management and security awareness education.
- Regulatory, legislative and contractual requirements are incorporated into the Information Security Policy, processes and procedures.
- The Company works towards implementing the ISO 27000 standards, the International Standards for Information Security.

- All breaches of information security, actual or suspected, must be reported and will be investigated.
- Business continuity plans is produced, maintained and tested
- Information security education and training will be made available to all staff and employees.
- The security of information is managed within an approved framework through assigning roles and coordinating implementation of this security policy across The Company and in its dealings with third parties.
- Specialist external advice is drawn upon where necessary to maintain the Information Security Policy, processes and procedures to address new and emerging threats and standards.
- The CEO is responsible for ensuring that all staff and employees, contractual third parties and agents of The Company are made aware of and comply with the Information Security Policy, processes and procedures.
- The Company auditors review the adequacy of the controls that are implemented to protect The Company information and recommend improvements where deficiencies are found.
- All staff and employees of The Company, contractual third parties and agents of The Company accessing The Company information are required to adhere to the Information Security Policy, processes and procedures.
- Failure to comply with the Information Security Policy, processes and procedures will lead to disciplinary or remedial action.

Human Resources Security

- The CEO ensures that all contracts of employment and any contracts of agency staff include a 'non-disclosure' clause.
- Security responsibilities are included in job descriptions and in terms and conditions of employment.
- Verification checks are carried out on all new employees, contractors and third parties.

Hardware and Software Environment Security

- Critical or sensitive information processing facilities housed in secure areas.
- The secure areas protected by defined security perimeters with appropriate security barriers and entry controls.
- Critical and sensitive information physically protected from unauthorized access, damage and interference.

Information Security Incident Management

- Information security incidents and vulnerabilities associated with information systems is communicated in a timely manner. Appropriate corrective action will be taken.
- All employees, contractors and third-party vendors is made aware of the procedures for reporting the different types of security incident, or vulnerability that might have an impact on the security of The Company assets.
- Information security incidents and vulnerabilities is reported as quickly as possible to the CEO.