Purpose

This document, the Information Security Policy of PJSC Softline (hereinafter referred to as the Policy), is the fundamental document defining the position, goals, objectives, and principles of PJSC Softline (hereinafter referred to as Softline) and its subsidiaries and affiliates (hereinafter referred to as S & A) in the area of information security. PJSC Softline and its S&A are hereinafter referred to as Softline or the Group.

General Provisions

Information security (IS) is the ability of information to maintain confidentiality, integrity, and availability. Furthermore, this concept can also include the ability to maintain authenticity, accountability, non-repudiation , and reliability.

For the purposes of this Policy, information assets include employees, information, business reputation, material assets, and business processes.

Softline's information security activities are based on the Group's development strategy, and the tasks it addresses contribute to the effective and secure development of Softline's business in the modern world of digitalization and digital transformation.

Validity period and amendments

This Policy is a local regulatory document of permanent effect. This Policy is approved, amended, and repealed by the General Director of PJSC Softline . The Policy is reviewed regularly, at least annually, or as needed.

Declaration of Information Security

By adopting the Policy, Softline declares and undertakes to implement appropriate measures to protect information assets from the risk of harm and losses arising from the implementation of information security threats.

Softline's management recognizes the importance and necessity of improving information security measures and tools in the context of evolving information security legislation and the increasing sophistication of information technologies.

Softline's management considers the geopolitical situation as a key factor in information security risk management, taking measures to protect against threats arising from political instability, sanctions regimes, international conflicts, and changing legislative requirements in different countries.

Softline's management initiates and oversees work in the field of information security.

Compliance with information security principles, rules and requirements is an element of the Group’s corporate culture.

Softline's information security managers and specialists must fulfill their duties responsibly, recognizing that the quality of their work directly impacts the security of the Group's information assets.

Softline employees must be guided by this Policy in their professional activities, interactions with external contacts, internal corporate interactions, personal development, and improvement of the information security culture.

Softline employee is responsible for compliance with all local regulatory documents in the field of information security.

Interaction with counterparties is regulated by legislation and concluded agreements.

Achieving information security goals while adhering to the principles will further strengthen competitive advantages, ensure compliance with legal, regulatory, and contractual requirements, and reduce the risks of loss of business reputation or damage to business reputation.

Information security objectives

Softline's information security management and support is aimed at achieving the following goals:

- Providing a secure information environment for business operation and development.
- Increasing competitiveness, business value and preserving business reputation for shareholders by reducing the level of information security risk.
- Compliance with legal requirements in the field of information security and personal data protection, as well as compliance with relevant contractual obligations.
- Improving the corporate culture of processing and protecting information, including personal data.
- Effective management of information security processes and continuous improvement of the information security management system.

Tasks in the field of information security

To achieve the goals, Softline has adopted the following tasks in the field of information security:

- Design, implementation and continuous improvement of the information security management system (hereinafter referred to as the ISMS).
- Softline's top management in the process of functioning of the ISMS.

Information security issues are regularly reviewed by authorized committees and/or working groups.

- Efficient use of resources allocated for information security. Cost effectiveness assessment.
- Ensuring the security of information assets Softline .
- Compliance with legislation, regulatory requirements in the field of information security and personal data protection.
- Improving technical, organizational and legal protection measures.
- Formation, accumulation, and development of competencies in the field of information security and personal data protection.

- Using a risk-based approach. Softline regularly conducts information security risk assessments and measures to improve the security of information assets.
- Information security incident management. Softline continuously improves its incident response mechanisms.
- Raising employee awareness. Softline employees regularly undergo mandatory information security training.
- Formalization of information security requirements. Requirements are recorded in local regulations and communicated to employees.
- Incorporating information security requirements into project activities. Information security requirements are developed and documented at the initial stages of project implementation.
- Employee background checks. All candidates for vacant positions undergo background checks in accordance with established procedures.
- Monitoring and continuous improvement of the ISMS based on the results of periodic audits (inspections).

Principles of information security

Softline defines the following principles for ensuring information security:

The principle of systematicity

Assets are viewed as interdependent components of a single system. The interactions between components are taken into account when analyzing information security risks and threats.

The principle of completeness (complexity)

To ensure information security, a wide range of measures, methods, and means of protection are used, the integrated use of which ensures the neutralization of current threats and the absence of vulnerabilities at integration points.

The principle of echeloning

Relying on a single line of defense is unacceptable. An information security system is designed so that the most protected security zone is located within other protected zones.

The principle of equal strength

The effectiveness of protective mechanisms should not be undermined by a weak link resulting from underestimation of threats or the use of inadequate protective measures.

The principle of continuity

Ensuring information security is a continuous, targeted process that involves taking protective measures at all stages of the asset life cycle.

The principle of reasonable sufficiency

"Absolute" asset protection is impossible. The selection of security measures adequate to current threats is based on a risk analysis.

The principle of legality

When selecting and implementing information security measures, Softline strictly adheres to applicable legislation and the requirements of regulatory legal and technical documents in the field of information security.

Controllability principle

The processes of ensuring and improving information security must be manageable, i.e. it is necessary to monitor, measure parameters and promptly adjust the processes.

The principle of personal responsibility

Responsibility for ensuring information security is assigned to each employee within the limits of his or her authority.

Liability for Violation of the Policy

Softline employees are required to comply with information security requirements and rules when working with information and information assets of the Group, its partners, and contractors.

Softline's high corporate standards and information security rules are mandatory for all Group employees without exception and must be taken into account in relationships with partners and contractors.

When using the Internet, communicating on social networks and instant messengers, using email, and other electronic means and communication platforms, Softline employees should exercise caution and restraint.

Each Softline employee shall bear disciplinary, civil, administrative, and criminal liability for failure to comply with information security requirements in accordance with applicable law.

Softline's information assets , as well as the information provided to them, are liable in accordance with contractual provisions and applicable law.

Appendix. List of minimum requirements for policy implementation at Softline PJSC and its subsidiaries and affiliates

This appendix to the Information Security Policy contains a list of minimum requirements for compliance with the Policy at Softline PJSC and its subsidiaries and affiliates, including requirements for the development and implementation of their own information security

policies and other regulatory documents related to information security. The General Directors of the subsidiaries and affiliates are responsible for compliance with the minimum requirements.

Organizational measures

Softline implements the following organizational measures to protect information security:

- Develops, approves at the management level and regularly updates the information security policy in accordance with the Softline security policy , as well as other applicable standards and requirements, taking into account the specifics of the subsidiaries and affiliates.
- Implements access procedures in accordance with the principle of least sufficient rights.
- Develops and enforces password protection policies for all users and service accounts. Password protection policies include requirements for password complexity, password change frequency, and password storage.
- By order of the organization's CEO, appoints persons responsible for information security, the security of personal data processing, and ensuring the security of personal data in personal data information systems (PDIS). These persons are responsible for compliance with information security requirements and the protection of personal data in accordance with the law.
- Organizes regular information security training for all employee categories. Training topics should cover current threats, including preventing phishing attacks, secure use of corporate resources, working with personal data, compliance with internal information security policies, and more.
- Organize regular testing of employees' knowledge of information security requirements. Test results should be used to identify knowledge gaps and guide further training.
- Ensures regular and timely updating of employees on new threats, information security incidents, and changes to company policies or procedures. This may include newsletters, publications on the corporate portal, webinars, etc.
- Ensures that new employees are informed of existing information security requirements during the hiring process.

Technical protection measures

Softline implements the following technical information security measures:

- Implements anti-malware protection measures, including installing and regularly updating anti-virus software on all workstations and servers.
- Scans all incoming email traffic for malicious attachments and links.
- Ensures regular automatic installation of software security updates for workstations and servers. If automatic installation is not possible, updates must be installed manually and monitored.
- Creates and stores backups of critical systems and data in an isolated environment. Regularly tests backup recovery to ensure data availability in the event of an incident.
- Implements network traffic control tools (firewalls) to ensure the security of network resources.

- Uses cryptographic methods to protect information when interacting with Softline information systems to ensure data confidentiality and integrity.

APPROVED

General Director of PJSC Softline V. Lavrov

Board of Directors of PJSC Softline (Minutes No. 05/25 dated May 21, 2025)