Information Security Policy

Purpose

This Policy is the main document regulating the activities of Softline Group in the field of information security

Corporate requirements in the field of information security are applied to all production regions and all business units of Softline Group.

General provisions

Information security is a state of data protection, characterized by the ability of staff, technical facilities and information technology to ensure confidentiality, integrity and availability of information when processing by technical means.

Information Security Policy was developed in accordance with the provisions of ISO / IEC 27001: 2013.

Information Security Policy is approved by the Chairman of the Board of Directors of Softline Group.

Policy shall be reviewed regularly at least once a year.

Information security objectives

In the field of information security Softline Group established the following strategic objectives:

- Improving the competitiveness of business of Softline Group;
- Compliance with the requirements of legislation and contractual obligations in terms of information security;
- Improving business reputation and corporate culture of Softline Group;
- Effective information security management and continuous improvement of information security management system;
- Achieving adequate protection measures against information security threats;
- Ensuring the security of corporate assets of Softline Group, including staff, material and technical values, information resources, business processes.

Information security challenges

Information security system of Softline Group should solve the following tasks:

- Involvement of senior management of Softline Group in the process of ensuring information security: information security activities initiated and monitored by senior management of Softline Group;
- Compliance with the requirements of Russian Federation legislation: Softline Group implements information security measures in strict compliance with current legislation and contractual obligations;
- Coherence in order to ensure information, physical and economic security: actions to ensure information, physical and economic security are carried out on the basis of a well-defined

cooperation between the involved departments of Softline Group and are agreed among themselves on the objectives, tasks, principles, methods and means;

- Application of cost-effective measures: Softline Group aims to choose information security measures taking into account their implementation costs, the likelihood of information security threats and the size of possible losses from their implementation;
- Checking of workers: all candidates for the vacant positions in Softline Group must necessarily be checked in accordance with established procedures;
- Documentation of information security requirements: in Softline Group all the requirements in the field of information security are fixed in the developed internal regulatory documents;
- Raising awareness of information security: the documented requirements in the field of information security are communicated to the employees of all business units of Softline Group and contractors with respect to the part related to them.

Information security principles

Systemic approach

In Softline Group assets are considered to be interrelated and mutually influencing components of a single system. In case of information security threats, the maximum possible amount of system behavior scenarios is taken into the account. The protection system is built taking into account not only all known channels of obtaining unauthorized access to information, but also considering the possibility of appearance of fundamentally new ways to implement security threats.

Complexity approach

A wide range of measures, methods and means of information protection is used in order to ensure information security. Their complex using implies the coordination of heterogeneous means in constructing the integrated protection system which blocks all the existing channels of threats and containing no weaknesses at the junctions of its separate components.

The Separation Principle

One cannot rely on a single protective line, no matter how safe it may seem. Information security system is constructed in such a way that the most protected security zone is placed inside other protected zones.

The principle of equal strength

The effectiveness of protection mechanisms must not be reduced to nothing by a weak link, arising as a result of underestimation of the real threats or the use of inadequate protection measures.

The Principle of Continuity

In Softline Group the ensuring of information security is a continuous and purposeful process, which implies taking the appropriate measures at all stages of the asset lifecycle.

The principle of reasonable sufficiency

Softline Group Management assumes that it is impossible to create an "absolute" protection of assets. Therefore the choice of means of assets protection adequate for real existing threats (i.e. providing the allowable level of potential damage in case of threats implementation) and is based on risk analysis.

The principle of legality

During the selection and implementation of measures and means to ensure the information security of the Softline Group strictly observes the legislation of the Russian Federation, the requirements of normative legal and technical documents in the field of Softline Group information security.

The controllability principle

All information security management and assurance processes in Softline Group must be controlled, i.e., it should be possible to monitor and measure the processes and components, to identify in time the information security violations and to take appropriate measures.

The principle of personal responsibility

Each employee is responsible for ensuring the assets safety within his powers.

Responsibility for violation of Information Security Policy

In case of violation of the established rules of work with the information assets the employee may be limited to access rights to such assets, and brought to justice in accordance with the Labour Code, the Code of Administrative Offences and the Criminal Code of the Russian Federation.

S.V. Chernovolenko,

Global CEO of Softline