Ensuring the security of the Softline Group of Companies (hereinafter referred to as Softline) in the context of its expansion into new areas and regions puts effective risk management in the area of security and protection from internal and external threats among the key factors for successful development.

In this regard, Softline undertakes to take all possible measures to protect its assets, namely personnel, material resources, information, business reputation, and business processes from the risk of harm, loss, and damage that may arise as a result of illegal activities.

Responsibility for ensuring security lies with the management of Softline and its business units.

The organization and direct implementation of the necessary security measures and their improvement is assigned to the Softline Security Department , whose main tasks are the continuous identification and assessment of internal and external threats to Softline security and an adequate response to them in conjunction with the heads of business units.

The Security Department develops security procedures and standards in accordance with corporate requirements (appendix to this Policy) and monitors their implementation by business unit managers and Softline employees . The Security Department Director's orders on matters within his or her purview are binding on business unit managers and Softline employees .

Softline employees must strictly adhere to the Corporate Security Requirements and promptly report to their functional manager any violations of Russian law, corporate policies, standards, and procedures, unethical behavior, or conflicts of interest that become known to them.

Softline's security is based on the principles of legality, respect for and observance of human and civil rights and freedoms, cooperation and mutual understanding, and personal responsibility. In all its interactions with organizations and individuals, Softline welcomes their commitment to the principles contained in this Policy.

General Director of the Softline Group of Companies
Lavrov V.E.

Corporate Security Requirements for Softline

Softline's corporate security requirements apply to all regions of operation and all Softline business units .

Business unit managers are responsible for ensuring the security of the Company's assets. Together with the Security Department, they conduct risk assessments and develop and implement measures and methodologies to ensure effective security risk management. All measures taken must comply with Softline's Security Policy and corporate ethics standards.

Softline maintains an open dialogue and consultation with all interested organizations and citizens to identify and resolve issues that may arise as a result of its activities, as well as to ensure effective security risk management.

The Vice President of Security provides expert assessments on strategic security issues to Softline's senior managers , coordinates the development of security standards and procedures, and oversees their implementation by business unit managers and Softline employees .

Security risk assessment is carried out on a regular basis at least once a year in all Softline business units .

Security measures are based on a comprehensive risk assessment and must be proportionate to those risks and cost-effective. Security requirements apply to all corporate assets, including personnel, inventory, information resources, and business processes, and are taken into account during the planning and implementation of all Softline projects .

Business unit managers, in conjunction with the Security Department, develop and implement an effective security management system, allocating resources and responsibilities to ensure that all Softline employees and partners understand the need to comply with these Security Requirements.

All candidates for vacant positions at Softline and its business units are subject to mandatory screening in accordance with established procedures.

When concluding any contract or agreement, the Security Department conducts a thorough check of potential counterparties in accordance with established procedures and makes its conclusion on the advisability of entering into contractual relations with them.

All security incidents are recorded and subject to internal investigation. If necessary, appropriate legal (disciplinary) measures are taken against violators.

The Director of the Security Department must be informed by the heads of business units about all security incidents that could significantly complicate Softline's operations or cause significant damage to its business reputation.

The Security Department is responsible for conducting all internal investigations into instances of illegal attacks on Softline assets , violations of corporate policies, standards and procedures.

Where appropriate, the Security Department, in coordination with business leaders, will coordinate with law enforcement and other government agencies, local governments, third-party organizations and their security services to ensure the security of Softline assets .