Information security and data protection

We are committed to maintaining stability and reliability among our portfolio companies and make every effort to protect the personal information of our employees and customers from leakage, theft, or loss.

The Fund has organized an Information Security Committee, which provides recommendations on ensuring information security in portfolio companies and maintains constant interaction with government agencies and other stakeholders to address security issues in the information space better.

The Fund has implemented the "Basic Rules of Information Security Policy" with applications in the form of methods, guidelines, and rules that cover the required activities of information security and IT specialists and all employees to implement measures to ensure information security. GRI 3-3

Work is underway to develop a Corporate Information Security Standard that regulates a general set of rules for ensuring information security and managing the process of coordinating activities in the Fund's group of companies. There are procedures for providing information security, resolving incidents, managing user access to information systems, etc. GRI 3-3

A cybersecurity risk register is formed annually, and a risk report is generated quarterly, including regarding the Fund's group of companies.

In 2023, audits of the Fund's portfolio companies were conducted to ensure compliance with information security requirements, and recommendations were developed for bringing into compliance and increasing the level of information security.

Our principles for minimizing information security risks are:

- rapid identification, analysis, and forecast of threats in IT that can negatively affect the stability and reliability of the Fund;
- assessment of the impact of adverse factors;
- prioritization of information security requirements;
- continuity of information security;
- controllability and effectiveness of measures.

Measures have been initiated to implement the international information security standard ISO 27001 at the Fund. A working group has been created to take part in the formation of a register of information assets and classify assets according to degrees of significance.

Also, to maintain users' cyber hygiene, the Fund's employees are trained and tested using specialized software.

We provide data protection based on the Monitoring Center created to support information security systems from external and internal threats to the IT infrastructure in the conditions of the Fund and the operational information security center of QazCloud LLP. Companies in the Fund Group continue to improve their information security systems. As part of the engagement, policy issues and projects to improve the level and ensure information security in portfolio companies were considered.

Ensuring the security of information systems is becoming increasingly important in the context of digital transformation and growing cybersecurity threats. Our efforts, in particular, aim to protect customer data's confidentiality.

The total number of information security incidents was 16,094 in the reporting year, with malware detection and unauthorized access/hacking accounting for 49%. All incidents are processed on time, preventing leakage of customer data. There were no incidents related to customer data