Information security and data protection

GRI 418-1 We aim to develop a robust information security management system that encompasses strategies, methods and processes for protecting information and IT assets from unauthorised access and risks that could compromise the confidentiality, integrity or availability of information.

The key strategic objectives of the Fund in the field of information security are to ensure availability, integrity, confidentiality and fault tolerance.

Our principles for minimising information security risks:

- promptly identify, analyse and forecast the development of threats in information technologies that may adversely affect the stability and reliability of the Fund's operations;
- assessing the impact of unfavourable factors;
- prioritisation of information security requirements;
- continuity of information security;
- controllability and effectiveness of measures.

The Fund has an Information Security Committee, which is responsible for developing recommendations aimed at improving the level of information security and maintains constant interaction with government agencies and other stakeholders to better address these issues.

GRI 3-3
GRI 418-1 For a systematic approach in this area, we have developed and implemented the Basic Rules of Information Security Policy, which include methodologies, instructions and rules. These documents are aimed at ensuring compliance with security requirements both by information technology specialists and all other employees of the Fund.

Some of the portfolio companies have implemented Information Security Policies, which are developed taking into account the specifics of their activities and oriented to the best international practices in the field of information security. For example, to ensure information security and protection of customers' personal data, Kazakhtelecom JSC, which provides telecommunications services to thousands of Kazakhstani citizens, adheres to a comprehensive approach: it maintains round-the-clock control of data at all stages of their life cycle, starting from the moment they enter the company's infrastructure and ending with their archiving or irretrievable destruction. In addition, the company uses such security elements as incorporation into the state cybersecurity system ESDI (unified gateway for Internet access), security of the Internet of Things, use of Honeypot traps (allows to study the attacker's strategy and determine the list of means by which real security objects can be struck), use of Machine Learning technologies and a number of other tools.

GRI 3-3 As part of improving the information security system, we have implemented the Corporate Information Security Standard, which covers all the basic principles and rules aimed at ensuring data protection and coordination of actions within the Fund's Group. The Corporate Standard is mandatory for the implementation of information security processes for the Fund and its portfolio companies.

In 2024, the Fund continued to strengthen information security consistently. In particular, we:

- started preparations for the introduction of best practices in information security management of the international standard ISO 27001;
- improved reliability and efficiency of the IT infrastructure. Technical and organisational measures were implemented to ensure stable and secure operation of information resources in accordance with modern IS requirements.
- implemented a range of solutions to protect against external and internal threats, including the introduction of modern software products and tools to prevent information leaks, vulnerability scanning and real-time threat analysis;
- conducted information security audits in two portfolio companies (NGK Tau-Ken Samruk JSC and Samruk Kazyna Construction JSC) as part of control and improvement of cyber resilience. Based on the results of the audits, recommendations were given to eliminate the identified risks;
- held training events and courses on information security for employees aimed at developing a safety culture when working with IT systems and corporate data.

GRI 418-1 The total number of reported incidents related to information security in the Reporting Year was 25,240, which is 57% higher than in 2023 (16,094 in 2023). Malware detection and unauthorised access/hacking attempts accounted for about 60% of cases. No customer data breaches were detected in the portfolio companies in the reporting period.