Information Security and Data Protection

Information security and data protection support business resilience and the continuity of the Fund's operations. Amid digitalisation and rising cyber threats, the Fund manages the protection of information assets on the basis of a unified Corporate Information Security Standard, which sets out requirements for protection architecture, risk management, internal audit and the segregation of access rights.

In 2025, we continued developing the system using a risk-based approach in line with the requirements of ISO 27001. We analysed and optimised the IT infrastructure and assessed the level of protection and process maturity. The results confirmed formalised processes, the allocation of responsibilities and the operation of a system that informs management on key information-security matters.

In terms of infrastructure protection, an inspection of IT systems was carried out, potential points of failure and vulnerabilities were identified, and external web resources were optimised using OSINT analysis. Black-box security testing was carried out, covering internal infrastructure, adjacent systems and employee resilience to social-engineering attacks.

Medium-severity vulnerabilities identified have been remediated; no material compromise scenarios capable of leading to loss of control over the infrastructure were detected. To improve fault tolerance, the placement of server and network equipment has been optimised, geo-redundancy has been provided for critical infrastructure, and modern solutions have been introduced for monitoring information-security events, preventing data leakage and scanning for vulnerabilities.

An important element of the cyber-resilience system is centralised monitoring and incident response. To counter cyberattacks, the Fund Group is delivering the CyberShield ("Kibershchit") project on the basis of QazCloud LLP, providing 24/7 monitoring of information-security incidents in the Fund and portfolio companies.

The Fund regularly scans the infrastructure using specialised licensed software, maintains lists of risk sources and cybersecurity events, and prepares regular risk reports.

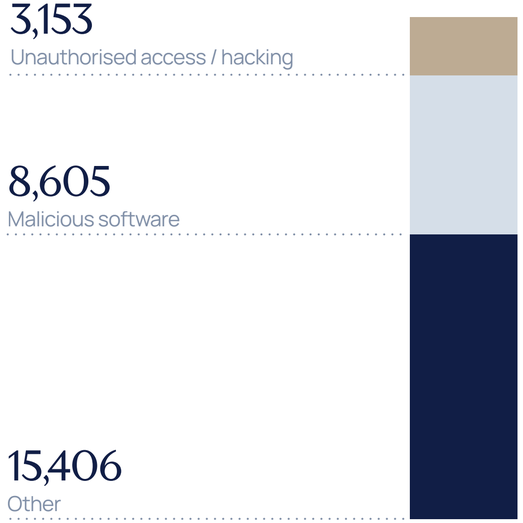
Under the corporate standard, portfolio companies submit information on incidents quarterly; this is analysed both at the level of the companies themselves and at the level of the Fund. This provides centralised control and the timely adoption of measures to mitigate threats to the confidentiality, integrity and availability of information systems.

In 2025, the Group recorded 27,164 incidents, an increase of 8.05% on 2024. The growth is due primarily to the expanded scope of monitoring and the higher sensitivity of detection systems. By severity, incidents of low and medium severity predominate, indicating a high share of events detected at an early stage.

The principal concentration of incidents was observed in a number of large Group organisations, including JSC NC Kazakhstan Temir Zholy (KTZ), NC QazaqGaz JSC, NC KazMunayGas JSC, and certain Group IT companies.

In the reporting period, 9,194 employees received data-security training, with more than 40% trained on programmes exceeding the mandatory requirements of the legislation of the Republic of Kazakhstan. The total volume of training was 17,077 hours across 113 training sessions, corresponding to an average of 0.54 hours per employee. This approach not only met regulatory requirements but also substantially raised the level of information security culture through the adoption of cybersecurity best practices.

Number of information-security incidents in 2025



9,194 EMPLOYEES

received safety training during the reporting period

17,077 HOURS

total volume of educational activities

~0.54 hours per employee

GRI 3-3