Information policy and security

IN 2023, KEGOC JSC CONTINUED TO IMPLEMENT ITS INFORMATION POLICY IN ORDER TO COMPLY WITH THE PRINCIPLES OF EQUITABLE, COMPLETE, RELIABLE AND PROMPT DISCLOSURE OF INFORMATION TO STAKEHOLDERS.

KEGOC JSC successfully conducted a secondary share placement (SPO) and as part of the information support of the issue, the Company actively interacted with the investment community and a wide audience of potential investors. Thus, in the reporting period, in addition to timely disclosure of information affecting the interests of shareholders and investors, the Company held a number of events for the media: briefings, interviews, 'Issuer Day' on the KASE platform, during which investors, professional securities market participants and media representatives familiarized themselves with the results of the Company's activities, the implementation of strategic plans and investment projects.

In order to create a positive investment image, KEGOC JSC continued to provide information and analytical services, build trusting relations between the Company and the expert community, investors and shareholders. To ensure promptness and accessibility of information essential for users, KEGOC JSC ensured publication in mass media, as well as on the corporate website and the Company's pages in social networks Facebook, Instagram, Telegram and Twitter of materials on production and financial activities, results and achievements over 26 years of the System Operator's operation, including the past forum of veteran power engineers, issue of 'green' bonds, early repayment of credit loans, inclusion of new 220 kV lines in the project of strengthening of power grids of the Company. Interviews and speeches of top management were also organized, and public hearings were held with the participation of interested parties to widely cover investment activities, implementation of the set tasks and achievements of the Company in various areas of activity.

When disclosing information, KEGOC JSC is guided by the protection of information constituting commercial, official and other secrets protected by the legislation, as well as information of restricted circulation.

Information security

The main purpose of information security (IS) activities is to ensure and improve the security of KEGOC JSC information assets, as well as to coordinate, plan and organize information security activities, including effective strategic IS management and increasing the maturity level of IS processes.

KEGOC annually undergoes internal and external audits of the information security management system (ISMS) for compliance with the international standard ISO 27001.

The ISMS is developed and implemented on the basis of ISO/IEC 27001:2013 and is an integral part of the Company's integrated management system.

The scope of application of the ISMS in KEGOC JSC is the information system of process management of the financial and economic block of KEGOC JSC, which ensures fulfilment of the main and auxiliary business processes.

To meet the requirements and define the Company's context, the Information Security Policy was approved.

In accordance with the information security regulations established in KEGOC JSC, work was carried out to analyse new criteria for information assets that are of value to KEGOC JSC. In 2023, KEGOC JSC will continue to strengthen measures to ensure the security of information assets.

Key achievements

Based on the results of the external audit for 2023, KEGOC JSC received a certificate of compliance with the international standard ISO 27001, which confirms that the Company meets high standards of information security management. This is a significant step towards ensuring the security of the Company's information systems and data.

By the end of 2023, all IS systems are working properly. The Company's cyber-attack defence systems are continuously monitored to ensure that they remain operational. IS system policies (DLP, SIEM, CyberArk) are updated. The corporate network is checked weekly using anti-virus software. The Company's protection system (Kaspersky) successfully detects and repels malicious software (encryption viruses). Confidential data is analysed and phishing mailings and spam are blocked using the data leakage prevention (DLP). At the moment, work is underway to customise the policies of the anti-virus software and DLP system.

The Information Security Division of the Security Department of KEGOC JSC, jointly with the employees of QazCloud LLP, carried out activities to expand the monitoring zone of ISOC. To date, the corporate network of the Company is fully connected to the UCIB (full connection to the Cyber Shield of Samruk-Kazyna JSC was made). The audit of authorised software in the Company within the framework of the approved Register of software used in KEGOC JSC was carried out.

In 2023, the Company's protection system (Kaspersky) detected and successfully removed malicious software related to viruses, worms and illegitimate software. Due to the measures taken to detect and remove viruses, there was no need for an internal audit. Phishing emails related to cryptocurrencies were blocked.

Awareness-raising

In accordance with the ISMS requirements, the Company has adopted a unified corporate ethics in IS matters, which supports employee awareness.

KEGOC JSC ensures appropriate competence (education, training, experience) of the personnel responsible for IS provision by means of technical training, special training at advanced training courses, briefings; a system of professional training and professional development of the personnel is also implemented.

In 2023, the following trainings were conducted for the Company's employees:

- What IS is;
- IS password protection;
- IS email;
- IS antivirus protection;
- IS Updates;
- Social Engineering.

In addition, in 2023, for self-education purposes, the Company's portal has an Information Security section. This section contains information on current threats, digests on information security and spam mailings. In addition, a mailing was sent to all employees of the ED, branches and subsidiaries informing them of the opportunity to familiarise themselves with the IRD and IS recommendations in the above section.

A test for IS awareness raising was developed. When a newly hired employee is hired, an induction training on IS is conducted and a briefing checklist is completed as per the HR Standard. In 2023, more than 100 people were briefed.

In 2023, the following trainings were conducted for the Company's IS employees:

- Training of key users on the Palo Alto Networks new generation firewall software and hardware complex;
- Training of key users on the PAM privileged user control system.

KEGOC JSC has developed processes to train users on protection procedures and proper handling of information resources. Processes have been developed to send and receive necessary information about KEGOC JSC rules and procedures, including requirements for security and other controls. These processes also apply to users of information systems from external organizations that have permanent or temporary access to KEGOC JSC information resources.

In order to raise awareness of KEGOC JSC employees, methodological developments on IS issues have been prepared. These materials are posted monthly on KEGOC JSC unified portal in the Information Security section.

Incident management

The Company has approved the Rules for Information Security Incident Management, which define the main measures, methods and means of preserving (maintaining) the operability of the Company's IS in the event of various IS incidents, as well as ways and means of restoring information and its processing in the event of IS and component malfunctions. The main objectives of the IS incident management process are to minimize damage, restore the IS to its original state as soon as possible and develop a plan to prevent similar incidents in the future.

The Company's employees and users of information systems shall promptly report through administrative channels events that potentially pose a security threat. The list and composition of such events shall be brought to the attention of users when informing them about ensuring information security in the performance of their official duties, as well as when training them on the rules of using information resources and services of information systems.

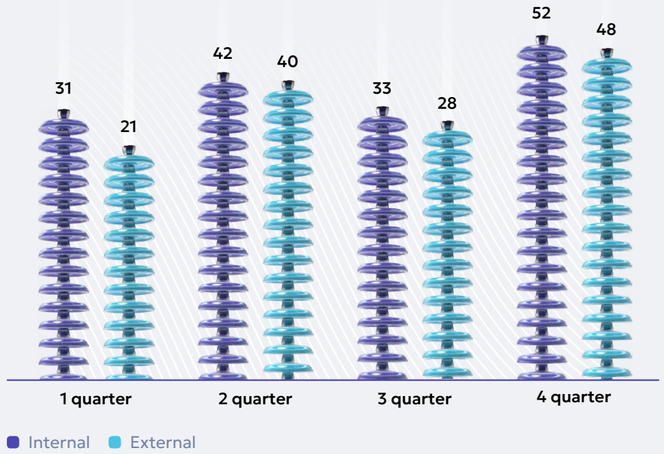
Users of KEGOC JSC information resources shall register any observed or suspected weaknesses in the security system and report them. Users shall immediately bring such incidents to the attention of authorized employees. Under no circumstances should they attempt to check suspected weaknesses in the information security system.

Users of KEGOC's information resources shall register all cases when the functioning of the software appears to them to be incorrect, i.e. not complying with the specification, and they shall report suspicions that the failure is caused by a malicious programme, e.g. a computer virus, to authorized employees.

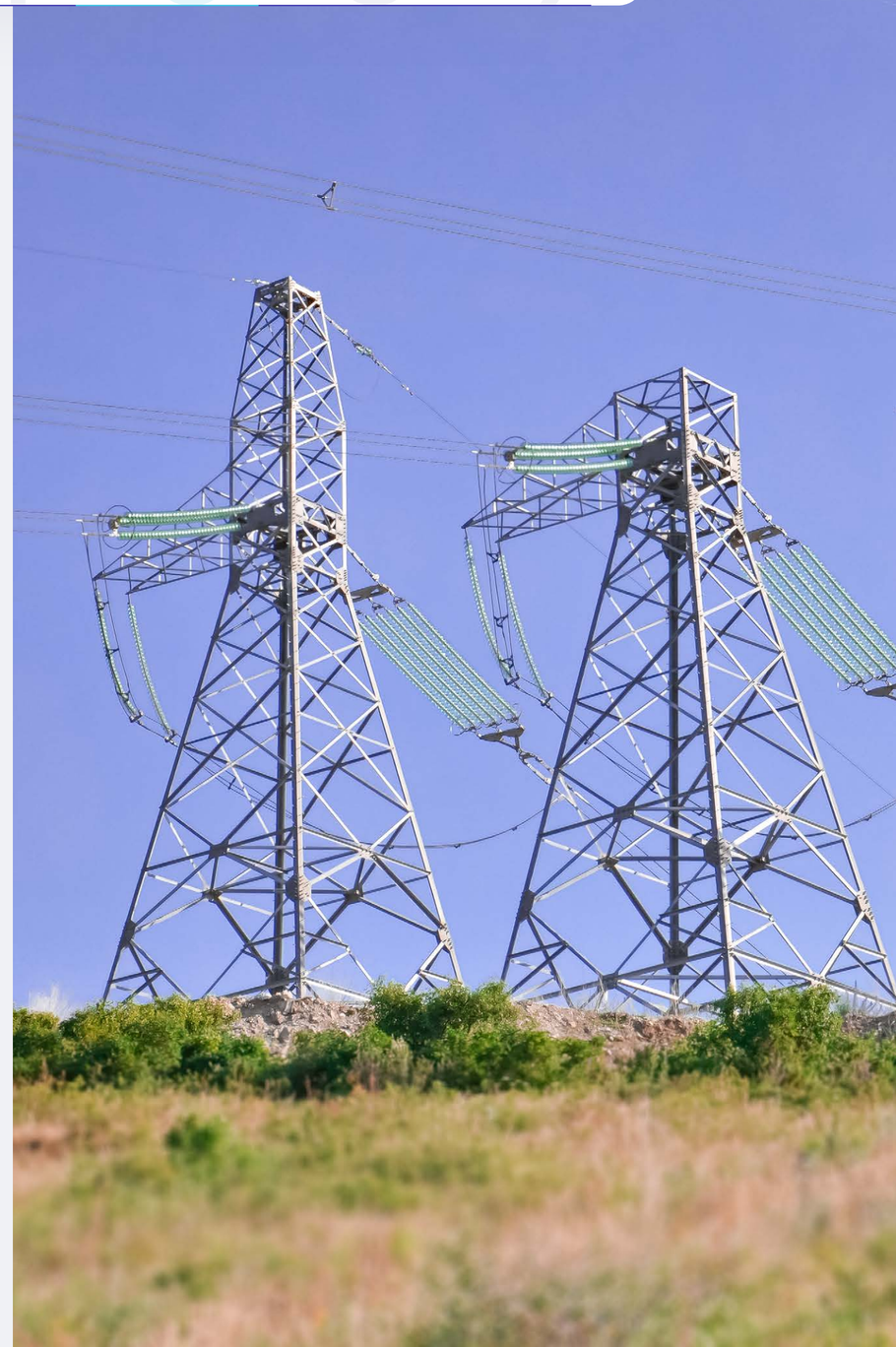
Users should not attempt to restore software functionality themselves by removing suspicious software.

At the end of 2023, 290 information security incidents were identified, for which appropriate measures were taken to minimize IS risks.

Distribution of incidents by quarter in 2023



The largest number of external incidents was registered in the category of 'viruses' detected on removable media. In accordance with KEGOC JSC Personnel Administration Rules, disciplinary penalties were imposed on employees for committing a disciplinary offence/information security incident at KEGOC JSC.



Emergency preparedness

The Company has established business continuity procedures aimed at limiting the degree of impact of internal and external negative factors on KEGOC JSC operations. In accordance with the Information Infrastructure and Information Objects Business Continuity Management, when information security incidents are detected, KEGOC JSC conducted testing and scheduled investigation of the cyber incident within the framework of the BCM. This Plan is tested every year.

The result of activities in 2023 was the prevention of information security incidents resulting in financial and reputational losses in respect of the Company's information assets.

External and internal audit

KEGOC JSC conducts external and internal audits of the ISMS in accordance with the Audit Plan. The audit is conducted for all processes of the system, establishing a link between the process objectives, implementation and results of the process, identifying weaknesses and areas for improvement.

The Company conducts annual external penetration testing in order to comply with legal regulations. Testing is carried out using various methods and techniques that have been selected with due regard to the specifics of the Company and information systems.

Risks and actions taken

Information security risk management is an element of KEGOC JSC corporate risk management system.

Information security risk assessment is carried out for all KEGOC JSC assets, based on which an assessment report and an IS Risk Management Plan are prepared.

To manage the identified risks, KEGOC JSC has developed a Plan of control measures for the implementation of ISMS security measures, a Plan of thematic information security training for employees, as well as a plan of priority information security measures and measures aimed at improving the level of information security of production systems.

We endeavor to continuously improve our information system security measures and ensure the reliability of our entire Company. We will continue to improve our processes and security measures in line with best practices and new technologies.

Privacy Policy

Ensuring confidentiality of information is an element of KEGOC JSC corporate risk management system. From the day of employment, the Company's employees sign a document on non-disclosure of confidential information in accordance with the requirements of internal documents and undergo appropriate training. The Company's contracts with suppliers contain a separate section on the conditions of confidentiality of the Company's data.

On a mechanism for informing consumers about privacy protections

In 2023, KEGOC JSC developed and adopted the Rules for ensuring information security when working with suppliers.

Indicators for the implementation of Goal 2

Name of KPI	2019 Fact	2020 Fact	2021 Fact	2022 Fact	2023 Plan	2023 Fact
LTIFR, coefficient	0	0	0.15	0.45	0.65	0.15
ESG rating		indicator is defined in 2022			30	51