01
02
03
04
05
06
07

INFORMATION POLICY AND SECURITY

IN 2024, KEGOC JSC SUCCESSFULLY CONTINUED IMPLEMENTING ITS INFORMATION POLICY, BASED ON THE PRINCIPLES OF EQUAL, COMPREHENSIVE, ACCURATE, AND TIMELY DISCLOSURE OF INFORMATION FOR STAKEHOLDERS. THIS POLICY ONCE AGAIN PROVED EFFECTIVE IN SUPPORTING THE COMPANY'S INVESTMENT ATTRACTIVENESS, STRENGTHENING TRUST FROM THE INVESTMENT COMMUNITY, AND ACHIEVING STRATEGIC DEVELOPMENT GOALS.

KEGOC JSC actively interacted with the expert community, shareholders, and investors through timely disclosure of material information about the Company's activities.

The following channels were used:

- publications in leading media outlets;
- corporate website;
- official social media pages (Facebook, Instagram, Telegram, Twitter);
- speaker appearances on television;
- comments and responses to journalists' inquiries.

The key informational events of 2024 were major achievements of KEGOC JSC. High profitability enabled the Company to successfully fulfill its obligations to shareholders. One of the most significant events was the launch of a project to connect the Western Kazakhstan power grid to the UPS of the country. To finance this project, loan agreements were signed with the European Bank for Reconstruction and Development and the Development Bank of Kazakhstan.

The Company's successful performance led to an upgrade in several credit ratings to investment grade by Moody's and S&P. Additionally, KEGOC JSC maintained high standing in the corporate sector, becoming a leader among Samruk-Kazyna portfolio companies in occupational safety compliance and achieving a 87% social stability level among production staff.

KEGOC JSC strictly complies with legal requirements for the protection of commercial, official, and other confidential information. Information security principles are integrated into all processes of disclosure and dissemination of corporate information.

Special attention was paid to procurement transparency within the Samruk-Kazyna Fund, which helped strengthen trust among international partners and investors.

KEGOC JSC's Information policy in 2024 once again demonstrated its effectiveness in supporting the Company's investment appeal, strengthening partnerships, and achieving strategic development goals. Further improvement of this policy remains a key priority for ensuring sustainable growth and successful implementation of the Company's investment programs.

INFORMATION SECURITY

The main goal of information security (IS) activities is to ensure and enhance the protection of KEGOC JSC's information assets, as well as to coordinate, plan, and organize IS activities, including effective strategic IS management and the improvement of IS process maturity levels.

The Information Security Management System (ISMS) has been developed and implemented based on ISO/IEC 27001 and is an integral part of the Company's integrated management system.

The scope of the ISMS at KEGOC JSC covers the information system managing the financial and economic processes of KEGOC JSC, supporting the implementation of core and auxiliary business processes.

To ensure compliance with requirements and define the Company's context, an Information Security Policy has been approved.

In accordance with KEGOC JSC's internal IS regulations, work has been carried out to analyze new criteria for information assets that are valuable to KEGOC JSC. In 2024, KEGOC JSC continued to strengthen measures to ensure the security of information assets.

KEY RESULTS

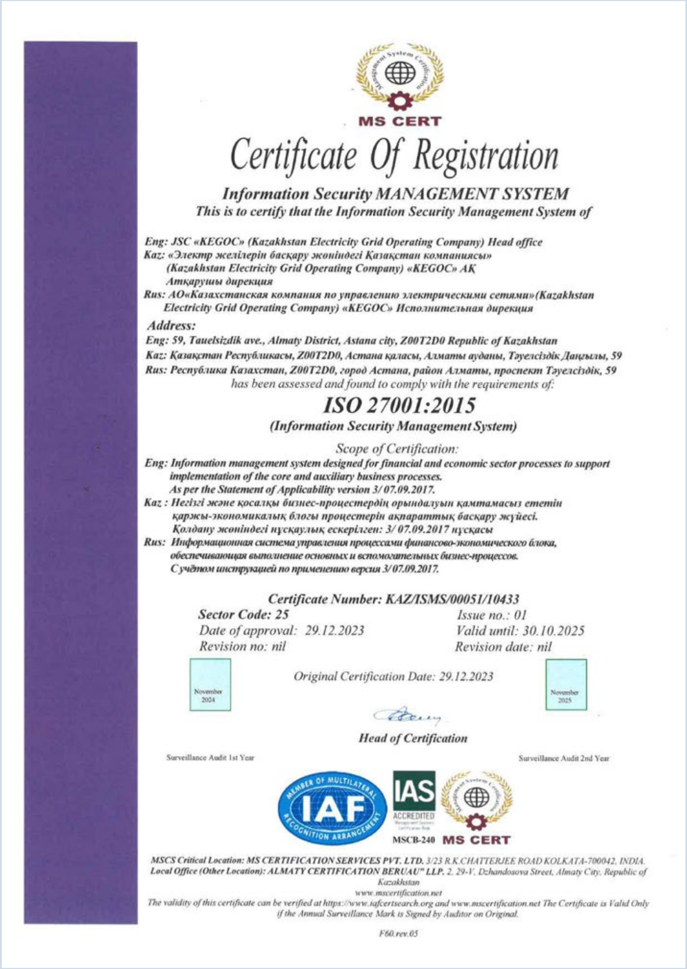
As a result of the 2024 external audit, KEGOC JSC received an ISO 27001 certification of compliance, confirming that the Company meets high standards in information security management. This is a significant step toward ensuring the security of the Company's information systems and data.

By the end of 2024, all IS systems are operating properly. Ongoing monitoring is carried out to ensure the operability of the Company's cyber protection systems. IS policies (DLP, PAM) are being updated. The corporate network is subject to weekly antivirus checks. The Company's antivirus software successfully detects and neutralizes malware (ransomware). Confidential data analysis (DLP) is performed, spam and phishing emails are blocked (anti-spam).

Two-factor authentication has been implemented for remote VPN access, significantly reducing the risk of workstation breaches.

Together with QazCloud LLP, KEGOC JSC conducted activities to expand the SOC monitoring zone. As of now, the Company's corporate network is fully connected to the SOC (fully integrated into Samruk-Kazyna JSC's Cyber Shield). An audit of authorized software in the Company was conducted within the framework of the approved Software Register used at KEGOC JSC.

In 2024, the Company's protection system (Kaspersky) detected and successfully removed malware related to worms and unauthorized software. Due to the successful implementation of virus detection and removal measures, no internal investigations were required. Phishing emails related to cryptocurrencies were blocked.



MS CERT

Certificate Of Registration

Information Security MANAGEMENT SYSTEM

This is to certify that the Information Security Management System of

Eng: JSC «KEGOC» (Kazakhstan Electricity Grid Operating Company) Head office
Kaz: «Электр желілерін басқару жөніндегі Қазақстан компаниясы» (Kazakhstan Electricity Grid Operating Company) «KEGOC» АҚ Атқарушы дирекция
Rus: АО«Казахстанская компания по управлению электрическими сетями»(Kazakhstan Electricity Grid Operating Company) «KEGOC» Исполнительная дирекция

Address:
Eng: 59, Tauelsizdik ave., Almaty District, Astana city, Z00T2D0 Republic of Kazakhstan
Kaz: Қазақстан Республикасы, Z00T2D0, Астана қаласы, Алматы ауданы, Тәуелсіздік Даңғылы, 59
Rus: Республика Казахстан, Z00T2D0, город Астана, район Алматы, проспект Тәуелсіздік, 59

has been assessed and found to comply with the requirements of:

ISO 27001:2015

(Information Security Management System)

Scope of Certification:

Eng: Information management system designed for financial and economic sector processes to support implementation of the core and auxiliary business processes.
As per the Statement of Applicability version 3/ 07.09.2017.
Kaz : Негізгі және қосалқы бизнес-процестердің орындалуын қамтамасыз ететін қаржы-экономикалық блогы процестерін ақпараттық басқару жүйесі.
Қолдану жөніндегі нұсқаулық ескерілген: 3/ 07.09.2017 нұсқасы
Rus: Информационная система управления процессами финансово-экономического блока, обеспечивающая выполнение основных и вспомогательных бизнес-процессов.
С учётом инструкцией по применению версия 3/ 07.09.2017.

Certificate Number: KAZ/ISMS/00051/10433

Sector Code: 25
Date of approval: 29.12.2023
Revision no: nil

Issue no.: 01
Valid until: 30.10.2025
Revision date: nil

November 2024

Original Certification Date: 29.12.2023

November 2025

Head of Certification

Surveillance Audit 1st Year

Surveillance Audit 2nd Year

MSCB-240 MS CERT

MSCS Critical Location: MS CERTIFICATION SERVICES PVT. LTD. 3/23 R.K.CHATTERJEE ROAD KOLKATA-700042, INDIA.
Local Office (Other Location): ALMATY CERTIFICATION BERUAU" LLP. 2, 29-V, Dzhandosova Street, Almaty City, Republic of Kazakhstan
www.mscertification.net
The validity of this certificate can be verified at https://www.iafcertsearch.org and www.mscertification.net The Certificate is Valid Only if the Annual Surveillance Mark is Signed by Auditor on Original.

F60.rev.05

AWARENESS RAISING

In accordance with the requirements of the ISMS, a unified corporate ethics policy on information security (IS) has been approved in the Company, supporting employee awareness.

KEGOC JSC ensures appropriate competence (education, training, experience) of personnel responsible for IS by conducting technical training, specialized advanced training courses, briefings, and implementing a system of professional training and staff development.

In 2024, training sessions were conducted for Company employees to raise awareness about cyber hygiene and compliance with the Company's Information Security Policy. Employees were tested to assess their level of awareness.

Additionally, for self-education purposes, a dedicated "Information Security" section exists on the Company's portal, which contains information on current threats, IS digests, and spam mailings.

Upon hiring a new employee, an introductory IS briefing is conducted, and a briefing checklist is completed in accordance with the Personnel Management Standard. In 2024, 54 employees underwent this briefing.

KEGOC JSC has developed processes for user training on protection procedures and the proper handling of information resources. Processes have been established for providing and receiving necessary information on KEGOC JSC rules and procedures, including security requirements and other control measures. These processes also apply to users from external organizations who have permanent or temporary access to KEGOC JSC's information resources.

To enhance employee awareness, methodological materials on IS assurance were prepared. These materials are posted monthly on the KEGOC JSC unified portal in the "Information Security" section.

INCIDENT MANAGEMENT

The Company has approved Information Security Incident Management Rules, which define the basic measures, methods, and tools for maintaining the operability of the Company's IS in the event of various IS incidents, as well as methods and tools for restoring information and processing processes in case of IS or component malfunctions. The main objectives of the IS incident management process are to minimize damage, promptly restore the original state of the IS, and develop a plan to prevent similar incidents in the future.

Company employees and IS users must immediately report through administrative channels any events that potentially pose a security threat. The list and nature of such events must be communicated to users during briefings on information security responsibilities and training on the use of information systems and services.

Users of KEGOC JSC's information resources are required to log any observed or suspected vulnerabilities in the security system and report them. Users must promptly inform authorized personnel of such incidents. Under no circumstances should they attempt to test the suspected vulnerabilities themselves.

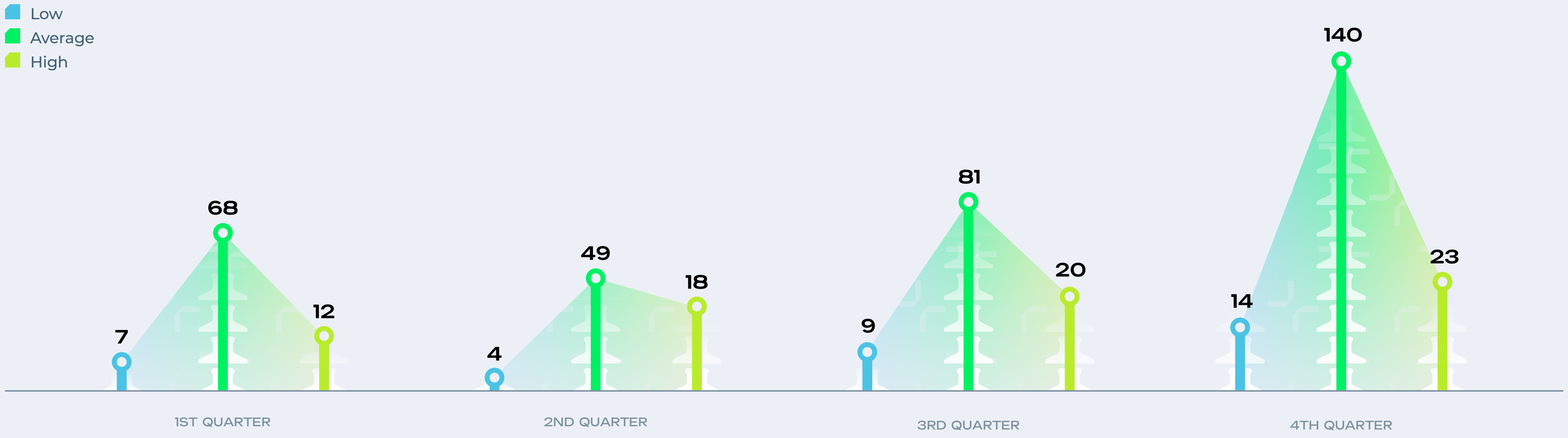
Users of KEGOC JSC's information resources are also required to log all cases where software behavior appears incorrect, i.e., does not match specifications. If there is suspicion that a failure was caused by malicious software (e.g., a computer virus), users must report this to authorized personnel.

Users must not attempt to independently restore software functionality by removing suspected malicious programs.

By the end of 2024, 445 information security incidents were identified, and corresponding measures were taken to minimize IS risks.

The highest number of IS incidents was recorded in the "Malware" category, identified on users' workstations.

Distribution of information security events by quarter in 2024



01
02
03
04
05
06
07

EMERGENCY PREPAREDNESS

The Company has established business continuity procedures aimed at limiting the impact of internal and external negative factors on the activities of KEGOC JSC.

In accordance with the Business Continuity Plan for the information infrastructure and information assets, KEGOC JSC conducted testing of the BCP in the event of detected information security incidents. This plan is tested annually.

As a result of activities in 2024, no information security incidents occurred that would cause financial or reputational loss to the Company's information assets.

EXTERNAL AND INTERNAL AUDIT

At KEGOC JSC, external and internal audits of the ISMS are conducted in accordance with the Audit Plan. The audit covers all system processes, establishing links between process goals, implementation, and outcomes, identifying weaknesses and areas for improvement.

The Company undergoes annual re-certification for compliance with the ISO 27001 standard.

To comply with legal requirements, the Company conducts annual external penetration testing. The testing uses various methods and techniques selected based on the specifics of the Company and its information systems.

RISK MANAGEMENT AND MEASURES TAKEN

Information security risk management is an element of KEGOC JSC's corporate risk management system. Risk assessment in the field of information security is carried out for all assets of KEGOC JSC, based on which a risk assessment report and an Information Security Risk Treatment Plan are developed.

To manage the identified risks, a Control measures plan for implementing ISMS security measures at KEGOC JSC, a Thematic information security training plan for employees, as well as a Priority information security measures plan and activities aimed at increasing the level of information security of production systems have been developed.

KEGOC JSC strives to continuously improve information system security measures and ensure the reliability of the entire Company's operations. The Company will continue to improve its processes and security measures in accordance with best practices and new technologies.

TO CONFIRM THE COMPLIANCE OF KEGOC JSC ISMS, A CERTIFICATION AUDIT WAS CONDUCTED IN 2023 BY THE INDEPENDENT CERTIFICATION BODY "MS CERTIFICATION SERVICES PRIVATE LIMITED" (INDIA), AND A SURVEILLANCE AUDIT WAS CONDUCTED IN 2024, BOTH OF WHICH CONFIRMED THAT THE ISMS MEETS INTERNATIONAL STANDARDS REQUIREMENTS.

Confidentiality assurance is an element of KEGOC JSC's corporate risk management system. From the first day of employment, Company employees sign a non-disclosure agreement for information constituting confidential data in accordance with internal documentation and undergo appropriate briefing. Contracts with suppliers include a separate section specifying the terms for ensuring the confidentiality of Company data.