Information security

According to the Information Security Policy of Samruk-Energy JSC, the company aims to organize its activities to ensure information security (IS) in accordance with the ISO/IEC 27001 standard "Information technology. Security techniques. Information security management systems." In this regard, internal regulatory documents have been approved, and the following activities are being carried out:

- Development and updating of the IS management system;
- Identification of IS risks and owners of information assets;
- Assessment and processing of IS risks;
- Coordination of the development/implementation of control measures;
- Execution of IS measures;
- Monitoring of IS risks, reporting;
- Improvement of the IS management system.

The responsibility for ensuring information security is assigned to the "Security" Department, which is a structural unit separate from other structural units involved in the creation, support, and development of informatization objects. According to the approved organizational structure, the Department reports directly to the Chairman of the Board of Samruk-Energy JSC. In terms of IS, this structural unit is responsible for the following functions:

- Development of regulatory and procedural documentation and requirements for IS;
- Ensuring interaction between business units on IS issues;
- Control over the compliance with IS requirements;
- Monitoring the activities of subsidiaries and affiliates in the field of information security;
- Interaction with state authorized bodies in the field of ensuring the company's information security;
- Coordination of actions related to IS risks;
- Interaction with the Information Security Operations Center.

In the process of ensuring IS, the company considers the following main directions:

- Information security management;
- Technical support for information security;
- Control and response to information security incidents.

Within the process of managing IS, the company has developed the following documents that regulate IS work:

- Information Security Policy of Samruk-Energy JSC;
- Rules for ensuring the information security of information systems at Samruk-Energy JSC;
- Instructions for ensuring the security of confidential information at Samruk-Energy JSC.

The technical support function for IS is carried out by the Security Department and specialists from Energy Solutions Center LLP. This function involves ensuring IS using software and hardware mechanisms to protect the company's information assets. The main activities for ensuring information security in the company currently include:

- Providing antivirus protection for the company's corporate network and branches by using a software suite for protection against malicious code;
- A demilitarized zone (DMZ), used to enhance the level of information security of the company's corporate network and resources that have internet access. The DMZ is implemented based on a software and hardware complex of packet filters Firewall, in addition to which a system for preventing intrusions is implemented for additional packet filtering at the distribution level. The software control used to track sent and received emails. This system blocks spam senders within the perimeter of Samruk-Energy JSC and analyzes emails for the presence of malicious software, controls software to prevent leaks of confidential information beyond the corporate network.

The function of control and response to IS incidents is carried out by employees of the "Security" Department and specialists of Energy Solutions Center LLP, registered by the Operational Center for Information Security (OCIS) and means of the software and hardware complex for information security:

- Centralized collection, storage, and analysis of security event logs;
- Detection of incidents in real-time;
- Prioritizing incidents;
- Control over the incident correction process and

compliance with response time (SLA);
- Creation of reports on compliance with regulatory requirements.

Results on the control and response to IS incidents are recorded in the following reports:

- A monthly analytical report analyzing the state of the information security infrastructure of Samruk-Energy JSC within the framework of the contract with OCIS;
- A quarterly report on information security risks for the Board of Directors of Samruk-Energy JSC;
- An annual report on information security (cybersecurity) provision is generated, as well as an analysis and assessment of the adequacy of internal controls of Samruk-Energy JSC in terms of protection and maintenance of IT systems and infrastructure for the Audit Committee and the Board of Directors of Samruk-Energy JSC.

Throughout the year, awareness of the IS management system is enhanced by annually approving a work plan for the development of educational materials to increase the awareness of the Company's employees (reminders, screensavers, videos), distributing updates about new requirements and preventive measures for IS. Annually, Company's employees are tested online on knowledge of information security norms as per established procedures.

In 2023, 'Adaptation course' training was conducted for all newly hired employees, which also includes information security training.

GRI 418-1

During the reporting period, the Company did not record any substantiated complaints about breaches of confidentiality, leaks, theft and/or loss of customer data.

Information Security Operations Center

Samruk-Energy JSC is connected to the Operational Center for Information Security for 24/7 monitoring of all information security events under a contract with QazCloud LLP, which provides the following services:

- Round-the-clock monitoring of IS events recorded by information security event management and monitoring systems and external perimeter protection systems;
- Round-the-clock monitoring of IS events recorded on the customer's server equipment and network devices (hereinafter referred to as the Monitoring Zone);
- Identification of IS incidents that have occurred in the Monitoring Zone;
- Sending information to the customer about detected incidents and methods for responding to them, and providing recommendations for their elimination;
- Providing expert support during incident response;
- Responding to incidents coming from the external Internet network to the customer's perimeter;
- Conducting investigations of IS incidents;
- Three-tiered support line of the OCIS, consisting of team collaboration in ensuring IS monitoring (Red team and Blue team). The Blue team ensures the protection of the infrastructure by monitoring events and responding to cyber threats around the clock. The Red team professionally identifies vulnerabilities in the infrastructure;
- Protection of web applications and WEB traffic;
- Protection against DDOS attacks;
- Weekly IS digest;
- Conducting an audit (penetration test), including external penetration testing and vulnerability identification.

The company's cybersecurity initiatives are approved in the Information Technology and Digitalization Strategy of Samruk-Energy JSC for 2023–2025.