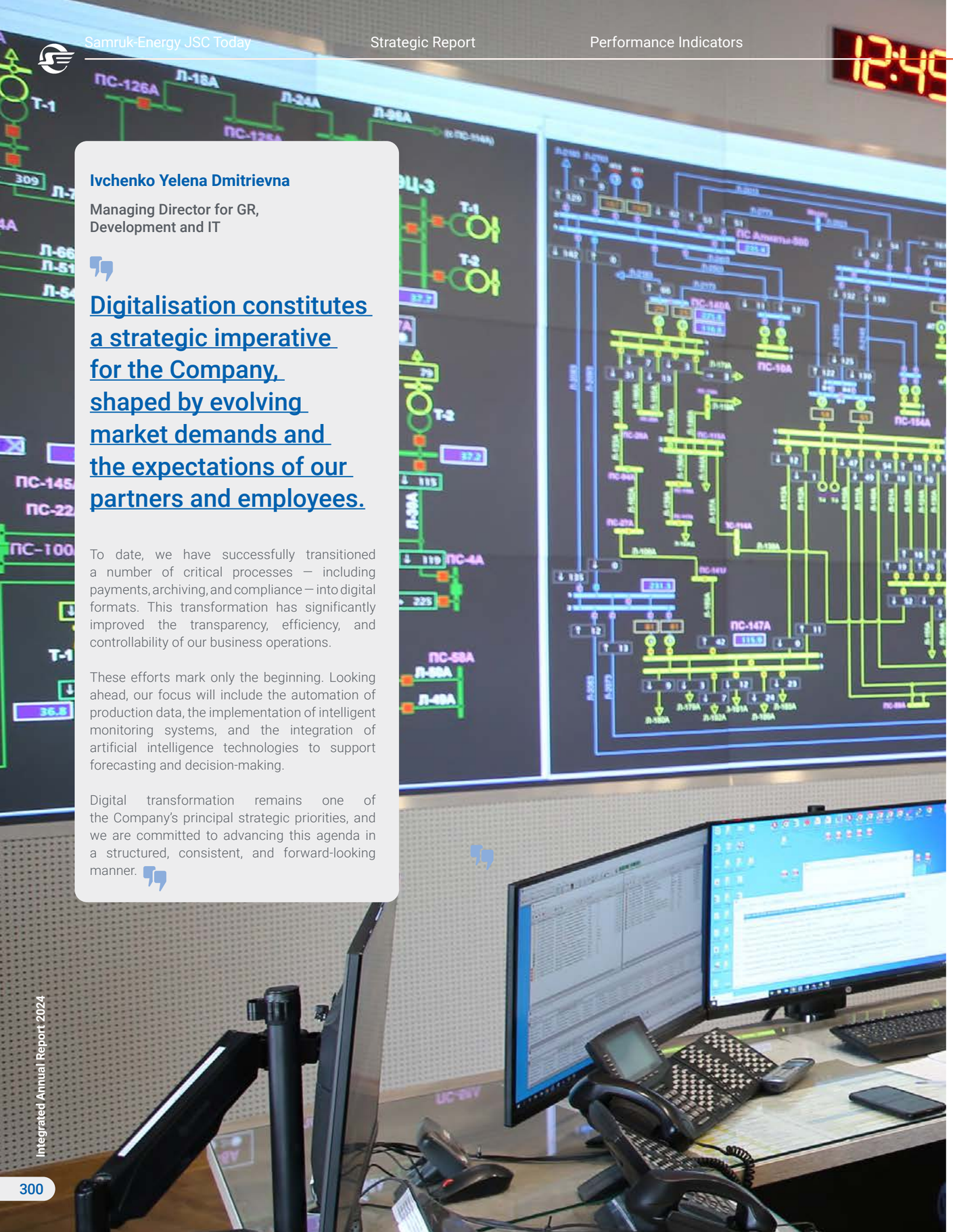

Ivchenko Yelena Dmitrievna

Managing Director for GR, Development and IT

Digitalisation constitutes a strategic imperative for the Company, shaped by evolving market demands and the expectations of our partners and employees.

To date, we have successfully transitioned a number of critical processes — including payments, archiving, and compliance — into digital formats. This transformation has significantly improved the transparency, efficiency, and controllability of our business operations.

These efforts mark only the beginning. Looking ahead, our focus will include the automation of production data, the implementation of intelligent monitoring systems, and the integration of artificial intelligence technologies to support forecasting and decision-making.

Digital transformation remains one of the Company's principal strategic priorities, and we are committed to advancing this agenda in a structured, consistent, and forward-looking manner.

Information security

GRI 3-3

In accordance with the Information Security Policy of Samruk-Energy JSC, the Company aims to build an information protection system that complies with the international standard ST RK ISO 27001 "Information Technologies. Methods and means of ensuring security. Information security management systems". To realise this goal, internal regulatory documents were developed and approved, and the following key measures are being implemented:

- Development and updating of the information security management system (ISMS);
- Identification of information security risks and identification of information asset owners;
- Information security risk assessment and processing;
- Coordinate the development and implementation of control activities;
- Execution of information security measures;
- Information security risk monitoring and reporting;
- Continuous improvement of the information security management system.

Responsibility for ensuring information security in the Company is assigned to the Security Department, which is an independent structural subdivision and is directly subordinated to the Chairman of the Management Board of Samruk-Energy JSC. In its information security activities, the unit performs the following key functions:

- Development of regulatory and administrative documentation and information security requirements;
- Ensuring interaction between business units on information security issues;
- Monitoring compliance with information security requirements;
- Monitoring of information security activities of subsidiary and affiliates;
- Interaction with state authorities on the Company's information security issues;
- Coordination of information security risk management activities;
- Interaction with the Information Security Operations Centre.

There are three main areas of consideration in the Company's IS assurance process:

- Information Security Management;
- Technical provision of information security;
- Controlling and responding to information security incidents.

Information security management

As part of the information security management process, the Company has developed a number of documents that regulate work in this area:

- Information Security Policy of Samruk-Energy JSC;
- Rules for ensuring information security of information systems in Samruk-Energy JSC;
- Instruction on ensuring safety of confidential information in Samruk-Energy JSC.

Technical support of information security

The function of information security technical support is performed by the Security Department together with the specialists of Energy Solutions Centre LLP. Technical support means a set of measures aimed at protecting the Company's information assets using modern software and hardware.

Key activities carried out within the function:

- Providing anti-virus protection for the corporate network and branches using specialised anti-malware software;
- Creation of a demilitarised zone (DMZ) to increase the level of information security of the corporate network and resources with access to the Internet. The DMZ is implemented on the basis of a software and hardware complex of Firewall packet filters (firewalls), which provides additional packet filtering at the distribution level;
- Control software for monitoring sent and received e-mails. The system allows blocking spam senders in the perimeter of Samruk-Energy JSC, analysing e-mails for malware and preventing leakage of confidential information outside the corporate network.

Controlling and responding to information security incidents

The function of controlling and responding to information security incidents is performed by employees of the Security Department together with specialists of Energy Solutions Centre LLP. All incidents are registered and processed in the Information Security Operations Centre (ISOC) using the IS software and hardware complex.

Key activities include:

- Centralised collection, storage and analysis of security event logs;
- Real-time incident detection;
- Prioritisation of incidents;
- Oversee the incident remediation process and adherence to response times;
- Creation of compliance reports.

The results of monitoring and incident response are documented in the following reports:

- Monthly analytical report containing analysis of the state of information security infrastructure of Samruk-Energy JSC under the contract with Information Security Operations Center;
- Quarterly report on information security risks for the Board of Directors of Samruk-Energy Information Security Operations Center;
- Annual report on ensuring information security (cyber security), as well as analysis and assessment of sufficiency of Samruk-Energy JSC's internal controls for the Audit Committee and the Board of Directors.

During the reporting period, work was carried out to raise awareness of the information security management system. An annual work plan is approved, within the framework of which training materials, such as memos, screensavers and videos, are developed for all employees of the Company. A mailing list of information security innovations, requirements and preventive measures is also organised. Every year, all employees of the Company take an online test for knowledge of information security norms, which confirms their competence in this area.

At the time of recruitment, all new employees undergo an Adaptation Course, which includes information security training. In 2024, this training was provided to all newly hired employees, ensuring high awareness and compliance with information security standards from the very beginning of their employment with the Company.

GRI 418-1

During the reporting period, the Company did not record any substantiated complaints about breach of confidentiality, leakage, theft or loss of customer data

Information Security Operations Centre

Samruk-Energy JSC is connected to the Information Security Operations Centre (hereinafter referred to as the ISOC), which monitors all information security events in 24/7 mode. The ISOC is provided under a contract with QazCloud LLP, which provides the following services:

- Round-the-clock monitoring of information security events recorded by information security event monitoring and management systems, as well as external perimeter defence systems;
- Round-the-clock monitoring of information security events occurring on server equipment and network devices (hereinafter referred to as the Monitoring Zone);
- Identification of information security incidents that occur in the Monitoring Area;
- Records of identified incidents, as well as incident response methods and recommendations for remediation;
- Provide expertise in the incident response process;
- Conducting investigations of information security incidents;
- Three-level ISOC support line consisting of a team effort to provide IS monitoring, including a Red team and a Blue team. The Blue team protects the infrastructure by monitoring events around the clock and responding to cyber threats. The Red team, in turn, professionally identifies infrastructure vulnerabilities;
- Protection of web applications and WEB traffic;
- Protection from DDOS attacks;
- Weekly information security digest;
- Audit (penetration test), including external penetration testing and vulnerability identification.