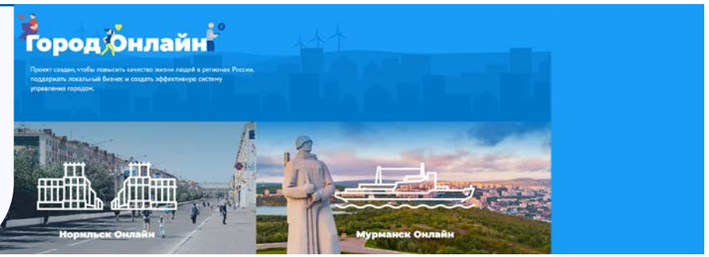
Digitalisation in regions of operation



GRI 203–1, 203–2

The City Online project is set to improve the quality of life of people living in small and medium-sized towns in the Far North and the Far East by providing infrastructure and digital services in various areas of life and making habitual services more accessible to remote areas.

The platform is available as a website and a mobile app in five cities: Norilsk, Dudinka, Monchegorsk, Murmansk, and Krasnoyarsk. Currently, the web and mobile versions of the platform offer 28 and 16 services, respectively. The most popular are GO.Media, Playbill, Broadcasts (web version only), Map, and Transport. In the near future, we plan to develop services that will help municipal employees promptly interact with each other and with residents of the city in the shared information space.

Major City Online infrastructure services include:

- a city air monitoring programme with a predictive environmental assessment model in Norilsk, Monchegorsk, Nickel, and Zapolyarny seeking to improve the urban environment quality and the comfort of people's lives;
- a mobile school education system in the Murmansk Region. The system was deployed in 2022 and has already made a better and more equal level of education available to different social groups and minimised the impact of downtime days during school period.

To meet the Company's production needs with high-speed communication and to improve the quality of life in the Norilsk Industrial District by creating conditions for broadband Internet access, enhancing the quality of services and expanding the range of communication services provided, Nornickel implements the Fibre Optic Communication Line (FOCL) Construction Project in Norilsk. The project involves the construction of a 956 km fibre optic communication line from Novy Urengoy to Norilsk.

In 2022, in response to growing demand from the population in the Norilsk District, the bandwidth of the transport network was increased from 40 Gbps to 200 Gbps, which now enables customer traffic to grow to 85 Gbps, with less than 1% of traffic used for the Company's needs.

As mobile and fixed-line Internet access remains one of the key conditions for high quality of life in the modern world and is the driver behind digital services, in order to improve the availability of high-quality communications, we held a promotion campaign in 2022 for telecom operators providing services to end users, involving an average discount of 15%. The new tariff policy helped develop high-speed tariff plans of operators in the city and resulted in a twofold more affordable pricing on average in 2022. In addition, 15 schools in the Norilsk Industrial District were connected to the Internet on preferential terms.

More than **180** thsd users
registered on the platform

Almost **1.5** million
unique visitors

About **55** thsd
mobile app installs

Corporate security

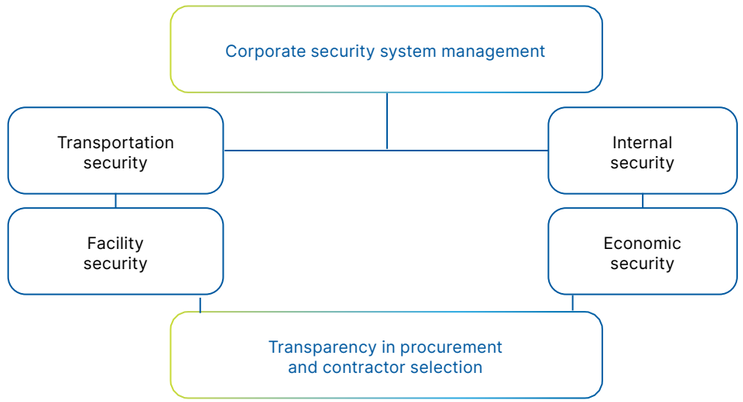
The corporate security system underpins the sustainability of Nornickel's business processes. The Company has developed a comprehensive corporate security management system comprising five main blocks.

The Company has a dedicated Corporate Security Unit to manage corporate security issues. In addition, the Company has established and is expanding a network of analytical situation centres. The regulatory framework in this area is defined by the Russian laws, applicable international norms and internal standards, and Nornickel's by-laws.

All senior managers of the Company, including the Board of Directors and the Management Board, are involved in the processes of drafting and improving regulatory documents aimed at ensuring corporate security. In March 2022, the Board of Directors approved PJSC MMC Norilsk Nickel's Policy on Countering Corporate Fraud. The requirements of the Policy are in line with the principles of honest and responsible business conduct, emphasising the Company's commitment to improving its corporate culture and adherence to best corporate governance practices and high ethical standards.

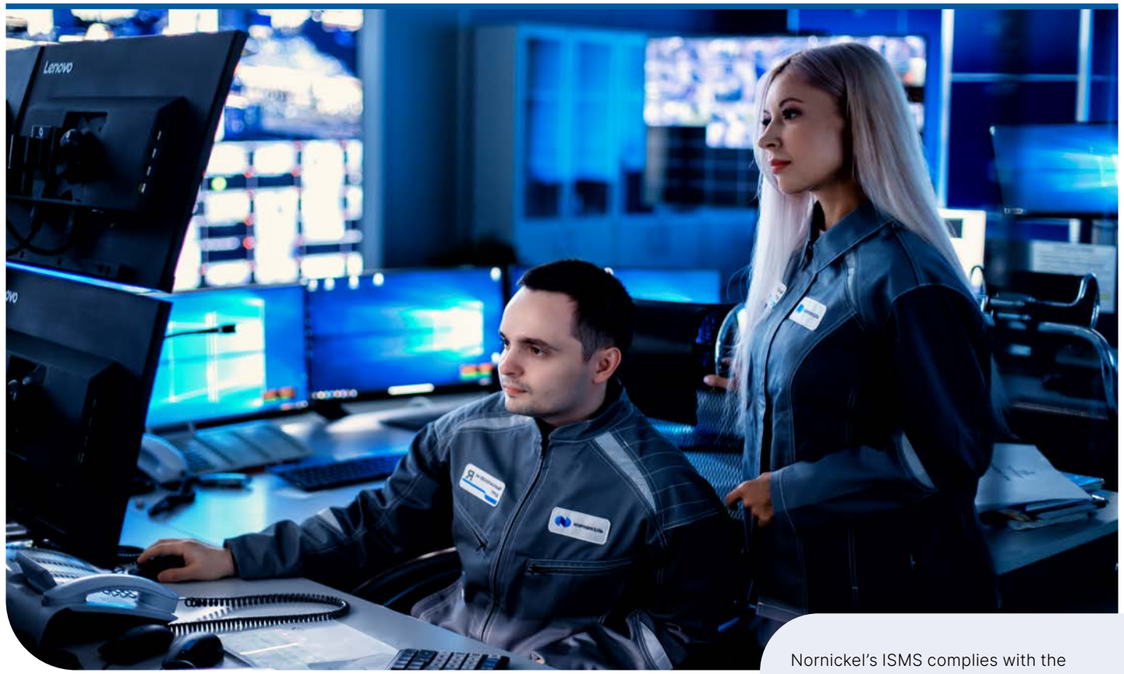
The Policy unifies a set of systemic measures for the prevention, detection and counteraction to corporate fraud.

Corporate security management system



Objectives of the Policy on Countering Corporate Fraud

1. Preventing, detecting and mitigating the risk of corporate fraud. Protecting legitimate interests of the Company, its subsidiaries, their shareholders/participants, and safeguarding assets.
2. Reaffirming zero tolerance to any form or manifestation of corporate fraud.
3. Creating a consistent, Company-wide understanding of the essence of fraud, as well as a uniform standard of conduct for the prevention and suppression of fraud.
4. Preventing violations of laws on combating corporate fraud by the Company or its subsidiaries or employees.



Ensuring information security

Nornickel has a highly integrated information system for all of its businesses. Information is a valuable resource for the Company, while information security guarantees business continuity. Nornickel has its own Information Security Management System (ISMS) in place. The ISMS covers day-to-day production management, supplies of feedstock and process materials, as well as control over production and finished product shipment targets.

To support robust information security, the Company is subject to regular ISMS audits for compliance with personal data and critical infrastructure protection requirements and international standards on cyber security management, testing and assessment of data protection, vetting inspections to check information security in river and marine navigation, and other control procedures.

Nornickel's ISMS complies with the norms and requirements of ISO/IEC 27001:2013. In 2022, four of Nornickel's sites confirmed the high efficiency of their information security management processes:

1. Murmansk Transport Division;
2. Nadezhda Metallurgical Plant;
3. Copper Plant;
4. Talnakh Concentrator.

The external auditor noted the facilities' high preparedness to new threats and challenges. The Company demonstrated risk control effectiveness and readiness for unexpected changes, confirming its ability to achieve goals related to securing production processes.

In addition to analytical situation centres, the Company has in place an Information Security Incident Response Centre. If any suspicious content or activity is detected by users, the relevant notice is given to the Response Centre. The Centre assesses the possible negative impact on the Company's information systems and takes measures to prevent and eliminate the consequences of incidents. In its work, the Centre relies on the best domestic and global practices of cyber security process management and advanced technological solutions.

In 2022, there was a significant increase in cyber attacks on Russian companies. To minimise the risks, Nornickel took additional comprehensive measures, including proactive ones, to ensure the security of its information infrastructure. In the reporting year, over 20,000 information security events and more than 1,000 incidents were handled by the Response Centre staff.

The Company's confidential information is protected by special technical protection tools that allow detecting unauthorised access attempts through the main channels, including email and file exchange. If unauthorised attempts to withdraw confidential information are identified, an internal review and investigation procedure is initiated in accordance with the Company's regulations.

The Company recognises the risk of incidents and emergencies affecting the stability of Nornickel's information systems. To ensure the continuity of the Company's operations, Nornickel developed and documented information security processes and procedures. These procedures are tested at least quarterly to ensure that they are up-to-date.

To protect the personal data of various types of subjects, including the personal data of third parties, the Company applies a set of organisational and technical measures. Technical protection is ensured by means of anti-virus protection, prevention of information leaks, control of removable media, analysis of security events. The Company also has a Personal Data Processing Policy and a number of by-laws regulating the processing and protection of personal data.

Information security training

In accordance with the Rules of Raising Awareness in Information Security, all employees of the Company are regularly trained in information security.

All new employees of Nornickel are familiarised with by-laws governing information security requirements and undergo additional induction training. In 2022, some 7,400 newly hired employees were familiarised with by-laws on information security, and approximately 4,300 new employees received additional information security induction training.

Nornickel develops annual staff training plans based on current trends and newly identified risks and cyber threats. Employees of Nornickel's Head Office and facilities across the Company's footprint take regular knowledge tests. In 2022, there were about 70 scheduled and 5 unscheduled e-learning training sessions for almost 18,500 Group employees.

In 2022, almost were trained
18.5 thsd employees

The knowledge gained is further applied to combat information security threats. To this end, the Company arranges recurrent training and workshop sessions dealing, among other things, with simulated fishing attacks and other threats to IT infrastructure. It helps test the quality of cyber security systems, practice employee actions in case of an information security threat, and improve the overall level of the corporate information security system. Analysis of training session results helps us revise existing and develop new instructions for employees. Information updated after training sessions is included in a quarterly newsletter circulated among the heads of the Company's units. Employees are informed of what to do via by-laws pertaining to information security if suspicious activity is detected.

In addition, there are regular newsletters to inform employees about current information security threats and digital hygiene rules. In 2022, we circulated 27 themed newsletters among all employees of the Group.