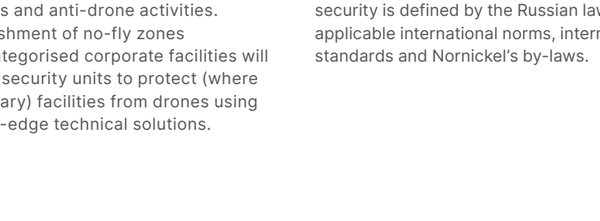
CORPORATE SECURITY

How has the Company's corporate security evolved over the past 20 years?

Corporate security improvements are one of the key drivers behind the resilience of Nornickel's business processes: in 2007, the Company developed professional competence standards for security employees; in 2017, Nornickel oversaw the establishment of the Club of Information Security in Industry, a cross-industry association; in 2018, the Group approved its Information Security Policy, and contributed to the creation of the National Association of International Information Security and drafting of the Security Charter for Critical Industrial Facilities; finally, in 2019, the Company piloted a system of analytical situation centres, which is currently gaining significant momentum. Given current external challenges, we reviewed our approach to information security to reflect continued pivot towards technological sovereignty and transition to a service-based model.

To minimise the Company's exposure to a wide range of risks, Nornickel employs a comprehensive approach suggesting integration of corporate security components into all business processes.

Corporate security components



The Corporate Security Unit manages security issues within the Company, including by coordinating the work of different business units, navigating government relations, monitoring production facilities, preventing incidents, and implementing modern technologies. In 2023, the Corporate Security Unit set up a new function responsible for coordinating the operation of unmanned aerial vehicles and anti-drone activities. Establishment of no-fly zones over categorised corporate facilities will enable security units to protect (where necessary) facilities from drones using cutting-edge technical solutions.

Nornickel is developing a network of analytical situation centres operated through a single analytical software platform for aggregating and processing information required to ensure the security of key business processes. In early 2024, a new segment of the system was put into operation, with Kola MMC joining the Group's corporate security ecosystem.

The regulatory framework for corporate security is defined by the Russian laws, applicable international norms, internal standards and Nornickel's by-laws.

In accordance with the Policy on Countering Corporate Fraud approved by the Board of Directors in 2022, the Company takes consistent steps to prevent, detect and combat abuses, corporate fraud, and corrupt practices. In the reporting year, these activities included:

- embedding violation indicators (signs of price fixing arrangements, conflict of interest, lobbying procurement participants, unjustified restrictions) into the system ensuring the economic security of procurement activities to form a comprehensive basis for abuse prevention;
- upgrading the counterparty due diligence methodology;
- developing a course on combating corporate fraud and integrating it into the Group's employee training framework. This course was successfully completed by the current employees of the Company.

Furthermore, in 2023 we addressed corporate security concerns associated with the implementation of strategic investment projects seeking to protect the legitimate economic interests of the Company in contractor relations, HR and facility security.

A dedicated Centre for Chemical and Forensic Research and Expertise equipped with cutting-edge analytical equipment started operating

on fundamentally new premises to address important economic security issues at production facilities. This helped significantly expand the Centre's remit, enabling it to run a wide range of chemical and analytical tests to provide technical assistance to manufacturing, control and analysis units in assuring product quality, investigating the causes of emergencies at production sites, conducting in-depth chemical, mineralogical and structural research of materials and substances used in the development of new concentration and metallurgical solutions, and in exercising special external control over the quality and accuracy of non-ferrous and precious metal analysis. The Centre developed a comprehensive methodology for analysing and identifying metal-bearing materials, which earned praise from the International Platinum Group Metals Association.

Nornickel actively collaborates with business partners, metals and mining companies, government authorities and other stakeholders to enhance its corporate security. In 2023, the Company participated in a meeting of the International Platinum Group Metals Association, won a prize at the R&D conference “Transport Safety Formula. Law. Knowledge”, and implemented federal security regulations.

In 2023, more than 520 training exercises, 242 joint drills and 22 dedicated tactical drills were held to ensure a high level of facility security workforce and equipment preparedness.

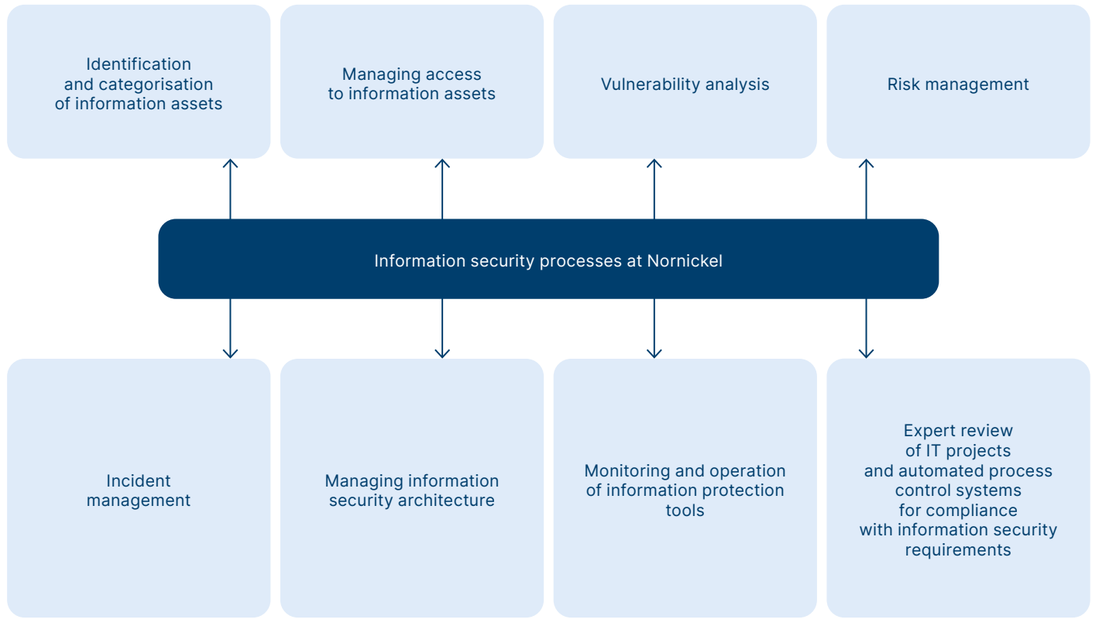
Ensuring information security

In 2023, the Company analysed existing external challenges and current trends in the Russian market to review its information security approach. Among other things, Nornickel reorganised its information security function, while also drafting and approving a strategy for its further development, which suggests continued pivot towards import substitution of information security solutions and transition to a service-based model.

Nornickel Sfera, the Company’s subsidiary, possesses extensive technical competencies across core information and process security areas, and offers a full range of key services to the Group’s facilities.

The Company takes consistent steps to protect the process infrastructure of its production sites and to mitigate risks. With cyber attacks increasingly numerous and sophisticated and some employees continuing to work from home, additional measures are required to ensure the information security of corporate resources and infrastructure.

The Company has implemented all the necessary information security processes.



The operation of the Information Security Management System (ISMS) is governed by the Company’s internal regulations (MMC Norilsk Nickel’s Information Security Policy, information security guidelines and standards) in line with best global practices.

Nornickel’s priority in ensuring the security of automated process control systems is implementing basic protection measures (tools and systems) at the greatest possible number of facilities and production sites equipped with automated process control systems. In the reporting year, the emphasis was placed on using domestic solutions.

The 2023 internal audit praised the information security function for its achievements in protecting automated control systems. The audit recommendations are expected to be implemented in 2024.

Cyber incidents are yet another focus area in the domain of information security. In order to deal with cyber incidents, the Company uses cutting-edge technical solutions, and keeps abreast of domestic and global cyber defence practices. Relevant procedures are regularly tested (at least once a quarter) to assess Nornickel's preparedness to respond to modern cyber attacks. Any employee who detects suspicious content or activity on corporate devices can report it to the information security function. Experts assess the possible negative impact on the Company’s information systems and takes measures to prevent and eliminate the consequences of incidents.

New vulnerability management strategies were drafted and rolled out in the reporting year.

Theyseek to counter new types of attacks and provide for the continuous protection of the Company's systems, including by implementing the DevSecOps strategy focused on ensuring security throughout the software development lifecycle.

Personal data (including third party data) is protected in accordance with applicable Russian laws. The security experts employ a comprehensive range of organisational and technical tools, including anti-virus protection, prevention of information leaks, control of removable media, analysis of security events, and personnel training to raise awareness about compliance with personal data requirements. In 2023, personal data processing was aligned with the latest legal requirements and internal regulations.

Information security highlights for 2023

>6,000
audits conducted in response to information security grievances submitted by the Company's employees

>18,000
information security events handled

57
operated systems
underwent vulnerability analysis, with bottlenecks identified and remedies proposed

13 Group companies
aligned personal data processing with relevant legal requirements and internal regulations

ISO/IEC 27001:2013

Nornickel's Information Security Management System complies with ISO/IEC 27001:2013.

In 2023, five of Nornickel's sites confirmed the high efficiency of their information security management processes:

- **Murmansk Transport Division;**
- **Kola Mining and Metallurgical Company (Kola Division);**
- **Nadezhda Metallurgical Plant (Norilsk Division);**
- **Copper Plant (Norilsk Division);**
- **Talnakh Concentrator (Norilsk Division).**

The external auditor noted strong involvement of the management in the ISMS processes and preparedness of the facilities to respond to new threats and challenges.

A series of audits is planned for 2024 as part of transition to ISO/IEC 27001:2022.

Information security training

Raising employee awareness about data protection and digital hygiene is an important element of the information security management system pursuant to the Company's internal regulations[1]. In 2023, Nornickel set a goal to enhance the culture of information security across the Group.

All new employees are familiarised with by-laws governing information security requirements and undergo additional induction training.

Every year the staff takes courses on the latest cyber threats and risks.

In 2023, there were about 95 scheduled and 19 unscheduled e-learning training sessions and on-site lectures for 34,104 Group employees.

Furthermore, the Company arranges regular drills dealing, among other things, with simulated fishing attacks and other user threats. The drill results are used to update employee instructions.

In addition, there are regular newsletters to inform the staff about current information security threats and digital hygiene rules.

34,104
Group employees
completed training sessions in 2023

Stakeholder engagement on information security

The Club of Information Security in Industry established at the initiative of Nornickel serves as a venue for sharing best practices and experiences in the realm of information security, and engaging in a public-private dialogue on relevant regulations. By the end of 2023, the Club had over 70 Russian companies as its members. The agenda covers the pressing issues of ensuring cyber security for businesses in the face of new challenges and threats.

In an attempt to give a boost to the information security market for the industrial sector, the Company held meetings with developers and vendors of information security products and services, and entered into strategic partnership agreements with some of them.

[1] Rules of Raising Awareness in Information Security of MMC Norilsk Nickel.