In 2024, the Data Platform and ML Platform were launched into commercial operation.

In the short term (2025–2026), ML clusters are scheduled for commercial launch. This will accelerate the implementation of digital production initiatives by removing the need for iterative design and deployment of integration infrastructure, as well as reduce the analytical load on production control and dispatch systems.

Video analytics

During the reporting period, Nornickel expanded the use of video analytics (computer vision) across its production processes in general, and in health and safety routines in particular. As part of this initiative:

- the automated PPE usage monitoring system, developed in-house, was rolled out at a Norilsk site production enterprise
- the range of detected H&S violations was expanded (working at height, entering hazardous areas around active equipment, and the unauthorised transport of people using machinery not intended for that purpose)
- a mobile computer vision system was created for safety control monitoring and supporting various work processes in areas where fixed surveillance cameras and communications channels are unavailable (testing is scheduled for 2025)
- optical identification of nickel cathode quality was commissioned in the nickel tankhouse at a metals and mining enterprise of the Kola site, enabling the automated sorting of saleable nickel by grade, ensuring appropriate quality premiums, and reducing commercial losses caused by human error
- development continued on a solution for monitoring mining machinery operation via video streams from onboard recorders: modules were created for recognising the actions of roof bolters, boom drills, and fan drills, which enables tracking machinery and equipment utilisation rates, improves oversight of work order completion, and enhances dispatch efficiency in mines.

Engagement with universities

Nornickel, jointly with Central University, launched the AI in Industry partnership master's programme. As of 1 September 2024, ten individuals enrolled in the Data Science and Data Engineering courses. Over two years of full-time study, they will acquire the necessary skills to work on projects implementing artificial intelligence solutions. The programme is taught by experts from Central University and Nornickel employees. Training is delivered in person at Central University's Moscow campus during evening hours.

The programme curriculum teaches students the fundamentals of programming, provides a solid foundation in Machine Learning, Deep Learning, Data Engineering, and MLOps, and explores business process automation, basic automation principles, and the application of artificial intelligence to workshop and production management.

First semester, Start level

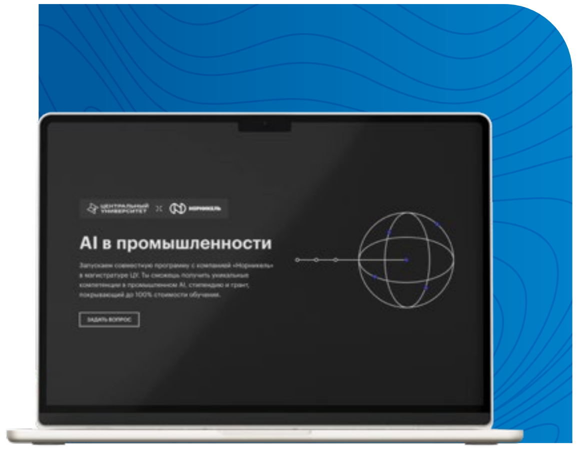
A training grant from Central University, with a RUB 30,000 stipend

Second semester, Medium level

An opportunity to take a paid internship at Nornickel and receive an additional grant equal to 50% of the one awarded by Central University

Pro level

A job offer from Nornickel and a 100% training grant funded by the Company



ЦЕНТРАЛЬНЫЙ УНИВЕРСИТЕТ x НОРНИКЕЛЬ

AI в промышленности

Запускаем совместную программу с компанией «Норникель» в магистратуре ЦУ. Ты сможешь получить уникальные компетенции в промышленном AI, стипендию и грант, покрывающий до 100% стоимости обучения.

ЗАДАТЬ ВОПРОС

Information security

Nornickel's contribution to the Data Economy and Digital Transformation of the State national project and the Digital Transformation of State and Municipal Administration, the Economy, and Social Sphere national goal

Targets and objectives under the national goal

m) Ensure network sovereignty and information security on the internet

The Company's approach to information security (IS)

Nornickel considers the prevention of information security threats a critical responsibility. This priority arises from the substantial impact of potential information security risks across all areas of life, the need to protect critical information infrastructure, and the emerging challenges of cyber resilience in the modern era.

Relevant UN SDGs

9 INDUSTRY, INNOVATION AND INFRASTRUCTURE

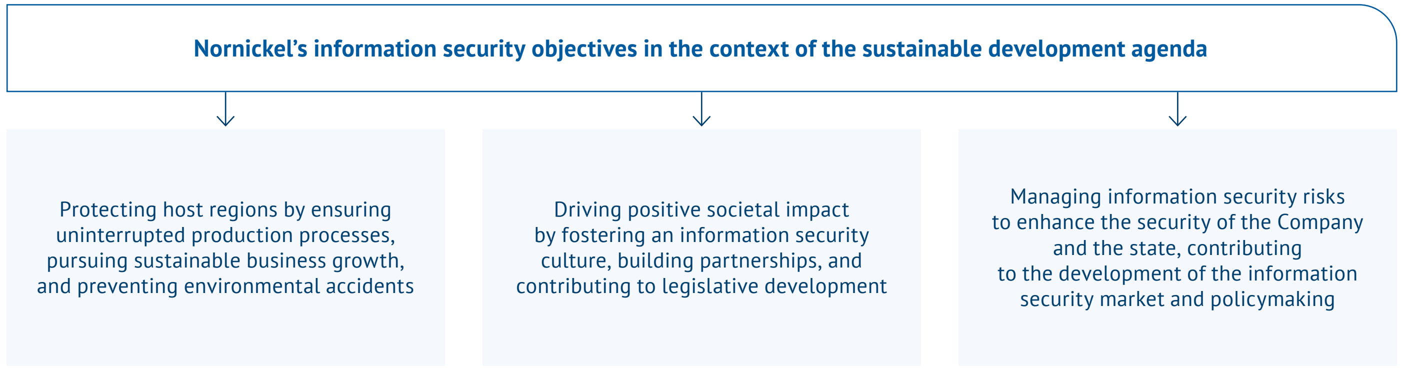
Related federal projects

- Domestic Solutions
- Cybersecurity Infrastructure

Nornickel's key initiatives and focus areas

- Protecting the Company's information systems and infrastructure
- Supporting import substitution and domestic solutions
- Contributing to market development by establishing and strengthening strategic partnerships
- Contributing to policymaking and best practices
- Fostering an information security culture among employees

Going forward, the Company plans to continue along its defined strategic paths, with a focus on strengthening partnerships, fostering dialogue between customers and contractors to minimise third-party risks, and promoting an information security culture, including beyond the Company, as a contribution to the overall security of broader Russian society


Nornickel's information security objectives in the context of the sustainable development agenda

Protecting host regions by ensuring uninterrupted production processes, pursuing sustainable business growth, and preventing environmental accidents

Driving positive societal impact by fostering an information security culture, building partnerships, and contributing to legislative development

Managing information security risks to enhance the security of the Company and the state, contributing to the development of the information security market and policymaking

The operation of the Company's information security management system is governed by internal documents. MMC Norilsk Nickel's Information Security Policy applies to all employees and sets forth the goals, principles, rules, requirements, and restrictions pertaining to information security activities, including the respective roles and responsibilities of the Board of Directors and the Management Board. Top management, specifically the First Vice President – Chief Financial Officer, is responsible for identifying and updating the prioritisation of strategic information security areas, reviewing information security risks, and overseeing budgets for information security programmes and projects. Information security risks are monitored on a regular basis through relevant committees and corporate reporting. The Information Protection and IT Infrastructure Department is a dedicated unit responsible for Nornickel's information security.

In 2024, Nornickel improved its existing approaches to information security management. To ensure consistent development, the information security function strives to enhance its service model by aligning its approaches with best practices in the market. One of the function's key goals for 2025 is to boost the effectiveness of existing information security processes.

The Company's information protection strategy is built with consideration for both an increase in information security risks and the government's ongoing drive to promote import substitution of information technologies and IS solutions. Specifically, in 2024, Nornickel completed the import substitution process for data protection tools used in industrial automation systems within the Company's technology infrastructure.

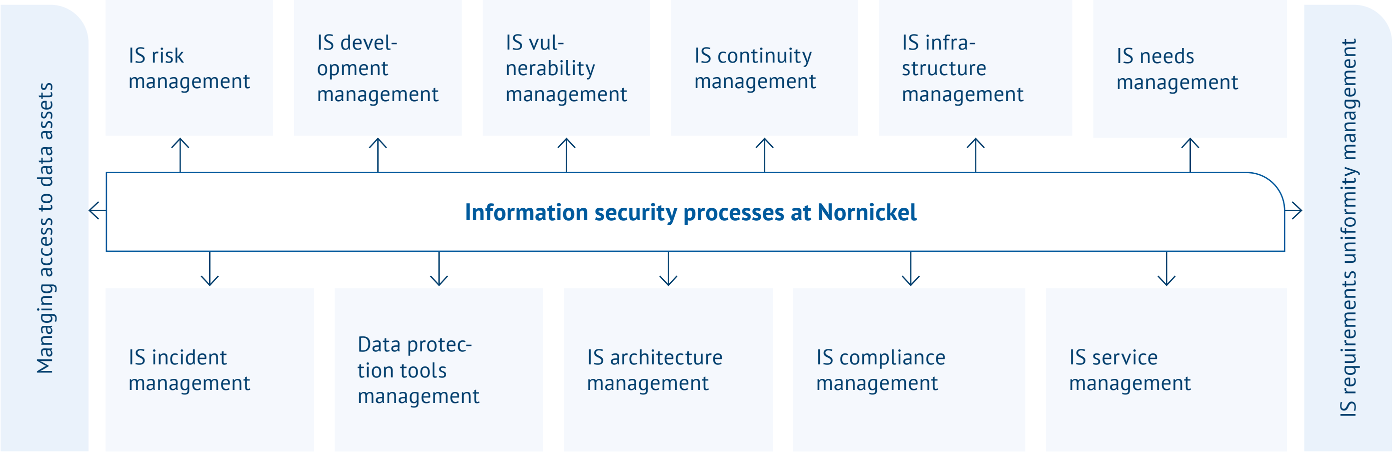
The Company shares its expertise with IS product developers and takes part in refining solutions that are subsequently scaled across the market, thereby ultimately influencing the Russian IS industry's development.

The Company is taking some extra steps to protect the technology infrastructure perimeters of its enterprises and mitigate the risks of production process disruption or shutdown.

With the Company still offering hybrid work schedules for office staff, the first stage of introducing two-factor authentication for employees was completed to minimise the risks associated with unauthorised remote access to corporate resources. The Company is continuously monitoring the security of its corporate systems to promptly identify and address vulnerabilities as well as prevent cyber intrusions.

[1] Risks related to cybercrimes against the Company's processes and systems as well as data privacy compliance risks are listed in the corporate risk management system. The Information Protection and IT Infrastructure Department is the owner of these risks. Information security risk factors, their assessment, and Nornickel's mitigation measures are presented in the Company's 2023 Sustainability Report and Nornickel's 2024 Annual Report.

To enhance the information security management system, in 2024, the Company developed and approved a model of corporate IS processes and implemented an IS process management system to aggregate information on key performance metrics and ensure high availability of IS services for internal customers within the service model, including through additional steps to boost protection against external cyber threats.


Managing access to data assets

IS risk management

IS development management

IS vulnerability management

IS continuity management

IS infrastructure management

IS needs management

Information security processes at Nornickel

IS incident management

Data protection tools management

IS architecture management

IS compliance management

IS service management

IS requirements uniformity management

Certification

Nornickel's information security management system (ISMS) was built in line with ISO/IEC 27001. Five Group enterprises have been certified to ISO/IEC 27001.

In 2024, activities aimed at transitioning site-level ISMS to ISO/IEC 27001:2022 were implemented to maintain cyber-defence processes at a high maturity level. The effectiveness of information security management processes across production sites was confirmed by audits. The independent auditor noted strong management engagement in ISMS processes and the preparedness of Group enterprises to respond to external threats and challenges. ISMS teams showed a high level of information security knowledge.

Security and vulnerability management

The Company has completed all activities planned for 2024 to boost the overall security of its automated process control systems (APCSs) and to implement audit recommendations from 2023.

The Energy Division's production enterprises completed their activities under the plan to implement basic process safeguards, facilitating the mitigation of IS risks at enterprises critical for the energy security of Group enterprises as well as cities and towns in the Far North.

In close collaboration with key information security market partners, the Company has refined a number of domestic solutions offered by leading manufacturers of technological and production process automation systems and aligned them with Nornickel's information security requirements.

In the reporting year, the Company enhanced its approaches to managing vulnerabilities and conducting vulnerability analysis of corporate systems, with a special focus on APCS testing. Vulnerabilities in operational systems were identified and promptly addressed, strengthening information security. Regular security analysis measures and drills to improve coordination with the response centre team also help identify and address weaknesses in security systems.

The Company is focused on improving IS processes throughout the software development lifecycle. Deploying the DevSecOps platform helps automate key security controls by integrating them directly into software development. The Company has bolstered its resilience against supply chain attacks by implementing a corporate software repository for all third-party software installations and updates.

>20 ths

IS events handled by the Centre's employees in 2024 (>18 thousand in 2023)

>1 ths

cyber incidents analysed by the Centre's employees in 2024

0

computer security incidents recorded across Nornickel's critical infrastructure facilities in 2024

6 ths

investigations into Nornickel employees' reports conducted in 2024

Cyber incident response system

Nornickel has in place a Cyber Incident Monitoring and Response Centre, which employs advanced technical solutions and best practices in managing cyber defence. The Centre's employees consistently demonstrate a high level of proficiency, as evidenced by the Nornickel team's exceptional knowledge and unique skills demonstrated in three competitions held in 2024.

Continuous monitoring of the IS landscape and sharing best practices with colleagues from other companies and market partners enable the Centre to implement proactive measures to block malicious activity.

Despite a significant growth in cyberattacks, the Company maintained the integrity of Nornickel's infrastructure, successfully repelling all attempts to damage it.

Any Nornickel employee detecting any suspicious content or activity on company devices can send an alert to the information security team for investigation. Experts assess the possible negative impact on the Company's information systems and take measures to prevent and eliminate the consequences of incidents.

Requirements for counterparties

In 2024, cases of compromised IT infrastructure were identified for several contractors, with response measures taken to block relevant contractors' access to Nornickel's infrastructure and prevent possible negative consequences.

The Company developed a contract section outlining information security requirements and liability for non-compliance by counterparties getting access to Nornickel's data assets under relevant contracts. In 2024, this section was already added to the general terms and conditions for Company contracts. In addition, the Company amended its standard confidentiality agreement / NDA to include the counterparty's obligation to ensure information security measures are implemented and to provide relevant details upon the Company's request. Mandatory two-factor authentication was also implemented for all third-party employees, along with a series of restrictive measures governing access for counterparties with privileged rights within information systems.

A methodology for evaluating the information security status of Nornickel's counterparties is currently under development. This will enable the Company to implement additional safeguards for its corporate data assets.

Personal data protection

Nornickel implements a set of legal, organisational, and technical measures to ensure the security of personal data (PD). Technical protection of PD involves anti-virus protection, leak prevention, monitoring of removable devices, analysis of security incidents, etc.

The Company places particular emphasis on maintaining legal compliance of its personal data processing. As part of this commitment, a relevant department at Nornickel developed and implemented corporate guidelines in 2024.

A methodology for lean PD processing was developed at the Company to reduce the risk of PD leaks by minimising PD processing within business processes.

8 Group enterprises brought their personal data processing procedures into full compliance with legal requirements and internal regulations

11 Group enterprises assessed their websites for compliance with legal requirements to PD processing

Information security training and communication

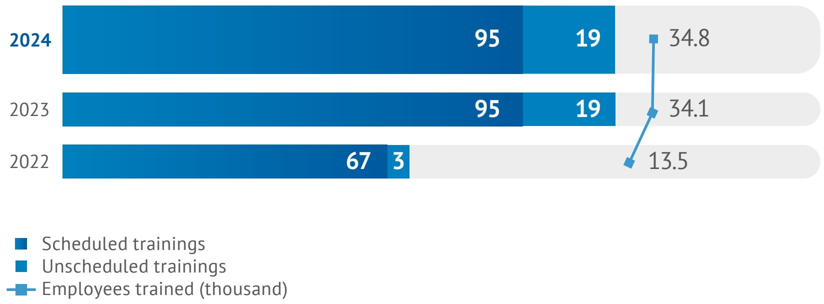
In line with its objective to foster an information security culture across the Group and reduce the impact of human error in IS incidents, Nornickel places particular emphasis on raising awareness among all employee categories about IS requirements and digital hygiene practices.

Information security issues are covered during mass corporate events and strategic sessions. Employees are updated via internal communication channels: publications on the intranet portal, mailings, corporate messenger, postings on bulletin boards, and videos on screens in common areas.

Employees receive regular training on relevant IS topics, including online courses and training sessions updated to reflect the evolving threat landscape and legislation.

To enhance employees' vigilance and practice the sequence of actions in case of an information security incident, the Company runs regular drills, including simulations of phishing attacks and other current unlawful practices that affect users. Following the drills, instructions for employees are updated.

Nornickel also prioritises the personal information security of employees and their families, implementing initiatives for employees' children (such as cybersecurity games, meetings with experts, and educational videos on IS fundamentals).



Cybersecurity culture is an integral part of Nornickel's cultural DNA – one that extends beyond the Company and contributes to both business resilience and national cybersecurity efforts.

Partnerships and best practice sharing in information security

Established at Nornickel's initiative, the Information Security in Industry Club (BIP-Club) brings together chief information security officers and IS experts to share expertise, engage in public-private dialogue, develop universal information security requirements, explore innovative solutions, and foster mutually beneficial partnerships.

In 2024, BIP-Club continued its activities and, as part of a public meeting for market participants, brought together for the first time vendors, integrators, customers, and market regulators to discuss their approaches, requirements, and expectations for partners, as well as outlooks for productive collaboration under the import substitution programme.

In addition, the Company used BIP-Club to propose to the information security community a Code of Ethics for the Information Security Market, containing a set of principles that will help improve the maturity of the market and foster better cooperation between customers and contractors.

Nornickel engages in strategic collaborations with leading market players to develop and introduce cybersecurity solutions designed to bolster the cyber resilience of the metals and mining industry.

Nornickel also collaborates with a number of leading Russian universities on joint projects, encouraging and recruiting young talent to pursue careers in industrial information security.

> **The agreement with Nornickel is aimed at the continuation and expansion of our cooperation, consolidation of expertise, efforts, and resources to ensure information security in the metals and mining sector. Our experts note the increased focus of attackers on critical information infrastructure and predict a rise in destructive attacks on Russian companies. Together with Nornickel, we will be able to make a significant contribution to the industry's cyber resilience to be prepared for growing threats and challenges.**
>
> **Mikhail Oseevsky,**
> President of Rostelecom