ANTI-CORRUPTION AND INTEGRITY

Starting in 2015, all of the Company employees sign an agreement setting out their obligations in the anti-corruption area. All of the Company's employees are familiarised with the corporate Anti-Corruption Policy and related regulations.

2016 milestone

November 2016

the Company joined the United Nations Global Compact, which aims to promote recognition and practical application of ten basic principles of human rights, labour, environment and anti-corruption by businesses worldwide.

The Company complies with anti-corruption laws of the Russian Federation and other countries where it operates, as well as with applicable international laws and internal regulations. This promotes the Company's reputation and strengthens trust and confidence of shareholders, investors, business partners and other stakeholders. As part of its effective anti-corruption combat, the Company has developed and approved the following anti-corruption regulations:

- Business Ethics Code;
- Code of Conduct and Ethics for Members of the Board of Directors;
- Anti-Corruption Policy;
- Regulation on the Product Procurement Procedure for MMC Norilsk Nickel's Enterprises;
- standard anti-corruption agreement – appendix to the employment contract;
- Regulation on Information Security;
- Regulation on the Prevention and Management of Conflicts of Interest;
- Regulation on Business Gifts;
- Procedure for Anti-Corruption Due Diligence on Internal Documents at the Head Office of MMC Norilsk Nickel;
- Regulation on the Conflict of Interest Commission;
- Information Policy.

Having joined the Anti-Corruption Charter of the Russian Business, **the Company implements dedicated anti-corruption measures based on the Charter and set forth in the Company's Anti-Corruption Policy**. In November 2016, the Company joined the United Nations Global Compact, which aims to promote recognition and practical application of ten basic principles of human rights, labour, environment and anti-corruption by businesses worldwide.

Starting in 2015, all of the Company employees sign an agreement setting out their obligations in the anti-corruption area. All of the Company's employees are familiarised with the corporate Anti-Corruption Policy and related regulations.

The Company ensures functioning of the Preventing and Fighting Corruption page on the corporate intranet containing information on anti-corruption regulations adopted, measures taken, preventive procedures introduced, legal training sessions organised and law-abidance promotion efforts taken.

Nornickel's Corporate Security Unit continuously identifies, analyses and assesses the financial, corruption, reputational and other risks entailed by large-scale operations, with close attention paid to business reputation, reliability and solvency of potential partners and counterparties.

Regulating the conflict of interest

One of the key anti-corruption measures is timely prevention and management of conflicts of interest. Procedures for assessing and settling conflicts of interest are set forth in the Regulation on the Prevention and Management of Conflicts of Interest at MMC Norilsk Nickel. As part of the regulation, the Company has approved the standard declaration form for reporting conflicts of interest, to be filled in by candidates applying for vacant positions or by the Company's employees whenever required.

The regulation extends to all employees of the Company and sets forth key principles that include obligation of each employee to disclose a conflict of interest, as well as non-retaliation for reporting the conflict of interest.

On top of that, the Company has undertaken measures aimed at preventing potential conflict of interest involving the directors and senior managers. From December 2016, members of the Board of Directors are required to annually submit information on relatives and family as per the approved form.

The Company takes measures aimed at identifying related-party transactions. All measures combined, undertaken

To make a report, anyone is invited to call a toll-free 24/7 hotline:

+7 800 700-19-41,
+7 800 700-19-45,

or e-mail to
skd@nornik.ru.

in order to identify and prevent conflicts of interest, minimise the probability of negative consequences for the Company.

Insider information

The Company implements initiatives to prevent unauthorised use of insider information. In accordance with Federal Law No. 224-FZ of 27 July 2010 On Prevention of Unlawful Use of Inside Information and Market Manipulation and on Amendments to Certain Legislative Acts of the Russian Federation, as well as the Market Abuse Regulation of the European Parliament and of the Council No. 596/2014 of 16 April 2014, the Company keeps a list of insiders, reviews by-laws and corporate events, to control implementation of measures as provided for in the Russian and international legislation, which includes disclosure of insider information. The Company also undertakes other measures aimed at preventing unlawful use of insider information.

From December 2016, members of the Board of Directors are required to annually submit information on relatives and family as per the approved form.

Corporate Trust Service

The Corporate Trust Service is part of the Internal Control Department and helps the Company's management to promptly respond to reports of abuses, embezzlement and other violations. Employees, shareholders and other stakeholders have an opportunity to report any actions that will or might result in financial damages or be detrimental to the business reputation of the Company. The key principles underlying the Corporate Trust Service include guaranteed confidentiality for whistleblowers, timely and unbiased consideration of all reports. In no circumstances does the Company impose sanctions (dismissal, demotion, deprivation of a bonus) against the employee who submitted a report to the Corporate Trust Service.

To make a report, anyone is invited to call a toll-free 24/7 hotline: +7 800 700-1941, +7 800 700-1945, or e-mail to skd@nornik.ru.

Information on received and processed reports is disclosed annually by the Company as part of its CSR report.

Comprehensive security framework

In 2018, the corporate security was ensured through continuous review of corporate risks and threats. The comprehensive corporate security system underpinned by the MBO (Management by Objectives) principles enabled the Company to promptly respond to key risks in economic, corporate, information and physical security, counter embezzlement and illicit trafficking of precious and non-ferrous metals, and efficiently prevent in-house corruption.

In 2018, the corporate security was ensured through continuous review of corporate risks and threats.

As the Company is engaged in manufacturing and selling products containing precious metals, Nornickel's Corporate Security Unit developed a comprehensive identification methodology for products containing precious metals which have been stolen or illicitly traded. The methodology have gained recognition internationally and was further developed into an automated information retrieval wizard powered by a unique databank of strategically important raw materials.

As part of its efforts to improve the effectiveness of the measures against cross-border illicit trading and smuggling of precious metals, the Company participates in developing a unified databank of products of Russian and South African MMCs.

Nornickel complies with anti-terrorism requirements and enhances security of the Company's strategic power and transportation facilities. In 2018, Nornickel conducted 126 routine training sessions and organised four tactic drills together with the Federal Security Service, Ministry of Internal Affairs, EMERCOM and National Guard of the Russian Federation. The main objective of these activities was to enhance anti-terrorist security at industrial and social sites.

As part of its efforts to improve the effectiveness of the measures against cross-border illicit trading and smuggling of precious metals, the Company participates in developing a unified databank of products of Russian and South African MMCs.

In 2018, Nornickel conducte

126

routine training sessions

and organised four tactic drills together with the Federal Security Service, Ministry of Internal Affairs, EMERCOM and National Guard of the Russian Federation

The Company has an Information Security Policy in place

that defines relevant business processes and areas including governance processes at strategic and tactical levels, operational processes, and corporate governance responsibility for information security.

As part of its information security framework, Nornickel:

- categorises information assets and assesses information security risks;
- manages information security requirements at different stages of the information system life cycle;
- ensures compliance with the legal and regulatory information security requirements;
- manages its information security architecture;
- uses technical means to ensure information security of assets;
- raises awareness in information security;
- manages information security incidents;
- ensures information security of the process control system;
- conducts information security assessment and reporting.

The Company pays close attention to safety and confidentiality of the employee and counterparty personal data.

The implemented solutions allow to identify and properly respond to new threats and risks.

Monitoring of cyber security performance is part of the Company's information security management system and information security assessment and reporting. The results of performance assessment of cyber security systems are reviewed at a corporate level and are circulated to the governance bodies and employees through corporate procedures and initiatives.

On top of that, Nornickel's Information Security Charter for Critical Industrial Facilities, an initiative proposed at a meeting of the Club of Information Security in Industry, stood the test of Russian companies and was welcomed at the Partnership of State Authorities, Civil Society and the Business Community science forum (tech version of Davos) held in Germany. The Charter was praised at the OSCE's cyber security conference in Rome and was handed over to the OSCE Secretariat for review as part of proposals for combating cyber threats and attacks on information infrastructure.