Speaking at a session of the Club of Information Security in Industry, Norilsk Nickel's Head of Information Security and IT Infrastructure Dmitry Grigoryev has called for the industrial sector to build a collective security system.

Referencing Nornickel's information security initiatives that have come out valid and workable both on a corporate and global scale, Mr Grigoryev said: "The Information Security Charter for Critical Industrial Facilities developed by our experts has proved viable. Following successful validation by the club members and leading international experts alike, the charter is now under review at the OSCE."

Mr Grigoryev also praised the role of the club in promoting effective cyber secury collaboration among its members.

"The club is more than just a forum for discussion, it is a 'think tank' for generating viable cyber strategies for the Russian industrial sector — those fit for the ever-changing challenges and threats, and leading to robust and economically viable outcomes. I believe our next step is to build a practical interaction framework for the Russian industrial companies to combat massive cyber attacks on their infrastructures. We will be ready to present a blueprint for that at the next session of the club," said Mr Grigoryev.

Andrey Krutskikh, Russian President's special envoy on cyber security, who participated in the session, supported Nornickel's endeavours, pointing to the need for the Russian Ministry of Foreign Affairs and the Russian private sector to consolidate efforts in pushing this agenda forward at the UN, OSCE, BRICS, and SCO level.

The President's advisor also welcomed the recent positive momentum emerging for the government and business community to harmonise their efforts — including those in the realm of information security — on the global stage.

"We all see that the global cyber security dialogue needed to address the threats like hacking, cyber terrorism and attacks on information infrastructure has turned into a grotesque contest of everyone blaming one another. Its political bias is a setback to the progress of building a generally accepted system of global cyber security. In the face of economic globalisation and process digitalisation, a pragmatic and reasonable advocacy of the business groups representing the backbone of the country's economy can be of significant value for carving out a basic set of clear-cut cyber security rules and standards of conduct. Cyber security of Russian companies and their assets is an imperative for the country's economic well-being," Mr Krutskikh said.

The session's agenda also centred around the themes of cyber security economics and the potential risks and benefits coming with stronger reliance on cloud technologies, with a special focus made on the external impact on corporate information security policies, including the choice of vendors and suppliers.

Notes to editors:

The Club of Information Security in Industry was established in 2017 at Nornickel's initiative. It is an informal network of information security officers from the Russian industrial sector. Its members include Severstal, Enel Russia, NLMK Group, Renova Group, Polyus, Lukoil, Transneft and others.

The Information Security Charter for Critical Industrial Facilities is a body of cyber security rules and standards of conduct developed by Nornickel's experts with a view to combating unfair competition and preventing damages to industrial facilities caused by misuse of information and communication technologies.

The draft Charter was approved by the 12th International Forum titled Partnership of State Authorities, Civil Society and the Business Community in Ensuring International Information Security, that took place in Garmisch-Partenkirchen (Germany) in April, and was subsequently presented at the OSCE-wide Conference on Cyber/ICT Security held in Rome in September 2018.

*1 November 2018*