Information Security

GRI 418-1

While technological progress provides opportunities for our business, it also brings threats. Transitioning to the remote work made cyberattacks become increasingly common. To counter these threats, Metinvest is taking a comprehensive approach to enhancing its information security measures.

We protect data privacy and adhere to applicable laws on the collection, use and protection of personal information.

The Group also operates an internal document system and works to and systematically improve it. In particular, we have in place an information security strategy and policy, as well as regulations and instructions that govern specific processes. The main provisions for protecting confidential information are set out in our Privacy Policy Statement, which we last updated in March 2020.

Metinvest is guided by recognised industry standards and approaches on cybersecurity issues. At the Group level, we use the ISO 27001 standard to ensure information security. We are implementing NIST SP 800 approaches for process optimisation and comply with GDPR and Ukrainian regulations to protect data privacy. We employ MITRE solutions as a problem-solving tool to improve our threat detection capabilities. We also use best

practice and configurations from the CIS Benchmarks security library as technical guidelines.

The Group uses a combination of technical and organisational measures to ensure information security. We achieve multi-layered protection of our IT infrastructure through the usage of modern solutions such as firewalls, intrusion prevention systems, cloud infrastructure protection (Azure Security Centre and web application firewalls), network traffic analysis, analysis of atypical operations and activity (user behaviour analytics), and centralised monitoring and management of IT components (configuration management and vulnerability management).

The core component of our information security management efforts is our cybersecurity centre. It is especially helpful in cases where we are dealing with highly skilled attackers who use methods to bypass automated defence mechanisms. The centre monitors Metinvest's IT infrastructure and production processes, preventing cyberattacks against the Group and coordinating the work of IT departments during incidents.

Data Leakage Prevention System

We perform private data inventory, classification and leakage risk assessment using the following:
– Employing data marking and encryption tools
– Identifying and blocking unauthorised data transfer attempts
– Training employees about how to work safely with information
– Monitoring high-risk transactions and roles
– Revalidating access rights and powers
– Providing secure connections to corporate resources
– Using secure corporate video conferencing and document collaboration tools

Metinvest employs the five functions of the NIST Cybersecurity Framework (identify, protect, detect, respond, recover) to provide a comprehensive protection mechanism that makes extensive usage of technology and machine learning. To increase employee awareness about information security issues, we are introducing an IT security basics briefing, mini-courses on specific aspects of information security, in-person trainings for automated process control system personnel and periodic training cyberattacks for the Group's employees.

To maintain an adequate level of protection and determine future development priorities in this area, Metinvest systematically conducts internal audits and targeted external audits of the information security function's effectiveness. As part of our continuous improvement, we track operational metrics for each process and perform self-assessments to ensure compliance with best practice. In 2020, we began verifying the reliability of our security through the engagement of ethical (white hat) hackers to perform multi-vector penetration testing. This type of verification employs the same attack methods as actual hackers. It helps us to understand what to prioritise when adjusting system security and provides an opportunity for continuous improvement and training of our team under real-life security conditions.

In 2020, Metinvest demonstrated the high level of its information security practices by receiving a score of 49% in the Microsoft Secure Score rating, which is 15 percentage points above the average score for similar companies in the industry.