

Information security

In today's world, information is a valuable resource, and its protection is critical to business operations. We strive to meet the highest standards in this area and successfully prevent cyber attacks and other IT incidents.

Key documents

Internal regulations:

- ▶ Information Security Policy
- ▶ Policy for Control of Information Security Management Systems
- ▶ Password Policy
- ▶ Regulations on User Account and Access Management
- ▶ Procedure for Drafting and Amending Firewall Rules
- ▶ Information Security Compliance Standard for Creating Information Systems and Services
- ▶ Personal Data Processing Policy

External regulations:

- ▶ Decree of the President of the Russian Federation No. 250 On Additional Measures to Ensure the Information Security of the Russian Federation dated 1 May 2022
- ▶ Resolution of the Government of the Russian Federation No. 1272 On Approval of a Model Regulation on the Deputy Head of the Body (Entity) Responsible for Ensuring its Information Security in the Body (Entity), and a Model Regulation on a Structural Unit within the Body (Entity) Ensuring its Information Security dated 15 July 2022
- ▶ Federal Law No. 98-FZ On Trade Secret dated 29 July 2004
- ▶ Federal Law No. 149-FZ On Information, Information Technologies and Information Protection dated 27 July 2006
- ▶ Federal Law No. 152-FZ On Personal Data dated 27 July 2006

Priority UN SDGs



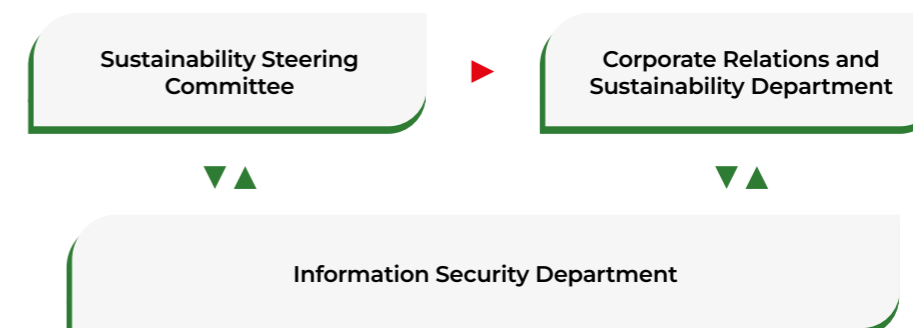
Our approach to information security management

Magnit's information security is based on a set of interrelated organisational and technical tools which comprise an integrated information security management and assurance system. Our comprehensive approach enables us to protect ourselves against modern cyber threats, comply with Russian legal requirements and international standards, and prevent financial,

reputational and other damage. The Company's information security system is designed and developed in line with global best practices.

Magnit has a formalised procedure for internal auditing, which falls within the remit of a dedicated department. We regularly assess information security risks and test our information systems on a quarterly basis.

Information security governance structure



▶ Administrative subordination
 ▶ Coordination under the sustainability strategy and advisory support

Information security (continued)

Cyber security system

In line with our commitment to maintaining a cyber security system, we identify and eliminate vulnerabilities in information devices, search for viruses and zero-day attacks¹, while also monitoring and responding to security incidents. Magnit monitors the integrity of software architecture across all of its external IT services. We carry out scheduled updates of network devices, servers and software.

We run daily scans of all of the Company's external addresses for known vulnerabilities and eliminate all threats. All of Magnit's web services are protected through web application firewalls (WAFs), designed to detect and block network attacks on web applications. We actively employ anti-DDoS solutions², and regularly scan open internet ports. Twice a year, Magnit conducts an external independent penetration testing of its IT system.




In 2022, we saw a significant increase in the number of cyber attacks on Magnit's IT assets. Tens of thousands of scanning and network attacks by hackers were detected, as well as more than 500,000 attempts to infect our IT infrastructure with malware through the email system. We have taken additional steps to enhance our security and were able to successfully withstand cyber attacks and avoid any disruptions in the infrastructure's operations.

Development of IT security competencies

One of our information security priorities is to make employees more aware of cyber security rules. We lay particular emphasis on the training and professional development of the employees at our IT Department who are involved in ensuring the operability of Magnit's IT infrastructure and

In addition, we have started transitioning to domestic IT security solutions as foreign vendors in this area have left the Russian market. In 2023, we will continue to implement information security tools offered by leading Russian developers.

To ensure the information security of our customers, we have implemented the Anti-Fraud system, which offers:

-  ▶ protection against interception and theft of account details used in Magnit's mobile application;
-  ▶ protection against fraudulent accrual and redemption of loyalty programme points;
-  ▶ access control to loyalty card data to prevent leakage of information on customer balances and card numbers.

In 2023, we plan to conduct an audit of personal data processing procedures to ensure compliance with the requirements of Federal Law No. 152-FZ On Personal Data dated 27 July 2006. In addition to this, we intend to develop DevSecOps³ processes and standardise approaches and tools used by our development teams.

information systems. Other departments working with IT systems in their day-to-day operations also hold regular trainings. We regularly train our employees working in various departments responsible for personal data processing.

Focus areas for raising employee awareness about information security

Safe operation of information systems

Corporate password policy

Detection of phishing and social engineering attacks

Corporate information security standards

To ensure the security of remote and hybrid work, we have developed and launched a distributed, geographically resilient, and scalable remote access system for all employees of the Company's head office and branches. This helped us ensure business process continuity and increase employee mobility. We are exploring opportunities to optimise office space, expand the geography of sourcing candidates for positions in the Company, and make our employees' work more comfortable.

We continue to focus on information security while navigating the transition to remote working. Among other things, our employees now always use two-factor authentication when connecting to the Company's systems, and also have various security products and policies run on their corporate devices which track and block attempts to gain unauthorised access and compromise users' accounts.

Protection of personal data

We have developed a systematic approach to protecting the personal data of our stakeholders and continuously monitor the existing and planned information systems to ensure that personal data is processed appropriately and lawfully. Employees working with user data, including those in the IT Department, are duly trained, and persons charged with organising the processing of personal data receive regular briefings. We have developed consent forms for the processing of personal data, which are required to be filled by each employee, and appointed people responsible for organising and monitoring the data protection process.

We believe it essential to raise awareness of information security, including personal data protection, among all our employees. We support and monitor business processes that require the processing of personal data as a means to safeguard the Company against possible sanctions from the government authorities. We also give guidance to experts from our subsidiaries on regulating the personal data processing matters.

Magnit has an established procedure for reporting personal data breaches. We maintain a log of IT security incidents in information systems for processing personal data; in 2022, no such incidents were reported. Furthermore, Magnit maintains a log of requests and enquiries regarding personal data from external stakeholders. In 2022, the Company received XX enquiries and provided a reasoned response in writing within the deadlines stipulated in the relevant by-laws.

We carry out regular risk assessments as part of internal audits, as well as analyse processed data, develop and update threat models for information systems, design and implement technical solutions to eliminate such threats, and draft guidelines and regulations that help us comply with the laws on personal data.

¹ Zero-day – an exposed software vulnerability or malware with no identified means of containment

² Anti-DDoS is a tool of protection against DDoS attacks, which aim to disrupt the computer system through a constant stream of requests.

³ DevSecOps (short for development, security, and operations) is the practice of integrating security testing at every stage of the software development process.