

TECHNICA NOVA BALTICA

People who create energy.

IT and Cyber Security

Last Updated 01.09.2025

IT and Cyber Security

To ensure protection of company and customer information, Technica Nova Baltica applies basic IT and cyber security practices proportionate to the size and nature of its operations.

IT infrastructure management

The company uses modern cloud-based collaboration platforms, primarily Microsoft 365, to store and process business information.

IT systems are configured and maintained by external IT service providers under the supervision of company management.

All systems are configured according to security best practices and regularly reviewed.

Device security

All devices used to access company systems must meet minimum security standards:

- devices must be protected with passwords or biometric authentication
- operating systems and software must be kept up to date
- antivirus or built-in system security mechanisms must be enabled
- devices must not be shared between users without appropriate access control

Where possible, company devices are centrally configured and secured.

Access control

Access to systems and information is granted based on the principle of least privilege.

This means that:

- users receive only the access necessary to perform their tasks
- access rights are reviewed periodically
- access is immediately revoked when cooperation ends

Privileged or administrative access is restricted to authorized personnel only.

Backup and data protection

To prevent loss of information:

- business data is stored primarily in secure cloud environments,
- backup mechanisms provided by the cloud platform are used,
- critical documents are stored in shared organizational repositories rather than local devices.

Network security

Employees are required to use secure networks when accessing company systems. Public or unsecured networks should be avoided or used only with appropriate precautions. Remote work is conducted using secure communication platforms such as Microsoft Teams.

Security monitoring and incident management

Any suspected cybersecurity incident such as:

- phishing attempts,
- unauthorized access,
- malware infection,
- data leakage.

must be reported immediately to the designated company contact or IT provider. Incidents are analyzed and appropriate corrective actions are implemented.

Awareness and training

Employees and collaborators are encouraged to follow good cybersecurity practices, including:

- recognizing phishing attempts,
- protecting login credentials,
- avoiding the use of unauthorized software,
- reporting suspicious activity.

Periodic reminders and guidance may be provided when necessary.