

TECHNICA NOVA BALTICA

People who create energy.

INFORMATION PROTECTION AND DATA SECURITY POLICY

Last updated 01.09.2025

1. Policy objective

Information security is the foundation of the trust placed in us by our partners, customers and associates. At Technica Nova Baltica, we strive to ensure that all data, regardless of its form and source, is protected in a responsible manner commensurate with the risks.

The purpose of this policy is to define the principles that help us maintain the confidentiality, integrity and availability of the information processed in the course of our business.

2. Scope

The policy applies to every person working with TNB – regardless of the legal form of cooperation – and to all information used in the course of projects, tasks and internal communication.

It covers both digital data (stored in the cloud or on electronic devices) and paper documents, e-mails, team chats and information shared during remote work.

3. Classification of information

To better protect information, we classify it into four categories that help determine the level of protection required:

- **Public** – intended for sharing on the website, in promotional materials, etc.
- **Internal** – information intended for internal use only, without permission for publication.
- **Confidential** – business data requiring confidentiality (e.g. customer data, contracts, projects).
- **Restricted** – information of particular importance, e.g. financial, legal, operational, design, the leakage of which could expose the company to serious consequences.

4. Access management

Access to information at TNB is based on the ‘need to know’ principle – it is only granted to those who need it to perform their tasks.

For security reasons:

- each person uses an individual account secured with a strong password,
- where possible, we use two-factor authentication (MFA),
- access is verified on a regular basis – especially when roles change or cooperation ends.

5. Digital security

All devices used to work with TNB must meet basic digital security standards.

We ensure that:

- Only approved platforms and tools (e.g. Microsoft 365) are used.
- we work in secure networks,
- we regularly update security software,
- we respond immediately to phishing attempts, suspicious messages or data breaches.

6. Physical document security

Although we process most data digitally, paper documentation also requires adequate security.

We apply the principle of restricted access and ensure that:

- confidential documents are stored in locked cabinets,
- printing is only done when justified,
- documents containing sensitive data are destroyed,
- they are not left unattended in public areas.

7. Confidentiality of project information

TNB has a policy of confidentiality – information related to projects, clients and business partners cannot be disclosed to third parties without express consent.

For some collaborations, we require the signing of non-disclosure agreements (NDAs).

8. Responding to incidents

If you notice a threat to data security – whether digital or physical – you should immediately inform the person coordinating the collaboration.

Every reported incident will be analysed, and if necessary, we will take corrective action and inform those who may be affected.

9. Education and awareness

We realise that information security depends not only on tools, but above all on attitudes. That is why every person who starts working with TNB is familiarised with this policy, and we remind them of the most important rules from time to time – in the form of communications or training.