

Information Security Policy

TAKTONUM GROUP N.V.

Version: August 18, 2025

This Information Security Policy (hereinafter the "Policy") establishes the principles, responsibilities, and requirements for protecting the confidentiality, integrity, and availability of TAKTONUM GROUP N.V. (WEI\$\$)'s information assets.

The Policy outlines the requirements for the acceptable use and protection of WEI\$\$'s assets, including information systems, data, infrastructure, and related resources. It applies to all employees, contractors, and third parties who have access to WEI\$\$ information or systems.

The purpose of this Policy is to:

- Ensure the security of information processed, stored, or transmitted by WEI\$\$;
- Protect WEI\$\$y and its clients from information security threats;
- Define responsibilities for maintaining information security;
- Support compliance with applicable laws, regulations, and contractual obligations.

Policy introduction and management

This Information Security Policy (hereinafter the "Policy") establishes the principles, responsibilities, and requirements for protecting the confidentiality, integrity, and availability of TAKTONUM GROUP N.V. (WEI\$\$)'s information assets.

The Policy outlines the requirements for the acceptable use and protection of WEI\$\$'s assets, including information systems, data, infrastructure, and related resources. It applies to all employees, contractors, and third parties who have access to WEI\$\$ information or systems.

The purpose of this Policy is to:

- Ensure the security of information processed, stored, or transmitted by WEI\$\$;
- Protect WEI\$\$y and its clients from information security threats;
- Define responsibilities for maintaining information security;
- Support compliance with applicable laws, regulations, and contractual obligations.

WEI\$\$ will verify compliance to this Policy through various methods, including but not limited to periodic walkthroughs, business tool reports, and internal and external audits.

1.1 Management intent

WEI\$\$ management is committed to using available means of communication and execution of management decisions to enforce this Policy throughout the organization. Overall, WEI\$\$ management is accountable for implementation of this Policy and will monitor the adherence based on the information available in form of relevant metrics, and input from risk and incident management processes.

1.2 Non-compliance

Violations of this Policy can have severe consequences for WEI\$\$ and its clients, such as reputational damages, civil, administrative, or criminal liability, and/or sanctions imposed by state authorities.

Policy statements

2.1 Requirements for data processing

Data owned by WEI\$\$ is classified into one of the following five categories:

- Public;
- Internal;

- Confidential.

The specialist of WEI\$\$ who processes «Confidential» information shall take necessary measures to hold such information from any person not entrusted with it by WEI\$\$.

It is prohibited to provide public network access to resources with confidential information, as well as to allow outside persons to work on computers containing this information.

Electronic confidential information shall be archived and protected from unauthorized reading and copying.

When copied to mobile devices, electronic files must be encrypted. By default, users are recommended to avoid storing any WEI\$\$ or client's data on mobile devices persistently. It is required to avoid printing confidential information unless necessary.

In case of any confirmed or suspected compromise of WEI\$\$ sensitive information, the specialist must report the event as security incident to Information Security Office.

It is required to avoid attachments of sensitive documents in information systems (e.g., Gmail, etc.).

2.2 Requirements for using software

Specialists of WEI\$\$ are provided with software necessary for performing assigned duties.

The software must be updated in accordance with the latest corrections and additions. After updating, the endpoint device shall be restarted if the system requires.

All software must be installed in compliance with applicable requirements.

Installation of additional (paid or free) software can be initiated by the Head of the structural subdivision or by the specialist of WEI\$\$ themselves (on condition that this was agreed with the specialist's immediate supervisor) and should be approved by Information Security Office.

When using the software, it is forbidden to:

- use the software not for its intended purpose;
- change the composition of the installed software on the specialist's endpoint device (install new software, change, or delete the software);
- bring external data carriers with any system or application software (including portable versions) that is not defined as a standard for WEI\$\$ and run the software on the endpoint device without authorization.

The specialists of WEI\$\$ are strictly forbidden to install and launch the following software:

- counterfeit software;
- software intended for receiving unauthorized access to the information systems or its components;
- software intended for cryptanalysis and password guessing of information system data accounts;
- malware or other software that may violate the information security of WEI\$\$;
- software intended for auditing of the WEI\$\$ network;
- software intended for hidden remote access.

The Head of Information Security Office can allow the specialist of WEI\$\$ to use the forbidden software on an individual basis (upon the request of the customer, for a technical task, etc.).

2.3 Requirements for using anti-virus software

Anti-virus software shall be standardized and installed on every endpoint device.

Anti-virus software shall be updated in accordance with the latest improvements and add-ons and installed upon delivery.

Stopping anti-virus software from running is only allowed upon approval by the Head of Information Security Office.

The specialists of WEI\$\$ are forbidden to:

- use software, electronic documents and/or any other electronic information not scanned by anti-virus;
- send files not scanned by anti-virus by email;
- download information from insecure websites on the Internet;
- stop operation of anti-virus software without authorized permission.

If the endpoint device is suspected of being infected, the specialist of WEI\$\$ shall proceed as follows:

- stop all operations and do not perform any information sharing on the infected endpoint device;
- immediately notify the System Administrators or Information Security Office about the probable infection through a Service Desk request created in the Jira system.

In some cases, the regulations for using anti-virus software may differ from the internal requirements.

2.4 Requirements for remote work

To ensure remote access, the specialist is given credentials (login, password, token, etc.) that relate to remote access.

If the credentials are compromised or suspected of being compromised, the specialist of WEI\$\$ shall immediately notify the System Administrators or Information Security Office through a Service Desk request created in the Jira system.

The specialist of WEI\$\$ is forbidden to:

- record the credentials (login and password) on any mobile storage device;
- disclose the credentials (login and password), or any other information on remote access to the third parties;
- try to establish any other network connection after the VPN/TSG-connection has been made;
- provide the third parties, including relatives, with corporate mobile communication device (laptop, GPRS modem, etc.).

2.5 Requirements for using Internet

Specialists of WEI\$\$ are allowed to access the Internet resources from their endpoint devices using either the access provided to specialists of WEI\$\$, or channels approved by the authorized

All actions in the WEI\$\$ network and information systems may be monitored. Specialists of WEI\$\$ are provided with the notice (login banner) that their actions may be monitored during the login to the information systems. Users consent to this notice by continuing the login process into the internal systems. WEI\$\$ Management must ensure that individuals are held accountable and responsible for actions initiated under their electronic signatures, to help deter record and signature falsification. When electronic signatures are used, their usage should be controlled.

When using the Internet, WEI\$\$ specialists should not:

- send operational information via public email servers (e.g. Yahoo | Mail, Weather, Search, Politics, News, Finance, Sports & Videos, etc.) and by other means of Internet communication, unless otherwise provided in the agreement with the customer;
- store operational data on the Internet;
- browse for information not officially required;
- use Internet access for personal or leisure purposes, especially those that can cause violation of intellectual property rights or malware infections;

- independently download, install, customize, and use any software for online work (various «bots», clients for downloading and seeding files, email clients, proxy-servers, etc.);
- use anonymous proxy-servers;
- use torrent clients;
- distribute copyrighted information, materials containing viruses, serial numbers to commercial software, etc.;
- disclose logins and passwords for allowing unauthorized access to the WEI\$\$ network resources.

2.6 Actions to be taken in case of security incidents

In case of security incident, WEI\$\$ specialists must immediately inform the Information Security Office via e-mail, Slack, Service Desk Jira Ticket and/or any other suitable means of communication. Examples of security incidents are:

- loss of user password;
- loss of personal electronic access card;
- system failure which caused data loss;
- access denial to network/servers;
- unauthorized access to the WEI\$\$ network.

Specialists of WEI\$\$ are not allowed to take any actions that are beyond their professional competence and/or job functions.

Specialists of WEI\$\$ shall take necessary measures to ensure the saving of all possible evidence and proofs of information security incidents.

Specialists of WEI\$\$ shall immediately report information security incidents in any possible way (email, phone, request in the Jira system).

2.7 Other provisions

WEI\$\$ Management must ensure that all WEI\$\$ specialists, contractors and third-party system users are aware of the limits existing for their use of the organization's information and assets associated with information processing facilities and resources. Specialists of WEI\$\$ shall store results of their work and other important data on the WEI\$\$ servers (for example, corporate Google Drive, project servers, Confluence database, Jira, file server), from where they are centrally backed up.

Guest/anonymous, shared/group, emergency and temporary accounts must be specifically authorized through the corresponding approval in the request ticket and their use should be monitored.

To maintain an appropriate level of the information security specialist of WEI\$\$ shall:

- take part in project or WEI\$\$-wide information security trainings;
- contribute to the monitoring activities undertaken regarding network monitoring, access distribution, and compliance with other requirements set forth in this Policy.

Signature of Managing Director:

Eduards Kalnins



Date: August 18, 2025