Labkotec Group Information Security Policy

The primary goal of information security is to ensure the continuity of the information and services for which Labkotec Group is responsible in all circumstances, i.e. from an IT perspective, to enable the availability of the organization's data and ICT solutions, as well as the integrity and confidentiality of the information used in all circumstances.

Important targets to be secured in terms of the information security of operations include persons, facilities, equipment, telecommunications, information systems, services, and information and data sets in all their forms. The aim is to secure the operation of operational systems and the information network and to secure the provision of services in normal and emergency conditions.

Labkotec Group's information security principles have been agreed to:

- Information security and data protection are part of Labkotec Group's daily operations and risk management. Risk management is carried out at the company level, as well as at the product and service level.
- We conduct regular internal and external audits and audits to assess the effectiveness of our cybersecurity risk management in the services we provide.
- We maintain a register of our critical sites and related functions
- There are up-to-date backups of critical data in our service, which are located in secure locations
- In terms of access rights and access control, we use multi-factor authentication for the organization's critical systems and the services we provide, and we implement role-based access management in our organization, which assigns access according to employee roles and responsibilities.
- We have automated systems in place that detect deviations in real time and report them to information security officers
- We have established practices for recovering from exceptional situations, communication and, if necessary, restoring data
- Things are done in a secure manner, which means protecting information from a wide range of threats. The purpose is to ensure the continuity of (business) operations and to manage (business) risks.
- To achieve information security, appropriate security mechanisms are implemented, consisting of operating principles, software and hardware functions.
- Control, monitoring, reporting and monitoring related to information security are organised through the information security team. The information security team consists of at least Indutrade IT's information security officer, the person responsible for the information security of Labkotec Group's products, and a member of Labkotec Oy's management team
- We set clear cybersecurity criteria for our suppliers and ensure that they are met. For example, LabkoNet service providers are required to have ISO 27001 certification or equivalent, and we require contract manufacturers to have either information security certification or information

security policies and practices for critical information and security of supply. The cyber security of the LabkoNet service is regularly monitored in cooperation with the service provider.

- We maintain Labkotec Group's information security with up-to-date software updates, as well as the competence of our personnel through information security and cyber security training. Each supervisor ensures that the information security and data protection regulations and instructions are trained and familiarized with the personnel
- To ensure physical security, we use a variety of access control systems (such as electric locks and authentication methods) in our organization to prevent unauthorized access to critical facilities.

Approved by management team of Labkotec Oy at 17.03.2025