Integrated Management System

ISO 45001
ISO 14001
ISO 9001 ISO 27001 ISO 50001

Annex
Policy of the Apator Group
Information Security Management System (ISO 27001) and Cybersecurity System (the Act on the National Cybersecurity System/the KSC Act)

In the Apator Group, information security is crucial for business continuity, implementation of key and important services and achieving the assumed goals. This translates into our commitment to protect information, information systems and other supporting assets.

We are committed to ensuring that our approach to information security and cybersecurity management is responsive to current external and internal threats and is fully integrated into our operations and ongoing business processes, enabling them to be conducted in a reliable and responsible manner.

For that purpose, as part of the Integrated Management System, the Information Security Management System (ISMS) has been established, implemented, maintained and continuously improved in accordance with the requirements of the PN-EN ISO/IEC 27001:2022 standard, the Act on the National Cybersecurity System (the KSC Act) and the NIS2 Directive.

We achieve our objectives by:

- ✓ maintaining the confidentiality, availability and integrity of information by handling information in accordance with the applicable legal requirements and the requirements of the ISMS, internal documents and cybersecurity documentation,
- ✓ acting within the framework of applicable law for the benefit of the client, including consideration of client expectations in the area of information security,
- ✓ constant compliance with the requirements of the ISO 27001 standard and applicable provisions of regulations and agreements regarding information security, in particular the KSC Act and the Act of Processing of Personal Data,
- ✓ integrating the ISMS into the overall management structure, the business processes in place and the Management System,
- ✓ making employees aware of the importance of their work and the significance of their contribution to the effectiveness of the ISMS, as well as the consequences of noncompliance with the requirements of the ISMS and the KSC Act,
- ✓ employee training in the field of information security and cybersecurity,
- ✓ locating our servers in a local professional Data Processing Centre,
- ✓ sharing IT resources of the Group in a secure manner,
- ✓ implementation of innovative IT technologies in the field of security and IT systems,
- ✓ conducting information security and cybersecurity risk assessments at scheduled intervals and when changes affecting the ISMS and Cybersecurity System occur or are planned,
- ✓ documented incident management process, including major incidents and business continuity in relation to information security and legal requirements for handling cybersecurity incidents,
- ✓ regular assessment of this policy, the achievement of the objectives of the ISMS and those in the area of cybersecurity, risk handling plans taking into account the strategic direction of the organisation,
- ✓ monitoring the functioning of the ISMS and the Cybersecurity System, assessment of the effectiveness of the implemented safety measures,
- ✓ involvement of the management in creating the conditions for the improvement of the ISMS and the Cybersecurity System and taking advantage of opportunities for further development.

Based on the framework of this policy, the management ensures sufficient resources for the effective functioning of the Information Security Management System and Cybersecurity System, sets specific operational objectives in the field of information security on an annual basis and commits to the continuous improvement of the Management System of the Group.

The Information Security Management System Policy (ISO 27001) and Cybersecurity System (the KSC Act) are known to all employees. They are responsible for adhering to it and applying it in their daily activities.

Maciej Wyczesany
President of the Management Board
Apator Group

Ver. 1/2025; 29 January 2025