

INFORMATION SECURITY POLICY

of BorsodChem Zrt.

„Information security is one of the cornerstones of our continuous operation and competitiveness.”

The protection of IT resources and the data processed using them is of paramount importance to the operation of BorsodChem Zrt. Information security and the proper management of data assets are essential for safe and continuous chemical production, the smooth operation of business processes and the maintenance of reliable business relationships.

In view of the above, BorsodChem Zrt. is committed to information security and secure data management as follows:

- We plan, operate and continuously develop our information security and data protection activities in a planned manner, taking into account changes in our operating environment and our own operations.
- We set information security objectives at regular intervals and measure and review the performance and effectiveness of our information security activities.
- The Company's management provides the resources necessary to achieve the objectives set in the area of information security.
- Our goal is to ensure that our information security activities comply with EU Directive 2022/2555 (NIS2) and the relevant and other Hungarian legal requirements in force at any given time. We comply with our data processing obligations towards our partners. We pay due attention to the processing of personal data to ensure that our activities comply with EU General Data Protection Regulation 2016/679 and the relevant Hungarian legal requirements.
- We evaluate our information assets in terms of confidentiality, integrity and availability, and perform risk assessments on the IT systems and environment that manage these assets, thereby ensuring the adequate protection of information and the continuous, secure operation of the organisation.
- Our information security activities are risk- and cost-conscious: we tailor our protective measures to the threats and potential business impacts, ensuring that their cost is proportionate to the damage we seek to prevent.
- We develop a detailed internal set of rules for our information security activities, ensuring consistent enforcement of information security requirements, risk reduction and legal compliance. We review the rules regularly.
- We ensure that our employees are aware of their data management and data security tasks and responsibilities. We ensure that our users are aware of information security threats and have the knowledge necessary for the safe and proper use and operation of the systems.
- We ensure the reliable and secure operation of information processing systems through documented operating procedures and planned and supervised change management.
- We take information security considerations into account when purchasing new information systems and developing existing systems.
- We ensure that our suppliers and contractors affecting our information assets or IT systems meet our information security requirements. We evaluate and qualify our partners to the extent necessary.
- We strive to prevent information security incidents and disruptions and to minimise any damage. We investigate any incidents that arise in a documented manner and take the necessary corrective measures.

Kazincbarcika, October 2025



László Kruppa
President