INFORMATION SECURITY POLICY

We are a company engaged in the research, manufacture and sale of specialised crystal products for detectors, lasers and other industrial applications. For this purpose, we make significant use of information and communication technologies (ICT), within the framework of which we process both our own company data and the data of our business partners.

We ensure that the data within our information and communication technologies is protected from cyber threats.

1 - Principles

- When it comes to information security, we don't invent what is already invented and proven. We are therefore inspired by cybersecurity legislation, in particular the European Directive 2022/2555 on measures to ensure a high common level of cybersecurity in the Union, known as the NIS 2 Directive, and its implementation into Czech law and decrees.
- When setting up an information security system, we are inspired by the international standard ISO/IEC 27001 Information Security Management System.
- Hazards associated with the operation of information technology are repeatedly analysed, e.g. according to ISO/IEC 27005 Information Security Risk Management.
- Since we cannot afford prolonged ICT inoperability, we also take inspiration from ISO 22301 Security and Resilience – Business Continuity Management Systems.
- We are not satisfied with the ISMS system setup and risk analysis, but we continuously check it through audits according to the ISO 19011 Management System Auditing Directive.
- We focus on an important potential source of information security breaches – the person as an employee, former employee or external collaborator. We educate and motivate all groups of IT users in a differentiated and repeated way, starting with top management.
- We address the security of ICT resources comprehensively using up-to-date technical means and personal experience of information security experts.
- We also verify the security of ICT resources by independent penetration tests.
- We are guided by the principle of "reasonable sufficiency". We know that we cannot completely eliminate risks, and we know that we need funds for other important purposes. For each measure, we carefully balance the level of risk reduction against the necessary costs and resources needed to implement the measure.

CRYTUR, spol. s r.o. | Na Lukách 2283 | 511 01 Turnov | Czech Republic
+420 481 319 511 | FAX +420 481 322 323 | sales@crytur.cz | www.crytur.com

2 - Communication

- We communicate information security issues externally as little as possible and only in general terms. More detailed information could become a guide to the form of a cyber attack.
- Any communication with the National Cyber and Information Security Agency (NCISA), on the other hand, must be open, but it must be verified that it is indeed the NCISA.
- Communication of information security issues within the company should take place mainly in the context of training on accepted security policies.

In Turnov 1st of May 2024 (revision 4-0) - Process E5

Dr. Jindřich Houžvička
CEO

CRYTUR, spol. s r.o. | Na Lukách 2283 | 511 01 Turnov | Czech Republic
+420 481 319 511 | FAX +420 481 322 323 | sales@crytur.cz | www.crytur.com