UAB Critical Security
Company code: 300646885
VAT code: LT100004541418
Saulėtekio al. 15 Vilnius
Confidentiality classification: public information

INFORMATION SECURITY MANAGEMENT SYSTEMS

INFORMATION SECURITY POLICY

1. Information about the company

UAB "Critical Security" (hereinafter - CS) is a company operating since 2007, which was founded by a group of cyber security specialists. The company does not belong to any group of companies. Since its inception, the company has been providing high-quality security assessments and penetration tests to clients in the European Union for various organizations.

Our team consists of experienced and certified security professionals. We take a proactive approach to cyber security, helping organizations identify potential risks before they become major problems. With extensive experience working with clients from a variety of industries around the world, including finance, healthcare, education, and technology, we are well positioned to address the unique security challenges of each industry.

Company services:

- Network penetration testing
- Web and mobile application tests
- Red team testing
- Social engineering
- Cloud security audit
- Source code security review
- Internet of Things (IoT) and hardware security audit
- Mainframe penetration testing
- Digital forensics and incident response
- Malware analysis

2. Information security management system

It is important to protect the confidential data and intellectual property of CS employees, partners and customers, so CS management decided to implement an information security management system (ISMS) in accordance with LST ISO/IEC 27001:2022. ISMS is designed to protect information from loss, unauthorized disclosure or alteration and other illegal actions.

ISVS applies to all CS employees, interns, etc., legal entities who are granted access to CS data on the basis of contractual relations.

3. Objectives of the information security management system

Protect information from loss, unauthorized disclosure or alteration, and other illegal actions by ensuring accessibility, confidentiality, and accessibility.

Ensure effective management of information security risks to an acceptable level by implementing risk management measures.

Minimize damage to CS in the event of an incident or avoid an incident.

4. Obligations of CS management for information security

Establish general information security management objectives.

Ensure necessary resources for ISVS.

Comply with information security obligations established in the legal acts of the European Union, the Republic of Lithuania, the General Data Protection Regulation and contracts with clients and employees.

Identify ISVS improvement tasks, select measures, plan their implementation.

Create conditions for CS employees to improve information security knowledge.

5. Ensuring information security

We have obliged CS employees to familiarize themselves with the requirements set out in ISVS policies and procedures and to comply with them.

We use the following organizational, human, physical and technological information security measures (including but not limited to):

- Supplier management
- Acceptable use of information tools
- Malware management
- Business continuity
- Electronic communication
- Computer network security
- Secure communication
- Employee training
- Incident management
- Business continuity
- Vulnerability management
- Mobile device management
- Telecommuting

We obliged CS suppliers and subcontractors to comply with the information security requirements established by the ISVS by issuing instructions, signing data processing agreements, confidentiality agreements, and conducting audits.

We are constantly improving the ISVS by conducting internal audits, identifying non-conformities, and implementing corrective actions, looking for ways to improve.

In case you have questions, to report a vulnerability or other issues, please contact us via e-mail: info@critical.lt.

If you have questions about the security of personal data, please read the Privacy notice https://www.critical.lt/privacy-notice

6. Information security system validity and maintenance

ISVS was approved and entered into force on 12/15/2023. We publish the management notice publicly to anyone to whom it may concern. We review the policy regularly, at least once every 1 year.