E-Smart Systems d.o.o.
Projecting, development, production, trade and implementation company in the field of Information Technologies
Republic of Serbia, 11030 Belgrade, Kneza Višeslava 70a, Tel: + 381 11 30 50 200
http://www.e-smartsys.com, office@e-smartsys.com
MB: 17247565, Reg.No: 01117247565, Business code: 6201, VAT: 101833141

L-IMS-008

Document code

Information Security Policy

At E-Smart Systems d.o.o. Belgrade, information is the basis of all business processes. For the Company, information security means preventing unauthorized access, disclosure, modification, destruction, or unavailability of information.

The primary goals of our efforts related to ensuring information security are:

- Maintaining trust in business relationships,
- Protecting the privacy of personal data,
- Securing of business operations,
- Complete compliance with: applicable laws, regulations, and standards in the field of security, internal information security policies, as well as the needs of the community,
- Risk treatment and application of security controls at an optimal cost level and in line with the business value,
- Continuous improvement of the information security management system, both at the technological and organizational level.

We plan, communicate, implement, monitor, measure the degree of achievement, and constantly align set goals with emerging changes in the environment and the business framework of the Company's operations.

The basic principles in the application of information security within the Company's operations are:

- Preserving the confidentiality, integrity, availability, authenticity of all information significant for the Company's operations and the non-repudiation of transactions performed on them,
- Secure collection, processing, storage, and deletion of all information arising from business operations with special attention paid to the personal data of all participants,
- Clear communication of all information security requirements to all interested parties,
- Timely and effective identification, assessment, and treatment of risks in the field of information security,
- Proactive monitoring of changes in applicable laws, regulations, and standards in the field of security and timely compliance with them,
- Selection and implementation of reliable and proven technologies for the implementation of security controls in the Company's information system in line with technological trends and recommended practice.

All employees of the Company, from the highest management to newly employed, are obliged to:

- Strictly adhere to the principles of applying information security mentioned in this policy,
- Develop and expand awareness and knowledge in the field of information security on a daily basis,
- Participate in trainings, courses, and knowledge checks in this domain,
- Conscientiously act in daily work in accordance with this policy, and
- Timely report incidents and events related to information security.

The Company's highest management is fully committed to continuous improvement of the information security management system, thus ISO/IEC 27001 was chosen as the framework for implementation. Accordingly, all internal policies and procedures, risk evaluations, and applied security controls are reviewed and updated at least once a year. All employees are therefore encouraged to participate in internal and external audits as well as in the work of professional forums and organizations in the field of information security.

At the Company level, role of the Information Security Representative of the Management has been established for over a decade. This role has been delegated responsibilities and full executive authority in this domain. The highest management actively manages the information security system through this role and consistently works on its strengthening. The highest management of the Company retains full responsibility for making decisions related to setting objectives, risk treatment, and changes in policies in the field of information security.

Given that information represents the basis of the Company's operations, all information related to the business is subject to the application of this policy, without exemptions and exceptions. In case of an exception, it must be clearly communicated with the Information Security Representative of the Management and the highest management, to find an adequate solution.

Deviations from this and all related policies and procedures in daily work are not allowed, and any violation of information security will be considered a violation of work duties and sanctioned in accordance with the Company's Employment Regulation act and the procedure for determining the Disciplinary responsibility.

History of changes:

Version	Date	Description of changes
1.0	01.07.2011.	The first version of the document
2.0	08.02.2013.	Document adapted to work practices
3.0	01.07.2014.	Policy in accordance with the requirements of ISO/IEC 27001:2013
4.0	06.02.2020,	Documentation template changed
5.0	02.03.2020.	Policy updated due to the opening of ZelenData Center
6.0	07.02.2024.	Policy in accordance with the requirements of ISO/IEC 27001:2022
6.1	08.04.2024.	History of changes and confidentiality level label added
6.2	22.09.2025.	Minor changes of the document

Signatures:

Mirna Kojić Veljović ESUFL001372703191

Digitally signed by Mirna Kojić Veljović ESUFL001372703191
Date: 2025.09.24 01:55:39 +02'00'