INFORMATION SECURITY POLICY

The information security policy aims to demonstrate in a clear and unambiguous way goal of SMART CITY ECO tocontinuously implement and improve its operations in in accordance with the requirements of the international standard ISO/IEC 27001:2013 (Information security management system- ISMS),respecting the principle of preserving confidentiality, availability and integrity of information and informational resources, and thus in that way provides and guarantees:

- protection of information and other information resources (people, processes, procedures, services, hardware, software, infrastructure, equipment...), as core values SMART CITY ECO, from all internal or external, intentional or accidental threats (computer fraud, espionage, hacking attacks, viruses, floods, fires, earthquakes, etc.), through establishment, implementation, application, monitoring, review, maintenance and improvement ISMS;
- business continuity;
- minimizing the eventual business damage by preventing security risks, i.e. reducing their impact to a minimum;

with what he improves his corporate image, profitability and competitive advantage.

The above mentioned is provided (implemented) through:

- Leadership relationship founder of SMART CITY ECO regarding the inclusion of all employees, on all levels, in achieving the goals of the company, which generally lead to a high level of information security;
- Compliance with strategic business plans and goals of SMART CITY ECO, relevant legal, regulatory and contractual requirements, as well as with the requirements of the standard ISO/IEC 27001:2013;
- Safety culture awareness of employees about their role and responsibilities;
- Respecting the interests of business clients, internal and external users and other interested parties;
- Preventing unauthorized access to information resources of SMART CITY ECO;
- Maintenance and improvement of the system of safety of employees, clients, information and property;
- A clear organization and division of responsibilities in terms of information security;
- Risk management in order to reduce the impact of security threats for SMART CITY ECO;
- Crisis situation management;
- Continuous reviews and improvements.

All employees, consultants, external consultants, temporary employees, contractors and subcontractors and third parties with which SMART CITY ECO has any business cooperation, should be aware of their obligations and responsibilities, as defined in their job description or contract, and to act in accordance with this policy.

They are responsible for preserving the confidentiality, availability and integrity of information and other informational resources of SMART CITY ECO at all stages of their life cycle, and that their actions do not impact their safety.

The founders of SMART CITY ECO are responsible for implementing the information security policy in their business processes as well as for its application by employees.

Failure to comply with the Information Security Policy entails disciplinary responsibility.

The founders of SMART CITY ECO ensure that this policy is communicated and understood to all interested parties, implemented and maintained at all levels in SMART CITY ECO and at least once a year reviewed to respond to any changes in the risk assessment or risk management plan.

This policy has been approved by the CEO of SMART CITY ECO and provides a framework for further setting up the company's relevant goals and basic principles for establishing an effective information security management system (ISMS).

Novi Sad,Serbia 10.07.2018.

Author: CTO, Saša Dobo
Approved: CEO, Slobodan Ćulum