

SC ISPE SA is a company specialized in technical, financial and institutional consulting, project management, studies, research and development, basic and detail design/engineering services in the following fields: power (electricity and heat generation, transmission and distribution), environmental protection, industry, civil and industrial works, public services, infrastructure systems including land reclamation.

ISPE information security policy, according to ISO 27001/2013 is to maintain and enhance the renown gained for the services it provides, by continually improving their quality by modern management methods, compatible with the general strategy of the company and with the other defined management policies, in order to meet the demand of all parties involved (shareholders, clients, partners/co-workers, employees, civil society).

The general goals of this Policy are defined by the fact that the information resources, services, systems and their support infrastructure are strategic resources of ISPE; to compromise them might lead to the infringement of the contract clauses, compromising the competitive position, influencing ISPE credibility and capacity to reach the goals. Information security is contributing to the accomplishment of ISPE mission and targets by identifying and preventing risks, vulnerability and threats against ISPE information resources and processes.

ISPE takes all necessary steps to protect information resources against internal or external deliberate or accidental threats to assure that:

1. information, services and systems are protected against non-authorized access;
2. information confidentiality is kept;
3. information, services and systems integrity is kept;
4. information, services and systems availability is ensured when required by activity processes;
5. organization requirements and goals are fulfilled;
6. legal and regulating requirements are fulfilled.

ISPE is adopting a set of policies in the field of information security detailing the general principles related to information resources protection in specific fields: internal structure, relation with third parties, human resources management, physical security, communications and operations management, access control, security incidents management, activity continuity, ensuring conformity with internal norms, with legal regulating norms and contract provisions.

ISPE is operating an Information Security Management System to assure that:

- information security risks are identified, evaluated and managed;
- adequate security measures are implemented, kept and improved;
- policy goals are fulfilled;
- promoting continual improvement.

Information Security Management System applying as instrument of high performance management is determining me, as Chief Executive Officer, to approve this Policy and to assure the updating of the applicable policies to meet any amendment which might affect information security requirements and risks.

The **Information Security Team** is directly liable to formulate the Policy and to provide support and guiding for its implementation.

**All managers** are directly liable to implement the information security Policies in their field of liability.

Each ISPE **employee** is responsible to comply with this Policy and any other applicable policies and procedures related to ISPE information resources protection.

Failure to observe this Policy leads to disciplinary actions according to the internal rules up to cancelling the job contract and civil or punitive sanctions under certain circumstances.

The efficiency of the Information Security Management System is continually monitored through internal audits and periodical analyses performed by the management.

Chief Executive Officer,  
eng. Ion Eduard Chițescu



16.01.2017