Information Security Management Policy

The management and the personnel of NOSIS are committed to an effective Information Security Management System in accordance with the strategic goals of the company.

A. NOSIS, for its following activities: Financial Funding of Projects and Investments, Installation and Maintenance of Quality Systems, Management and Organization, Providing Software as a Service, **Market Research** is committed to develop and apply policies that will protect the information managed by the company from all kinds ofrisks , internal and external, and, henceforth, takes the sequent actions:

- It has adopted and implemented a specific control policy on physical access aiming at the protection of information from any unauthorized person.
- It prevents unauthorized access to digital files by applying an access control policy upon the electronic data.
- It minimizes the risks of loss, leakage or unauthorized access to data by adopting the good use of storage media policy.
- It ensures confidentiality of information via the policy of proper use of personal, sensitive and corporate data.
- It has defined, adopted and applied a copyright policy.
- It confirms the information safety and integrity through a backup policy.
- It prevents any malicious and deliberate violation of NOSIS network by applying a network fair usage policy.
- It prevents leak of information by applying the net worth policy.
- It enhances work flexibility always in accordance with the security of information it manages by adopting a secure remote working policy.
- It prevents the loss of data and critical information by applying a backup policy.
- It complies fully with the applicable legal and other requirements that has signed and accepted in terms of the information security.
- NOSIS security policy, along with its specific policies that deal with the safety of managed information, are reviewed once annually.
- It reviews risk assessment methodologyat least once a year.
- It promotes the customers' confidence towards action according to the international security and control systems standards.
- It continually improves the Information Security Management System by applying constant reviews of measurable safety objectives within the company's specific procedures and levels.
- It is committed to comply with the legal and other regulatory requirements, as well as with the obligations deriving from its business contracts.
- It has installed a mechanism for the continuous identification, assessment and management of threats towards the Information Security.
- It provides Protection Systems against unauthorized access.
- It verifies data confidentiality.

- It develops, applies and controls a Recovery Plan, as well as a Business Continuity Plan.
- It creates mechanisms in order to identify and evaluate the risks and the impact of any security breach.
- It communicates its Information Security Policies to every employee, client, supplier and partner, and to all interested parties as well.
- It develops, applies and communicates access control and remote access control policies, both reviewed and evaluated at least once a year.
- It develops, applies and communicates a teleworking policy and a policy on use of network services, both reviewed and evaluated at least once a year.
- It develops, applies and communicates a policy on the use of material in respect of which there may be intellectual property rights , which is reviewed and evaluated at least once a year.

NOSIS is committed to the Security Policy, which is disseminated to the whole of the company's workforce. Moreover, it guarantees this commitment by cultivating across the company's manpower the spirit of an inclusive and collaborative effort and, in addition, by providing all necessary resources so that everyone will adhere to the Security Policy and will promote any activity that constantly upgrades and improves the confidentiality, integrity, reliability and availability of information.

FOR NOSIS

...