INFORMATION SECURITY MANAGEMENT POLICIES

The main theme of TS EN ISO 27001:2013 information security management policy document is to demonstrate that Signum Technology ensures confidentiality of employees, customers, infrastructure, software, hardware, organization, 3rd party information and the information security for through the financial sources, maintains information security risk management assess the performance for information security management processes and maintains relations with 3rd parties regarding information security related matters.

In this regards, the targets of our ***information security management policies*** are

- To protect information assets of Signum Technology against all internal and or external threats whether consciously or not, maintain required information accessibility by processes as required, meet legal regulatory requirements, to work for continuous improvement
- To maintain continuity of three major elements of information management systems for all maintaining facilities

Confidentiality: Prevention of unauthorized access to sensitive information

Integrity: Consistency and integrity of information

Accessibility: Allowance of authorized employees to access the information if needed

- To be concerned with not only the security of the information on online platforms but also with written, printed, oral or any information on a relevant platform
- To provide all employees information security trainings and maintain information security awareness
- To report existing security related activities or suspicious disclosures to information security team and enable them to investigate the issue
- To prepare business continuity plans, maintain and test such plans
- To make periodic assessments to identify existing risks. According to assessments, to observe and follow up action plans
- To hinder all possible conflicts that may arise out of the contracts
- To meet business requirements and accessibility of information

GENERAL MANAGER