

Information Security Policy

As a service provider (IT, Marketing & Operations) and part of the supply chain for the essential services we have to comply with national standards, laws, and regulations. The growing information security threats require the establishment and implementation of a robust information security management and governance system. Taking this into account, the implementation and compliance with our security policies, guidelines and procedures is of great importance.

This policy document sets out the measures to be taken by all employees of Enigma Soft Technologies Pvt Ltd, IN (the “company”) to protect the company’s computer systems, infrastructure, environment and other information assets from damage and threats whether internal, external, deliberate, or accidental. The Directors have responsibility for maintaining and monitoring the policy and associated systems and procedures and for providing advice and guidance on their implementation based on the approved scope.

The implementation of the information security policy, systems, and procedures within their areas of responsibility and for adhering to the ISMS key principles laid out in the company’s ISMS policies & procedures in alignment with the evolving strategic direction for business growth.

The objective of the system is to :

- Reduce, so far as is reasonably foreseeable, the likelihood of an incident occurring which may affect the security of the information held by the Company.
- In the event of an incident, ensuring that business & service continuity is maintained and impact minimized.

This objective will be met by :

- The establishment, implementation, monitoring, and maintenance of an information management system that meets the requirements of ISO 27001:2013 as per the Data Protection Act 2018, the General Data Protection Regulation and any other relevant legislation in force from time to time.
- Ensuring that any changes to the environment, technology employed, threats or legislation are identified and resulting measures reviewed and implemented.
- Understanding the threats posed to information held by the company, its partners and clients.
- Evaluating the threats posed to the data held & systems operated and ensuring that appropriate risk treatments are in place to minimize them.
- Ensuring that all employees understand and fulfil their obligations with respect to information security.
- Setting annual ISMS objectives as a platform for ensuring that the ISMS system is compliant with the standard, relevant to the organization and ensures that the system is subject to continual improvement.
- This policy will be reviewed annually to ensure that it remains compliant to the standard and relevant to the company’s activities.

Atul Utturkar

Approved by

