Information Security Policy Statement & Objective

The objective of managing information security is to ensure that its core and supporting business operations continue to operate with minimal disruptions.

The Senior Management is committed to an effective Information Security Management System in accordance with its strategic business objectives.

"Sevaas commits to protect its information assets from all threats in order to maintain the confidentiality of information, rely upon the integrity of the information, ensure availability of information, comply with legal, regulatory, statutory and contractual obligations and ensure continual improvements towards organization wide Information Security Management System"

Information Security translates to preservation of the following goals:

- **Confidentiality:** Assurance that Information is accessible only to those authorized to have access.
- **Integrity:** Assurance of the completeness and accuracy of Information and its processing methods; and
- **Availability:** Assurance that authorized user has access to Information and associated assets when required. This is ensured by regular maintenance of hardware, updated and monitored operating systems, redundant critical resources, IS business continuity management, capacity management and other information security measures we take.

Information Security Objectives

Sevaas shall:

1. Develop and implement an Information Security Management Systems (ISMS) to protect organization's information and information systems reasonably and effectively from various internal and external threats.
2. Commit to comply with regulatory, legal and business requirements.
3. Ensure confidentiality, Integrity, and availability of Information Assets.

4. Communicate all pertinent security policies to employees and other interested parties as applicable.

5. Identify the information assets, to understand their vulnerabilities and the threats that may expose them to risk, through appropriate risk assessment.

6. Ensure that identified risks are mitigated through adequate controls as documented in the risk treatment plan.

7. Ensure annual information security awareness training of all employees.

8. Provide appropriate access controls for protection against unauthorized access adaptability.

Sevaas Information Security Policy is designed to provide a risk-based framework for protecting Information Assets of Sevaas. It applies to all Sevaas employees, contractors, and vendors.