Information Security policy

Protect the organizational and clients' information and data from internal and external threats by implementing framework with adequate controls, tools and processes.

Objectives:

- **Maintain confidentiality, integrity, availability and safety of information and data**
- **Manage risks related to information security, cybersecurity and physical security**
- **Drive compliance of information security and data privacy controls across all systems**
- **Comply with legal, regulatory and contractual requirements of interested parties***
- **Avoid breaches from internal and external sources.**
- **By ensuring that entire staff is given sufficient security training and support to ensure competency for their area of work through education, training and experience, where appropriate communicate the importance of effective Information Security Management System and of conforming to the security requirements**

This policy will be communicated to all employees and organizations working for or on our behalf. Employees and other organizations are expected to co-operate and assist in the implementation of this policy, whilst ensuring that their own work, so far as is reasonably practicable, is carried out without risk to themselves, others, or the environment.

This policy will be reviewed annually by top management and where deemed necessary will be amended and re-issued. Previous versions of this policy are archived. This policy is available to relevant interested parties, upon reasonable request.

Damodar Rao Gummadapu
Chairman

*Interested parties include customers, shareholders, employees, government agencies, regulatory bodies, emergency services (police, ambulance, firefighters, etc.), employees' families, media, suppliers, contractors, outsourced partners, publishers, service providers, etc.

Review Date: 12th May 2023 Rev.08, Issue:08