INFORMATION SECURITY POLICY

NETRADYNE

ADDRESS
9191 Towne Centre Drive Suite 200 San Diego,

CA 92122, USA

Information Security Policy Statement

Purpose: Our organization is committed to safeguarding our information assets and protecting the confidentiality, integrity, and availability of our data. This Information Security Policy Statement outlines our dedication to maintaining a secure and resilient information environment.

Scope: This policy applies to all employees, contractors, and third-party personnel who have access to our information assets, including but not limited to systems, networks, data, and physical facilities.

Objectives:

- Ensure the confidentiality of sensitive information by implementing appropriate access controls and encryption measures.
- Maintain the integrity of data by implementing mechanisms to prevent unauthorized modification or tampering.
- Ensure the availability of information systems by implementing robust backup and disaster recovery procedures.
- Comply with relevant laws, regulations, and industry standards pertaining to information security.
- Continuously improve our information security posture through regular risk assessments and security audits.

Roles and Responsibilities:

Management: Provide leadership, allocate necessary resources, and promote a culture of security awareness.

Information Security Officer: Oversee the development, implementation, and enforcement of information security policies and procedures.

Employees: Comply with security policies and procedures, report security incidents promptly, and participate in security training and awareness programs.

Security Framework: Our organization adopts industry best practices and follows the guidelines outlined in the ISO 27001 standard as the foundation of our information security program.

Security Controls:

Access Controls: Implement strong authentication mechanisms, least privilege principles, and regular access reviews.

Data Protection: Classify data based on sensitivity, encrypt data in transit and at rest, and enforce data handling procedures.

Incident Response: Establish an incident response plan, including procedures for detecting, responding to, and recovering from security incidents.

Security Awareness: Conduct regular training and awareness programs to educate employees about information security best practices.

Compliance: Our organization is committed to complying with applicable laws, regulations, and industry standards related to information security.

Training and Awareness: We provide comprehensive training and awareness programs to ensure that employees understand their responsibilities, are aware of security threats, and know how to protect our information assets.

Review and Revision: This policy will be reviewed annually and updated as necessary to address changes in technology, business practices, and regulatory requirements.

Acceptance and Enforcement: All employees are required to read and acknowledge their understanding of this policy. Non-compliance may result in disciplinary action, up to and including termination.

Signature: Saravanan Sankaran
Date: Jun 02, 2023
Title: Senior Director, Infosec & IT