Information Security Management System (ISMS) Policy

At ANHVL, we are committed to implementing and maintaining an Information Security Management System (ISMS) in accordance with internationally recognized standards such as ISO/IEC 27001. This ISMS Policy outlines our approach to protecting the confidentiality, integrity, and availability of information assets.

Scope - This policy applies to all employees, contractors, and third parties who access, manage, or process ANHVL's information assets.

We aim to:

Preserve confidentiality - that is, to protect information provided by ANHVL' customers, employees and other associates, against unauthorised access or disclosure.

Maintain integrity - that is, to protect information assets from unauthorised or accidental modification, ensuring the accuracy and completeness of the organisation's assets.

Ensure availability - that is, to ensure that information, assets and infrastructure are available as and when required adhering to the organisation's business objectives.

- Assess risks to the business at regular intervals and implement preventive and corrective controls accordingly.
- Identify and define secure work areas within office perimeter and enforce secure access to the same.
- Top Management to be involved to establish Information Security Objectives
- Continual Improvement of the ISMS are recorded through Internal Audit, MRM, Performance Matrix and Risk Assessment.
- Identify and define secure work areas within the office perimeter and enforce secure access measures.
- Involve top management in establishing and overseeing Information Security Objectives.
- Record continual improvement of the ISMS through Internal Audits, Management Review Meetings (MRM), Performance Metrics, and Risk Assessments.
- Obtain timely information about technical vulnerabilities in information systems, evaluate exposure, and take appropriate measures to mitigate associated risks.
- Fulfil regulatory, legislative, and other business requirements.
- Protect the privacy of patient information by implementing stringent access controls, encryption, and data protection measures to prevent unauthorized access, disclosure, or misuse. Ensure compliance with applicable legal, regulatory, and industry standards.
- Identify, maintain, and regularly review business continuity plans for critical processes and infrastructure to minimize business downtime.
- Ensure prompt reporting of security incidents and weaknesses, follow ed by thorough corrections, root cause analysis, and corrective actions.
- Provide ISMS training to staff with effective post-training evaluations.
- Conduct ISMS committee meetings to discuss ISMS effectiveness.
- Demonstrate ANHVL's commitment to establishing, implementing, maintaining, and continuously improving the ISMS through this policy.
- This policy is reviewed at least annually or in the event of a significant change. Personnel will be notified of any changes to the policy via our official website https://neotiagetwelsiliguri.com / https://neotiahealthcare.com
- For any questions or security concerns, please contact us at it.slg@neotiahealthcare.com

Approved By: Date: 25-07-2024

Parthiv Vikram Neotia
Whole Time Director