Prudential Bank Limited

ISMS Policy Statement Communication to all Internal and External Stakeholders

The commitment to information security is of priority to Top Management Members of the Bank and will be demonstrated through the Information Security Management Systems (ISMS) Policy and the provision of appropriate and adequate resources to develop and improve ISMS and its associated controls.

Top management will also ensure that a systematic review of the performance of the ISMS program is conducted on a regular basis to ensure that the ISMS objectives are met, and issues are identified through the audit program and management processes. Management's Review may include departmental and other management meetings.

This Information Security Policy outlines the commitment of Prudential Bank to maintaining the highest standards of information security in line with the requirements of the Information Security Management System. Prudential Bank recognizes the importance of safeguarding information assets and respecting individuals' rights. The ISMS policy serves as a framework for establishing, implementing, maintaining, and continually improving our information security practices and applies to all information assets, systems, processes, personnel, and third parties that access, process, or store information on behalf of Prudential Bank.

Framework For setting Information Security Objectives

1. Information Classification: Prudential Bank classifies information into categories such PBL Restricted, PBL Confidential, and Public. The classification level determines the appropriate handling, access controls, and encryption measures.

2. Access Control: Access to information is granted based on the principle of least privilege. Users are granted access only to the information necessary for their roles. Access control mechanisms, including strong authentication, are implemented, and regularly reviewed.
3. Risk Management: Regular risk assessments are conducted to identify, assess, and mitigate potential threats and vulnerabilities. Appropriate controls are implemented to manage identified risks.
4. Security Awareness and Training: Prudential Bank provides ongoing security awareness and training to all personnel, contractors, and third parties to ensure they understand their responsibilities and are equipped to make informed security decisions.
5. Incident Management: An incident response plan is in place to effectively manage and respond to security incidents. Incidents are reported, investigated, and appropriate measures are taken to prevent future occurrences.

Prudential Bank is committed to complying with the requirements outlined in this policy and any applicable laws, regulations, and standards. The policy is regularly reviewed to ensure its effectiveness and relevance in addressing the changing landscape of information security and privacy.

All employees, contractors, and third parties are expected to comply with this policy. Non-compliance may result in disciplinary action.

This Information Security Policy reflects Prudential Bank's commitment to maintaining the confidentiality, integrity, and availability of information assets while respecting individuals' privacy rights. By adhering to the principles and practices outlined in these policies, Prudential Bank aims to build and maintain trust with its stakeholders.

Date of Policy: 20th January 2025

Signed by: Management.