## Information Security Policy Statement

This policy statement defines the framework within which the management system (information security management system) will be managed across PremiumTrust Bank and demonstrates Management commitment and support for information security management system throughout PremiumTrust Bank.

This policy is the primary policy from which all information security-related policies emanate.

## Scope

This policy is applicable to all PremiumTrust Bank personnel, contractors, vendors, and other parties, and covers all information entrusted to or owned by PremiumTrust Bank and stored, processed, or transmitted on the organization's information systems and operated by the organization.

## Information Security Definitions

In these policies, "information security" is defined as **Preserving the Availability, Confidentiality, and Integrity of the organization's Information assets** (this includes physical and electronic information, cardholder data, etc.) throughout the organization to preserve its competitive edge, assets, profitability, legal, regulatory as well as contractual, compliance and commercial image.

**Preserving**
This means that Management, Staff, Contractors, Project Consultants, and any External Parties have, and will be made aware of their responsibilities (which are defined in their job descriptions or contracts) to preserve information security, report security breaches and act in accordance with the requirements of the Information Security policies. All staff will receive information security awareness/training.

**Confidentiality** – ensuring that information is accessible only to those authorized to have access.

**Integrity** – safeguarding the accuracy and completeness of the information and its associated processing methods. This refers to protection against unauthorized modification.

**Availability** – ensuring that authorized users have access to information and associated information processing systems when required.

**Information assets**
The information assets include information printed or written on paper, transmitted by post, or spoken in conversation, as well as information stored electronically on servers, website(s), extranet(s), intranet(s), PCs, laptops, mobile devices, and PDAs' as well as any other digital or magnetic media, and information transmitted electronically by any means. In this context "data" also includes the sets of instructions that tell the system(s) how to manipulate information (i.e., the software: operating systems, applications, utilities, etc.). The physical assets include but not limited to computer hardware, data cabling, telephone systems, filing systems and physical data files.

## Policy Implementation Responsibilities

Within the field of Information Security Management System, there are a number of key roles that need to be undertaken to ensure successful protection of the business from risk.

Full details of the responsibilities associated with each of the roles and how they are allocated within PremiumTrust Bank are given in a separate document PTB Roles, Responsibilities and Authorities. The

ISMS Manager shall have overall authority and responsibility for the implementation and management of the Management System, reporting on its performance to top management and ensuring that it conforms to the requirement of the ISO 27001 standard.

## Information Security Objectives

PremiumTrust Bank has set the following major information security objectives:

**Objective 1** - Achieve 100% protection of Confidentiality and integrity of Premium Trust Bank Information assets.
**Objective 2** - Achieve 90% Information Security Awareness culture across the organization.
**Objective 3** - Provide assurance of information systems resilience – 99.6 availability.
**Objective 4** – Ensure 90% percent compliance with PremiumTrust Bank requirements, contractual, regulatory, and legal requirements.

## Information Security Management System Policy

PremiumTrust Bank is committed to the confidentiality, integrity and availability of its information assets and shall implement measures through the establishment.

Premium Trust Bank is committed to continual improvement of its information security program to protect the organization's information assets against all threats.

Premium Trust Bank is also committed to complying with all applicable legal, regulatory, and contractual requirements related to information security in its services and operations.

In accordance with ISO27001, PremiumTrust Bank will analyze and understand its information security risks helping the Bank decide what it needs in place to meet our information security objective.

Premium Trust Bank will understand applicable requirements and in accordance with our risk assessment, we will, as appropriate, implement what is necessary to meet those requirements.

All users and custodians of information assets owned by or entrusted to PremiumTrust Bank shall comply with this policy and exercise a duty of care in relation to the storage, processing, and transmission of the organization's information and information systems.

## Exception and Exemptions

Any exceptions or exemptions to this policy will be documented in the PremiumTrust Bank Scope and its Statement of Applicability.

## Non-Compliance

Failure to comply with this policy and supporting policies and procedures may be considered a disciplinary offence. Therefore, compliance with this policy and all the organization's security-related policies and procedures, are mandatory conditions for every user of the organization's network resources.

No one is permitted to bypass the security mechanisms provided by the organization's systems or infrastructure for any reason. Breach of the policy or security mechanism may warrant disciplinary measures, up to and including termination of employment/contract.

**MD/CEO**