



**PremiumTrust Bank**

## **Access Control Policy**

**Classification: Internal**  
**April 2023**  
**Document Number: PTB/ISMS/ACP/A9001**

## Document Control Sheet

### Version and Update History

Date	Document Version	Document Revision History	Document Author/Reviser
April 3, 2023	1.0	Document creation	Information & Cyber Security Group

### Change Control

Change Clause/Frequency
The contents of this document are subject to change control on a twelve (12) months review cycle.

## **Table of Content**

Purpose .....	4
Scope.....	4
Policy Statement.....	4
Disciplinary Actions.....	5

## **Purpose**

The control of access to PremiumTrust Bank information assets is a fundamental part of the organization's information security strategy. Accordingly, this policy has been established to forestall the unauthorized or uncontrolled access, misuse of user privileges, or unauthorized disclosure to third parties, that may result in security breaches, damage, misuse, or theft of PremiumTrust Bank information and information systems.

## **Scope**

This policy applies to all PremiumTrust Bank information systems. All PremiumTrust Bank personnel and contractors including vendors shall comply with this policy.

## **Policy Statement**

1. Access requests to PremiumTrust Bank information and information systems shall be authorized and documented.
2. Access rights to PremiumTrust Bank information and information systems shall be granted to individuals based on job classification and function.
3. Access rights to PremiumTrust Bank information processing system shall be based on the principle of least privilege as determined by their role.
4. Access to all PremiumTrust Bank information systems shall be through unique user identification and additional authentication methods.
5. The creation and usage of access credentials shall conform to best practice authentication requirements in accordance with the password policy.
6. When required, access rights to vendors and other third parties shall be monitored and disabled when not in use.
7. The allocation and use of privileged access rights shall be controlled.
8. PremiumTrust Bank personnel and third parties shall be made aware of their responsibilities for maintaining effective access controls.
9. Access rights of suspended and exiting staff shall be immediately disabled and revoked respectively.
10. Access rights shall be reviewed Quarterly.

## **Disciplinary Actions**

Violation of this policy may result in disciplinary action, which may include:

- Termination for employees and temporaries.
- Termination of employment relations in the case of contractors or consultants.
- Dismissal of interns and volunteers.

Additionally, individuals and connecting organizations are subject to loss of access privileges to PremiumTrust Bank information systems, civil, and criminal prosecution as may be deemed necessary.