PremiumTrust Bank

User Access Management Process

Classification: Internal

April 2023

Document Number: PTB/ISMS/UAMP/A9002

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

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

Access Control Procedure

Introduction

The control of access to PremiumTrust Bank information assets is a fundamental part of a defense in depth strategy to information security. If PremiumTrust Bank is to effectively protect the confidentiality, integrity and availability of confidential and sensitive data, a comprehensive mix of access controls must be validated to be in place.

User Registration and Deregistration

A request for access to the organization's information systems must first be submitted to the Head of Technology for approval.

The IT officer will create the user account which will have a unique username that is not shared with any other user and is associated with a specific individual.

An initial password will be created on account setup and communicated to the user via secure means. The user will be required to change the password on first use of the account.

When an employee leaves the organization under normal circumstances, their access to computer systems and data will be suspended at the close of business on the employee's last working day.

In exceptional circumstances where there is perceived to be a risk that the employee may take action that may harm the organization prior to or upon termination, a request to remove access may be approved and actioned in advance of notice of termination being given.

User accounts will be initially suspended or disabled only and not deleted.

User Access Provisioning
Each user will be allocated access rights and permissions to computer systems and data that are commensurate with the tasks they are expected to perform.

User Password Reset
Steps to resetting user account on Active Directory

1. When a user requests a new password, you'll receive a password reset request in email. To reset the password, open the app launcher and select Admin.

2. In the Microsoft 365 admin center, select Users, Active users, and then select the key icon next to the user who requested the reset.

3. Select Auto-generate password to have a random password automatically created.

4. Select Reset

5. Select the Send password in email check box.

6. You'll see your email address in the Email the new password to the following recipient's box. Add the user's alternate email address or any address you choose.

7. Choose Send email and close.

The user will receive an email with the password reset instructions.

Removal or Adjustment of Access Rights
Where an adjustment of access rights or permissions is required e.g., due to an individual changing role, this will be carried out as part of the role change. Inactive user accounts will be disabled after 30 days of inactivity.

Management of Privileged Access Rights
Access to admin level permissions will be allocated to individuals whose roles require them.

Review of User Access Rights
Access rights will be reviewed by checking the assigned user permissions to information systems in the cloud environment on a quarterly basis.