PremiumTrust Bank

Guidelines for Working in Secure Areas

Classification: Internal
April 2023
Document Number: PTB/ISMS/GWSA/A7.6

Status: APPROVED

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

Guidelines for Working in Secure Areas

Introduction

Secure areas are required to protect PremiumTrust Bank information assets from a loss of confidentiality, integrity or availability, but such areas only remain secure if the personnel and third parties accessing them abide by the rules designed to be used within them.

This document states a set of rules to ensure that an area remains secure and applies to PremiumTrust Bank and all secure areas in which PremiumTrust Bank infrastructure is located.

Guidelines

For all personnel, third parties, and other stakeholders who are given access to a PremiumTrust Bank secure area, the following dos and don'ts will apply.

Dos:

- ✓ Ensure you understand the specific instructions for all secure areas to which you are granted access.
- ✓ Challenge and/or report anyone not wearing an ID.
- ✓ Remain vigilant whilst within the secure area.
- ✓ Always escort your visitors.
- ✓ Inspect all deliveries as soon as possible.
- ✓ Check that doors and windows are secure before leaving if you are the last one out of the secure area.
- ✓ Inform security of visitors that you are expecting.
- ✓ Check vacant areas for signs of unauthorised access.

Don'ts:

- × Tell anyone about the secure area if you are requested not to
- × Allow anyone to tailgate behind you through a secure entry point.
- × Keep secure doors open for longer than necessary.
- × Allow anyone to work in the secure area on their own unless by prior arrangement.
- × Lend anyone your ID card.
- × Expose your ID card to possible theft or loss.
- × Tell anyone your password.
- × Write your password down.
- × Use of photographic, video, or audio recording equipment within secure areas.
- × Leave classified information unattended in clear view.
- × Plugging any electrical device into a power supply unless specifically authorized to do so.
- × Tampering with any equipment installed.
- × Connecting any device to a network.
- × Archiving a larger amount of paper materials.
- × Storing flammable materials or equipment.

× Smoking, eating, and drinking.

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 for 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.