



PremiumTrust Bank

Context, Requirements and Scope

PTB/CRS/23/0001

Version 1.0

Classification: Internal

March 2023

Document Number: PTB/ISMS/CRS/C40

Document Control Sheet

Internal

Version and Update History

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

Change Control

Change Clause/Frequency
This document's contents are subject to change control on a twelve (12) month's review cycle.



Contents

1	Introduction	4
2	Information Asset Labeling	4
3	Screen Displays	4
4	Electronic Messages	5
5	File Transfers	5

1 Introduction

Internal

The purpose of this document is to set out how information assets will be labeled according to the information security classification scheme in place within PremiumTrust Bank and the specific controls that must be used when handling information of a particular classification.

2 Information Asset Labeling

A system of protective marking will be utilized for personnel and applicable third parties to be aware of how specific information will be managed as indicated in the below table:

Labeling Guideline	Hardcopy	Softcopy (Electronic)
Secret	State marking on the front page and in the header/footer of every document page when printed	State marking on the front page and in the header/footer of every document page when printed. Mark exterior container with classification incorporated into the media itself
Confidential	State marking on the front page and in the header/footer of every document page when printed	State marking on the front page and in the header/footer of every document page when printed. Mark exterior container with classification incorporated into the media itself
Internal Use	State marking on the front page and in the header/footer of every page of the document when printed.	State marking on every page of the document when printed. Mark container exterior.
Public	No marking required.	No marking required.

3 Screen Displays

Information systems and network devices which allow an authorized user access to classified information will include a warning of this fact upon logon which requires user acknowledgement of some form.

4 Electronic Messages

Classified information sent within email attachment(s) must include the classification clearly in accordance with the PremiumTrust Bank information security classification scheme.

5 File Transfers

Procedures for classified information sent via file transfer must include a step in which the recipient is clearly informed of the classification level of the information being transmitted before it is sent.