PremiumTrust Bank

Information Classification Policy

Classification: Internal
April 2023
Document Number: PTB/ISMS/ICP

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 Contents

1. Introduction

PremiumTrust Bank collects a great deal of confidential information about its employees, partners and clients. Some of this information is processed, stored electronically and/or transmitted across networks to other computers. Breach of this information could lead to business losses, lawsuits and financial loss. Information Classification helps to identify the different kinds of information assets within the organization and helps to determine the appropriate level of protection that should be assigned to these information assets.

1.1. Purpose

The purpose of this policy is to ensure that information assets are appropriately classified based on an information classification policy to indicate the need, priorities, and expected degree of protection when handling the information.

1.2. Scope

This policy applies to all information assets existing in any form which have been created, acquired, or disseminated using the organization's resources and relating to any of the organization's business activities, employees, or customers.

This policy also establishes requirements for appropriate classification, protection, control and management of all the organizations' information assets processed or generated using the organization's information technology resources, which include data or information that is:

- Stored in database applications
- Stored on computer systems
- Transmitted across internal and public networks
- Printed or handwritten on paper etc.
- Stored on removable media such as flash drives, external drives and other similar media
- Stored on fixed media such as hard disks and disk sub-systems
- Presented on slides, overhead projectors, using visual and audio media Generated, transmitted or stored in any other relevant format

1.3. Audience

This policy is applicable to all permanent employees, contract workers, temporary employees and third parties that uses the information assets of the company which includes but is not limited to information, network links, workstations (laptops, desktops), servers, software, network devices (switches, wireless routers, wired routers, gateways, bridges), network accessories (cables etc), software licenses, printers, scanners, and all its associated data and

information assets.

1.4. Definitions

Custodian:
Entity that is responsible for implementing the controls specified by the owner. The custodian is responsible for the processing and storage of information.

Owner:
Entity that is accountable for and has authority over information. The owner is responsible for classifying the information; ensuring necessary security controls are in place, protecting the confidentiality, integrity and availability of the data. The owner delegates responsibility of day-to-day maintenance of the data protection mechanisms to the custodian.

2. INFORMATION CLASSIFICATION POLICY

2.1. Policy Statements

Information will be classified as follows;

PUBLIC/UNCLASSIFIED
This classification applies to all information meant for public use. Their disclosure will not inversely impact the company, its employees, and all relevant stakeholders. Examples include newsletters, flyers, information available on the company's website or social media, etc.

INTERNAL
This classification applies to information not approved for general circulation outside PremiumTrust Bank, where its disclosure would inconvenience the organization or management, but is unlikely to result in financial loss or reputational damage. Examples include internal memos, internal project reports, etc. Security at this level is controlled but normal.

CONFIDENTIAL
This classification applies to information which is designated for use only for intended/authorized users within the organization and must be protected at all times. Authorized approvals must be obtained before release to any other unauthorized employee. Such information includes impending mergers or acquisitions, corporate plans or designs, employee appraisal reports, payroll information, medical/health reports, budgets etc and other sensitive information pertaining to clients.

CLASSIFICATION CATEGORIES	PUBLIC	INTERNAL USE	CONFIDENTIAL
Creation	Moderate environment. Designated/Any Designated Personnel	Controlled environment. Designated/Any Designated Personnel	Highly controlled environment. Designated/Authorized Personnel
Transmission and Distribution	Through company or personal e-mail	Through company's email or personal e-mail in the advent of non-availability of company's e-mail.	Through company's e-mail accounts Apply encryption (pdf) before sending electronically outside organization.
Storage	Normal company-controlled environment	Store on shared portal for group access. Printed copies should be stored under lock.	Store only on designated systems (encrypted) or shared portal Printed copies should be stored under lock.
Disposal	Normal company-controlled environment	Use document shredder Supervised disposal and physical destruction of electronic storage disk.	Use document shredder Supervised disposal and physical destruction of electronic storage disk.
Logging of Security-related Events	There is generally no need to log security incidents relating to public classification items unless subject to	Incidents where Internal information has been compromised should be recorded and investigated in accordance	Incidents where Confidential information has been compromised should be reported to senior management immediately and flagged as a major incident. They will be

	criminal activity such as large-scale theft of material.	with the organization's security incident management procedures.	recorded and investigated in accordance with the organization's security incident management procedures.
Declassification	Public information will not be subject to declassification as it is already at the lowest level	Internal information may be declassified to "Public" with the permission of the asset owner at which time the control specified in section 2.1 above will apply	Confidential information may be declassified to "Internal" or "Public" with the permission of the asset owner at which time the controls specified in the relevant section above will apply.

2.2. Information Resource Handling

- Information resources of the organization whether in electronic or non-electronic format, must be properly handled and controlled based on the information sensitivity and criticality.
- Labelling, retention, storage, encryption, release, and destruction of information must comply with established organizational policies and procedures.

2.3. Information Labelling

- Classified data or information included in electronic media (e.g., disks, diskettes, tapes) and hardcopy output (e.g., printouts, screen prints) must be legibly and durably labelled as either CONFIDENTIAL or INTERNAL.

3. Disciplinary Actions

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

- Termination for employees and temporary employees.
- 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.