INFORMATION SECURITY DEPARTMENT

Information Security Policy

2023

Document Control

Version No.	Date of Change	Type of Change	Description	Prepared by
1.0	*Nov/2023*	*Develop*	*Develop and publish the document*	*ISMS Manager*

This document is approved by the Information Security Steering Committee in November 2023.

Table of Contents

Document Control 2
Table of Contents 3
INTRODUCTION 4
SCOPE 5
TERMS AND DEFINITIONS 6
CONFIDENTIALITY STATEMENT 7
Purpose 8
Ownership 8
Statement 8

INTRODUCTION

Information is among **INVESTBANK**'s most valuable assets, and **INVESTBANK** relies upon that information to perform its business activities. Therefore, the security of information assets is one of **INVESTBANK**'s business objectives. Security shall be integral to each of **INVESTBANK**'s employee profiles and objectives. It is the policy of **INVESTBANK** to protect the organization's information assets from all types of threats, whether internal or external, intentional or accidental, through a corporate-wide commitment to security that is designed to detect, prevent, and mitigate information security-related risks and in compliance to the applicable laws and regulations.

The guiding Principles:

INVESTBANK shall preserve the confidentiality, integrity and timely availability of information by setting up, maintaining, continually monitoring and improving an information security management system (ISMS). The management of information security at **INVESTBANK** should follow the Plan, Do, Check and Act (PDCA) process cycle to control and continually improve the information security management system and the security program, as follows:

- **Plan**: This stage establishes objectives and processes required to deliver the desired results of the information security management system.
- **Do**: This stage executes the ISMS activities considering results of the previous stage.
- **Check**: This stage evaluates the performance of the ISMS and ensures continuous review.
- **Act**: This stage introduces required improvements to fix identified gaps and nonconformities to the stated objectives and requirements.

SCOPE

The scope of the information security management system at **INVESTBANK** includes all types of information belonging to **INVESTBANK** (written, spoken, digital, etc.) in all formats (paper, digital media, etc.) regardless of their physical location (on-premises, on the cloud, etc.) and in any state (stored, being processed or being transmitted). The scope also applies to all users of information assets including temporary and permanent **INVESTBANK** employees, customers, consultants, vendors, business partners and contractors' personnel, regardless of geographic location.

TERMS AND DEFINITIONS

Confidential information	Information that is not intended to be made available or disclosed to unauthorized individuals, entities or processes.
Information asset	A body of information recognized as 'valuable' to the organization is defined and managed as a single unit.
Information security	The protection of information assets from the risks threatening them. Protecting information assets covers the confidentiality, integrity and availability of information assets, besides providing other services such as non-repudiation, authentication, authorization and more. Information security includes cybersecurity and physical security.
Information Security Management System	Defines policies, methods, processes, and tools to ensure sustainable information security in the organization. This includes introducing policies and procedures and systematically implementing administrative, physical and technical measures that must be continuously controlled, monitored, and improved. The goal is to ensure an appropriate level of protection for the confidentiality, availability, and integrity of information within the scope and identify, analyze, and mitigate cybersecurity risks.
Information system	Set of applications, services, information technology assets, or other information-handling components.
Interested party	A stakeholder person or organization that can affect, be affected by, or perceive itself to be affected by a decision or activity.
Ownership, Asset owner	The person with the final corporate responsibility of data protection would be held liable for any negligence when it comes to protecting the company's information assets. The person who holds this role is responsible for assigning a classification to the information and dictating how the information should be protected.
Personnel	Persons doing work under the organization's direction.
Policy	intentions and direction of an organization, as formally expressed by its top management.
User	An interested party with access to the organization's information systems.
Third-party	Non-**INVESTBANK** employee who engaged in direct business with the bank.

CONFIDENTIALITY STATEMENT

Classification of this document is Public. This document should not be reconstructed, reproduced, or circulated without the prior approval of the Information Security Department.

POLICY CONTENTS

Purpose

This policy aims to provide **INVESTBANK**'s management direction and support for Information Security per **INVESTBANK**'s business requirements and relevant laws and regulations. The 'Information Security Policy' sets the guiding principles for managing information security and cybersecurity at **INVESTBANK**.

Ownership

The owner of this document is the ISMS Manager. Any changes or updates to the document shall be explicitly approved by him.

Statement

Accordingly, **INVESTBANK** is committed to orderly and efficient service delivery through strict adherence to security policies, procedures and practices. It shall ensure the safety of assets and the completeness and accuracy of records, thereby delivering assurance to all customers and stakeholders. As a sign of its commitment, **INVESTBANK**'s management at the highest level and the board of directors have reviewed and approved this policy. They shall ensure adherence to its policies and procedures.

In this direction, the Information Security Policy states the following:

- **INVESTBANK** shall determine external and internal issues relevant to its purpose and affect its ability to achieve its information security management system's intended outcome(s).
- **INVESTBANK** shall understand and analyse the needs and expectations of the various internal and external stakeholders by determining interested parties relevant to the information security management system and the relevant requirements of these interested parties, which will be addressed through the information security management system.
- **INVESTBANK** shall determine the boundaries and applicability of the information security management system.
- **INVESTBANK** is committed to establish, implement, maintain and continually improve an information security management system, including the processes needed and their interactions.
- **INVESTBANK**'s top management is committed to demonstrate leadership and commitment with respect to the information security management system.
- Information security and topic-specific policies shall be defined, approved by management, published, communicated to and acknowledged by relevant personnel and interested parties, and reviewed at planned intervals and if significant changes occur.

- **INVESTBANK** shall review the information security policies and procedures regularly or when significant changes occur to the business or the technology environments to maintain their suitability, adequacy and effectiveness.
- The information security management system at **INVESTBANK** must comply with the relevant regulations, legislations, and contractual mandates.
- When planning for the information security management system, **INVESTBANK** shall determine any existing risks and opportunities and treat them systemically.
- **INVESTBANK** shall establish and maintain consistent and measurable information security objectives at relevant functions and levels.
- **INVESTBANK** recognizes that acquiring and maintaining the necessary competencies is very important for the success of the information security management system.
- **INVESTBANK** shall ensure that persons doing work under the organization's control shall be aware of the information security policy and requirements relevant to them and the implications of not complying with the security requirements and policy.
- **INVESTBANK** shall ensure effective internal and external communications relevant to the information security management system.
- **INVESTBANK** shall document and control information determined by the organization as being necessary for the effectiveness of the information security management system.
- **INVESTBANK** shall ensure proper and effective planning, implementation and control of the operational processes required by the information security management system and needed to meet the security requirements and achieve the security objectives.
- **INVESTBANK** shall establish the process to ensure the information security management system's monitoring, measurement, analysis and evaluation.
- **INVESTBANK** shall ensure the continuous and planned auditing of the information security management system.
- The top management of **INVESTBANK** shall review the organization's information security management system at planned intervals to ensure its continuing suitability, adequacy and effectiveness.