<Company Logo>

Wise East Bank

ISMS_POL_COM_v0.1

Document Owner : The Information Security Officer

Information Security Management System

(ISMS) (ISO 27001:2022)

Revision History

Version	Created / Changed by	Reviewed by	Approved by	Date	Change Description
0.1	Debjit Das	Supritha D V		18-01-25	Draft created

Table of Contents

1. Introduction

This policy outlines the guidelines and requirements for ensuring compliance with applicable legal,regulatory, statutory, and contractual obligations in accordance with ISO/IEC 27001:2022 standards.
The organisation is committed to meeting all compliance requirements to protect information assets, avoid legal penalties, and maintain trust with customers, partners, and stakeholders.

2. Scope

2.1 Geographical Scope

India.

2.2 Functional Scope

All business functions, services, and activities that are subject to legal, regulatory, and contractual compliance requirements.

2.3 Organizational Scope

This document is related to all organisational divisions, including Senior Management, Compliance Officers, Department Heads, and Employees.

3. Terms and Definitions

Terms	Definitions
Major Change	Refers to any significant alteration to this procedure or related factors that could materially impact the purpose, implementation, or compliance of the document.
ISMS	Information Security Management System
Compliance	Fulfilment of specified requirements
Non-Compliance	non-fulfilment of compliance obligations
Audit	review of a party's capacity to meet, or continue to meet, the initial and ongoing ***approval agreements*** as a ***service provider***

4. Roles and Responsibilities

4.1 Senior Management :

- Approve and oversee the implementation of compliance-related policies and procedures.
- Ensure adequate resources are allocated for compliance management.

4.2 Compliance Officer / Department :

- Identify applicable compliance requirements and maintain a compliance register.
- Conduct regular internal audits and assessments.
- Report compliance status to senior management.

4.3 Department Heads :

- Implement compliance requirements in their respective areas.
- Ensure employees are trained and aware of relevant compliance obligations.

4.4 Employees :

- Follow all applicable compliance requirements.
- Report any suspected compliance breaches immediately to the Compliance Officer.

5. Policy Statement

The organisation is committed to complying with all applicable legal, regulatory, statutory, and contractual obligations. Compliance is a core element of our ISMS and is essential for maintaining the confidentiality, integrity, and availability of organisational information.

No activities shall be undertaken that may cause a breach of applicable compliance requirements. All employees, contractors, and third parties are expected to be aware of and adhere to this policy.

6. The Policy Description

This policy establishes a structured approach to identifying, implementing, and maintaining compliance with applicable legal, regulatory, statutory, and contractual requirements. It ensures that compliance obligations are integrated into daily business operations and that deviations are promptly addressed.

6.1 Identification of Compliance Requirements

All relevant compliance obligations—legal, regulatory, statutory, contractual, and internal—shall be identified, documented, and kept current. The Compliance Officer maintains a **Compliance Register** that is regularly updated to reflect new or amended obligations. This ensures the organisation is aware of all applicable requirements before engaging in any activity that may have compliance implications.

6.2 Documentation & Recordkeeping

The organisation will maintain clear, accessible records of compliance-related documents, including policies, procedures, audit reports, training records, and incident reports. This documentation will be retained in line with regulatory retention requirements and will be readily available during audits or inspections.

6.3 Integration into Operational Processes

Compliance requirements will be embedded into departmental and operational procedures. This includes incorporating regulatory requirements into contracts, procurement processes, IT system configurations, and data handling practices. The aim is to ensure compliance is not an afterthought but an integral part of business workflows.

6.4 Training & Awareness

All employees will receive compliance training relevant to their roles. This includes induction training for new hires and refresher courses for existing staff. Training will cover applicable regulations, company policies, reporting procedures, and potential consequences of non-compliance. Awareness campaigns will be conducted to keep compliance top-of-mind across the organisation.

6.5 Monitoring & Auditing

Regular internal audits, compliance reviews, and monitoring activities will be conducted to ensure adherence to applicable requirements. Findings from these reviews will be documented, and corrective actions will be tracked to completion. External audits may be conducted as required by contractual or regulatory bodies.

6.6 Non-Compliance Management & Corrective Actions

Any instance of non-compliance will be reported immediately to the Compliance Officer. A root cause analysis will be conducted, and corrective actions will be implemented promptly to prevent recurrence. Where necessary, regulatory authorities will be notified in accordance with legal obligations.

7. Related Documents

ISO/IEC 27001:2022

Information Security Policy

Online Browsing Platform (OBP)

IEC 60050 - International Electrotechnical Vocabulary - Welcome

Compliance Register

Internal Audit Procedure

Risk Management Policy

8. Report

KPIs	Target	Frequency	Location
Percentage of Non compliance Incident	0	monthly	Compliance Register
Percentage of staff trained in compliance	100 %	anually	Training Records
Percentage of compliance audits	100 %	monthly	Audit Reports

completed on time			

9. Review of Document

This document shall be reviewed once a year or after a significant or major change to the procedure takes place.