CRESCENT BANK

TRUST BEYOND BANKING.

Information Security Policy

Information Security Policy

DOCUMENT CLASSIFICATION	Internal
DOCUMENT REF	ISMS-DOC-05-2
VERSION	1
DATED	7 September, 2025
DOCUMENT AUTHOR	Sheheryar Altaf
DOCUMENT OWNER	Ali Khan, ISMS Project Manager

Revision History

VERSION	DATE	REVISION AUTHOR	SUMMARY OF CHANGES
1	6 September, 2025	Sheheryar Altaf	Initial Draft
2	7 September, 2025	Sheheryar Altaf	Added minor corrections

Distribution

NAME	TITLE
Mr. Ahmed Khan	CEO
Mr. Bilal Qureshi	CFO
Ms. Sara Malik	CISO
Mr. Kamran Pervaiz	Compliance & Audit Head

Approval

NAME	POSITION	SIGNATURE	DATE
Mr. Ahmed Khan	CEO	_____	8 September, 2025
Mr. Bilal Qureshi	CFO	_____	9 September, 2025
Ms. Sara Malik	CISO	_____	10 September, 2025

Contents

Tables

1. Introduction

This document defines the information security policy of Crescent Bank.

Crescent Bank manages sensitive financial documents and customer information. Information security is critical to our operations, not only to protect customer trust but also to comply with regulatory requirements. Our top management is committed to ensuring that information security is taken seriously across the organization and that a robust Information Security Management System (ISMS) is established, maintained, and continually improved.

Crescent Bank has implemented an Information Security Management System (ISMS) in line with the international standard ISO/IEC 27001. This standard defines the requirements for an ISMS based on globally recognized best practices.

2. Purpose

The purpose of this policy is to establish a foundation for information security at Crescent Bank and to ensure compliance with ISO/IEC 27001 and applicable regulatory requirements such as SBP's ETGRM framework. Crescent Bank adopts a risk-based approach to information security, ensuring that risks are regularly assessed, prioritized, and treated in line with ISO/IEC 27001 and regulatory requirements.

3. Objectives

All information security objectives are measurable and monitored in line with Clause 6.2 of ISO/IEC 27001

1. Protect sensitive financial and customer information.
2. Improve the organization's overall security posture.
3. Provide a framework for supporting policies and controls.
4. Ensure compliance with legal, regulatory, and contractual obligations.

4. Scope

This ISMS scope is formally defined and maintained in accordance with Clause 4.3 of ISO/IEC 27001:

Scope Type	Included Elements
1. System Scope	Core banking (Temenos T24), Internet & mobile banking, payment systems, ATMs, POS, servers, databases, network infrastructure, backup & DR systems
2. Physical Scope	HQ (Karachi), critical branches, Data Center & DR site (Islamabad), server rooms, ATM locations, digital banking servers, source code escrow (external provider, Zurich)
3. Organizational Scope	IT , Security , Risk & Compliance, Operations (Retail, Lending, Digital Banking), HR (PII handling),and Financial (sensitive transactions)

5. Policy Statements

Policy statements are the core of our information security policies and guide all supporting policies to align with ISMS objectives, regulations, and best practices.

1. Confidentiality, Integrity, and Availability (CIA)
Crescent Bank commits to protecting information to ensure it remains confidential, accurate, and available to authorized users when needed.

2. Risk Management
Information security risks will be identified, assessed, evaluated, and treated to minimize potential harm to the organization and its customers.

3. Management Commitment
Top management will provide leadership, resources, and support to ensure information security is prioritized and enforced across the organization.

4. Business Continuity and Backup

Critical operations and services will be maintained and recovered to ensure continuity in the event of a disruption. Information and systems will be backed up appropriately to support business continuity and recovery objectives.

5. Asset and Inventory Management

All information assets, including hardware, software, and data will be inventoried. Data will be classified, and protected according to their criticality and sensitivity.

6. Third-Party and Supplier Security

Suppliers and third parties with access to our information must comply with the organization's information security requirements.

7. Continual Improvement

The ISMS will be continually improved to enhance information security, adapt to emerging risks, and meet business objectives.

8. Internal Audit and Review

The effectiveness of information security controls will be annually reviewed through audits and management oversight.

9. Training and Awareness

Employees will be trained and made aware of information security responsibilities to promote a culture of good cyber hygiene and security practices.

10. Incident Response

Crescent Bank will establish and maintain processes to detect, respond to, and recover from information security incidents to minimize impact and ensure business continuity.

11. Regulatory Compliance

Crescent Bank will comply with all regulatory guidelines, including SBP ETGRM, to ensure information security aligns with legal obligations.

6. Roles and Responsibilities:

Name	Title	Responsibility	Reports To
Mr. Ahmed Khan	CEO	Provides strategic oversight and ensures top-level commitment to information security, aligning security initiatives with overall business objectives.	—
Mr. Bilal Qureshi	CFO	Manages budget allocation for ISMS and information security initiatives. Oversees financial audits related to security	CEO
Ms. Sara Malik	CISO	Leads the information security program, including ISMS, risk management, and security operations. Oversees the security team and ensures alignment with organizational goals and compliance.	CEO
Mr. Saqib Zulfiqar	Digital Banking Head	Supports the CISO in implementing information security initiatives and ensures compliance with ISMS requirements within the department.	CEO
Mr. Mubeen Paracha	Retail Banking Head	Supports the CISO in implementing information security initiatives and ensures compliance with ISMS requirements within the department.	CEO

Mr. Musa Ajmal	Financing Head	Supports the CISO in implementing information security initiatives and ensures compliance with ISMS requirements within the department.	CEO
Mr. Tariq Umer	Operations Head	Supports the CISO in implementing information security initiatives and ensures compliance with ISMS requirements within the department.	CEO
Mr. Asim Muneer	HR Head	Ensures data privacy and protection of sensitive information, supports implementation of information security initiatives, and ensures ISMS compliance within the HR department.	CEO
Mr. Kamran Pervaiz	Compliance & Audit Head	Ensures the bank complies with regulatory requirements, such as SBP guidelines, and oversees internal audits related to information security and compliance	CEO
Mr. Abdullah Ali	Data Protection Officer (DPO)	Ensures protection of customer and employee data, maintains privacy compliance, and implements data protection measures across the organization.	CISO
Mr. Ali Khan	ISMS Project Manager	Manages the ISMS and related resources, ensuring effective implementation, optimization, and ongoing maintenance of information security processes.	CISO
Ms. Sidra Imran	Technical Lead	Leads the technical implementation of ISMS in line with ISO standards. Performs oversight SOC, penetration testing, and incident response teams, with a primary focus on resolving technical security issues.	ISMS Project Manager

7. Legal & Regulatory Obligations

Crescent Bank will comply with all applicable laws, regulations, and standards, including SBP guidelines (ETGRM), PCI DSS, and relevant data protection laws. Compliance will be monitored and maintained to ensure alignment with legal, regulatory, and contractual obligations.

8. Policy Communication

The policy will be published on the bank's internal portal. All new employees must review it and complete an assessment. Regular tabletop discussions will be held monthly with management to reinforce awareness and ensure consistent understanding.

9. Enforcement / Disciplinary Actions

Non-compliance with this policy will result in immediate notification from Security teams and may lead to suspension of access privileges. Employees will be required to complete awareness training before access is restored. Continued or severe violations may result in disciplinary actions in line with the bank's HR policies

10. Continual Improvement

Crescent Bank policy regarding continual improvement is to:

Crescent Bank will continually improve its ISMS to stay effective with business, regulatory, and technology changes. Ongoing awareness and training will be provided. Vendors must align with our standards through SLAs. Improvements will be driven by audits, risk assessments, metrics, and feedback, and will be reviewed during management reviews.

11. Review and Maintenance

This policy will be formally reviewed annually to ensure it remains effective, relevant, and aligned with business and regulatory requirements. Additional reviews will be conducted following significant incidents, organizational changes, or updates to regulatory guidelines. Senior management will carry out tabletop exercises and provide feedback during reviews, and all improvement actions will be documented and tracked.