Reem Community Bank PSC

Data Protection Policy

April 2026

Version No: 1.0	Issue Date: 18/04/2026	Date Effective:

DOCUMENT HISTORY

Version	Date/Month	Author	Description
1.0	01-Jan-2026	Head of Information Security	Original document

REVIEWED/RECOMMENDED BY

Name	Title	Date	Signature
Mrs. Sara Al Bin Ali	Chief Executive Officer		
Mr. Seraj Al Faidi	Deputy Chief Executive Officer		
Mr. Mohamed Al Zamil	Chief Operating Officer		
Mr. Mohamed Roshdy Elbastaweesy	Chief Technology Officer		
Mr. Vaibhav Maheshwari	Head of Risk		

MAK MR MZ VM SF SA

Contents

1. Executive Summary 5
2. Introduction 5
3. Definitions 5
4. Purpose and Scope 7
5. Distribution 7
6. Document Control 7
7. RACI Matrix 8
8. Data Protection Policy 8
   - 8.1 Data Collection 8
   - 8.2 Data Access 9
   - 8.3 Data Handling and Data Transfer 9
   - 8.4 Storage of Data 9
   - 8.5 Protection of Data 10
   - 8.6 Data Retention and Archival 10
   - 8.7 Data Retention Schedule 11
   - 8.8 Data Disposal and General Guidelines 13
   - 8.9 Data Disposal by Destruction 14
   - 8.10 Removable Media 14
   - 8.11 Medium-wise Destruction Process 14
9. Data Retention and Deletion RACI Matrix 15
10. Policy Compliance 15
11. Waiver Criteria 15
12. References 16

Annexure A: Controls Description 16

Annexure B: Glossary 17

Reem Community Bank PSC ("Reem Community Bank"), is committed to provide customized financing solutions in the UAE. It is fully operated under Central Bank UAE guidelines. **Reem Community Bank** offers a range of solutions tailored to the needs of its customers. It is headquarters in Abu Dhabi and serves customers across the UAE.

VISION

To be the market leader in specialized commercial lending and financing for a wide range of businesses.

MISSION

To offer a customized, timely and transparent finance platform for businesses and entrepreneurs.

VALUES

- ✓ *Business Excellence:* Reem Community Bank prides ourselves on its speed and quality of execution. In addition to its expanding product offering, Reem Community Bank is also able to offer the support and services of our group partners. Every aspect of our work is in partnership with our clients. We always aim to meet our clients' expectations.
- ✓ *Agility:* Our ownership structure and broad lending experience provide a solid foundation to support our clients' business needs. Reem Community Bank can provide finance terms that allow for rapid drawdown and tailored structures, in a manner that is generally not offered by conventional banks.
- ✓ *Partnership:* Our commitment to our clients goes beyond any individual transaction. We respect our clients as our partners and invest our comprehensive capabilities into achieving their goals.
- ✓ *Respect and Integrity:* Ethical behavior is an integral part of everything we do. Our performance is underpinned by our transparent vision and compliance with all relevant financial regulations.

1. Executive Summary

Reem Community Bank PSC ("**the Company**" or "**RCB**") is licensed and regulated by the Central Bank of the UAE to conduct banking operations.

Senior Management for the purpose of this policy will be anyone who is a member of Reem Community Bank' Executive Management (herein refer to as "**EXM**").

The use of "must" "will" or "shall" in any policy statement indicates mandatory compliance. The use of "may" indicates a recommendation which may be implemented where applicable i.e. good practice.

2. Introduction

Reem Community Bank PSC is committed to protecting the confidentiality, integrity, and availability of its information assets, including personal data and sensitive business information. This Data Protection Policy establishes the principles, requirements, and controls for the secure collection, access, use, storage, retention, and disposal of data across the organization.

The policy is aligned with applicable regulatory and legal requirements in the United Arab Emirates, including data protection obligations, and supports Reem Community Bank's Information Security Management System (ISMS) framework based on ISO/IEC 27001:2022. It applies to all employees, outsourced staff, and third parties who handle or have access to Reem Community Bank information assets.

Through this policy, Reem Community Bank aims to ensure that data is handled responsibly and securely, risks related to data breaches are minimized, and trust is maintained with customers, partners, and stakeholders.

3. Definitions

Acronyms	Definitions
CB	UAE Central Bank
CEO	Chief Executive Officer
COO	Chief Operating Officer

CTO	Chief Technology Officer
EXM	Senior / Executive Management
FCR	Finance Company Regulations issued by CB in 2023
HOC	Head of Compliance
DPO	Data Protection Officer
ITD	Information Technology Department
IT	Information Technology
ISMS	Information Security Management System, which encompasses requirements of ISO 27001:2022, Information Assurance Standard (IAS), and PCI: DSS.
ISMC	Information Security Management Committee
IA	Internal Audit
HoIA	Head of Internal Audit
HOR	Head of Risk
HOIS	Head of Information Security
RCB / The Company	Reem Community Bank PSC
End Users	All Reem Community Bank employees, outsourced staff, and external entities, including outsourced vendors, cloud service providers (CSPs), and fintech or strategic partners who access and use Reem Community Bank's information systems and associated assets to perform job-related responsibilities or fulfil contractual obligations. This includes those connected to Reem Community Bank systems under outsourcing arrangements and in alignment with the Consumer Protection Standards (CPS) issued by the Central Bank of the UAE (CBUAE).
Information Assets	This includes Reem Community Bank electronic and computing equipment, personal equipment, information in hard copies and soft form, hardware, software, human resources, physical assets, and service assets of Reem Community Bank, whether hosted in-house, outsourced

	to a third party, or stored in the cloud, which hosts RCB information.

4. Purpose and Scope

The purpose of this document is to enumerate the controls for data protection, retention, storage, and disposal of business-sensitive information & personal data that is collected, created, processed, stored, maintained, or transmitted by Reem Community Bank. This Policy is designed to safeguard the privacy and integrity of information, including personal, financial, and transactional data, as well as sensitive business information defined at the organizational level and also ensure adherence to relevant laws and regulations.

This policy applies to all End Users and functional/business units.

This policy also applies to all Information, Communication, Technology, and Computing assets (hereinafter referred to as Information Assets) of Reem Community Bank, whether hosted in-house, outsourced to a third party, or on cloud.

In the event of any conflict, the laws and regulations of the United Arab Emirates (UAE) shall always supersede this policy.

5. Distribution

The Data Protection Policy will be made accessible to all staff of Reem Community Bank. A copy should also be made accessible on the Company's intranet.

6. Document Control

The Data Protection Policy shall be reviewed at least on an annual basis and as whenever required to reflect developments in the Requirements.

Amendments to the Data Protection Policy will be initiated by HOIS, reviewed by CTO and HOR and approved by the ISMC, prior to its application.

Following the approval of the amendments by the ISMC, the document change control table will be updated.

7. RACI Matrix

R-Responsibility: Role responsible for getting work done
A-Accountable: The Role that is ultimately accountable for the success or failure of a task.
C- Consulted: The Role that is consulted and whose opinions are sought
I-Inform: The role that is kept informed on progress

Roles / Activities	ISMC	DPO	HOIS	HoDs	ITD
Approval and enforcement of Policy	A	R	C	C	I
Implementing Policy	A	R	C	I	R
Adhere to policy	A	R	C	I	R
Review of Policy	A	R	C	C	I
Monitoring compliance with policy	A	R	-	-	-

8. Data Protection Policy

The Data Protection Policy is detailed below.

8.1 Data Collection

Reem Community Bank collects personal information to:

i. Users shall collect and process only the minimum necessary sensitive/personal data required to perform the task.
ii. HoDs must ensure that all decisions regarding the collection and use of RCB data comply with the law and align with RCB policies and procedures.
iii. Consent of data subjects must be obtained wherever required, and such consent must be explicit, informed, and recorded.
iv. Cross-border transfers of personal data shall not take place unless compliant with UAE laws and subject to DPO/Legal approval.
v. Each stored data item shall be labelled with the record name, record type, original data owner, information classification, required retention period based on business need and/or regulatory requirement, and any special details (e.g., related to cryptographic keys).

8.2 Data Access

i. Access to personal data and sensitive business information shall be restricted to authorized users only.
ii. Authorization must be obtained from the relevant HoDs or the designated authority before accessing such data.
iii. Where access to personal data and business sensitive data has been authorized, use of such data shall be limited to the purpose required to perform RCB business.
iv. End Users must respect the confidentiality and privacy of individuals whose records they access. They must observe ethical restrictions applicable to the information accessed and comply with relevant laws and policies concerning the access, use, or disclosure of such information.
v. Notification of a user's termination or removal of authorized access to personal data and business-sensitive data must be conveyed immediately to the IT department.

8.3 Data Handling and Data Transfer

i. Personal data shall not be transferred by any method to people who are not authorized to access that information. End Users must ensure that adequate security measures, like encryption, are in place at each destination when transferring personal data and business-sensitive data.
ii. Personal data and business-sensitive data shall be protected from unintended or unauthorized access. End Users must protect from unauthorized viewing of such information, which is displayed on their computer screens. End Users must not leave personal data and business-sensitive data unattended and accessible.
iii. Personal data and business sensitive data shall not be taken off premises unless the End User is authorized to do so.
iv. Physical protection from theft, loss, or damage shall be implemented for mobile devices that can be easily moved, such as a PDA, EID Readers, or Laptops.
v. Media containing personal data and business-sensitive data shall be protected against unauthorized access, misuse, or corruption during transportation beyond Reem Community Bank's physical boundaries.

8.4 Storage of Data

i. All personal data and business-sensitive data must be stored securely to prevent unauthorized access, alteration, or loss.
ii. Data stored electronically must be protected using appropriate and effective technical controls such as access restrictions, encryption, and up-to-date anti-malware solutions.
iii. Physical records containing personal or sensitive information must be stored in locked cabinets or secured areas with restricted access.
iv. Data stored on portable media (e.g., USB drives, external hard drives, CDs) must be encrypted and physically secured when not in use.

v. Cloud storage or third-party storage services may only be used if approved by the IT department or the designated authority and are compliant with applicable data protection requirements and regulations.

vi. Data in cloud storage must be hosted within UAE (where applicable) or in jurisdictions approved by CBUAE/Board Risk Committee.

vii. End Users must ensure that data stored on local devices (e.g., desktops, laptops) is regularly backed up to an approved secure storage in accordance with Reem Community Bank's backup policy.

8.5 Protection of Data

i. All personal data and business-sensitive information must be protected against unauthorized access, disclosure, alteration, or destruction.

ii. End Users must implement appropriate security measures such as strong passwords, encryption, and secure authentication methods when accessing or handling sensitive data.

iii. Confidential data must not be shared or disclosed to unauthorized individuals, either within or outside the organization.

iv. Data protection controls must be applied consistently across all storage locations, including local devices, shared drives, cloud services, and removable media.

v. End Users are responsible for reporting any suspected or confirmed data breach, loss, or unauthorized disclosure immediately to the Information Security and IT department.

vi. Systems and applications used to process or store sensitive data must be kept up to date with the latest security patches and regularly monitored for vulnerabilities.

vii. Penetration testing and vulnerability assessments must be conducted at least annually, with remediation plans approved by the CTO.

8.6 Data Retention and Archival

i. Personal and business-sensitive data shall not be retained longer than necessary for the purposes it was collected and processed.

ii. Personal and business-sensitive data that are not currently required for active organizational operations may be archived, provided that all retention requirements have been fulfilled.

iii. HoDs shall determine the criteria for inactive record status in their departments, based on the need for the records, available storage space, and legal/statutory requirements.

iv. The required retention periods, by record type, shall comply with business, legal, and regulatory requirements. Secure deletion of personal and business-sensitive data shall be performed when it is no longer needed for legal, regulatory, or business reasons.

v. The records, both physical and electronic, shall be stored in secure locations and have off-site backups at physically secure locations (as applicable).

vi. A half-yearly review (automated or manual) shall be performed for identifying and securely deleting stored personal data that exceeds defined retention requirements.

vii. For retention of Records containing personal and business sensitive data a "Data Retention Schedule" describing the records and the official retention period for each type of record created or maintained by Reem Community Bank should be developed and maintained.

viii. Inactive physical records shall be stored in secure, climate-controlled areas to prevent unauthorized access, damage, or loss from temperature fluctuations, fire, water damage, pests, and other hazards.

ix. "Backup/Shadow" records should be destroyed once it is confirmed that they only contain duplicates of records stored elsewhere and do not include any original materials.

8.7 Data Retention Schedule

To categorize records containing personal and business-sensitive data, it is necessary to determine whether a particular item constitutes a record, and thus, is subject to a record retention and disposition schedule. Some of the characteristics of a record are:

i. Contains legal or regulatory compliance information.
ii. Evidences a transaction.
iii. Contains personal data.

When making retention decisions, Reem Community Bank shall categorize records into the following categories and establish a retention period for each category, regardless of the medium (paper or electronic) based on business needs, regulatory requirement and owner requirements.

Category	Retention Period	Example
Category 1 Records with enduring value	Permanent	a. Appointment calendars of executives b. Documentation of departmental and organizational decisions and operations c. E-mail transmittals messages containing no substantive information that are sent only to provide attachments. Because the legal authenticity of an e-mail requires retention of its metadata (the transmission of data), transmittals may supply a key part of the record d. Grant proposals, approvals, reports e. Policy, program, and Policy directives

Category 2 Documents with considerable value	5-10 years unless required longer for legal or regulatory purposes	a. Budget records b. Financial records c. Supply orders and receipts d. Legal Records e. Finance and Accounts f. Project Documents – Client-related g. Project Documents – Internal h. Employee Records i. Financial Records j. Marketing Consents k. Client Contact Information l. Customer Communication Records
Category 3 Documentation with limited value	3- 5 years unless required longer for legal or regulatory purposes	a. Day-to-day administration b. Office services and equipment requests and receipts c. Travel itineraries d. Workload reports e. Client / Platform Service Data
Category 4 Documentation with a deflating value	1-3 years unless required longer for legal or regulatory purposes	a. Visitor's entry register b. Utilities records c. Housekeeping/pest control records d. Security Council Meeting Minutes e. Corrective Action Record f. User Registration & Deregistration Record g. Incident Log h. Asset Record i. Risk Assessment Record j. List of Applicable Legislations k. Server Logs l. Nonconformity Reports m. Change Request Record n. Change Request Impact Analysis Record Software License Usage Monitoring o. Report p. Bandwidth Monitoring Report q. H/W and S/W Verification Records r. Antivirus record of user machines s. Backup logs t. Backup restoration logs u. Network Access Authorization Records v. Media Disposal Records w. Visitor Logbook x. Contract for Leased Line

		y. Contract for Antivirus Protection
Category 5 Documentation of little or no long-term value	0-90 days or until no longer needed for reference	a. Copies of publications or other published reference materials b. Drafts, except for mission-critical documents, program and policy changes ,or original creative,artistic, and scientific works c. Informational, e.g., holiday closings, notifications of meetings, retirement celebrations, etc. d. Junk and SPAM mail, whether received via e-mail, fax, or traditional mail e. Personal correspondence, e-mail, text messages, etc. f. Routine requests for information or publications and replies g. Scheduling of work assignments, work-related trips, and visits h. Video footage of the CCTV system

8.8 Data Disposal and General Guidelines

i. The proper destruction of records is essential to creating a credible records management program to ensure compliance with applicable legal and regulatory requirements and Reem Community Bank policies. Records containing personal and sensitive business information shall only be destroyed during business hours; records that are currently involved in, or have open investigations, audits, or litigation pending, should be tagged as 'IN USE' and should not be destroyed, discarded till the end of such investigation. Decision to dispose all such in use data must be approved by the owner.

ii. No primary records of any type belonging to Reem Community Bank may be destroyed until they have met retention requirements established by Reem Community Bank policies and regulatory guidelines.

iii. When retention requirements have been met, records must be either immediately destroyed or placed in secure locations for controlled destruction later.

iv. Data shall be disposed of using industry-accepted secure disposal guidelines (to ensure deleted data is unrecoverable) as soon as the specified retention period is complete, and all disposal activities must be logged, approved, and subject to internal/external audit review.

v. Personal data and sensitive business information shall be disposed of upon the request of the Data Subject or by the direction of regulatory authorities. The Data Subject/ Regulatory Authority shall be informed of the deletion of the requested personal data, along with supporting evidence. Any personal data related to third parties must be redacted or removed before disclosure.

8.9 Data Disposal by Destruction

When a record is no longer required to be retained, it should be properly destroyed and the destruction documented. Deleting data and emptying the "Recycle" folder or "Trash" bin from electronic storage media such as CDs, hard drives, and tapes does not permanently destroy the information. Printers and photocopiers with document memory capability may also require data cleaning before sale or disposal. Overwriting must meet NIST SP 800-88 or equivalent secure sanitization standards. Hard drives, USB or flash drives, and other plug-in type devices.

Storage media shall be sanitized by running special software programs or following the manufacturer's instructions for full chip erasure. If the drive is no longer operational, cables should be cut, and the drive disassembled. Its platters should be damaged by drilling holes, hammering, or cutting them with metal snips.

Damaged devices containing personal and sensitive business information shall not be sent out to vendors for repair. All personal data on the asset shall be destroyed by means of low-level formatting/degaussing before any other standard data deletion method.

8.10 Removable Media

Documents, drives, and other materials containing personal and sensitive business information must be shredded by their owners using a crosscut shredder. These shredders shall be located in a secure area, with containers kept under lock and key.

Special shredders capable of shredding optical media (e.g., CDs, DVDs) may also be utilized. Diskettes or other types of media that are unsuitable for shredding should be disassembled, and the media should be destroyed by puncturing, cutting, or sanding.

8.11 Medium-wise Destruction Process

Upon the expiry of the retention period, the following methods shall be used to destroy information securely.

Asset/Medium	Process	Performed By
Digital documents (e.g., MS Word, Excel/PPT)	Deleted upon the information owner's approval	Respective IT administrator
IT Configuration	Deleted upon information IT Head / ISMS Manager's approval	Respective IT administrator
Printed Paper	Shredded	HODs
Paper Files	Shredded	HODs
Tapes/media	Degaussing/physical destruction (Subject to environment	Respective IT administrator

MAK MR MZ VM SF SA

	controls)/kept in store (records maintained)	
Email	Deleted upon HoD's approval	Email owner
All other categories	Deleted upon HoD's approval	Respective information Owner
Media (Flash drive/hard drives/CD/DVD)	Upon approval by the ITD/HOIS: Option 1 – securely stored. Option 2 - formatted. Option 3 – secure wipe - using a third-party tool	Respective IT administrator

9. Data Retention and Deletion RACI Matrix

Role / Activity	Data Owner	HOD	ITD Helpdesk	ITD Manager	DPO	HOIS
Retention & Deletion of Business Data	R	R, A	C, I	C, I	A	C
Retention & Deletion of PII Data	R	R, A	C, I	C, I	A	C
Retention and Deletion of Client Data	R	R, A	C, I	C, I	C	C
Retention and Deletion of Platform Data	R	R, A	C, I	C, I	C	C

10. Policy Compliance

i. All End Users must comply with the applicable information security policies, standards, procedures, and guidelines. Reem Community Bank HoDs must ensure continuous compliance monitoring within their units.

ii. Any employee found to have violated this policy and other applicable UAE laws & regulations may be subject to disciplinary and corrective action, up to and including termination of employment. Penalties or disciplinary action will be consistent with the severity of the incident, as determined by an investigation, and may include, but not be limited to:
   a. Loss of access privileges to information assets
   b. Other actions as deemed appropriate by management, Human Resources, and the Legal Department.

iii. All exceptions must be communicated through the Policy Waiver Request Form, as defined in the waiver criteria.

11. Waiver Criteria

i. Requests for waivers from this framework shall be formally submitted to the ISMC, including justification and attributed benefits, and must receive ISMC approval. These

waivers are intended solely for exceptional situations involving non-compliance with the policy for a specified period, which may not exceed one year.

ii. The waiver shall be monitored to ensure its concurrence within the specified period of time and exceptions. After the completion of waiver time period, the need for the waiver should be reassessed and re-approved, if necessary.

12. References

The following are directly relevant to this policy:

i. Annexure A: Controls Description
ii. Annexure B: Glossary
iii. CBUAE Consumer Protection Standards
iv. UAE Data Protection Law

Annexure A: Controls Description

Control Reference (ISO 27001:2022)	**Control Description**
A.8.13 Information backup	Backup copies of information, software and systems shall be maintained and regularly tested in accordance with the agreed topic-specific policy on backup
A.8.10 Information deletion	Information stored in information systems, devices or in any other storage media shall be deleted when no longer required.
A.5.34 Privacy and protection of personal identifiable information (PII)	The organization shall identify and meet the requirements regarding the preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements.
UAE IA Regulations	**Control Description**
M5.2	Compliance with information security legal requirements
T3.5	Backup
T4.4	Information sharing protection
M2.3	Information security risk treatment
M2.4	Ongoing information security Data Protection

Annexure B: Glossary

i. **Information Security:** Preservation of confidentiality, integrity and availability of information.
i. **Confidentiality:** Ensuring that information is accessible only to those authorized to have access.
ii. **Integrity:** Safeguarding the accuracy and completeness of information and processing methods.
iii. **Availability:** Ensuring that authorized users have access to information and associated assets when required.
iv. **Data:** Includes all stored information which may be in electronic or paper-based forms and is processed by the business activities.
v. **Application Systems:** Include all manual and programmed procedures which process the data.
vi. **Technology:** Covers hardware, operating systems, databases, networks etc.
vii. **Facilities:** All the resources including building and utility resources used to house and support the information systems.
viii. **People:** include the staff and human resources and skill sets which are at the core of the business organization of Reem Community Bank.
ix. **Information Assets:** All the Information, Communication, Technology and Computing assets of Reem Community Bank whether hosted in-house or outsourced to a third party or on a cloud.
x. **End Users:** All employees (permanent, consultants) and non-employees (contractors, suppliers, vendors, etc.) of Reem Community Bank who have access to and use Reem Community Bank' s information systems to perform their daily job-related responsibilities or to meet their contractual obligations.
xi. **Asset:** The object/ service/ person, which has been of value to the organization by virtue of its/their utility. It may directly or indirectly affect the work / process flow thus affecting Information Security.
xii. **ISO Control:** Selected from ISO/IEC 27001:2022 Standard, these controls seek to reduce the risk by reducing the threat, vulnerability, or frequency, thereby enhancing the information security of the Asset by improving the Confidentiality, Integrity or Availability. A control is only suggestive of an idea and can be applied in many ways to achieve the desired level of security.
xiii. **Privacy**: Information provided by employees, customers and others is protected such that it is used solely for the stated purposes of the enterprise's customer privacy policies, the provider has authorized such use, and its use is in compliance with all local government privacy regulations.
xiv. **Personal Information**: Information classification that relates to their "privacy" type. This could be either customer related information or private information related to staff (like medical records).

xv. **Business Sensitive Data**: Information requiring some protection, not generally available internally. Security requirements include single-factor authentication (logon ID and password), authorization required on an "as needed" basis, and a mandated 128-bit encrypted work session using Secure Sockets Layer (SSL) and a minimum web browser version requirement or equivalent.

xvi. **Authentication**: The identification requirements associated with an individual using a computer system. Identification information must be securely maintained by the computer system and can be associated with an individual's authorization and system activities.

Three types of factors are used to provide authentication: a) Something you know (i.e., a password) b) Something you have (i.e., a certificate or smart card) c) Something you are (i.e., a fingerprint or retinal pattern).