May 2025
Version: 3.0

Customer Data Privacy and Protection Policy

EL-NILEIN BANK (ENB)
ABU DHABI

VERSION: 3.0
ISSUE DATE: MAY 2025

Version Control:

Prepared By	Date	Version	Comments
Consultant	July 2020	1.0	This is the 1st version, and the review shall be in March 2022
Consultant	April 2022	2.0	Updated as per CB observations and Revised to include the Consumer Protection Regulation as per instructions from the Central Bank of UAE
Consultant	May 2025	3.0	This is the 3rd version, and the review shall be in May 2027 or if the CBUAE changes the requirements

Reviewed by:

Name	Date	Version	Version Control
Information Security Mr Hani Salah	May 2025	3.0	This is the 3rd version, and the review shall be in May 2027 or if the CBUAE changes the requirements
Consumer Protection Ms. Malaz Nazim	May 2025	3.0	This is the 3rd version, and the review shall be in May 2027 or if the CBUAE changes the requirements

Approval:

Approved by	Date	Version	Signature
General Manager Ms. Nazik Muhagir	May 2025	3.0	
Deputy General Manager Dr. Issamelden Gaffar	May 2025	3.0	
Head of Compliance Mr. Mohamed El Gaily	May 2025	3.0	
Head of Risk Management Mr. Osama Ahmed	May 2025	3.0	
Head of Information Technology Mr Abuzar Elsadig	May 2025	3.0	
Information Security Mr Hani Salah	May 2025	3.0	

Contents

1. Introduction

Article 120 of UAE Decretal Federal Law No. (14) of 2018 Regarding the Central Bank & Organization of Financial Institutions and Activities provides that:

1) All data and information relating to customers' accounts, deposits, safe deposit boxes and trusts with Licensed Financial Institutions and related transactions shall be considered confidential in nature, and may not be perused, or directly or indirectly disclosed to any third party without the written permission of owner of the account or deposit, his legal attorney or authorized agent, and in legally authorized cases.
2) Such prohibition shall remain valid, even until end of the business relationship between the customer and the Licensed Financial Institution for any reason.
3) Chairmen and members of boards of directors, managers and employees of Licensed Financial Institutions, and experts, consultants and technicians assigned to perform functions therein, are prohibited from disclosing any information or data on their customers; their accounts or deposits or transactions relating thereto, or enable third parties to peruse them, except in legally authorized cases.
4) Such prohibition shall apply to all agencies and Persons, and whoever, by virtue of his profession, position or nature of work, is able to, directly or indirectly, peruse such information and data.
5) The Central Bank shall establish rules and conditions organizing exchange of banking and credit information, in its capacity as the competent Regulatory Authority in the State in this regard.
6) The provisions of item nos. (1) and (2) of this article shall be without prejudice to the following:
    a. The powers legally vested on security and judicial authorities, the Central Bank and its employees.
    b. The duties assigned to auditors of accounts of the concerned institutions.
    c. The obligation of the concerned institutions to issue, upon request of the beneficiary, a certificate of the reasons for declining to cash a check.
    d. The obligation of the concerned institutions to issue a certificate of partial payment of value of a check, where the consideration for payment is less than the value of the check, pursuant to the provisions of the referenced Commercial Transactions Law.
    e. The right of the concerned institutions to disclose whole or part of the data relating to the customer's transactions, in order to establish its right in a legal dispute in respect of such transactions, with its customer.
    f. Provisions of established laws and international agreements in the State, in addition to anti-money laundering, terrorist financing and illegal organizations provisions.

El Nilein Bank, Abu Dhabi ("ENB" or the "Bank") is committed to respect the confidentiality and security of the customer's personal data and customer's assets, and to treat them in accordance with the laws of the United Arab Emirates and regulations, standards and guidelines issued by the Central Bank of UAE. The Bank uses, processes, discloses and shares customer's personal data with third parties only for specified purposes and in accordance with the general terms and conditions of the banking relationship agreement with the customer or specific terms and conditions of the Bank's products and services availed by the customer.

2. Ownership of the document

The Bank's **Information Technology Department (ITD) and Consumer Protection Unit (CPU)** are the primary stakeholders and owners of this document and any changes suggested by any other stakeholder require the approval from the **Head of ITD and Head of CPU** or the designated officer prior to proceeding with amending the document.

This Policy will be reviewed annually or more frequently (Change in regulations & laws), to ensure it is kept up to date. All amendments, additions or deletions to the Policy will be properly documented and authorized/approved prior to implementation.

This document will also be amended or its contents improved in the event that the bank amends or improves its operational functionalities or where regulatory changes are implemented through UAE Central Bank.

This Policy will be posted on the Bank's internal Share-Folder. Access to it will be restricted to Bank's staff only on need-to-know bases with approval of the Document owner.

This Policy document must not be copied or revealed to third parties without the written permission of the document owners. Unauthorized sharing of this document (both hard copies and electronic copies) with individuals and entities outside the Bank is strictly prohibited.

A Version Register will be maintained by the Owners that shows the Policy version information relating to the version number, version date, section (s) amended.

3. Collection of Personal Data

The Bank collects personal and non-personal information through the customer's interaction with the bank when they open accounts, obtain financial services, make transactions and through the use of the Bank's web/mobile search applications.

Personal information that the customer may voluntarily provide through such interactions includes (but not limited to):

(a) Customer name
(b) Contact information e.g., address, telephone and email
(c) Date of birth.
(d) Gender
(e) Place of birth
(f) Identification card details / travel document (passport) details; e.g., Issued date, expiry date, place of issue, document number
(g) Occupation details including designation and period of occupation.
(h) Employment details e.g., address, telephone and email
(i) Home country details e.g., address, telephone and any person to contact in home country.
(j) Other account and/or card numbers held with the bank
(k) Data provided in executing funds transfers and payments;

In addition, the bank may automatically collect personal information including:

(a) Information the customer provides the bank through feedback and online chats.
(b) Mobile device identification data; and/or
(c) Dates and times when the relevant mobile application accesses the banks servers;
(d) Non-personal information about banking and non-banking transactions;

(e) Version of the relevant mobile application the customer is using;

(f) Type of operating system the customer is using;

(g) Device model and manufacturer;

(h) Internet service provider or mobile service provider; and/or

The bank may also collect customers' personal information directly in a number of other ways, including:

(a) When the customer applies for any product on the bank's website.

(b) When the customer provides it on-line or by any other method of communication, for example, on "contact us" forms, or when providing it through the course of the banker customer relationship

(c) technical information, including the Internet Protocol (IP) address used to connect to the internet, may be collected from the customer when they visit the banks website.

The bank may obtain personal information indirectly from third parties in the following ways:

(a) following an introduction to the bank by another third party, such as an accountancy firm, law firm or management consultancy;

(b) if another person provides the customers information to the bank when they apply to obtain a product:

i. on the customers' behalf; or

ii. that is to be held jointly with the customer; or

iii. on behalf of a business, charity, trust or other organisation of which the customer is a director, shareholder, owner, trustee or beneficiary (as applicable); or

iv. they have nominated the customer as a guarantor under the bank's agreement with them, or to provide any other security, or informed the bank that the customer is a donor or lender of any deposit monies or occupier of any security property;

(c) when the bank carries out searches for the purposes of processing the banks application and/or during the course of the customers relationship with the bank; or

(d) in response to the bank marketing activities, the customer requests information about the bank's products via a third party (e.g., websites and social media platforms).

4. How customer Data is used

The Bank will only use the customer personal data when the law permits it. Most commonly, the bank will use the customer's personal data under the following circumstances:

(a) Where it is necessary for the bank's legitimate interests (or those of a third party) and the customer's interests and fundamental rights do not override those interests.

(b) Create, manage and maintain the customers experience on the bank's channels (web sites).

(c) Operate, evaluate and improve the banks business and the products and services offered.

(d) Analyse and enhance the banks marketing communications and strategies (including by identifying when emails sent to customers have been received and read).

(e) Analyse trends and statistics regarding visitors' use of the bank's web sites, mobile applications (if any) and social media assets.

(f) Protect against and prevent fraud, unauthorized transactions, claims and other liabilities, and manage risk exposure, including by identifying potential hackers and other unauthorized users.

(g) Notify the customer from time to time about relevant products and services operated and offered by ENB.

(h) Comply with a legal or regulatory obligation.

(i) Perform the contract that the bank is about to enter into, or have entered into, with the customer.

(j) Where it is necessary for the purposes of legal proceedings.

5. Data Security and Access to customers Personal Data

The Bank has put in place appropriate security measures to prevent the customer's personal data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, the bank has limited the access to customer's personal data to those employees, agents, contractors and other third parties who have a business need to know. They will only process the customer personal data on the banks instructions and are subject to a duty of confidentiality.

The Bank has established procedures to deal with any suspected personal data breach and will notify the customer and any applicable regulator of a breach where the bank is legally required to do so.

The following will be observed in relation to customer data:

(a) Information in the system shall always be accessed by the staff engaged in processing the customer transaction or request. The customer's account shall not be accessed as an isolated instance where their details are enquired for reasons other than that requested by the customer.

(b) All dormant accounts will be restricted to normal staff. Only managerial staff or those authorized will have access to data of dormant account customers.

(c) Access to the banks system server environment will be granted to authorize personnel of the bank. In case a maintenance is performed on the customer database, the system to reflect an audit trail of all the changes implemented and the log reviewed by independent authorized personnel of the Bank.

(d) Server access room holding customer data information will be monitored by CCTV coverage and controlled by dual key / magnetic card door accessing device, where the access would have to be given by the IT Manager.

(e) All customer scanned files archived in the servers within the bank or are externally with third party service providers will follow proper data privacy protocols during its establishment.

(f) The customer physical files will always be stored in locations that are accessed under dual control. Such files will be kept in an environment which is safe from fire, termites, flood and any other natural calamities. Removal of physical file from such storages will be managed through a formal request by authorized staff and the movement of files noted in the registers of the storage location and mentioned as an incoming item in the departments requesting them.

(g) Staff should refrain from taking copies from physical files unless it is mandated by a requirement concerning the banks interest.

(h) Staff should never take screen shots of the customer details by their phones. This will reflect on all of the bank's information and any violation of taking photographs of sensitive information will be severely dealt with.

Firewalls have been placed in the web servers to protect from unwarranted intruders. The banks systems are scanned and monitored regularly to prevent any unauthorized and fraudulent access and against potential vulnerabilities.

As the security of ordinary email cannot be guaranteed, the customer should only send email to the Bank using the secure email facility on the bank's website on the option "contact us" or from an email address previously registered with the bank at the time of account opening or subsequently thereafter. The Bank will always respond only after verifying the records held of the email address details.

6. Administration and Management of Personal Data

The Bank will make reasonable efforts to ensure that the customer's personal data is accurate and complete, if the customers personal data is likely to be used by the Bank to make a decision that affects the customer, or disclosed to another organisation. However, this would mean that the customer must also update the bank of any changes in their personal data from time to time. The Bank will not be responsible for relying on inaccurate or incomplete personal data arising from the customer not updating the bank of any changes in their personal data from time to time in a timely manner.

The Bank will also put in place reasonable security arrangements to ensure that the customer personal data is adequately protected and secured. Appropriate security arrangements will be taken to prevent any unauthorised access, collection, use, disclosure, copying, modification, leakage, loss, damage and/or alteration of customer's personal data. However, the Bank cannot assume responsibility for any unauthorised use of personal data by third parties which are wholly attributable to factors beyond its control.

The Bank will also put in place measures such that personal data in its possession or under its control is destroyed and/or anonymised as soon as it is reasonable to assume that;

(a) the purpose for which that personal data was collected is no longer being served by the retention of such personal data;

(b) retention is no longer necessary for any other legal or business purposes.

(c) record retention period, as required under the Laws and regulation or as per Bank's Record Retention Policy, has expired.

7. Marketing Communications sent to customers

The Bank will use the customer information (data) and send marketing communications in instances were:

(a) if the customer has requested information from the Bank or used the banks services

(b) if the customer has provided the Bank with their details such as a business card.

(c) The customer has not opted out of receiving marketing messages.

As per the UAE law, the customer can ask the Bank to stop sending marketing messages at any time by following the "opt-out" links/option on any marketing message sent to the customer or by contacting the Customer Service Team of ENB at any time. Where the customer opt-out of receiving these marketing messages, this will not apply to personal data provided to the bank for other purposes.

8. Disclosure of customer data with third parties

8.1 The bank will respect the confidentiality of the personal data the customer provides. In that regard, the Bank will not disclose the customer's personal data to third parties without first obtaining the customers consent permitting the Bank to do so. However, please note that the Bank may disclose the customer's personal data to third parties without first obtaining their

consent in certain situations, including, without limitation, the following where the instances listed are not intended to be exhaustive.

(a) cases in which the disclosure is required or authorised based on the applicable laws and/or regulations;

(b) cases in which the purpose of such disclosure is clearly in the customer's interests, and if consent cannot be obtained in a timely manner;

(c) cases in which the disclosure is necessary to respond to an emergency that threatens the life, health or safety of the customer or another individual;

(d) cases in which the disclosure is necessary for any investigation or proceedings;

(e) cases in which the personal data is disclosed to any officer of a prescribed law enforcement agency, upon production of written authorisation signed by the head or director of that law enforcement agency or a person of a similar rank, certifying that the personal data is necessary for the purposes of the functions or duties of the officer;

(f) cases in which the disclosure is to a public agency and such disclosure is necessary in the public interest; and/or

(g) where such disclosure without the customers consent is permitted by the law of the United Arab Emirate.

8.2 The Bank may have to share the customer's personal data with the parties mentioned below.

(a) Internal Third Parties.

The Bank may share the customer's personal information with other affiliated companies within the Bank's group so that they can provide the customer with relevant products and services. This type of processing is necessary to enable the Bank to take steps at the customers' request prior to the customer entering into a contract with a company within the Bank's group.

(b) External Third Parties.

(i) Anyone acting on the customer's behalf with authority to do so, such as a power of attorney or the customer's professional advisors.

(ii) Legal and regulatory bodies such as the United Arab Emirates Central Bank, the Securities and Commodities Authority (SCA), fraud prevention agencies, the Bank's professional advisors and/or the courts when it is necessary for the Bank's legitimate interests (e.g., to obtain legal advice or for fraud prevention purposes) and/or when the Bank have a legal obligation to do so.

(iii) Organisations that provide the Bank with business support services. This processing is undertaken as it is necessary for the performance of the Banks agreement with the customer and is necessary for the bank's legitimate interests for its commercial operations.

(iv) Third parties who have introduced the customer to the Bank (such as an intermediary or broker) in order for them to manage their records about the customer, to ensure that the type of business that they refer to the Bank is appropriate and to help the Bank resolve any complaint made by the customer and/or any dispute between the Bank and the customer.

(v) Market research organisations which the bank engage to assist in developing and improving its products and services. This type of processing is necessary for the Bank's legitimate interests for its commercial operations.

(vi) Any person or entity that is to provide, or has provided, any security of guarantee (and their professional advisors) in respect of the customer's agreement with the Bank and

their professional advisors. This type of processing is necessary for the fulfilment of the Banks contract with the customer in terms of enabling the Bank to recover any finance amounts advanced under the Bank's agreement with the customer.

(vii) Any entity (and their professional advisors) that provides funding to the Bank, any entity that provides the Bank with debt or equity finance and any potential purchasers of any part of its business. This type of processing is necessary for the Bank's legitimate interests to enable for the funding of its business.

8.3 The Bank may choose to sell, transfer, or merge parts of its business or its assets or may seek to acquire other businesses or merge with any other entities. If a change happens to the banks business, then the new owners may use the customer's personal data in the same way as set out in this Privacy Policy.

8.4 ENB requires all third parties to respect the security of the customer's personal data and to treat it in accordance with the laws of the United Arab Emirates. The bank does not permit third-party service providers to use the customer's personal data for their own purposes and only permit them to process such personal data for specified purposes and in accordance with the bank's instructions and as per any non-disclosure agreement signed.

9. Updating the Banks Data Protection Policy

As part of the banks efforts to ensure that it properly manages, protect and process the customer's personal data, the bank will be reviewing its policies, procedures and processes from time to time.

ENB reserves the right to amend the terms of this policy at its absolute discretion. Any amended policy will be posted on the banks website or in an applicable channel. The customer will need to be encouraged to visit the Bank's website (or an applicable channel) from time to time to ensure that they are well informed of the Bank's latest policies in relation to personal data protection and their privacy.

10. Customers Rights on their Data

The Customer will have the right to:

(a) Request access to their personal data. This enables the customer to receive a copy of the personal data the bank holds about the customer and to check that bank is lawfully processing it.

(b) Request correction of their personal data that the Bank holds about the customer. This enables the customer to have any incomplete or inaccurate data the bank may hold about them corrected, though the bank would need to verify the accuracy of the new data provided. This would be applicable to deletion of data which are obsolete. All such amendments will have a system audit trail which can be accessed through the banking system that reflects the amendment done, the date and time and the staff details performing the amendment as well as the staff authorizing the changes in the system

(c) Object to processing of customer's personal data where the Bank is relying on a legitimate interest (or those of a third party) and there is something about the customer's particular situation which makes the customer want to object to processing on this ground as they feel it impacts on their fundamental rights and freedoms. The customer also has the right to object where the bank would process their personal data for direct marketing purposes. In some cases, the Bank may demonstrate that is has compelling legitimate grounds to process the customer information which override their rights and freedoms.

(d) Request restriction of processing of the customer's personal data. This enables the customer to request the bank to suspend the processing of their personal data in the following scenarios:

(i) if the customer wants the Bank to establish the data's accuracy;

(ii) where the customer needs the Bank to hold the data even if it no longer requires it as the customer may need it to establish, exercise or defend legal claims; or

(iii) the customer objects to the Bank's use of their data but is needed by the bank to verify whether it has overriding legitimate grounds to use it.

(e) Request by the customer for the transfer of their personal data to a third party. The Banks provide to a third party the customer has have chosen, their personal data in a structured, commonly used, machine-readable format. Note that this right only applies to automated information which the customer initially provided consent for the Bank to use or where the Bank used the information to perform a contract with the customer.

(f) Withdraw consent at any time where the Bank is relying on consent to process the customer's personal data. However, this will not affect the lawfulness of any processing carried out before the customer withdraw their consent. If the customer withdraws their consent, the Bank may not be able to provide certain products or services to the customer. The customer will also, under certain circumstances, have the right to data portability, meaning that the customer has the right to receive their personal data in a structured, commonly used and machine-readable format to transmit those data to another authority

(g) The customer will be able to exercise any of their rights set out above by contacting the customer service staff.

11. Retention of Customer Data

All practical steps will be taken to ensure that personal information will not be kept longer than necessary and that ENB will comply with all legal, statutory and regulatory requirements concerning the retention of personally identifiable information

ENB will only retain the customer's personal data for as long as necessary to fulfil the purposes it was collected for, including for the purposes of satisfying any legal, accounting, or reporting requirements.

To determine the appropriate retention period for personal data, the Bank considers the laws and regulations of UAE, the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of the customers' personal data, and the purposes for which the Bank would process the personal data.

12. Complaint Process

If the customer has any complaint or grievance regarding how the bank is handling the customers personal data, the customer is required to contact the Bank with their complaint or grievance via email to the Consumer Protection Unit at Bank's Website, or drop it in the box provided in the customer service area of the Bank's branch, or meet a customer service representative and lodge the case.

The Bank will always strive to deal with any complaint or grievance that the customer may have promptlyand fairly.

The Bank will try to respond to all complaints in accordance with Complaint Handling Policy of the Bank.

13. Policy Guidelines on Consumer Data Protection

13.1 Consumer Data Protection

ENB will ensure that the following Policy guidelines on **Consumer Data Protection, as per Consumer Protection Regulation** issued by the Central Bank of UAE vide circular number 444/2021, are followed by all of its staff meticulously and that there will not be any breach of any sort when discharging their duties towards the Bank's customers.

1) ENB will establish a function in their organization that is responsible for Data Management and Protection including responsibility for maintaining policies, procedures, systems and controls to protect Consumers' Personal Data and information against misuse, unauthorized access and undue processing and analysis. ***(Article 6.1.2.1)***
2) The Bank will have policies that specify duration of record keeping and Data retention in accordance with the applicable laws, regulations and business. ***(Article 6.1.2.2)***
3) The Bank will have appropriate security and monitoring measures in place to detect and track unauthorized internal access or use of Consumer information. Any breach of access, misuse or unauthorized release must be recorded including any harm done by such breach for future reporting to and review by the Central Bank. ***(Article 6.1.2.3)***
4) ENB will notify the Central Bank of all significant breaches of Consumer Data and information and notify any Personal Data breach to Consumers where a breach may pose a risk to the financial and personal security of the Consumer without undue delay. The Bank is liable for reimbursing any direct costs incurred by the consumer for actual harm done as a result of the breach. ***(Article 6.1.2.4)***
5) ENB will ensure that Consumers are able to make informed choices with respect to providing expressed consent as to their Data being collected, used and shared with third parties and within the Bank. ***(Article 6.1.2.5)***
6) The Bank prevent the misuse of Consumer information and Data. ***(Article 6.1.2.6)***

13.2 Protection of Consumer Assets, Information and Data against Fraud, Misappropriation and Misuse

ENB will ensure that the following Policy guidelines on **Protection of Consumer Assets, Information and Data against Fraud, Misappropriation and, as per Consumer Protection Regulation** issued by the Central Bank of UAE vide circular number 444/2021, are followed by all of its staff meticulously and that there will not be any breach of any sort when discharging their duties towards the banks customer/s.

1) Without prejudice to other laws and regulations, ENB will treat Consumers' information relationships and business affairs as private and confidential. ***(Article 6.2.2.1)***
2) The Bank will put in place strict internal controls to effectively protect Consumers' deposits, savings, funds held by stored value facilities and other assets as well as Consumer information and Data, against internal frauds. ***(Article 6.2.2.2)***
3) The Bank will apply sufficient resources to be able to detect both external and internal frauds quickly and ensure they are fully addressed with future prevention measures. ***(Article 6.2.2.3)***
4) ENB will compensate Consumers in a timely manner for financial losses and expenses resulting from Financial Crimes, misappropriation, cyber-attacks and misuse of assets and information unless it can be proven that the loss was due to the gross negligence or fraudulent behaviour of the Consumers. ***(Article 6.2.2.4)***

5) ENB will ensure their security and protection systems are updated and have the capacity to develop and adopt new approaches to cyber security as required. ***(Article 6.2.2.5)***

6) The Bank will demonstrate they have carried out sufficient Consumer awareness activities related to educating Consumers of the need to protect themselves from Financial Crime. ***(Article 6.2.2.6)***

14. Procedures to safeguard Consumer Data and Assets

Officer In Charge of Consumer Protection Unit (OIC of CPU), in coordination with relevant stakeholders, will ensure adherence of the following activities to comply with requirements of the Consumer Protection Regulation and accompanying Standards relating to **Consumer Data Protection** and **Protection of Consumer Assets, Information and Data against Fraud, Misappropriation and Misuse**:

14.1 Policies, Procedures and Systems

14.1.1 The business units' staff (Retail and Corporate) together with and marketing staff will inform consumers in Writing with respect to how their personal information will be processed. e.g., collected, used, disclosed, Data mined and profiled.

14.1.2 The Banks Information Technology function will take measures to;

(a) protect Consumer Data and maintains the confidentiality of the Data, including when it is held, accessed or used by Authorized Agents.

(b) Be responsible for ensuring Data protection and individual Consumer confidentiality with respect to any profiling, Data mining, marketing and sale of financial services through use of new technologies and social media.

(c) Provide a safe, secure and confidential environment in all of its delivery channels to ensure a high level of confidentiality and privacy of Personal Data.

(d) Have a proper Data Management Control Framework with policies, procedures, system controls, and checks and balances to protect Consumer Data and to identify and resolve any incidents of information security breaches, when they may occur.

(e) Apply more than one evidence of identity verification for electronic services where the consumer's identity verification is conducted online.

(f) Advise consumers through digital channels regarding any directed and repeated attempts of online fraud on their accounts for the consumers to take additional precautions.

(g) Secure digital transaction processing and controls, implement detailed activity monitoring and enhance consumer identification methods in accordance with the Central Bank's requirements for strengthening Digital Channels.

(h) Access to personal information and Personal Data of Consumers is limited to authorized business lines and their Staff only.

(i) Logs are maintained for audit and supervisory purposes, recording the names of Staff who have accessed Consumer databases and the timing. Such records must be provided to the Central Bank as and when requested.

14.1.3 The Senior Management of the Bank will have a legal obligation of confidentiality towards a consumer except:

(a) When disclosure of Consumer Data is properly imposed by a legal authority; or

(b) When disclosure is made with the expressed consent of the Consumer, or through a representative nominated by the consumer.

14.1.4 The Banks Human Resource function will ensure that;

(a) Employees are provided training and awareness programs on their Data control framework for accessing and handling consumer Data and reporting security and policy breaches.

(b) The importance of protecting Consumer's Data is promoted as an ongoing responsibility of Staff with reminders sent on an annual basis.

14.2 Data Management of Data Protection

14.2.1 The Banks Board has designated responsibility and accountability for the Data Management and Protection function to a senior position in management who reports directly to Senior Management. The function will be responsible for ensuring oversight of and compliance with the Data Management Control Framework and any related requirements for Data protection and privacy laws of the UAE and the Central Bank.

14.2.2 The Data Management and Protection function ensures that:

(a) Adequate monitoring and preventive controls are in place to detect any unauthorized or accidental loss, misuse, modification, access, disclosure or destruction of Personal Data;

(b) Verifications are regularly carried out on the legitimacy of Data collection, access to Data, Data integrity and the electronic procedures and address any issues identified;

(c) Controls are commensurate with the criticality and sensitivity of the relevant systems and Data handled;

(d) Detailed monitoring of records and the actions taken are maintained for 5 years.

14.2.3 The Banks Data Management and Protection Function will:

(a) Annually reviews and improves the adequacy of the Data Management Control Framework for the collection, classification, storage, usage, transfer, protection, correction and destruction of Personal Data;

(b) Monitors, investigates and reports to Senior Management any material incidents of accidental or unauthorized access, loss, alteration, transfer, destruction, use, modification or disclosure of Data;

(c) Participates in the handling and investigation of privacy related Consumer Complaints and reports the conclusion of the investigation to the head of the Complaint Management function, who then corresponds with the Consumer and provide the Institution's findings in Writing.

14.2.4 The Data Management and Protection function will issue reports to the Senior Management and the Board on significant Data management violations and breaches immediately.

14.2.5 Senior Management will ensure proactive measures are taken to address the violation / breach and to improve Data management systems and safeguards the confidentiality and privacy of Consumers' Personal Data.

14.2.6 The Bank will without delay, inform Consumers of unauthorized access to, and/or loss, destruction or alteration of Consumers' Personal Data where it may reasonably pose a risk to the Consumer's financial and personal security and/or where it may pose reputational harm to a Consumer.

14.2.7 The Bank will notify the Central Bank immediately of all significant breaches of Personal Data.

14.3 Expressed Consent by Consumers

14.3.1 The Banks Business units and all of its senior management will ensure that Personal Data will be:

(a) Collected for a lawful purpose directly related to the Financial Activities of the Bank;

(b) Adequate and not excessive in relation to the stated purpose;

(c) Collected with appropriate security and protection measures against unauthorized or unlawful processing and accidental loss, destruction, or damage.

14.3.2 The Banks Business units will ensure that;

(a) Before requesting the consent of a Consumer to share Personal Data, they have proactively disclosed in Writing to a Consumer its intent to use and/or share Personal Data and with whom the Consumer's Personal Data will be shared.

(b) The Consumer gives his/her expressed consent freely and explicitly to a request for the use and/or sharing of Personal Data by The Bank.

(c) The request for consent is expressed in clear and plain language and informs the Consumer of his/ her right to refuse to provide expressed consent.

(d) It obtains informed and expressed consent before using and sharing a Consumer's Personal Data for direct marketing or transferring the Personal Data to Authorized Agents for direct marketing.

(e) A copy of the expressed consent is retained for 5 years after the relationship with the Consumer has terminated.

(f) The Consumer has the right to withdraw expressed consent for the following at any time:

(i) The processing of Personal Data by The Bank except where Persona Data is required for business operations related to the Consumer's Products and Services; and

(ii) Personal Data sharing with Authorized Agents and other third parties for purposes such as but not limited to sales and marketing.

(g) Provides the following disclosures to the Consumer prior to a Consumer entering any contract,

(i) That The Bank only collects Data / Personal Data for a lawful purpose directly related to a function or activity of the Consumer.

(ii) Whether the collection is obligatory or voluntary for the Consumer to provide the Data / Personal Data;

(iii) Where it is obligatory for the Consumer to provide the Data / Personal Data, the consequences for failing to provide the Data / Personal Data as required;

(iv) A future withdrawal of expressed consent by a Consumer shall not affect the lawfulness of Data processing based on the prior expressed consent. Unless specified otherwise, the withdrawal takes effect within complete 30 calendar days of the Consumer requesting the withdrawal with The Bank;

(v) When Data / Personal Data of the Consumer is being processed by or on behalf of The Bank, provides a description of the Data / Personal Data being processed;

(vi) When other external information on the Consumer is collected by The Bank and the source of that Data / Personal Data;

(vii) The Consumer's right and means to request access to and to request correction of the Data / Personal Data and how to contact The Bank with any inquiries or Complaints in respect of the Data / Personal Data;

(viii) The choices and means The Bank offers the Consumer for limiting the processing of Data / Personal Data

14.4 Sharing with Authorized Agents

14.4.1 The Bank's Business Units and Administration functions that engages any Authorized Agent to whom some part or the entire delivery of the Financial Product and/or Service is outsourced,

will ensure that they comply with the banks policy regarding Data management and protection including secure handling procedures and applying proper controls when discharging their duties.

14.4.2 The Banks Information Technology function will ensure that;

(a) access to a Consumer's Personal Data by Authorized Agents is properly authorized in Writing by The Bank, regularly monitored, and appropriately restricted in line with the purpose of the access given.

(b) The Where Personal Data is shared and retained outside of The Bank's own network such as with Authorized Agents, The Bank and Authorized Agents use encryption techniques to suitably encrypt Consumer Data and take measures for the secure transfer of Data.

(c) The Bank is responsible for ensuring any outsourced technology that uses or retains Personal Data meets the highest standards of security, encryption and protection and are regularly audited and verified for vulnerabilities

14.4.3 The Banks Administration function along with the banks Legal counsel will ensure that;

(a) All legal contracts with Authorized Agents relating to the Outsourcing of functions and services includes appropriate provisions for safeguarding confidentiality of Personal Data and prohibits the unauthorized disclosure of confidential Personal Data by Authorized Agents.

(b) The Authorized Agents report to The Bank's Data Management and Protection function significant breaches of Personal Data.

(c) The Bank's obligation to protect all Consumer Data extends to the actions of all Authorized Agents.

14.4.4 The Banks Compliance function ensure that;

(a) In the event of a termination of an Outsourcing contract with a Third Party, The Bank ensures and is able to demonstrate that all Personal Data is either retrieved from the Third Party and/ or is destroyed.

(b) Where the Consumer provided expressed consent to The Bank for sharing Data to a Third Party, The Bank confirms in any contract with a Third Party that the Third Party has no further right to share the Data or use it for other unauthorized purposes unless required by the laws in UAE.

14.5 sharing with Authorized Credit Information Agencies

14.5.1 The Risk Management function will ensure that only the minimum information is permitted to be shared, when the Bank is required to provide Consumer Data to government-authorized Credit Information Agencies as may be prescribed.

14.5.2 Consumers are informed by the banks business unit functions of this requirement and are advised as to the possible limitations of accessing future Financial Products and/or Services based on the Consumer records provided to these agencies.

14.5.3 If an update or correction is required, the business unit function through a central reporting department of the bank reports the update or correction to the Credit Information Agencies within seven (7) complete business days of The Bank having been notified by the Consumer.

14.6 Standards for Retention of Consumer Records

14.6.1 The Banks Compliance department will ensure that;

(a) All Personal Data, documents, records and files are securely retained for a minimum of five (5) years. The retention period begins, depending on the circumstances, from the date of the most recent of any of the following events:

(i) Termination of the Business Relationship or the closing of a Consumer's account with The Bank;

(ii) Completion of a casual transaction (in respect of a Consumer with whom no Business Relationship is established).

(b) After the lapse of the mandatory retention period for retaining Consumer records, all reasonable steps are taken to ensure that all Data / Personal Data is destroyed or permanently deleted if it is no longer required for the purpose for which it was collected and processed or no longer required by law:

(c) All Consumer and transaction Data are held and stored within the UAE as prescribed by the Central Bank

(d) Procedures and methods for retention of Consumer Data are reviewed on an annual basis

14.6.2 The Banks Risk Management function will ensure that;

(a) All Standards related to confidentiality and security is maintained after the termination of the relationship until the Personal Data is destroyed.

(b) The Banks business units or any other function dealing with customers, do not process or use Personal Data for any period longer than is necessary for the fulfilment of the purpose for which that Personal Data is required.

14.6.3 The Banks data security function and risk management function ensure that;

(a) At a minimum, The Bank establishes a safe and secure backup of all the Consumer Data and transactions in a separate location for the required period of retention specified.

(b) The Bank ensures there is secure retention of Consumer Data that would prevent any unauthorized or accidental loss, misuse, modification, access, disclosure or destruction.

14.7 Notification to the Central Bank

14.7.1 Where breaches of the Data Management Control Framework occur regarding the unauthorized access or release of Consumer Personal Data, The Banks Human Resources records any disciplinary actions taken against any Staff, agents or contractors responsible for the breach.

14.7.2 The Banks Risk Management Function will maintain records of such events for five (5) years after the event being recorded.

14.7.3 The Banks Compliance Department or any other function that deals with UAE Central Bank will ensure that;

(a) Records are made available to Central Bank upon request.

(b) The Bank notifies the Central Bank of any material Data breaches, losses, destruction or alteration when they occur, in a manner, as may be prescribed by the Central Bank.

14.8 Protection of Assets

14.8.1 The Bank's Senior Management will be responsible and accountable for security of assets and will be require to ensure that stringent internal control structures are in place and monitored including:

(a) The proper segregation of duties, roles and responsibilities of management and Staff within The Bank;

(b) Operational risk mitigation;

(c) Application of logistical access security;

(d) Access rights and security on electronic Data and to assets;

(e) Physical security of the Consumer assets and records;

(f) Completeness of documentation relating to business processes, policies, controls, and technical requirements in accordance with UAE's anti-money laundering and terrorism financing guidelines.

14.8.2 The Banks Risk Management function will need to implement stringent safeguards and verifications in order to protect unclaimed assets including the assets in the form of Stored Value Facilities, digital money, and dormant accounts and to ensure effective monitoring and reporting of any attempts to access them.

14.8.3 The Banks Credit Administration function will ensure that, collateral provided by the Consumer / guarantor is properly secured and protected by The Bank.

14.8.4 The Bank business function (Retail and Corporate) will act honestly, fairly and professionally and takes into account the best interests of Consumer, while managing the collateralized assets.

14.8.5 The Banks compliance function will ensure that;

(a) A robust internal risk-based policy is in place to update Consumers' KYC documents, including expired identification documentation.

(b) Where Consumers have failed to respond to the Bank's written notices requesting the Consumer to provide required identification details to update the Bank's records, The Bank must after a notice period of 90 calendar days or after such period as may be prescribed by the Central Bank, temporarily block Debit & Credit Cards for all types of transactions, including ATM withdrawals.

Note - However, all other operations in the accounts of the Consumers are permitted through the branch. The Bank does not levy any charges on such temporary blockage of the Consumers' use of their cards.

14.8.6 The Business units along with Compliance or fraud prevention function;

(a) Undertakes Consumer education initiatives and undertake fraud awareness campaigns every year and more frequently if there is evidence of heightened fraudulent activity.

(b) Implements an ongoing duty to educate and advise Consumers in Writing as to the security precautions that need to be taken to access their financial services including:

(i) Avoidance of using simple passwords or numbers associated with personal dates;

(ii) The financial liability on the Consumers if they provide their password or personal identification number (PIN) to anyone or leave them written down and accessible to others to observe;

(iii) Advising Consumers on how they should and can change passwords and PINs periodically;

(iv) Cautiously entering the PIN at an ATM or POS Terminal to ensure they are not being observed;

(v) Protecting access to their cheque book.

14.8.7 The Banks Head of Information Technology will ensure that;

(a) Payment instruments/terminals (such as ATMs) and online banking channels are progressively upgraded with the latest technology, particularly to prevent the use of counterfeit cards, and inspected regularly in accordance with the Central Bank's guideline on preventing ATM Card frauds.

(b) The Banks ATMs are secure, whereby it has:

(i) Installed and maintained PIN pad shields to prevent the recording of Consumer PINs while using ATMs or POS terminals;

(ii) Installed Anti-Skimming devices to prevent the magnetic stripe being read. Operators immediately withdraw from service any ATM that has been compromised;

(iii) Installed sensors to detect the presence of skimming devices and to send alerts to the operator and/or shutdown the ATM;

(iv) Ensures digital security cameras are within the ATM;

(v) Applies any other advances in security as deemed necessary to protect Consumers;

(vi) Monitors and investigates reported ATM issues from Consumers.

(c) The Bank conducts periodic maintenance of all ATMs including verification of its proper functionality and ensuring security has not been breached (e.g., illegal keypad replicators and cameras).

(d) A record of the verifications on each machine is maintained for a period of one year and made available for inspection by the Central Bank.

14.8.8 The Bank may be held liable for any direct losses incurred as a result of any breaches of The Banks' security controls.

14.8.9 The Banks Risk Management function will;

(a) Effectively perform and document their due diligence measures when verifying the background and competence of any Third Party that will represent The Bank and/or have access to or possession of the Consumer's assets, information and Data.

(b) Ensures their Authorized Agents have equivalent level of fraud control, coordination and monitoring for all activities performed by their Staff on behalf of the Bank.

14.8.10 The Banks Human Resource department will ensure that

(a) Due diligence is performed before hiring Staff and ensures verification of all fit and proper requirements are fully commensurate with responsibilities and functions of the positions.

(b) Provides adequate and up to date Staff training on its control framework to ensure Consumers' assets are securely handled.

14.9 Fraud Detection

14.9.1 The Banks Risk Management function will ensure that;

(a) Adequate systems and processes are in place to monitor and respond to external fraud activities commensurate with the type of risk associated with the Financial Product or Service and the frequency of Consumer transactions.

(b) It monitors and documents trends on the number and type of incidents for fraud, attempted frauds and Consumer Complaints in order to determine if there is any evidence of weakness in the security and detection measures.

(c) It reports significant fraud events immediately to the Central Bank in a manner as it may be prescribed.

14.9.2 The Bank through its communication channels will inform the Consumer of the procedures for reporting cases of theft, loss and fraud.

14.10 Fraud Investigation and Reporting

14.10.1 The Banks Risk Management function will ensure that a fraud reporting function is setup to investigate Financial Crime Compliance.

14.10.2 The Bank's management through its communication channels will ensure that;

(a) When a specific pattern of frauds or deception is identified, timely notifications are issued to Consumers to promote awareness and preventative measures.

(b) The notice provides a contact method for Consumers to report fraud incidents or make inquiries.

14.10.3 The Banks Compliance Department or any other function that deals with UAE Central Bank will ensure to;

(a) Report all Consumer Complaints arising from external, internal and attempted frauds, as well as any apparent vulnerabilities in the security and online systems to the Central Bank on a quarterly basis.

(b) Files a summary annual report by January 31st to the Central Bank on the trends and significant incidents of fraud and attempted frauds including a description of the preventative measures taken.

15. Reference to Bank's Policies and Procedures

a) Customer Complaint Handling Policy

b) Customer Service Charter

c) Dormant Account Policies and procedures

d) Cyber Security Framework

e) Consumer Protection Policies and Procedures