SAWJI BANK

Always with you...

SUNDARLAL SAWJI URBAN CO-OP. BANK LTD; JINTUR

Digital Banking Policy

Classification:	Strictly for BANK Use Only.
Department:	E-Banking Department
Author:	Adv. Jayashree Nangare
Version Control:	Version No. 1.0
Date of Issue:	**22-11-2019**

Amendment Record

Amendment No.	Release Date	Description Of Change	Prepared By	Approved By
V1.0	22-11-2019	**DIGITAL BANKING POLICY**	CISO	Board of Director

Head Digital Banking **Chief Information Security Officer**

Chief Executive Officer **Chairman**

Content		
Sr. No.	**Particulates**	**Page No.**

ATM Policy

1. INTRODUCTION

- SUNDARLAL SAWJI UBRAN CO-OPERATIVE BANK LTD., JINTUR was Founded in 1965 is serving for its customers on various channels. Being top bank in Co-Operative section, BANK is providing its customers advance services and features.
- In the age of electronic and mobile devices banking sector has shown a tremendous growth. BANK has also taken various initiatives in order to keep in competition with growing banks.
- Today, almost every commercial bank branch is at some stage of technology adoption: core banking solution (CBS), or alternate delivery channels such as internet banking, mobile banking, phone banking and ATMs. Hence with emerging technology there arises a need of security, in terms of finance, data and other aspects of information.

2. OBJECTIVE:-

- To achieve safe, sound and resilient ATM network and cash flow biding with the technological standards mentioned as per RBI and IT ACT 2000 and IT Amendment Act and other governing laws.
- This document identifies security guidelines for ATMs, considering the protection that can be provided by the hardware and the software of the ATM itself against attacks aimed at compromising sensitive data acquired, stored, exported, or in any way processed by the device.
- The Policy is formulated for the IT department and ASP Provider or the Banking cell taking in or working for the ATM related services

3. SCOPE:

- This policy document covers the implementation of new features, operations, roles and responsibilities in ATM channel and services.

4. RESPONSIBILITY

- The Administrative Management is responsible for approval and execution of the ATM Policy. The time of review of policy and the management of the same will be taken care by IT Manager.

5. OVERSIGHT AND PUBLIC POLICY GOALS

- The Bank monitors and review ATM services from time to time and ensure that:

  1. The legal and regulatory environment is appropriate and keeps pace with domestic developments;

  2. International standards are complied with in respect of infrastructures and cards to reduce risk and increase safety and efficiency; and

3. The provision of services by the Head Office is fair and based on objective criteria.

6. MANAGEMENT RISK ANALYSIS:

- Bank has been following and implemented the process of identifying, measuring, monitoring and managing all potential risk in ATM transactions.
- Bank is identifying, monitoring and keep track report of the following on regular basis.

i. Total no. of active ATMs
ii. Time Logged on / Settlement time.
iii. Number of Cardholders.
iv. Number of transactions i.e. withdrawals and transfers
v. Total amount transacted through withdrawals and transfers.
vi. ATM internal process and services.
vii. Operations of ATM channel.
viii. Legal Risk.
ix. Incident Management.
x. Risk Management.

7. ATM RISK MANAGEMENT:

BANK would review the risk and monitor ATM services by following below mentioned aspects:

- Monitoring and checking that all ATM should be equipped with mechanism preventing skimming attacks,
- Applied mechanism to monitor that each ATM is equipped with only one card holder interface,
- Continues surveillance on all ATM that they are equipped with security Cameras,
- Take all necessary steps to protect ATM assets and Application,
- Managing and identifying various hazards to which ATM centers that may exposed including natural disaster or otherwise,
- Identifying the controls that are in operation to reduce possible impacts of threats/risks,
- Following all the security controls and guidelines suggested by PCI DSS,

- Firewall should be configured and be kept up to date and should allow only known application traffic inward and outward,

- Patch management program for ATM operating system and applications should be in place to ensure ATM software is well patched,
- Software White listing solution for ATMs and it should be in place and an anti-virus must be installed and always updated,
- Develop an incident management system and an incident response plan prepared for rapid deployment in case of a compromise. This is to ensure ATM frauds are reported in real time,
- ATM software must be updated regularly,
- ATM operators should migrate to EMV chip and pin card and should eliminate magnetic stripe fall back. This will mitigate the risk of skimming cards,
- Segregation of ATM network from the rest of the bank's network by using a firewall and virtual local area networks,
- ATM PC BIOS must be secured,
- A password policy must be in place to ensure only strong passwords are used on ATMs and each user has their own unique password,
- All communications on the ATMs that is encrypted including communication between the PC core and the cash dispenser,
- All unused services and applications must be removed from the ATM to reduce the attack surface,
- Ensuring ATM physical security like CCTV and alarms when installing the ATM.

8. TYPES OF ERRORS

Bank have management/handling plan for the following errors can occur due to mechanical failure at the ATM terminal:

i. ATM dispenses less cash to the customer but the amount is debited correctly
ii. The customer's account is debited twice but the cash is only dispensed once by ATM
iii. The Customer's account is debited but cash is not dispensed by ATM

9. ATM SECURITY MEASURES:

- **The ATM Audit Log**

  Record and track of ATM audit Log that provides recorded information after incident.

- **Encryption**

  All ATM system installed are encrypted and updated time to time.

- **Software Audit**

  Perform software audit of all installed and active ATMs to analyze the ATM operations.
  Monitoring operations of ATMs and detect possible tampering with the programs.
  Perform audit to detect that program are being properly executed and not being over-ridden or bypassed.

10. CONTROLS

This requirement should be addressed with the controls implemented at different levels of ATM implementation, such as General Application Control, Business Process Control, and Application Process Control, CIA Controls.

- **General ATM operation and Organizational Controls:**

  The operation and organizational controls must be segregated among the individuals, There are two main important elements in an ATM systems; firstly the magnetic card and secondly PINs. Segregation of duties shall be maintained by assuring that making of the PINs is not to be carried out by people who are processing the cards.
  Following segregation is to be followed by Bank:
  - Application testing from systems design and programming
  - System software programming from Application programming

- **Business Process Controls**

  Bank personnel having access to cards must be denied access to PINs whenever the cards are prepared and processed. Bank takes care of segregation of duties that no one person shall handle all the transaction. Bank makes sure that.

11. ATM TECHNOLOGICAL STANDARDS AND SECURITY MEASURES :

Bank has established secured network and implemented security measures for mitigating risk in ATM operations, which are listed as below:

a) All ATMs shall be operated for cash replenishment only with digital One Time Combination (OTC) locks.

b) All ATMs shall be grouted to a structure (wall, pillar, floor, etc.), except for ATMs installed in highly secured premises such as airports, etc. which have adequate CCTV coverage and are guarded by state / central security personnel.

c) Bank also rolling out a comprehensive e-surveillance mechanism at the ATMs to ensure timely alerts and quick response.

- **Monitoring**

The following scope is inclusive of problem determination and resolution tasks which Bank is considering for central management of ATMs, all of which can be performed remotely with good ATM monitoring and management tools:

a) Gracefully reboot the ATM; allow current transactions to finish before rebooting!
b) Retrieve log files and security events.
c) Retrieve performance information about memory, disk space, CPU usage, process lists, network ports, etc.
d) Restart critical services on the ATM.

- **Integration**

  Management and security tools that Bank has been used successfully in ATM systems which are mentioned below:

- Central authentication of user accounts used at the ATM.
- Inventory systems to track information about ATM hardware and software.
- Network monitoring systems to analyze the network performance of the ATMs.
- **Cryptographic Key Management for ATMs**

  Bank applies key management process which is associated with financial transactions and for encrypting PIN Pad.The very essence of protection in an encrypted environment is the secrecy of the key.

- **Firewalls and Network Isolation**

  Bank has installed software based firewall protection which has been the most security measure as it cannot be compromised through physical access alone.

  Bank has established effective network isolation and intrusion detection/ risk mitigation tools. Bank uses network isolation or network encryption techniques to ensure that cardholder data cannot travel outside the ATM system itself. Bank has a good core set of layered security which involves network isolation, tested operating system hardening, secure operating processes, and central monitoring/management tools.

12. SECURITY AND CONTROL OF PIN (PERSONAL IDENTIFICATION NUMBER)

PINs are stored in encrypted form and should be stored in database file for security purposes. The PIN mailers are prepared separately and also bank has taken necessary actions to check that PIN is not being misused by any Bank employee. Bank ensures that Pin is activated only upon the use of card by the customer at the ATM.

For security and confidentiality reasons all systems documentation concerning PIN generation/encryption and decryption key must be under 3D level security controls all time.

- **Bank is implementing controls while providing ATM services are mentioned as below:**

i. PIN mailers should not have direct access to the customer's account number or any account related information.

ii. Access controls and authorization to any addition, deletion or changes to ATM transaction details should be implemented

iii. Any changes to cardholder details should be authorized by the officer at the next level.

iv. Realistic maximum transaction and maximum daily total limits should be implemented for ATM withdrawals.

v. Printed receipts should be dispensed by the ATM for every ATM transaction.

vi. Every ATM transaction should be acknowledged by e-mail or short message script sent to the mobile phone to confirm or alert the user that a transaction was performed.

13. APPLICATION CONTROL AND SECURITY:

There are well-known information systems security issues associated with applications software, whether the software is developed internally or acquired from an external source. Attackers can potentially use many different paths through the application to do harm to the business. To determine the risk to itself, Bank has been evaluating the likelihood associated with the threat agent, attack vector and security weakness and combines it with an estimate of the technical and business impact to the organization. Together, these factors determine the overall risk.

The following are the important Application control and risk mitigation measures are implemented by Bank:

1. Each application has an owner which will typically be the concerned business function that uses the application

2. Some of the roles of application owners include:

- Prioritizing any changes to be made to the application and authorizing the changes
- Deciding on data classification/de-classification and archival/purging procedures for the data pertaining to an application as per relevant policies/regulatory/statutory requirements

- Ensuring that adequate controls are built into the application through active involvement in the application design, development, testing and change process
- Ensuring that the application meets the business/functional needs of the users
- Ensuring that the information security function has reviewed the security of the application
- Taking decisions on any new applications to be acquired / developed or any old applications to be discarded
- Informing the information security team regarding purchase of an application and assessing the application based on the security policy requirements
- Ensuring that the Change Management process is followed for any changes in application
- Ensuring that the new applications being purchased/developed follow the Information Security policy
- Ensuring that logs or audit trails, as required, are enabled and monitored for the applications
- All application systems are tested before implementation in a robust manner regarding controls to ensure that they satisfy business policies/rules of the bank and regulatory and legal prescriptions/requirements. Before the system is live, clarity on the audit trails and the specific fields that are required are captured as part of audit trails and an audit trail or log monitoring process including personnel responsible for the same.
- Bank incorporates information security at all stages of software development. This would assist in improving software quality and minimizing exposure to vulnerabilities. Besides business functionalities, security requirements relating to system access control, authentication, transaction authorization, data integrity, system activity logging, audit trail, security event tracking and exception handling are required to be clearly specified at the initial stages of system development/acquisition. A compliance check against the bank's security standards and regulatory/statutory requirements is also done.
- All application systems have audit trails along with policy/procedure of log monitoring for such systems including the clear allocation of responsibility in this regard. Every application affecting critical/sensitive information, for example, impacting financial, customer, control, regulatory and legal aspects, provides for detailed audit trails/ logging capability with details like transaction id, date, time, originator id, authorizer

id, actions undertaken by a given user id, etc. Other details like logging the IP address of the client machine, terminal identity or location may also be considered.

- Applications also provide for, inter-alia; logging unsuccessful logon attempts, access to sensitive options in the application, e.g., master record changes, granting of access rights, use of system utilities, changes in system configuration, etc.
- The audit trails are stored as per a defined period as per any internal/regulatory/statutory requirements and it are ensured that they are not tampered with.
- There are documented standards/procedures for administering the application, which are approved by the application owner and kept up-to-date.
- The development, test and production environments are properly segregated.
- Access is based on the principle of least privilege and "need to know" commensurate with the job responsibilities. Adequate segregation of duties is enforced.
- There are controls on updating key *'static'* business information like customer master files, parameter changes, etc.
- Any changes to an application system/data are justified by genuine business need and approvals supported by documentation and subjected to a robust change management process. The change management would involve generating a request, risk assessment, authorization from an appropriate authority, implementation, testing and verification of the change done.
- Potential security weaknesses / breaches (for example, as a result of analyzing user behavior or patterns of network traffic) are always identified.
- There are appropriate measures to reduce the risk of theft, fraud, error and unauthorized changes to information through measures like supervision of activities and segregation of duties.
- Applications do not allow unauthorized entries to be updated in the database. Similarly, applications do not allow any modifications to be made after an entry is authorized. Any subsequent changes are made only by reversing the original authorized entry and passing a fresh entry.
- Direct back-end updates to database not be allowed except during exigencies, with a clear business need and after due authorization as per the relevant policy.
- Access to the database prompt is restricted only to the database administrator.

- Robust input validation controls, processing and output controls are built in to the application.
- Alerts regarding use of the same machine for both maker and checker transactions are considered.
- Bank obtains application integrity statements in writing from the application system vendors providing for reasonable level of assurance about the application being free of malware at the time of sale, free of any obvious bugs, and free of any covert channels in the code (of the version of the application being delivered as well as any subsequent versions/modifications done).
- For all critical applications, either the source code is received from the vendor or a software escrow agreement which is in place with a third party to ensure source code availability in the event the vendor goes out of business. It is ensured that product updates and programme fixes are also included in the escrow agreement.
- Applications are configured to logout the users after a specific period of inactivity. The application ensures rollover of incomplete transactions and otherwise ensures integrity of data in case of a log out.
- There are suitable interface controls in place. Data transfer from one process to another or from one application to another, particularly for critical systems, not has any manual intervention in order to prevent any unauthorized modification. The process are automated and properly integrated with due authentication mechanism and audit trails by enabling "Straight Through Processing" between applications or from data sources to replace any manual intervention/semi-automated processes like extracting data in text files and uploading to the target system, importing to a spreadsheet, etc. Further, proper validations and reconciliation of data is carried out between relevant interfaces/applications across the bank. The bank suitably integrates the systems and applications, as required, to enhance data integrity and reliability.

14. GENERAL INFORMATION REGARDING DELIVERY CHANNELS

- Provision of various electronic banking channels like ATM/debit cards/internet banking/phone banking are issued only at the option of the customers based on

specific written or authenticated electronic requisition along with a positive acknowledgement of the terms and conditions from the customer. Customer is not being forced to opt for services in this regard. Bank provides clear information to their customers about the risks and benefits of using e-banking delivery services to enable customers to decide on choosing such services.

- When new operating features or functions, particularly those relating to security, integrity and authentication, are being introduced, the bank ensure that the customers have sufficient instruction and information to be able to properly utilize them.
- To raise security awareness, Bank sensitizes customers on the need to protect their PINs, security tokens, personal details and other confidential data.
- Bank is responsible for the safety and soundness of the services and systems they provide to their customers. Reciprocally, it is also important that customers take appropriate security measures to protect their devices and computer systems and ensure that their integrity is not compromised when engaging in online banking. Customers implement the measures advised by their Bank regarding protecting their devices or computers which they use for accessing banking services.
- In view of the constant changes occurring in the internet environment and online delivery channels, management institute a risk monitoring and compliance regime on an ongoing basis to ascertain the performance and effectiveness of the risk management process. When risk parameters change, the risk process are updated and enhanced accordingly. Re-evaluation of past risk-control measures and equations, renewed testing and auditing of the adequacy and effectiveness of the risk management process and the attendant controls and security measures taken are conducted.

15. CUSTOMER AWARENESS ON FRAUDS

- **CREATION OF CUSTOMER AWARENESS ON FRAUDS**

1. Customer awareness is one of the pillars of fraud prevention. It has been seen that alert customers have enabled prevention of several frauds and in case of frauds which could not be avoided, helped in bringing the culprit to book by raising timely alerts. Bank thus aim at continuously educating its customers and solicit their participation in various preventive/detective measures. It is the duty of all the groups in Bank to

create fraud risk awareness amongst their respective customers. The fraud risk management group shares its understanding of frauds with each group, identify areas where customer awareness is lacking and if required, guide the groups on program's to be run for creation of awareness amongst customers. The groups ensure that in each of their interaction with customers there is at least one message to make the customer aware of fraud risk.

2. The following are some of the recommended measures to create awareness amongst customers:

- Publications in leading newspapers
- Detailed 'do's and don'ts' on the web site of the bank
- Messages along with statement of accounts, either physical or online
- Messages printed on bank's stationery such as envelopes, card covers, etc.
- SMS /Email alerts for security tips(OTP/CVV/PIN/CARD/Transaction alerts Message) on phone banking when the customer calls
- As inserts or on the jackets of cheque books
- Posters in branches and ATM centers
- Interstitials on television and radio

3. It is ensured that the communication to the customer is simple and aimed at making them aware of fraud risks and seeking their involvement in taking proper precautions aimed at preventing frauds. Such communication is reviewed periodically by the fraud risk management group to judge its effectiveness.

16. EMPLOYEE AWARENESS AND TRAINING

1. Employee awareness is crucial to fraud prevention. Training on fraud prevention practices are provided by the fraud risk management group at various forums.
2. Bank uses the following methods to create employee awareness:

- Class room training programs at the time of induction or during risk related training sessions
- Publication of newsletters on frauds covering various aspects of frauds and containing important message on fraud prevention from senior functionaries of the Bank
- E-learning module on fraud prevention
- Online games based on fraud risks in specific products or processes
- E-tests on prevention practices and controls

- Detailed ‘do’s and don’ts’ put up on the worksite of the employee
- Safety tips flashed at the time of logging into Core Banking System (CBS), screen savers, etc.
- Emails sent by the respective business heads
- Posters on various safety measures at the work place
- Messages/discussions during daily work huddles

17. THREATS TO ATM NETWORKS

As other networks, ATM networks will suffer a lot of threats. ATM threats/attacks can be divided into physical and logical attacks. Physical attacks involve attacking the ATM physically like exploding the ATM safe to have access to the ATM safe money. In physical attack, cyber criminals use methods such as solid and gas explosives, as well as uprooting the ATM from the site and then using other method to get access to safe and secure network. Other physical attack involves placing gadgets to ATM by cyber criminals that copy ATM card data and reproduce it on another blank card that can be used to perform unauthorized transaction from cardholder’s account. Logical attacks include malware attacks to instruct ATM to perform the transaction. This attack can be achieved by gaining physical access on the ATM in order to install malware on the system or it can be injected using network. Types of attacks on ATM network are as follows:

- **ATM Card Skimming Attacks**

  ATM card skimming attack is a physical threat which has been the number one ATM threat globally in the past. ATM skimming refers to the stealing of the electronic card data, aiding the criminal to counterfeit the card. A skimmer is a device that is installed on a card reader making a customer believe they are inserting their card in a ATM card reader. The skimmer reads the data from a card's magnetic stripe or EMV chip when a client inserts a card into the ATM. Some skimmers have the capability to read data from an EMV card chip at a distance. ATM skimming attacks are however on the decrease due to deployment of anti-skimming solutions, payment card industry data security standard (PCI DSS), EMV technology and contactless ATM functionality. Customers are unable to notice a problem and experience a normal ATM transaction until their account is defrauded. The most common places where skimmers are placed

on the ATM. Multifactor authentication using biometrics can be used as an added security mechanism against this type of fraud.

- **Eavesdropping Skimming Attack**

  A new type of skimming attack called Eavesdropping Skimming has emerged and expanded predominantly in the world. The attack targets ATM motorized card readers on older model of ATM called personas. The attacker penetrates the ATM facial to have access to the card Reader of the ATM. A skimmer is then fitted directly onto an electrical node that carries card data on the card reader. On Personas ATMs, the attacker targets the card reader electronic control board by creating a hole behind the ATM card orientation window. In the newer attacks against ATMs, the attacker has changed the method but has maintained the principle. The variance in the way this attack is performed on the two different ATM series shows how sophisticated ATM cyber-criminals are.

- **ATM Card Shimming Attack**

  ATM card shimming attack is a Man-in-the-Middle attack in which the cyber-criminal inserts a device into the ATM card reader that intercepts and records the data flowing between the EMV chip and the ATM card reader . This data could then possibly be reused to clone a magnetic stripe card. EMV chip data and magnetic stripe data have different check values (CVVs) and therefore the data that is captured from the EMV chip card can't be used to clone a magnetic stripe. Card Shimming is neither vulnerability with a chip card, nor with an ATM. It is therefore not necessary to add protection mechanisms against this form of attack to the ATM. If the proper authorization procedure is followed during an ATM transaction, counterfeit cards can be immediately detected. This attack can only be successful if an issuer neglects to check the CVV when authorizing a transaction. All issuers must therefore make these basic checks to prevent this category of fraud.

- **ATM Card Trapping Attack**

  ATM Card Trapping steals the physical card itself through a device attached to the ATM. Cyber-criminals place a device directly over or into an ATM's card reader slot. These devices are designed to capture cards after customers' insert them. In a magnetic stripe environment or chip-and-signature environment, the PIN does not need to be compromised and therefore having an ATM is enough to compromise a customer's account.

- ***ATM Cash Trapping Attack***

  Cash trapping is where the cyber-criminal uses a device to physically trap the cash that is dispensed and comes to collect it once the customer has left the ATM location. This fraud involves placement of money traps or false presenters in front of the ATM dispenser. When processing a transaction, an ATM dispenses notes into the trap set by cyber-criminals rather than present the money to the customer. The customer assumes the ATM has malfunctioned and leaves. The cyber-criminal then returns, removes the money trap or false presenter, and leaves with cash that was intended for the customer. Cash trapping however mostly succeeds with insider involvement. ATM owners must put measures in place that helps mitigate insider threats.

- **Transaction Reversal Fraud**

  Transaction Reversal Fraud (TRF) involves the creation of an error that makes it appear as though the cash has not been dispensed. The account is re-credited the amount 'withdrawn' but the criminal pockets the money. It could be a physical grab (similar to cash trapping) or a corruption of the transaction message. The attacker achieves this by creating a fault on the ATM during a cash dispense operation causing the host switch to reverse the transaction. The account will not be debited although the criminal will remove the cash from the ATM. To avoid being caught, attackers use stolen or skimmed cards. The attacker causes an error on the card reader during cash dispense operation. The correct PIN is entered and cash requested. After the transaction is authorized by the host switch, the ATM counts the cash and positions it behind the cash dispenser shutter waiting to be dispensed. The card is ejected and the attacker waits for the ATM transaction to time out and attempt to capture the card. At this point the attacker holds the card and prevents it from being captured and then forces the cash dispenser shutter open and removes the stacked cash. The ATM reports a card jam and reverses the transaction.

- **Social Engineering/Phishing Attacks**

  The Victim is tricked into revealing his/her authentication information (PIN). It can be physically or through electronic means. e.g., rogue websites are set up by the perpetrators to collect authentication information from un-suspecting customers in the name of necessary updates or changes being carried out by their 'Bankers'. The user ends up divulging his card sensitive data to the rogue site.

- **Operational Fraud**

  The ATM dispenser is manipulated in this type of fraud. The ATM is configured to dispense big denominations as smaller ones, there-by giving out more money than should be dispensed. This can be achieved by either loading wrong denomination notes in the wrong money cassettes or by making a wrong configuration in the software.

- **Malware Attacks**

  Malware attacks are usually easier with insider involvement as physical access is necessary to deploy the virus. However, this attack is possible online today. The malware file or device is placed on the ATM; its control device is then triggered to give remote control to the perpetrator through a custom interface which enables capture of card numbers and PINs through the private memory space of transaction-processing applications installed on a compromised ATM. Magnetic stripe cards are very vulnerable to this type of attack. Deployment of effective anti-malware software can help mitigate this class of attacks.

- **Man-in-the-Middle Attack**

  This class of attack occurs when malware is placed within the banks network and compromises the banks network infrastructure. The network traffic is monitored and the malware listens for transaction messages from the ATMs

  When the malware recognizes a cash withdrawal transaction message from a bank card, it intercepts the corresponding host response from the ATM switch and changes the authorized dispense amount to a larger sum than requested and approved by the ATM switch. In order to perform the fraud, an attacker will initiate a withdrawal transaction at any ATM on the compromised bank network. The attacker will use a pre-defined known card number. The transaction will be intercepted and the card number will be recognized by the malware. It will then wait for the host response to the withdrawal request. The malware will intercept the host response message and modify it to a larger amount therefore the ATM will dispense far more money than what is debited from the account. A variation of the attack, is where the malware intercepts the request, and returns an authorization message such that the transaction host is unaware of the request.

- **Ransom-ware Attacks**

  A serious malware called “WannaCry” encrypts the files on end-points that are

running Microsoft operating system software, rendering them inaccessible. The files are only decrypted upon payment of a sum of money known as ransom. This malware attempts to infect other end-points on the same network. The malware does not specifically target Banking and Retail systems or their functionalities but ATMs like any other Windows based system are also at risk of this attack. There have been unconfirmed media reports that some ATMs in India have experienced this attack.

Prevention of infection via phishing emails by implementation of technical and organizational measures,

Segment and secure local area Network(LAN)/ virtual LAN(VLAN) with intrusion detection and prevention mechanisms to avoid infection and distribution of malware via the network,

- **ATM Jackpotting Attack**

The term ATM Jackpotting comes from the term Jackpot. In this type of attack, cyber-criminals get huge sums of money from the ATM at once. Cyber-criminals use two methods to perform this attack.

18. ATM INCIDENT MANAGEMENT POLICY AND PROCEDURES

The Bank has developed, communicated and implemented formal systems and procedures for detecting and reporting incidents relating to exceptional situations in day-to-day administration of IT and information security related areas. The Bank ensures that the incidents are reported in time to the appropriate authorities and corrective actions are taken immediately to provide the IT Service to Users as quickly as possible and to avoid the recurrence of such events in future

Definitions

"ATM" Automated Teller Machine is a computerized machine that provides the customers of banks the facility of accessing their accounts for dispensing cash and to carry out other financial transactions without the need of actually visiting a bank branch.

"Incident" is a term related to exceptional situations or any event which is not a part of the standard operation of a service and which causes or may cause an interruption to or a reduction in the quality of service or a situation that warrants intervention of senior management. An incident is detected in day to day operations and management of the IT function.

"INCIDENT RESPONSE" set of actions taken to protect and restore the normal operating condition of computers and the information stored in them when an adverse event or incident occurs; involves contingency planning and contingency response.

"INCIDENT HANDLING" Same as Incident Response.

"INTRUSION" any intentional event where an intruder gains access that compromises the confidentiality, integrity, or availability of computers, networks, or the data residing on them

"CHAIN OF CUSTODY" verifiable documentation that indicates the sequence of individuals that have handled a piece of evidence and the sequence of locations where that evidence has been stored, including dates and times. For a proven chain of custody to occur, the evidence is accounted for at all times.

"CONSTITUENCY" Implicit in the purpose of a Computer Security Incident Response Team is the existence of a constituency. It is the group of users, sites, networks or organizations served by the team. The team must be recognized by its constituency in order to be effective.

Responsibilities

- ✓ Provide a (secure) channel for receiving reports about suspected incidents.
- ✓ Provide assistance to members of its constituency in handling these incidents.
- ✓ Disseminate incident-related information to its constituency and to other involved parties.

Procedures

- ✓ Functions of IT Department with respect to Incident management
- ✓ The System administrators shall handle the technical and organizational aspects of incidents. In particular, it will provide assistance or advice with respect to the following aspects of incident management
- ✓ Investigating whether indeed an incident occurred.
- ✓ Determining the extent of the incident.
- ✓ Incident Coordination
- ✓ Determining the initial cause of the incident (vulnerability exploited).
- ✓ Facilitating contact with other similar sites who have reported the incident (if applicable).
- ✓ Facilitating contact with appropriate law enforcement officials, if necessary.

- ✓ Making reports.
- ✓ Composing announcements to users, if applicable.
- ✓ Incident Resolution Removing the vulnerability.
- ✓ Securing the system from the effects of the incident.
- ✓ Evaluating whether certain actions are likely to reap results in proportion to their cost and risk, in particular those actions aimed at an eventual prosecution or disciplinary action: collection of evidence after the fact, observation of an incident in progress, setting traps for intruders, etc. Collecting evidence where criminal prosecution, or Disciplinary action, if contemplated.

Data Collection & Analysis

- ✓ In addition, IT department will collect statistics concerning incidents which occur within or involve the bank's information resources, and will notify the relevant parties proactively as necessary to assist it in protecting against known attacks.
- ✓ The incidents noted are analyzed by the quality function on a semiannual basis to identify trends, if any. A database containing following information for each incident noted is prepared for future use:

Type of Incident

- ✓ Impact Analysis on the affected IT assets or business process
- ✓ Ways of detecting the incident
- ✓ Ways of resolution of incident
- ✓ Down time requirements
- ✓ Contact details for reporting and resolution

Information Services: List of departmental security contacts, administrative and technical.

These lists will be available to all users inside the bank and general public, via commonly available channels such as Intranet/World Wide Web.

Incident Handling & Management

i. **Constituency**

- ✓ An IT Department's constituency can be determined in any of several ways. For example it could be a company's employees or its paid subscribers, or it could be defined in terms of a technological focus, such as the users of a particular operating system.
- ✓ The definition of the constituency should create a perimeter around the group to whom the team will provide service. The policy section of the document (see below) should explain how requests from outside this perimeter will be handled.

ii. **Detection and initial reporting:**

- ✓ An incident may be detected by anybody in the bank. The concerned personnel should immediately bring it to the notice of the person designated by IT department. The person so designated should escalate the issue as per escalation guidelines. The initial reporting covers following:
- ✓ Time of the incident
- ✓ Nature of the incident
- ✓ Probable cause of the incident
- ✓ Effect of the incident
- ✓ Mode of resolution of the incident
- ✓ Activity log in case the incident involves desktop / server / network operating systems or any of the applications.

iii. **Documentation and formal reporting:**

- ✓ A person designated by departmental head should maintain the central database of all such incidents. The person so designated, after analyzing the extent of exception and facts of the incident, should appraise the related IT department personnel. A detailed risk and impact analysis for the incident should be carried out by the IT team. (Refer to Annexure A, B and C for the formats of Incident management documentation).
- ✓ The IT department should ensure that all incidents are categorized based on the nature of each incident and are held in a database created for the purpose. The database should be able to provide information on demand and have the capability to perform analysis on the data contained within. The bank‘s employees encountering incidents would thus be able to access the incident database and possibly find

solutions if the incident had occurred before. Frequently asked questions should also be incorporated into the database to assist the user in finding solutions to incidents encountered.

iv. **Monitoring:**

✓ All the major incidents should be reviewed and monitored by the Security Administrator and discussed in the Technology Committee meeting every month. The magnitude and criticality of the incidents may prompt the System / Database / Network Administrators to discuss and take action on the incidents immediately instead of at fixed intervals.

v. **Development of corrective action plan:**

✓ The IT department, in consultation with affected System administrator or any other person it deems fit should prepare the corrective action plan for the incident. The action plan, though specific to each case, should typically cover the following:

✓ Facts and explanation / reasons for the incident

✓ Corrective action to be taken

✓ Estimated cost of implementing the corrective action

✓ Estimated time frame, start date and end date

✓ Personnel responsible for taking the action

✓ Information exchange with other Incident Handling teams

✓ The IT department can share information with other incident management teams and general public with prior permission from Executive Director.

✓ Annexure A –Incident Reporting Form

Department:	Date:
Name of the employee:	Department:
Facts of the incident:	
Signature:	

✓ Annexure B Reporting of the incident to Level 2

Department:	Date:
Incident reported by:	Incident occurred on:
Facts of the incident:	
Analysis of the incident by Head of Department and impact:	
Signature: Systems Administrator / Operator in charge of the branch	Signature: Head

ATM Cum Debit Card Acceptance Of Use Policy

Policy for governing the Sundarlal Sawji Bank Debit card (ATM-CUM-DEBIT CARD)

Definitions:

The "**Member Bank**" refers to Saraswat Co-operative Bank limited, Mumbai.

The "**Sub member Bank**" refers to Sundarlal Sawji Urban Co-operative Bank limited, Jintur.

The Bank, our, us or we refers to Sub member Bank that is Sundarlal Sawji Bank.

Sundarlal Sawji Bank a body corporate constituted under the Maharashtra Co-operative Society Act (Acquisition and Transfer of Undertaking) Act 1960 having its Registered Office at APMC Market Yard, Yeldari Road Jintur, which expression shall mean and include its successors and assigns.

The SIL refers to Saraswat InfoTech Ltd., Mumbai, is application service provider.

Cardholder, you, your refers to a customer of the Bank, who has been issued and authorized to use the Sundarlal Sawji Bank Debit Card.

The issuer in relation to cardholder means the Bank.

The card means the "Sundarlal Sawji Bank Debit Card" issued by the issuer to Cardholder.

Account in relation to Debit Card means an account opened and maintained by Sundarlal Sawji Bank for the purpose of routing card related transactions under this agreement, which also includes an account of a customer of the Bank who has agreed to these terms and conditions and is authorized to operate the Bank account and thereby use the banking Services including ATM services and includes those having joint accounts, Multiple users.

Customer includes any individual, sole proprietorship firm, partnership, company, co-operative society, association and corporation, association of persons, trust or other legal or natural entity or organization.

ATM means any Automated Teller Machine in India whether of the Bank or a shared network ATM located displaying RUPAY logo which honours the Debit Card.

A **PIN** means the personal Identification Number (required to access ATMs) allotted to the Cardholder by the Bank or chosen by the cardholder from time to time.

Charges shall mean all amounts charged to the account under this terms including but not limited to purchase of goods, services or cash by use of the Card, joining fee, annual fees, interest charges, finance charges, transaction charges, service charges and any taxes, applicable from time to time.

Merchant or Merchant Establishment shall mean any company, establishment, and/or person wherever located, which a RUPAY Card Scheme Member Bank has approved and made arrangements with, to accept and honour the card, for the sale of goods and service to Cardholders. This shall include among others, stores, shops, restaurants, airline organizations etc. advertised by the BANK or RUPAY.

"**BM**" means Branch Manager.

"**NPCI**" stands for National Payment Corporation of India

"**EDC**" or "Electronic Data Capture", refers to Electronic Point-of-sale swipe terminals, whether displayed by or on behalf of Bank or any other Bank at which, amongst other things, the cardholder can use his fund in his account(s) held with the Bank to process the transaction at a Merchant Establishment. „Transaction" means any instruction given, by a cardholder by using his card, to the Bank to effect action on the account. (Examples of transactions can be retail purchases, cash withdrawals, etc.)

The CARD:

The Sundarlal Sawji Bank Debit Card shall be issued on the basis of an application in the prescribed format subject to such eligibility norms the issuer may fix from time to time. The issuer at its sole discretion may refuse issuance or renewal of card without assigning any reason whatsoever.

The cardholder shall be deemed to have unconditionally agreed to be bound by the Terms and conditions by acknowledging receipt of the card in writing or by signing on the reverse of the card or by incurring a charge on the card. However, the account holder may refuse to be issued a card subsequent to have applied but has not accepted for whatsoever reasons. In such cases, if the card is already received by the branch of issue, the card shall be destroyed by cutting into two pieces. No refunds shall be made of the charges for the card, which were ordered and subsequently refused.

The Sundarlal Sawji Bank Debit Card is valid only in India. The card is valid up to the last day of the month of year Indicated on the face of the card unless cancelled/invalidated earlier. On expiry/earlier cancellation/ invalidation, the Card must be destroyed by cutting into two pieces and shall be returned to the issuer.

A Membership renewal fee will be charged at the time of renewal of cards on expiry. Annual fee at the prevailing rate will be levied at the time of issuance of the card which will be collected by debiting to the account for each of the card issued to the account and then annually during the month in which the card was originally issued. The fees are subject to revision by the Bank from time to time.

The Cardholder will be responsible for all facilities granted by the Bank in respect of the card and for all related charges. A tariff of charges has been given elsewhere in this document, which is subject to changes from time to time. The Card along with the acknowledgment issued will be sent to the Branch who had forwarded the application. The applicant shall sign the acknowledgment and return it to the branch for having received the Card/s. The Cardholder shall sign on the reverse of the Card immediately on its receipt and shall take all reasonable care for its safe custody. The Cardholder shall also note down the Card Number and validity period, as imprinted on the Card, separately to enable him/her to furnish these details to the issuer in case of loss or theft of the Card as required in terms of Para.05 hereof. The renewal Card along with acknowledgment will be dispatched by the Issuer to the Branch where the Cardholder maintains his/her account.

The Card is a property of the Bank and the issuer reserves its right to cancel the Card and/or withdraw the privileges extended to the Cardholder under the Card at any time without assigning any reason. The issuer shall have absolute right to retrieve the cancelled/withdrawn Card and must be surrendered to an authorized person of the Bank on Demand. The cardholder shall ensure that the identity of the authorized person of the Bank is established before handing over the card. Continued possession and/or use of such card by the Cardholder would constitute an illegal act exposing the Cardholder to legal proceedings.

The issuer may at its Sole discretion and without the Cardholder having to make specific request to renew, renew the Card whose validity has expired or is going to expire, for a further period presently of 5 years unless the Cardholder specifically indicates his wish to the contrary (Informing at least 2 months in advance of the expiry period). And upon such renewal all the terms and conditions hereof shall apply to such renewed card.

The Bank will initially allocate a Personal Identification Number (PIN) to the cardholder. The cardholder may select his own PIN (any 4 digit number) if he would like to change it, depending on the availability of such facility in our ATM. The PIN issued to the cardholder for use with the Card or any number chosen by the cardholder as a PIN, will be known only to the cardholder and to the personal use of the cardholder and are non-transferable and strictly confidential. A written record of the PIN should not be kept in any form, place or manner that may facilitate its use by a third party. The PIN should not be disclosed to any third party, under any circumstances or by any means whether voluntary or otherwise. The cardholder shall be liable for any damages arising from a failure to keep secrecy of the PIN.

In case the cardholder already has Sundarlal Sawji Bank ATM card, on his acceptance/deemed acceptance of the Debit card, the ATM card issued to him, (if any) will be cancelled/deactivated by the Bank subsequently.

Use of the CARD

The Cardholder must not permit any other Person to use the Card and should safeguard it from misuse by retaining it under his/her personal custody at all times. The Cardholder's account will be debited immediately with the amount of any withdrawal, transfer and other transactions effected by the use of the card. The cardholder will maintain sufficient funds in the account to meet any such transactions and shall not be entitled to overdraw the account(s) with the Bank or withdraw/purchase by the use of the Debit Card in excess of any agreed overdraft limit.

In case of cards linked to multiple accounts, transactions at ATMs (where account selection option is not available), Merchant Establishments and Cash withdrawals through EDCs will be affected on the primary account linked to the card. In case there are no funds in this account, the Bank will not honour

The transactions even if there are funds available cumulatively or severally in other accounts linked to the same card.

The Bank and RUPAY Card shall not be liable when a merchant for any reason refuses to accept the Debit card or the ATM/EDC has not rendered the requested service of the Debit card cannot be used as a result of any defect, blocking, deactivation, temporary insufficiency of cash in the ATM, technical or communication failure.

Merchant Location Usage (POS Transaction)

The card is acceptable at all electronic Point-of-sale across the Globe which display the RUPAY Card Logo. The card is for electronic use only and will be accepted only at Merchant Establishments that have an electronic Point-of-sale swipe terminal. Any usage of the card other than electronic use will be deemed unauthorized and cardholder will be solely responsible for such transactions. The card Is operable with the help of the cardholders signature or the PIN at EDC terminals installed at Merchant Locations depending on the functionality of the EDC terminal. Use of the Card at Member Establishment will be limited by the limit assigned for all such transactions for a day, irrespective of the credit balance in the account(s).

Transactions are deemed authorized and completed once the EDC terminal generates a sales slip. The amount of the transaction is debited from the primary account linked to the card immediately. The cardholder should ensure that card is used only once at the Merchant Location for every purchase. The sales slip will be printed each time the

card is used and the cardholder should ensure that there is no multiple usage of card at the Merchant Location at the time of purchase.

Authority to charge the Cardholder's account in respect of purchases made/to be made services availed/to be availed would be given by Cardholder's either in the form of charge slip or such other form as the Bank may prescribe. Signature of the Cardholder on such form/form together with the Card No. Noted thereon or any sales slip not personally signed by the cardholder, but which can be proved, as being authorized by the cardholder, shall be conclusive evidence as between the issuer and the Cardholder as to the extent of liability Incurred by the Cardholder and the Issuer shall not be required to ensure that the Cardholder has duly received the goods purchased /to be purchased or has duly received the services availed/to be availed up to his/her satisfaction.

The Bank accepts no responsibility for any surcharge levied by any merchant establishment and such amount will be debited to the cardholder's account. However, some transactions (like at Railway Stations & Petrol pumps) may attract a service charge as per the Industry practice in addition to the Amount of transaction which will be debited to cardholder's account.

The Cardholder must retain his own copy of the charge slips. Copies of charge slips will not normally be provided by the Bank/issuer. However at its discretion and upon customer request, the Bank/Issuer may provide copies thereof if request is received in writing within 15 days from the date of transaction, subject to an additional fee, which charge is subject to change at the discretion of the Bank/Issuer.

The card is not to be used at Hotels during check-in and also at other locations where paying arrangement is done before completion of the purchase transaction or service. The card should not be used for any Mail Order/Phone order / purchases and any such usage will be considered as unauthorized.

Should the Cardholder choose to disagree with amount debited to his account, the same should be communicated to the Bank/Issuer within 15 days of the transaction date, failing which it would be construed that all charges are in order.

The Bank/Issuer is not responsible or liable for any defect or Deficiency in respect of goods and services charged to the Card. Any dispute should be settled directly by the Cardholder with the Member Establishment and failure to do so will not relieve the Cardholder of any obligations to the Bank/Issuer. No claim by the Cardholder against a Member Establishment will be a subject or set off or counterclaim against the Bank/Issuer.

Any purchase/availment of service and subsequent cancellation thereof (including purchase and cancellation airline/railway Tickets, etc) shall be treated as two different transactions. On receipt of refund/credit if routed through the Issuer, the actual net amount so received shall be held by the Issuer on behalf of the Cardholder free of Interest and settled against the claim made by the cardholder by crediting to the account subject to recovery of a service charge as may be fixed from time to time. The claim should be supported by some proof like cancelled charge slip copy, refund vouchers etc. All refunds and adjustments due to any merchant/device error or communication link will be processed manually and the account will be credited after due verification and in accordance with RUPAY rules and regulations as applicable. The cardholder agrees that any debits received during this time will be honored only based on the available balance in the Account (s) without considering this refund/adjustment. The cardholder also indemnifies the Bank from such acts of dishonoring the payment instructions.

The cardholder shall make use of the Card only for the purpose of making bona-fide purchase of goods or availment of services from such Member Establishments with whom the Bank may enter into arrangement for this purpose, or such Merchant Establishments who are authorized to accept Cards with RUPAY Card logo Or for making "Cash Withdrawal" as indicated in clause 04 hereof, Within the validity period of the Card. The Cardholder shall not, while making use of the Card commits any breach or violation of any law, rule or regulation that may be currently in force. The Issuer reserves the right to call for from the Cardholder and/or the Member Establishment full details of the transactions under the card, and the Cardholder shall agree to such disclosure. The Cardholder alone shall make use of the Card and shall not allow any other person to use the same on his/her/its behalf. The Card shall not be transferable.

The bank reserves the right and the cardholder agrees inter alia for the disclosure and share and receive from other institutions, credit referencing bureaus, agencies, statutory executive, judicial and regulatory authorities whether on request or under an order there from, and on such terms and conditions as may be deemed fit by the Bank or otherwise, such information concerning the cardholder's account as may be necessary or appropriate in connection with its participation in any Electronic Funds Transfer network. The bank also reserves the right of disclosure of information to third parties about the bank account of the cardholder or the transactions done through the use of the card where it is so necessary for completing transactions and/or when necessary to comply with law or government agency or court orders or legal proceedings and/or when necessary to resolve errors or to resolve other matters.

Any government charges, duty or debits, or tax payable as a result of the use of the card shall be borne by the cardholders and if imposed upon the Bank (either directly or indirectly), the Bank shall debit such charges, duty or tax to the cardholders account.

CASH WITHDRAWALS:

The card is accepted at any of Sundarlal Sawji Bank ATMs (Cash Points) and other bank ATMs/ displaying Rupay Card logo. The card is operable with the help of a confidential PIN at ATM locations. On receipt of the PIN by the cardholder from the Bank/issuer, he should ensure that the same is received in a sealed envelope and that there are no signs of tampering of either the envelope or the PIN mailer. All transactions conducted with use of the PIN will be the cardholder's responsibility and he will abide by the record of the transaction as generated.

The Cardholder may avail cash withdrawal in Indian Rupees with a minimum of Rs.100 or its equivalent and subject to a maximum of Rs. 25000 per day in multiples of Rs. 100 or any such amount as may be notified by the Issuer from time to time.

When the card is used at any other shared ATM, the bank will not accept responsibility for any dealings the cardholder may have with the other institutions including but not limited to such services. Should the cardholder have any complaints concerning any shared network ATM establishment, the matter should be resolved by the cardholder with the establishment and failure to do so will not relieve him from any obligations to the Bank. However, the cardholder should notify the bank of this complaint immediately.

There will be separate service charges levied for such facilities that will be fixed by the Bank from time to time and debited to the cardholder's account linked to the card at the time of making such transactions.

In the situation that the account does not have sufficient funds to debit such fees, the Bank reserves the right to deny the transaction. And the decision of the Bank is binding on the cardholder. Such service charges will be debited to the account irrespective of the fact that a transaction if successful or is a failed one.

The type of transactions offered on shared network ATMs may differ from those offered on the Bank's own network. The bank will only support the minimum transaction set that will be offered at the ATMs belonging to other networks. The Bank reserves the right to change the transaction set without any notice to the Cardholder.

For all cash withdrawals at Sundarlal Sawji Bank ATM, any statements/ receipts issued by the ATM at the time of withdrawal shall be deemed conclusive, unless verified and intimated otherwise by the Bank. Any such verification shall likewise be final and conclusive and this verified amount will be binding on the Cardholder.

LOST OR STOLEN CARD

If the Card is lost/stolen, the Cardholder shall immediately notify the branch (which has issued the card)/nearest branch /Switch room with full details, including the Cardholder's name, the Card Number and its validity period as imprinted on the Card. If this information is given orally, it must be confirmed in writing within 7 days. The Cardholder shall furnish to the Issuer all information in his/her possession as to the circumstances of loss/theft and take all reasonable steps, such as informing the issuer by quick mode of communication, lodge a complaint with local police etc. to recover the lost/stolen Card and shall also assist the Issuer to recover it.

In case of suspected theft of a Card, the Cardholder has to lodge a report with the local police and has to send a copy thereof to the issuer. Subject to compliance by the Cardholder, with these requirements, the Cardholder's liability arising as a result of any other person unauthorized using lost/stolen Card for purchase transactions after the receipt by the issuer (branch of issue) of information of loss/theft of the Card will be ZERO. However there will be no such coverage provided on cash withdrawals done through ATMs, as such transactions require the use of a PIN, which is confidential to the cardholder. In case the Cardholder recovers the card which was reported as lost/stolen, he/she shall not make any further use of it and it shall be surrendered to the issuer along with a full report giving the details of its recovery.

The Cardholder will be fully liable for all the charges on the Card in the event that it is lost but not reported in writing as above to the Bank/Issuer and the Cardholder hereby indemnifies the Bank/ Issuer fully against any liability (civil/criminal) loss, cost, expenses or damages that may arise due to loss or misuse of the Card. In the event the transactions are received by the Bank/Issuer after the Card has been reported lost or stolen but before the receipt of the Cardholder's written confirmation and police complaint/FIR as above, the Cardholder shall continue to be fully liable for all amounts debited to the cardholder's account.

A fee of Rs 150 per Card or such other amount as may be fixed by the Bank from time to time shall be charged from the Cardholder for placing the lost/stolen Card in the Hot List, This fee has to be paid compulsorily whether the lost/stolen Card is to be replaced or not.

PRICING STRUCTURE: (CHARGES/FEES)

ATM Use Charges

1. Membership Fee: 120.
2. Activation Fee: Free.

3. Annual Maintenance Fees: Rs. 120.
4. Hotlist/Duplicate card on account of loss of card: Rs. 120.
5. Replacement card: Rs. 120.
6. Transaction charges at Sundarlal Sawji Bk. ATMs: NIL.
7. Transaction charges at other Bank ATMs: It varies from Rs. 15 to Rs. 25 per transaction.
8. Balance enquiryat other bank. ATMs: Rs. 10 per occasion limits.

POS Use Charges

1. Per Day POS transactions at Merchant Establishments: Rs. 50,000.
2. per Day ATM Cash Withdrawal: Rs. 25,000.00.

In addition to above service tax if applicable and at applicable rates from time to time will also be charged. The fees/charges/Limits indicated here are as prevalent currently and are subject to revision by the Bank from time to time. Annual Fee/Renewal Fee will be collected in advance. First collection of the Annual fee will be starting of new financial Year (i.e. linking by the branch) and subsequent collections on the 1st day of the corresponding month of issue of each year.

GENERAL CONDITIONS:

The Cardholder shall undertake to furnish to the Issuer, changes, if any in respect of any information furnished in the application form within 7 days from the date of occurrence of such changes. The Issuer may take cognizance of such changes only after the expiry of 30 days from the date it duly receives the information.

All suits and proceedings against the Issuer relating to any claims, dispute or differences arising out of or in respect of the Card shall be instituted only in the courts situated in the city of Bangalore where the Head Office of the Issuer is situated and no court/forum situated in any other place shall have jurisdiction to entertain or decide such matters the Issuer may, however at its option institute any such suit or proceedings against the Cardholder at any place where the Cardholder resides or carries on business or works for gain or maintains his/ her/ its account with any branch of the Issuer.

The Issuer reserves their right to add to, delete from these Terms and Conditions as they think fit in their absolute discretion and without assigning any reason whatsoever and such changes shall be binding on the Cardholder.

Guideline Policy for General User

The debit card is valid for use in INDIA and member of NPCI Banks ATM only. The card is valid for a period of 5 years, valid from the date of issue till the last day of the month of expiry.
Verify whether your name is imprinted correctly on the face of the card. If not, take up the matter with your branch of issue.
Sign across signature panel at the back of your card, to prevent misuse of the card.
Collect the PIN mailer from the branch and ensure that the PIN number is not tampered. If any signs of tampering is found, immediately surrender the card & PIN to the branch of issue.
Protect your card and do not Give access to any one to have your card.

Bend or scratch the card as damage will be caused to the magnetic stripe on the reverse of the card which contains important information about the card.
Before due date the card will be automatically renewed and sent to your branch from whom you may collect and continue to use the card.
If you do not wish to renew the card, for any reason, the branch of issue has to be intimated at least 2 months in advance.
If the renewed card has not been received by you within the expiry date of the earlier card, please do take up with the branch immediately.

USAGE AT MERCHANT OUTLETS:
Sundarlal Sawji Bank Debit Cards affiliated to RUPAY are accepted at all Merchant Establishments displaying RUPAY Logo.
The Merchant should have an electronic (Point- of- sale) swipe terminal.
Usage is permitted up to Rs. 50,000 per day at Merchant locations say, Restaurants, Hospitals, Departmental Stores, Textile outlets, Jewelleries etc.
Present your debit card for payment of the purchase amount. The merchant will swipe the card in the point-of-sale machine for authorization. After a successful authorization, a charge slip is generated from the POS machine. Ensure for correctness of the amount and sign the charge slip exactly as appearing on the reverse of your card. Collect back your card and your copy of the charge slip.
Please retain the charge slip copy till you verify the amount as appearing in your bank statement of account.
There are certain exceptional cases where you may be billed extra service charges while making use of your Card with MEs such as Petrol Bunks, Railways, etc. Only if you agree to bear extra charges, you should proceed with the transaction. Such service charges together with the charge slip amount will be debited to your operative account.
Please note that since signature verification is essential for debit card transactions you need to be physically present along with your card at the time of purchase.
ATM:
Your DEBIT-CARD is linked with ATMs (Automated Teller Machines) for easy access to the cash, 24 hours a day. Your DEBIT CARD is accepted not only at Sundarlal Sawji Bank ATMs but also at all ATMs of other banks which are member with NPCI.
Instructions for operations in ATMs:
The ATM Cash Withdrawal limit is Rs. 25,000 per day. Please insert the card in the top right corner in the Card Insert slot. Then the machine will respond to you with the message “Enter your PIN No”.
Key in your PIN No. within 15 seconds and follow the instructions given on the screen.
IMPORTANT:
Please collect the card from the ATM and also the cash immediately; else the ATM will swallow the card/cash as the case may be.
Other services, offered at our ATMs are: (1) Cash withdrawal (2) Balance enquiry (3) Mini Statement (4) Request for cheque book (5) Statement request, (6) PIN change.

Note:
For any ATM operational assistance/clarifications contact the Branch Manager or the ATM officer in charge of ATM switch room.
Customer Care PHONE NO. 912241561111/22
DISPUTE:

As the transactions are debited on line, any dispute relating to a transaction should be reported to the branch of issue of card within 15 days from the date oftransaction. The branch in turn will take up with Card Division regarding the transaction disputed who will take steps for resolving the dispute.

SAFE CUSTODY:

Please preserve your valuable Sundarlal Sawji Bank DEBIT CARD carefully and do not let it fall into wrong hands.

Please check your wallet/pouch once in a while and ensure that your card is always safe.

Despite the above, if you lose your Sundarlal Sawji Bank DEBIT CARD, please inform the same to your Branch/Switch room your Name, Card Number & Validity so that the card can be hot listed.

Simultaneously, please lodge a police complaint immediately detailing the loss. A copy of the police complaint along with your detailed letter confirming the loss should be sent to the branch of issue within a week from the date of reporting the loss. Fresh letter of request should be given to the branch for issue of New DEBIT CARD.

Please avoid loss on account of someone misusing the lost/stolen card by promptly reporting the loss of the card for hot listing.

If you trace the lost card after reporting the card loss, please do not use it, since it will not be honored by the MEs (Merchant Establishment)/branches. Please destroy the card beyond use and confirm the Branch of issue of the card.

Terms and Condition:-

By accepting and/or using the card / signing on the reverse of the Debit Card the cardholder accepts the terms and conditions set out for Sundarlal Sawji Bank debit Card unconditionally and will be bound by them and accepts the onus of ensuring compliance with the relevant Reserve Bank of India (RBI) regulations, Exchange control Regulations, Foreign Exchange Management Act and any other corresponding enactment in force from time to time. The cardholder will also continue to remain bound by the terms and conditions of operations of his Savings Bank Account/ OD Accounts/Current Accounts with Sundarlal Sawji Bank.

These terms and conditions shall be known as “Sundarlal Sawji Bank Debit Card rules and shall have come into effect immediately.

FAQs For ATM
DEBIT/CREDIT CARDS

Automated Teller Machine (ATM)?

Automated Teller Machine is a computerized machine that provides the customers of banks the facility of accessing their accounts for dispensing cash and to carry out other financial transactions without the need of actually visiting a bank branch.

What Type Of Cards Can Be Used At An ATM?

The ATM cards/debit cards, credit cards and prepaid cards (that permit cash withdrawal) can be used at ATMs for various transactions.

What Are The Services / Facilities Available At ATMs?

In addition to cash dispensing ATMs may have many services / facilities such as:

- Account information
- Regular bills payment
- Purchase of Re-load Vouchers for Mobiles
- Mini/Short Statement

How Can One Transact At An ATM?

For transacting at an ATM, the customer insert (swipe) their card in the ATM and enter their Personal Identification Number (PIN).

Can These Cards Be Used At Any Bank ATM In The Country?

Yes. The cards issued by banks in India should be enabled for use at any bank ATM within India.

What Is A Personal Identification Number (PIN)?

PIN is the numeric password for use at the ATM. The PIN is separately mailed / handed over to the customer by the bank while issuing the card. This PIN has to be reset to a new PIN by the customer. Most banks force the customers to change the PIN on the first use. The PIN number should not be written the card, card holder etc as in such cases the card can be misused if card is lost / stolen.

What Should One Do If He Forgets PIN Or The Card Is Sucked In By The ATM?

The customer may contact the card issuing bank branch and apply for retrieval/issuance of a new card. This procedure is applicable even if the card is sucked in at another bank`s ATM.

What Should Be Done If The Card Is Lost / Stolen?

The customer may contact the card issuing Branch immediately on noticing the loss so as to enable the bank to block such cards.

Is There Any Minimum and Maximum Cash Withdrawal Limit per Day?

Yes, banks set limit for cash withdrawal by customers. The cash withdrawal limit for use at the ATM of the issuing bank is set by the bank during the issuance of the card. This limit is displayed at the respective ATM locations. For cash withdrawals at other bank ATMs, banks have decided to maintain a limit of Rs 10,000/- per transaction. This information is displayed at the ATM location.

Do Banks Levy Any Service Charge For Use Of Other Bank ATMs?

No charges are payable for using other banks` ATM for cash withdrawal and balance enquiry, as RBI has made it free under its "Free ATM access policy" since April 01, 2009. But banks can restrict the number of such free transactions to a maximum of five per month. For transactions beyond this minimum number of transaction, banks charge maximum of Rs 20/- + GST per transaction.

What Should Be Done In Case During The Cash Withdrawal Process, Cash Is Not Disbursed By The Account Gets Debited For The Amount?

The customer may lodge a complaint with the card issuing bank. This process is applicable even if the transaction was carried out at another banks ATM.

How Many Days Maximum Would The Bank Require To Re-Credit The Account For Such Wrong Debits?

As per the RBI instructions, banks may re-credit such wrongly debited amounts within a maximum period of 12 working days.

Is The Customers Eligible For Compensation For Delays Beyond 12 Working Days?

Yes. Effective from July 17, 2009, banks shall have to pay customers Rs 100/- per day for delays beyond 12 working days. This shall have to be credited to the account of the customer without any claim being made by the customer.

In Case The Compensation Is Not Credited As Mandated, What Recourse Does The Customer Have?

For all such complaints customer may lodge a complaint with the local Banking Ombudsman if the bank does not respond.

What is a SSUCBL Bank Debit Card?

A SSUCBL Bank Debit Card is a plastic card which provides access to ATMs for cash withdrawals, balance enquiries and mini statement. It also provides on-line electronic payment for purchases from your savings / current (individual) accounts.

What are the variants of SSUCBL Bank Debit Card?

Sawji Bank Debit Card – **Classic**

Whether Debit Cards can be issued in Joint accounts with operation condition "Jointly "?

Yes. The Debit Cards can be issued to 2 Signatories in Joint Accounts with operation condition jointly. Joint operation in ATMs using two cards with two distinct PINs, for withdrawal of cash, in case of Joint Accounts with operation condition "Jointly" and having only two joint holders, is available. However, such cards shall be issued at specific request of the Account Holder and shall be used only for Cash withdrawal in our bank ATM's only.

What is PIN (Personal Identification Number)?

- PIN is a unique 4 digit number that allows you to access your account through Debit Card at ATMs.
- Please keep your PIN safe.
- Please memorize the PIN.
- Do not write the same on any material which is accessible to unauthorized persons.
- Do not divulge the PIN to anybody, even to Banks' personnel.
- Do not keep the PIN and the Debit Card together.

How can I get a Debit Card?

Debit card can be obtained from the branch of SSUCBL Bank where you maintain the account by filling a Debit Card application form. In case of Non-Personalized card (without name) the card would be issued instantly. In case of personalized card (with name) the card would be issued within 7-8 working days

I have not received my personalized card even after 10 days of giving the request at the branch?

Please contact the branch. You will get an SMS on your registered mobile number on dispatch of the Card to your branch.

I have received the Debit Card but the PIN is not legible.

You should contact the card issuing branch and request for issue of replacement Card. Please destroy the old card. Bank will not preserve the PIN number and hence no reprint of the PIN is possible. PIN has to be generated afresh for the card. You can collect the replacement card & PIN from the branch after 15 working days.

Where my Debit card can be used?

Debit Card can be used on all the ATMs & merchant establishments displaying Visa/MasterCard/RuPay logo. You can also use your card for payments on the Internet. Debit card issued will be of Domestic validity. On specific request Debit cards with global validity will be issued.

How does the Debit Card work?

Insert your Debit card in ATM and follow the instructions displayed on the screen. On POS you need to swipe the card and sign the Bill after verifying the amount.

What is the validity of SSUCBL Bank Debit Card?

Validity of Debit cards are till the last day of the month shown under "valid thro' on the face of the card.

Are there any transaction limits for the Debit Card?

For SSUCBL Bank Debit Card – Classic the Cash Withdrawal at ATMs is limited to Rs 25,000 per day and for purchase transaction Rs. 50,000 per day

If Debit card is lost or misplaced what should I do?

Please call 02457-237699 / 912241561111 to get the card hot listed / blocked. Also inform the Branch where the card is issued, for blocking the card.

Now SSUCBL Bank Debit Card can be hot-listed / blocked by using Banks mobile Banking Application.

Is there any Fee for the issuance of Debit card?

Debit Card Cost:- 120 + GST (AMC will be free for First Year). An Annual Maintenance fee of Rs. 120 + GST is applicable for SSUCBL Bank Debit Cards - Standard from the second year onwards. Annual fee will be collected on last month of financial Year and every year till expiry of the card.

Is there any charge levied for use of the card for Cash withdrawal?

No charge is levied for use of the card for cash withdrawal at SSUCBL Bank ATMs. For cash withdrawals at other Bank ATMs, please refer to "Service Charges" Section in our Home Page.

Can a fresh Debit card be issued in lieu of lost/damaged card and what is the amount to be charged?

Cards damaged due to ware and tare will be replaced free of cost. Cards issued in replacement of lost card will be charged Rs. 80 + GST/-. However, hot listing charge of Rs. 120 + GST /- will be collected in all cases.

If lost card is subsequently found/traced and restored to cardholder, can it be reactivated?

Card once hot listed / blocked cannot be re-activated. You can make a request for issue of a fresh card.

What is Mini Statement?

It is a statement of account showing last 10 transactions made in the account.

How should I maintain the secrecy of PIN?

If at any time you feel that the PIN has been inadvertently or otherwise divulged to any one, you should change the PIN through any SSUCBL Bank ATM immediately.

How often can I change the PIN?

PIN can be changed any number of times.

How many accounts maximum can be linked to my Debit card?

Only one account can be linked to a Debit card.

Does Bank bear any liability for unauthorized use of the Card?

No. The responsibility is solely vested with the cardholder.

What is CVV No.?

On the back of Debit card (Classic) there are 7 digits out of which the last 3 digits are the card CVV no. This number can be used only for transactions on the Internet.

What is Add-On card facility?

There is no Add on Card facility for SSUCBL Bank Debit Cardholders.

Whether PAN is compulsory for applying for Debit card?

Yes. PAN is compulsory as per RBI guidelines. Wherever PAN is not available, form No. 60/61 as applicable has to be submitted.

Whether Debit card can be issued to joint accounts?

Debit card can be issued to joint accountholders where the operation condition is "severally".

My Debit card doesn't work successfully on ATMs?

Debit Card does not work successfully on ATMs due to any of the following reasons;

- You may be using the card before the expiry of 3 working days of receipt of the card from the branch, the time required for activation of the card.
- You may not have swiped the card properly. Try 2 to 3 times.
- The magnetic stripe of your card has been damaged / deteriorated due to which it is not accepted by any ATM where the card reader may be weak. In such a case you

may try at another nearby ATM and if still does not work, get it replaced by a new one from the Card issuing branch free of cost.

- Your account may be inoperative or frozen at branch level due to some reason. Please contact your branch to know the account status.
- You may be using wrong PIN.
- You might have selected the wrong account type i.e. savings instead of current or vice-versa.
- Connectivity from the ATM to your branch has failed. In such case please try after some time or use another ATM nearby.

My Debit card works successfully on SSUCBL Bank ATMs but not on other Bank's ATMs.

The problem may be due to connectivity failure at other bank ATM. Please try after some time when connectivity is restored. Alternately you may try another ATM nearby.

My Debit card works successfully on ATMs but not at POS terminals.

Debit card does not work successfully on POS terminals due to any of the following reasons;

- Connectivity failure at that particular time.
- Weak card reader of POS.
- Magnetic stripe of the card deteriorated / damaged.

You may use the card after some time when the connectivity is restored. Where the magnetic strip is damaged, you may obtain replacement card through your branch of issue, free of cost.

My card doesn't work on few ATMs of SSUCBL Bank.

The quality of the magnetic stripe of your card may be damaged / deteriorated due to which it is not accepted by few ATMs where the card reader may also be weak. Try at some other nearby ATM. In such case you may get the card replaced by a new one through your SSUCBL Bank branch, free of cost

What is the Insurance cover available for RuPay Debit card?

NPCI offers accident Insurance of Rs. **1 Lakh** for RuPay card. The Insurance is available till ATM card in service.

RTGS/NEFT Policy

Definitions

In these Terms and Conditions the following words and phrases have the meanings set opposite them unless the context indicates otherwise:

a) "**Account(s)**" refers to the Customer's bank account(s) maintained with Sundarlal Sawji Urban Co-op Bank Ltd., Jintur, to be used for operations through RTGS/NEFT, as specified in the RTGS/NEFT Fund transfer Form.

b) "**Business Day**" for the concerned branch of Sundarlal Sawji Urban Co-op Bank Ltd., Jintur shall mean a day other than:

1. Weekly offs, and any public holiday
2. A day on which the concerned branch of Sundarlal Sawji Urban Co-op Bank Ltd., Jintur is closed and cannot conduct regular banking business for / with its customers
3. A day on which RBI does not provide RTGS/NEFT, or
4. A day on which normal business cannot be transacted due to storms, floods, bandhs, strikes etc. or any circumstances beyond the control of Sundarlal Sawji Urban Co-op Bank Ltd., Jintur.

c) "**Customer**" means the applicant / remitter availing of RTGS/NEFT.

d) "**SSUCB**" means Sundarlal Sawji Urban Co-op Bank Ltd., Jintur Limited, a company incorporated under the Co-Operative Act, 1960 and having its registered office at Jintur, Maharashtra – 431 509 (which expression shall, unless it be repugnant to the subject or context thereof, include its successors and assigns).

e) "**SSUCBRTGS/NEFT**" Facility has taken under sub membership of Saraswat Co-operative Bank Ltd., Mumbai and RTGS/NEFT facility offered to Customers.

f) "**RBI**" means the Reserve Bank of India.

g) "**Regulations**" shall include RTGS (Membership) Business Operating Guidelines, 2004 and RTGS (Membership) Regulations, 2004.

h) "**RTGS/NEFT**" means the Real Time Gross Settlement System and Net Electronic Fund Transfer of RBI. Words or expressions used in these Terms and Conditions, but not specifically defined herein shall have the respective meanings assigned to them by Sundarlal Sawji Urban Co-op Bank Ltd., Jintur or RBI from time to time.

i) "RTGS (Membership) Business Operating Guidelines, 2004" shall mean the Real Time Gross Settlement System Business Operating Guidelines, 2004 issued by RBI, as may be amended or modified from time to time.

j) "RTGS (Membership) Regulations, 2004" shall mean the Real Time Gross Settlement System (Membership) Regulations, 2004 issued by RBI, as may be amended or modified from time to time.

k) "**NEFT**" means the National Electronic Fund Transfer of RBI

l) "**RTGS/NEFT Fund Transfer Application**" means an unconditional instruction issued by the Customer in writing to Sundarlal Sawji Urban Co-op Bank Ltd., Jintur, in form, manner and substance as Sundarlal Sawji Urban Co-op Bank Ltd., Jintur may prescribe or require, to effect a funds transfer for a certain sum of money expressed in Indian rupees, to the designated account of a designated beneficiary in India with a scheduled bank, that shall be effected by debiting the Account of the Customer.

Applicability of Terms

To avail / use the Sundarlal Sawji Urban Co-op Bank Ltd., Jintur RTGS/NEFT Facility a Customer shall submit to SSUCB a RTGS/NEFT Form with appropriate instruction. SSUCB shall be entitled, at its sole discretion, to accept and process or reject such RTGS/NEFTFunds Transfer Application.

The Terms and Conditions shall be in addition to and not in derogation of the regulations, circulars, orders, notifications, press releases, instructions issued by RBI from time to time, including the RTGS (Membership) Business Operating Guidelines, 2004 and the RTGS (Membership) Regulations, 2004, (hereinafter collectively referred to as the "Regulations") and any practices and / or policies followed by SSUCB from time to time (hereinafter referred to as "SSUCB Practices"). The Customer hereby acknowledges that the Customer has read and understood the Regulations and is aware of SSUCB Practices and / or shall make himself aware of the SSUCB Practices and agrees that the rights and obligations provided therein and in these Terms and Conditions in so far as it relates to the Customer shall be binding on him / it with regard to every RTGS/NEFT Fund transfer Application issued by him / it.

The Customer understands and agrees that availing the SSUCB RTGS/NEFT Facility shall not be construed as creating any contractual or other rights with or against RBI or any other participant in the RTGS/NEFT other than SSUCB.

SSUCB shall have no obligations to any person including any beneficiary (or any person claiming under or through such beneficiary) other than the Customer, for the execution of any RTGS/NEFT Funds Transfer Application. All obligations of SSUCB to the Customer in relation to any RTGS/NEFT Fund Transfer Application shall cease upon the execution of the RTGS/NEFTFundsTransferApplicationNot withstanding anything contained herein, all terms and conditions stipulated by SSUCB in connection with the Accounts shall continue to apply.

Scope of RTGS

RTGS is a payment system in which both processing and final settlement of fund transfer instructions happen real time. It is a gross settlement system where transfers are settled individually, i.e. without netting debits against credits. RTGS effects final settlement continuously rather than periodically and the settlements are immediate, final and irrevocable.

Scope of NEFT

National Electronic Fund Transfer **(NEFT)** application is built on Structured Financial Messaging System SFMS).The transactions in NEFT are settled in batches. Any transaction initiated after a designated settlement time would have to wait till the next designated settlement time. Contrary to this, in RTGS, transactions are processed continuously throughout the RTGS business hours.

Rights and Obligations of the Customer

The Customer shall be entitled, subject to the Regulations and the terms and conditions herein or as may be modified from time to time.Customer should submit RTGS/NEFT fund transfer application toavail RTGS/NEFT facility, which is complete in all particulars. The Customer shall be responsible for the accuracy of the particulars given in the RTGS/NEFT fund transfer application and shall be liable and responsible for any loss or damage arising on account of any error in the RTGS/NEFTFunds Transfer Application.

The Customer shall ensure availability of funds in the Account(s) towards the fulfillment of the fund transfer Application before / at the time of the submission of the RTGS/NEFT fund transfer Application by SSUCB as also for the payment of applicable fees and / or charges.

In case SSUCB, at its discretion, executes the Fund transfer Application without necessary funds being available in the Account for payment of fees and / or charges payable to SSUCB for providing access to or allowing the use of the SSUCB RTGS Facility for which SSUCB may extend a temporary loan / overdraft for the amount of such fees / charges which have not been paid or which is unavailable in the Account (hereinafter referred to as "Temporary Overdraft"), that the Customer shall pay / repay forthwith and in any case not later than the end of that Business Day. SSUCB shall be entitled to charge interest on the Temporary Overdraft at rates determined by SSUCB from time to time, for the period during which the Temporary Overdraft is outstanding. If the Customer does not repay to SSUCB the Temporary Overdraft with such interest as has accrued on it, before the end of that Business Day, SSUCBshall be entitled to charge further interest on such unpaid amounts at rates determined by SSUCB from time to time (hereinafter referred to as "Further Interest").

Notwithstanding the above, the Customer agrees that SSUCB shall be entitled, at all times, to debit, any and all of, the balances standing at any time to the credit of the Account (or other accounts of the Customer with SSUCB), for the payment of the fees and / or charges payable to SSUCB for providing

access to or allowing the use of the SSUCB RTGS/NEFT Facility and / or for repayment of the Temporary Overdraft and any interest (including Further Interest) payable on the Temporary Overdraft.

The Customer agrees that the fees and / or charges payable to SSUCB for providing access to or allowing the use of the SSUCB RTGS/NEFT Facility and the interest (including Further Interest) payable by the Customer on the Temporary Overdraft are reasonable.
The Customer agrees that the RTGS/NEFT fund transfer Application shall become irrevocable when such instructions have been executed and / or are in the RTGS for execution, and the revocation of such instruction is not possible.

a) Subject to the provision of sub clause (b) below, the Customer agrees that SSUCB shall be liable to the Customer, only in the event of any error in the execution of the instructions pursuant to a fund transfer arising on account of gross negligence or willful misconduct of SSUCB. In such an event, SSUCB's liability shall be limited to the refund of the excess amounts (if any) erroneously paid or reversal of the transaction if possible and practical, so to do and / or refund of any fees and / or charges which have been paid to SSUCB in relation to the Fund Transfer executed. In the event of a fund not having been fully effected (i.e. there being a deficiency or shortfall in the amount to be actually remitted / transferred) SSUCB's obligation and liability shall be limited to remitting / transferring such deficient amounts or amounts in shortfall, upon the same being brought to its notice and subject to availability of funds in the Account.
b) The Customer shall forthwith report to SSUCB any discrepancy in the execution of a fund transfer by SSUCB. The Customer agrees that, in any event, he / it shall not be entitled to dispute the correctness of the execution of the fund transfer or the amount debited to his Account.

SSUCB shall have the sole discretion to decide on the cut-off time for transmitting the settlement instructions. Fund transfer Application received after cut-off time will be completed on the next Business Day. Such cut – off time shall be notified to the Customers on Timings section of the website.The Customer agrees that it is aware that there is a risk of non-payment to the beneficiary on the day of the transaction. The same may be for any reason whatsoever, including a holiday at the beneficiary's branch. SSUCB or RBI or any other participant in the RTGS/NEFT shall not be liable, in any manner whatsoever, to the Customer for any such delay.

SSUCB shall have the sole discretion to decide on the cut-off time for transmitting the settlement instructions. Fund transfer Application received after cut-off time will be completed on the next Business Day. Such cut – off time shall be notified to the Customers on Timings

section of the website.The Customer agrees that it is aware that there is a risk of non-payment to the beneficiary on the day of the transaction. The same may be for any reason whatsoever, including a holiday at the beneficiary's branch. SSUCB or RBI or any other participant in the RTGS/NEFT shall not be liable, in any manner whatsoever, to the Customer for any such delay.

Rights and obligations of Sundarlal Sawji Urban Co-op Bank Ltd., Jintur

Sundarlal Sawji Urban Co-op Bank Ltd., Jintur shall endeavor to duly execute a fund transfer issued and authorized by the Customer, except when:

1) The funds available in the Account are not adequate or funds are not properly applicable / available to comply with the fund transfer and / or the payment of any fees and / or charges as applicable and the Customer has not made any other arrangement to meet its payment obligations in relation to the fund transfer and / or the any fees and / or charges as applicable.
2) The fund transfer is incomplete or it is not issued in the agreed form or when the RTGS/NEFT fund transfer Application has been filled in wrongly or has been received in advance of the date as specified in the RTGS/NEFT Funds Transfer Application.
3) The SSUCBwill display attached with notice of any special condition.

An acknowledgement of receipt of a RTGS/NEFT fund transfer shall not be construed as binding SSUCB to execute the same, other than in terms of these Terms and Conditions and the right reserved by SSUCB to reject or refuse the carrying on of any RTGS/NEFT Funds Transfer Application. The Customer agrees that no prior or written intimation or notice ofsuch refusal or rejection needs to be provided by SSUCB.

Feesand / or Charges SSUCB may levy fees and / or charges for use of SSUCB RTGS/NEFT Facility which will be notified by SSUCB to the customer from time to time. Any change in the fees and / or charges will be notified to the Customer by hosting the same on Fees Section of the website. The charges as above shall be in addition to any charges which RBI may levy on any given transaction.

Sharing of Information

The Customer irrevocably and unconditionally authorizes SSUCB to access all the Customer's Accounts and records for the purpose of providing the SSUCB RTGS/NEFT Facility. The Customer agrees that SSUCB may hold and process its personal information and all other information concerning fund transfer and / or its Account(s) on computer or otherwise in connection with the SSUCB RTGS/NEFT Facility as well as for analysis, credit scoring and marketing

RTGS Funds Transfer Application/Form

The Customer agrees and understands that the RTGS/NEFT fund transfer form is not negotiable instrument. It is merely an instruction to SSUCB to debit the Account and credit the beneficiary's account using RTGS. The Customer agrees and acknowledges that SSUCB has not made any representations to the Customer that the RTGS/NEFT fund transfer form is a negotiable instrument. The Customer agrees that SSUCB shall have no obligations to any person including any beneficiary (or any person claiming under or through such beneficiary) other than the Customer, for the execution of a RTGS/NEFT Funds Transfer Application.

The Customer agrees that instructions for making payments through the RTGS shall be accepted only in the form of an RTGS Funds Transfer Application/form. If subsequently SSUCB allows payment instructions to be made in any other mode and the Customer wants to avail of such modes, the Customer agrees to abide by such terms and conditions as SSUCB may stipulate for such modes.

The Customer also agrees to enter into, make, sign, execute, deliver, acknowledge and perform any agreement, deed, writing or thing that may in the opinion of SSUCB be necessary, proper and expedient for the aforesaid purpose.

Disclaimer of Liability

1. The user represents that he has read and understood the contents of Disclaimer, Privacy Policy and online security tips available on the Sundarlal Sawji Bank's website.
2. Sundarlal Sawji Bank shall not be liable for any incomplete information provided by the User while transferring funds through online NEFT/RTGS using Sundarlal Sawji Bank.
3. The instructions issued for online fund transfer under NEFT/RTGS facility shall be irrevocable and the User understands that he/ she shall not be entitled to revoke / cancel the same under any circumstances.
4. The User shall be solely liable and responsible for the correctness of all information pertaining to the Beneficiary and the Transaction. The User acknowledges that Sundarlal Sawji Bank shall not be in a position to verify such information regarding the Beneficiary.
5. The transfer to RBI for NEFT will be done on the date of instruction or on the next working day.
6. The actual time taken to credit the Beneficiary account depends on the time taken by the Beneficiary's Bank to process the payment for which Sundarlal Sawji Bank does not take any responsibility.
7. In case of any return/ rejection of funds transferred, the same will be restored back to the account originally debited. However, the user confirms that any delay in receiving the credit upon such return/ rejection Sundarlal Sawji Bank shall not be liable to pay any compensation nor that will be deficiency of service.

8. The Customer hereby confirms that he/she shall not hold Sundarlal Sawji Bank liable or responsible for delays/deficiencies in settlement of the Transaction due to system constraints, actions of other parties or any other circumstances beyond the control of Sundarlal Sawji Bank.

Illegal or improper use of the SSUCB RTGS/NEFT Facility shall render the Customer liable for payment of pecuniary charges or penalties which SSUCB may at its sole discretion decide or may result in suspension of the SSUCB RTGS/NEFT Facility to the Customer. The Customer hereby also agrees to fully indemnify and hold SSUCB and its subsidiaries and affiliates harmless against any action, suit, proceeding initiated against it or any loss, cost or damage incurred by it as a result thereof.

All the records (including electronic) of SSUCB generated by the transactions arising out of the use of the SSUCB RTGS/NEFT Facility, including the time the transaction recorded shall be conclusive proof of the genuineness and accuracy of the transaction. For the protection of both the parties, and as a tool to correct misunderstandings, the Customer understands, agrees and authorises SSUCB, at its discretion, and without further prior notice to the Customer, to monitor and record any or all telephone conversations (if any) between the Customer and SSUCB and any of its employees or agents or instruction provided by theCustomer to SSUCB.

SSUCB expressly disclaims all warranties of any kind, whether express or implied or statutory, including, but not limited to the implied warranties of merchantability, fitness for a particular purpose, data accuracy and completeness, and any warranties relating to non-infringement in the SSUCB RTGS Facility.

Indemnity

The Customer agrees, at its own expense, to indemnify, defend and hold harmless SSUCB, its subsidiaries and affiliates, and any of their directors and employees, representatives and / or agents against any claim, suit, action or other proceeding brought against them by a third party, to the extent that such claim, suit, action of other proceeding brought against such person is based on or arises in connection with any action of the Customer, including but not limited to:

1) A violation of the Terms and Conditions by the Customer.
2) Any use of the SSUCB RTGS Facility by the Customer.
3) Any misrepresentation or breach of representation or warranty made by the Customer contained herein.
4) Any breach of any covenant or obligation to be performed by the Customer hereunder.

The Customer agrees to pay any and all costs, damages and expenses, including, but not limited to, attorneys' fees and costs awarded against it or otherwise incurred by or in connection with or arising from any such claim, suit, and action or proceeding attributable to any such claim.

The Customer hereby agrees that under all circumstances, SSUCB's aggregate liability for claims relating to the SSUCB RTGS/NEFT Facility, whether for breach or in tort shall be limited to the transaction charges / fees or consideration paid by the client within the previous twelve (12) months for the service, excluding any amount paid towards transactions.

General Conditions

The laws of India shall govern these terms and conditions and/or the operations in the Account(s) maintained by SSUCB. Any legal action or proceedings arising out of these Terms and Conditions or in relation to the SSUCB RTGS/NEFT Facility shall be brought in the courts or tribunals at Jintur in Maharashtra. SSUCB may, however, in their absolute discretion commence any legal action or proceedings arising out of these Terms in any other court, tribunal or other appropriate forum, and the Customer hereby consents to that jurisdiction.

The clause headings in these Terms and Conditions are only for convenience and do not affect the meaning of the relative clause.

SSUCB may sub-contract and employ agents to carry out any of its obligations hereunder.

Any provision of these Terms and Conditions, which is prohibited or unenforceable in any jurisdiction, shall, as to such jurisdiction, be ineffective to the extent of prohibition or unenforceability but shall not invalidate the remaining provisions of these Terms and Conditions or affect such provision in any other jurisdiction. SSUCB shall have the right of set-off and lien, irrespective of any other lien or charge, present as well as future on the deposits held in the Account to the extent of all outstanding dues, whatsoever, arising as a result of the SSUCB RTGS/NEFT Facility extended to and/or used by the Customer.

MOBILE BANKING POLICY

1. Introduction

SUNDARLALJI SAWJEE URBAN CO-OPERATIVE BANK LTD Founded in **1965** is serving for its customers on various channels. Being top bank in Co-Operative section, BANK is providing its customers advance services and features. BANK has already launched its Internet Banking for customer and ready to move ahead on the next generation services of Mobile Banking.

In the age of electronic and mobile devices banking sector has shown a tremendous growth. BANK has also taken various initiatives in order to keep in competition with growing banks. National Payment Corporation of India (NPCI) has developed Mobile Banking program for the Banks.

BANK has completed all necessary steps with NPCI and we have done the soft launch for IMPS i.e. funds transfer with mobile device person to person (P2P) and person to account (P2A) andMerchant payment. With merchant payment module customers can pay the merchant via mobile device.

We are providing following services under mobile banking,

- Balance Enquiry
- Mini Statement
- IMPS-Funds transfer (Interbank & Intra Bank)
- Cheque book request
- Cheque status request
- Stop cheque request
- Email Statement request
- Physical statement request
- Account addition request
- ATM Pin re-generation Request

The application is developed in JAVA, Android, Blackberry phones and testing is in process for the same and expected to complete the development for other OS e.g. Apple Mobile banking application in this week. Apart from the above we can incorporate the use cases for financial Inclusion in Mobile Banking Application.

The term "**Application Owner**" is referred to BANK Development Department and BANK Alternate Channels Department.

2. Definitions:

In this document the following words and phrases shall have the meanings as set below unless the context indicates otherwise:

"**Account(s)"** shall mean any one or more accounts held and/or facilities provided to the Customer by Bank including but not limited to savings accounts, current accounts, term deposits or such other accounts and/or facilities as may be determined by Bank from time to time, for which the Facility is being offered or may be offered in future.

"**Alert(s)**" means the customized messages sent to the Mobile Phone Number as an SMS in response to the triggers set by the customer.

"**Customer**" shall mean a customer of BANK or any person who has applied for any product/service of BANK.

"**Sundarlal Sawji Urban Co-Op. Bank Ltd., Jintur**" refers to APMC Market Yard, Yeldari road, Jintur Dist .Parbhani 431509, registered under the Bombay Co-operative Societies Act, 1925 and deemed to be registered under the Maharashtra Co-operative Societies Act, 1960 and Multi State Co-operative Societies Act, 2002 and [licensed] as a bank under the Banking Regulation Act, 1949 and having its registered office APMC Market Yard, Yeldari road, Jintur Dist .Parbhani 431509 and corporateAPMC Market Yard, Yeldari road, Jintur Dist .Parbhani 431509

"**MBS**" shall mean Mobile Banking Service of the Bank and includes the service over the application/USSD/WAP/SMS Banking

"**Mobile Banking**" refers to the internet banking service offered or provided by **bank**to the User and which are described in the Terms by which the User may access information and give Name Bank instructions in respect of certain of User's Account(s) with the name Bank. Such Mobile Banking may be provided by bank directly or through its associates or contracted service providers or Affiliate.

"Mobile Banking app" shall mean the mobile banking application which can be installed on the mobile phone handset to access information pertaining to the Account(s).

"**User**" refers to a customer of bank and/or of the Affiliate of **Sundarlal Sawji Urban Co-Op. Bank Ltd., Jintur**, authorised to use Mobile Banking or a person requesting the Mobile Banking services. In case of the User being a minor, the guardian of such minor shall be permitted to use Internet Banking.

"**Personal Information**" refers to the information provided by the User to Bank.

"**SMS**" shall mean Short Messaging Service, which is the transmission of short text messages to and from SMS enabled devices including but not limited to mobile phones.

"**Service**" or "**Facility**" shall mean mobile banking facility (which provides the Customers, services such as information relating to Account(s), details about transactions and such other services as may be provided on the Mobile Phone Number by BANK, from time to time.

Other abbreviations used:

RBI -- Reserve Bank of India

NEFT - National Electronic Funds Transfer

RTGS - Real Time Gross Settlement

IMPS - Immediate Payment Service

MPIN – Mobile Banking Personal Identification Number

OTP - One Time Password

FD – Fixed Deposit

3. Objective:-

To achieve safe, sound and resilient mobile banking network and cash flow biding with the technological standards mentioned as per RBI and ITA 2000 and ITAA and other governing laws

Intended Audience

The Policy is formulated for Bank and or the Banking cell taking in or working for the mobile banking related services

4. Scope:

The scope of the policy is to maintain the Confidentiality, integrity, authenticity and non-reputability while performing mobile banking transactions.

5. Compliance

Mobile Banking Service offered by BANK would be in line with following,

- Mobile Banking guidelines Issued by RBI
- Regulations based on jurisdiction as may be modified from time to time
- Any governing provisions of other laws including Information Technology Act 2000, however, 2008 and amended 2011 ISO 270000 documents

6. Service provided under Mobile Banking

BANK would provide following services to Mobile Banking users

- **Non – Financial**
- BalanceEnquiry
- Mini Statement (last 5transactions)
- ChequeStatus

i) Cheque Book request
ii) Stop Cheque request
iii) Cheque Status request

- Fixed DepositInquiry
- Change login / transactionpasswords
- Manage Payee (registration ofbeneficiary)
- Demat balanceinquiry
- Demat Statement (last 3transactions)
- StatementRequest

i) Email Statement request
ii) Physical Statement request

- Addition of Account request
- ATM PIN re-generation request

- **Financial**
- **Funds Transfer (within Bank)**

1. P2P (Person 2 Person) – funds transfer to mobile number
2. P2A (Person 2 Account) – funds transfer to account number
3. P2M (Person 2 Merchant) – Merchant payments
4. Self-Linked Accounts
5. Third Party Transfer
6. Utility Bill Payment,
7. Stop Payment of Cheques,
8. Railway reservation

- **Immediate Payment Service (IMPS)**
- Through MMID (Mobile Money Identifier – P2P)
- Through IFSC (Account Number – P2A)
- Generate / Retrieve / Cancel MMID
- Manage Beneficiary

Bank to offer Mobile Banking facility to the customer subject to a daily cap of Rs.1,00,000/- per customer for both fund transfer and transaction involving purchase of goods.

7. Mobile Banking Roles and responsibilities

Operations Team: This team is responsible for managing SwiftCore related changes with respective of customer, Reconciliation, Dispute Management

Admin Team: This team is responsible of admin operations such as Registration, MPIN generation, Account addition; generate reports, print transaction password, NPCI Coordination etc.

- **Internal User**

Mobile Banking back office is handled centrally at HO by Mobile Banking Admin staff. There would be separate user IDs created for each user. A grand user named Super Admin shall have access to create and delete/suspend admin users.

Admins are divided into two groups as Maker Admin and Checker Admin. Maker Admin shall enter any request of enter data into the portal and Checker Admin shall verify everything entered by Maker Admin.

- **Registration**

Mobile Banking Service is given to the customers under following schemes,

Account type	Account Operation	Scheme Type
SB	Self	All SB schemes except minor
	Either or survivor (first holder)	
	Former or survivor (first holder)	
	Any one (first holder)	
CA	Proprietor	All CA schemes

Mobile registration for additional accounts will be done for those accounts which are having account type as defined in above table and which are listed under same customer ID.

- **Password**

Each user of Mobile Banking application will be allotted three types of password,

- MPIN: This is a 4 digit password used in order to log into the Mobile Banking Application and used under some requests such as generate OTP etc.
- Transaction Password: This is an alpha numeric password with 6-8 characters used for funds transfer (Inter Bank & Intra Bank)
- OTP: This is a 6 digit one-time password (one hour expiry) used for SMS based transactions as well for making merchant payments
- MMID: This is not a password but a 7 digit number assigned to an account in order to receive funds from other parties.

- **Transaction Password printing**

  After successful registration a hard copy of transaction password is generated for each user.
  Transaction Password will be printed by a user who authorizes records
  This password is then be stuffed into envelops and sent to respective branch through internal Currier.

- **Funds transfer**

  With Mobile Banking application users can send i.e. remit funds from their account to either another mobile i.e. P2P (Person 2 Person) or another account i.e. P2A (Person to Account) or another merchant for merchant payments i.e. P2M (Person 2 Merchant). Users can remit funds either by Mobile Banking application (JAVA, Android, iOS, Windows) or by WAP (Wireless access Protocol) i.e. with the use of Internet connection on mobile or by SMS. Each of these types are associated with limits as follows,

- For Application and WAP: Daily limit is INR 50,000 and calendar month limit is INR 250,000
- For SMS based: Daily limit is INR 1,000 and calendar month limit is INR 5,000
- Beneficiary Limit-NO LIMIT

- **Service Cancellation**

  The customer may request for cancellation of the Mobile Banking account any time by giving a written notice to home branch. The cancellation shall take effect on the completion of the process at Mobile Banking Cell.
  The customer will remain responsible for any transactions made through Mobile Banking until the time of such termination.
  The BANK will suspend the Mobile Banking account access anytime either entirely or with reference to a specific service or customer in following cases

- In case of breach of Terms by the customer.
- If it learns of the death, bankruptcy or lack of legal capacity of the customer, then the main account at the branch is closed which automatically closes the Mobile Banking account through legal advice.

  Service will also get cancelled or suspended if user deletes/cancels all the MMID associated with mobile number (this is an online request can be given using Mobile Banking application or SMS)

- **Cheque book request**

  Customers can give cheque book request via Mobile Banking Application/SMS. Only one cheque book request is accepted in a month.
  Cheque book requests are to be given to Admin department for further processing with 10 pages personalized cheque book for Saving account and 50 pages personalized cheque book for Current account.
  Cheque book charges are debited to customer account as required and as per the current Bank policy
  MB cell shall demand cheque book inventory from Admin department as required

- **Cheque Book return**

  If cheque books are not delivered to customers and if returned then Admin department should contact customer for resending the cheque book
  Admin department will call customer/branch and ask customer to collect the same from admin department

After 90 days cheque book will be destroyed.

- **Account addition**

  The mobile banking users can add accounts having account similar to registered account. For e.g.saving and current having operation as per registration policy.
  By using account addition request user can add multiple accounts listed under users customer id registered for Mobile Banking.

  The following should be enforced for customer accounts:

- The application should enforce minimum password length of 6 characters and maximum length of 8.
- System should not display the password as it is keyed in.
- Passwords should be alpha numeric combination.
- Application should enforce account lockout. Account lockout configured for 3 failed login attempts.
- Application should force new customer to change the password at first login as well as every fresh login.

- **Charges for request**

  For Mobile Banking Requests bank should recover charges from customers in following cases
  There are no additional charges apply to customers for availing Mobile Banking facility for 1st year. All the charges for physical statement, stop cheque, ATM pin re-generation will apply as per the current branch policy.
  Annual Maintenance Charges after 1st year: Rs. 100 proposed

- **Data Security**

  Adequate controls should be implemented to ensure confidentiality and integrity of data. 128-bit SSL should be enabled on the Mobile Banking Server to encrypt customer login and transaction details. Following types of areas must be monitored daily,

- Unauthorized user accessing information
- Loss of Data integrity
- Transaction flow

- **Security testing**

  Application should be tested for compliance with security policy before deployment. This includes following areas,

  - Testing needs to be done whenever there is a major application change including version upgrade
  - All vulnerabilities should be discovered and identified during the testing and fixed before application is deployed in production environment.
  - Mobile Banking structure is subjected to periodic Black Box penetration testing and Vulnerability Assessment

- **Audit Logs**

  A tracking in the Mobile Banking portal for each user is to be in place to capture latest changes done by users. If any users perform any action i.e. generate MPIN or modify customer data then those users details are captured for the audit purpose

- **Customer Account Security**

All new Mobile Banking customer accounts shall be created only after offline verification of credentials. Customer should not have the provision to create new account on mobile.

No one including the Bank employees should have access to the customer's Mobile Banking password while it is being generated and distributed.

Transaction password should be securely dispatched to the customer on a separate PIN mailer.

Customer should be informed about security measures to be adhered for secure Mobile Banking in the following areas

- MPIN
- Transaction password

These guidelines should be communicated to the customers either along with the password or by publishing user manual guide for customer or by publishing on the Mobile Banking web site (http://www.bank.com/mobile). Application owner is responsible for updating these guide lines based on new threats**.**

A) Server Security

The Mobile Banking application services should be protected by a firewall.Based on the risk levels the servers and external connections should be segregated across multiple segments.

The firewall can have the following segments:

- Web Server
- Application Server
- Database Server

The system admin team in consultation with the product head should design the firewall segments and rule base.

The fire wall should limit access to essential IP-Address/Ports.

There should be no direct dial up access to any of the Mobile Banking service. If dial up access needs to be provided, the dial up server should be separated from the mobile banking servers by a fire wall.

B) Redundancy

Adequate redundancy should be built into the network links

C) Anti-virus

Anti-virus software should be installed on all machines with risk of virus infection**.**

- ***Backup***

A) Backup process

Backups should be taken regularly to ensure that the data could be recovered when required as per the Information Security Policy of the Bank.

The application owner should identify the essential components that need to be backed up including the following:

- OS and application files
- Configuration files
- Data files
- Logs

o Web server logs

o Oracle Database server logs

B) Backup scheduling

Backup should be scheduled during non-peak usage hours.
Backup should take before and soon after any change in the application environment including application hardware upgrade.
The application owner should take into account the following parameters when deciding the type of backup, frequency of the backup and the type of media:

- Volume of transaction
- Criticality of data
- Recovery time constraints

Retention period is required for determining the rotation cycle for back up media and also for deciding on erasing old data for creating free disk space. This retention period is defined as per the standard Policy document of BANK

C) Security of Data on the Backup Media

Back up should protect as per the information security policy of the Bank. Attention is invited in particulars to the following areas:

- Prevention of unauthorized access to backup media
- Offsite storage and maintenance of appropriate environmental conditions
- Secure disposal of backup media
- Recovery testing of backup media

D) Migration Of Backup Data

If there is a change in business application software or application used for taking backup ,all previously backed up data that needs to be retained should be migrated to a format that is readable by the new application. If there is a change in backup media, all previously backed up data that needs to be retained should be transferred to the new media.

- ***Monitoring***

A) Log monitoring

- Date and time on all Core Banking Servers at Data Center should be set correctly to Indian Standard Time.
- OS database and application logs of the servers at Data Center should be monitored on daily basis.
- Automated tools should be used for analyzing the logs. System Admin team should identify and document all events that need to be tracked in the logs. The logs should be analyzed for events that would affect the security of the system including the following:

o Account created/deleted/disabled
o Password change for privileged account
o Start and stop of service
o Authentication failures
o System error or failures

- Change in configuration settings including file permissions or user privileges

  Application owner should nominate a team responsible for analyzing the log files and taking actions.Application owner should ensure that the same person whose activities are getting logged does not do log analysis .There should be separation of duties to ensure the independence.
  The security team should generate log report quarterly detailing security incidents observed in the logs and the action taken. This report should submit to the product head.

B) Security Monitoring

Network based IDS should be setup to monitor all access to Mobile Banking Service. Application owner should nominate a team responsible for analyzing and reporting on attacks detected by IDS.

The team responsible for IDS monitoring should generate weekly report on attacks detected and action taken. This report should be submitted to the application owner.

- ***Physical Security***

Centralized IT assets of Mobile Banking should be hosted in Data Center. Data center should have Physical protection as per the Information Security Policy of the Bank.
The Bank has assured that sensitive customer data, and security and integrity of transactions areprotected. And also taking necessary steps/actions for the mobile banking servers at the bank's end or at the mobile banking service provider's etc. and the Bank has followed ISO Standards and implementing as per Information Technology Act,

Application Owner should implement adequate physical security of IT assets related to Mobile Banking located outside the Data Center as per the physical security policy of the Bank.
The physical security measures should include-

- Physical access control with Identification and Authorization checks
- Redundancy in the power supply
- Environmental protection against temperature,fire,humidity,water,dust
- External recognized penetration testers in accordance with Security policy should test all security infrastructures periodically.
- In addition, banks should conduct regular information security audits on the mobile banking systems to ensure complete security.

- ***Incident Management***

An incident is a violation of an explicit or implied security policy.
The following actions can be classified as incidents:

- Abnormal system resource usage-If the Mobile memory utilization on a system is very high, the system could have been compromised. Attackers used compromised system for spreading viruses or attacking other Mobile leading to high resource utilization .system administrators need to track resource utilization and analyze reason for any abnormal usage.

- Users experience slow response- End user could experience slow response times if the application servers or the network has been compromised and is being used for malicious purpose. Virus or worm outbreak could lead to network congestion that would in turn cause application response to be slow and unstable .End users should report any drastic drop application response or system stability to system administrators.
- Data Corruption- Unauthorized modification or deletion of data or in ability to retrieve data in correct format ,web defacement
- Changes in user passwords – user should report to system administrator if they are not able to access the application with their passwords any authorized changes in user passwords; addition/ deletion of user accounts could be indication of system compromise.
- Traffic on non-essential ports - if there is network traffic on ports that are not used by any of the internal application this could be sign of a back door application in the network. The traffic should be tracked and reported by a monitoring team. If the backdoor application tries to traverse the firewall, the fire wall logs would track these.
- Attempts to gain unauthorized access – successful/unsuccessful attempts to gain access to the IT system and application supporting the Mobile Banking Application
- Unwanted disruption or denial of service – changes to the system hardware, firmware software characteristics without the application owner's knowledge .
- All internal users and system administrators of Mobile Banking should be responsible for identifying and reporting incidents. The system administrator should do a preliminary analysis to ascertain the cause and extent of damage.
- An incident report should be sent to the appropriate authorities in the Bank in the format laid down by the Bank's information Security Policy.

The bank may acquire necessary tools and systems for attacks.
The overall Information System Security Policy as applicable would govern the selection of the tools and systems. The policy will be reviewed by the application owner every year or at the time of any major changes in the existing environment, which would affect the areas, covered in this policy.

- ***Reporting***

The Mobile Banking System or The Mobile Banking Department should generate sufficient reporting to satisfy daily monitoring and control of transactions and activities. Additionally appropriate reports should be generated that provide the necessary information to track the effectiveness of the program. The Mobile Banking coordinator will report Mobile Banking activities to the executive committee on a quarterly or as needed basis.

- ***Internal Audit and compliance***

The internal Auditor and compliance officer will conduct a review of Mobile Banking on a quarterly basis. A report will be rendered to the Audit Committee.

- ***Internal Audit and compliance***

All financial product and services contain an element of risk, making effective risk management essential. Risk management is comprised of several factors:

- Identifying the risk
- Understanding the implication of the risk
- Measurement of the risk
- Setting acceptable risk tolerances and parameters
- Maintaining risk at acceptable levels

8. Technology and Security Standards

- **Fundamental of payment systems**

BANK is implementing Technology standards and security controls as per the RBI guidelines circular DPSS.CO.PD.mobile.Banking. Bo.2/02.23.001/2014-15 dated July 1, 2015. However, the bank is complying IT Framework, technology deployed is fundamental to satisfy and soundness of Mobile Banking payment system. Therefore, BANK is complying and following the Security Standards appropriate to the complexity of service offered, subject to following minimum standards set out as per the Mobile Banking Policy. As per the RBI Guidelines, , the Bank has applied in a way that is appropriate to the risk associated with services provided by the Bank and the system which supports these services.

- **Transaction Limits**

BANK is offering mobile banking facilities (financial) to its customers. Interbank Mobile Payment Service (IMPS) developed and operated by National Payment Corporation of India (NPCI) has also enabled real time transfer of funds through the medium of the mobile phone between accounts in different banks. The volume and value of mobile banking transactions is also showing in uptrend.

In terms of Para 2.1 of RBI circular dated December 24, 2009, a transaction limit of Rs. 50,000/- per customer per day had been mandated. On a review it has been decided to remove this cap. However, BANK., should place per transaction limits based on their own risk perception with the approval of its Board.

It is also clarified that the directions under Para 2 “Remittance of funds for disbursement in cash” of RBI circular dated December 24, 2009 stands superseded with the directions containedin its circular RBI/ 2011-12/213 DPSS.PD.CO.No. 622/02.27.019/2011-2012 dated October 05, 2011. Banks are required to put in place appropriate risk mitigation measures like transaction limit (per transaction, daily, weekly, monthly), transaction velocity limit, fraud checks, AML checks etc. depending on the bank’s own risk perception, unless otherwise mandated by the Reserve Bank.

- **AML checks**

BANK is operating customers accounts as per the Anti Money Laundering Act / KYC Guidelines. As per the RBI Guidelines, BANK., offering money transfer facility subject to adherence of KYC/AML Guidelines . BANK., is providing Money Transfer facility in safe, secure and efficient manner breadth of country. For this facility, the following terms are necessary.

Liberalizing the cash pay-out arrangements for amounts being transferred out of bank accounts to beneficiaries not having a bank account and enhancing the transaction cap from the existing limit of Rs. 50,000 subject to an overall monthly cap of Rs. 1500000 per beneficiary.

Enabling walk in customers not having bank account (for instance migrant workers) to transfer funds to bank account (of say family members of others) subject to a transaction limit of Rs. 50000 and a monthly cap of Rs. 1500000 per remitter.

Enabling transfer of funds among domestic debit/credit/pre-paid cards subject to the same transaction/monthly cap as at (ii) above.

- **Authentication**

  BANK is providing mobile banking services to its customers and also complying with the following security principles and practices for the authentication of mobile banking transactions:
  All mobile banking are permitted only by validation through a two factor authentication.
  One of the factors of authentication is mPIN or any higher standard.
  When mPIN is used, end to end encryption of the mPIN shall not be in clear text anywhere in the network.
  The mPIN shall be stored in a secure environment.

- **Level of Encryption and security standards**

  The Bank is having Proper level of encryption and security and implementing at all stages of the transaction processing. The endeavor are taken to ensure end-to-end encryption of the mobile banking transaction. Adequate safe guards are also in place to guard against the use of mobile banking in money laundering, frauds, etc. As per guidelines laid down in RBI circular with respect to network and system security are followed:
  Implementing application level encryption over network and transport layer encryption wherever possible.
  Establishing proper firewalls, intruder detection system (IDS), data file and system integrity checking, surveillance and incident response procedures and containment procedures.
  Conducting periodic risk management analysis, security vulnerability assessment of the application and network etc at least once in a year.
  Maintaining proper and full documentation of security practices, guidelines, methods, and procedures used in mobile banking and payment systems and keep them upto date based on the periodic risk management, analysis and vulnerability assessment carried out.
  Implementing appropriate physical security measures to protect the system gateways, network, equipment, servers, host computers, and other hardware/software used from unauthorized access and tempering, The Data Centre of the Bank and Service Providers should have proper wired and wireless data network protection mechanisms.

- **Physical Security measures**

  The dependence of banks on mobile banking service providers may place knowledge of bank systems and customers in a public domain, Mobile banking system may also make the banks dependent on small firms (i.e. mobile banking service providers) with high employee turnover. It is therefore, imperative that sensitive customer data, and security and integrity of transactions are protected. It is necessary that the mobile banking servers at the bank's end or at the mobile banking service provider's etc. if any, should be certified by an accredited external agency. In addition, banks should conduct regular information security audits on the mobile banking systems to ensure complete security.

- **Information Security Audits on mobile banking systems**

  For channels which do not contain the phone number as identity, a separate login ID and password are provided to ensure proper authentication, Internet Banking login ID's and Passwords are not be allowed to be used for mobile banking.
  The Bank is complying as per the Reasonable Security Practices & Procedures as per the Sec. 43A of IT Act, 2011 and also implementing technology standards as per RBI Guidelines of its circular issued in 2014-15 for the sake of Information Security breach, Bank is conducting regular Information Security Audits on Mobile Banking Systems to ensure safe, secured and soundness payment system to its customers. The Bank is conducting VNPT reports on yearly basis in this respect for audit purpose.

9. Customer Protection Issues

- **Security procedure**

The security procedure adopted by the BANK for authenticating users is recognized by law as a substitute for signature. As per RBI guidelines and information Technology Act, 2000, 2008 and amended 2011, the bank is providing particular technology and security procedure as a means of authenticating electronic record.

- **Authentication on Legal Risk**

  All the terms and conditions related to authentication procedure and legal risks of the customers are displayed as per RBI norms on our website. Bank shall ensure to its customers that they are made aware of the said legal risk prior to sign up.

- **Risk Control Measures**

  The BANK is maintaining secrecy and confidentiality of customers' accounts. In the mobile banking scenario, the risk of bank not meeting the above obligation is high. The BANK is exposing enhanced risk of liability to customers on account breach of secrecy, denial of service, etc. on account of hacking/other technological failures. Therefore, the Bank is, instituting adequate risk control measures to manage such risks.

  As per RBI guidelines BANK is disclosing risks, responsibilities and liabilities of the customers on their websites and/or through printed material.

- **No Stop Payment Privilege**

  As in an Internet banking scenario, in the mobile banking scenario too, there is very limited or no stop-payment privilege for mobile banking transactions since it becomes impossible for the banks to stop payment in spite of receipt of stop payment instruction as the transactions are completely instantaneous and are incapable of being reversed. Hence BANK offering mobile banking should be notified by the customers the time frame and the circumstances in which any stop- payment instructions could be accepted.

- **Precautionary Measures as per Consumer Protection Act.**

  The Consumer Protection Act, 1986 defines the rights of consumers in India and is applicable to banking services as well. Currently, the rights and liabilities of customers availing of mobile banking services are being determined by bilateral agreements between the banks and customers. Taking into account the risks arising out of unauthorized transfer through hacking, denial of service on account of technological failure etc. banks providing mobile banking would need to assess the liabilities arising out of such events and take appropriate counter measures like insuring themselves against such risks, as in the case with internet banking.

- **Payees and Payee's banks rights and obligations**

  Bilateral contracts drawn up between the payees and payee's bank, the participating banks and service provider should clearly define the rights and obligations of each party.

- **Terms and conditions on websites**

  The existing mechanism for handling customer complaint/s grievances may be used for mobile banking transactions as well. However, in view of the fact that the technology is relatively/new, BANK has set up a help desk and disclosed the details of the help desk and escalation procedure for lodging the complaints, on our website. A detail regarding the above procedure is made available to the customer at the time of sign up.

- **Responsibility and liabilities of customer**

  In cases where the customer files a complaint with the bank disputing a transaction, it would be the responsibility of the service providing bank to expeditiously redress the complaint. Banks may put in place procedures for addressing such customer grievances. The grievance handling procedure including the compensation policy should be disclosed.

- **Customer Complaint Grievances**

Customers' complaints/grievances arising out of mobile banking facility would be covered under the Banking Ombudsman Scheme 2006 (as amended up to May, 2007).

- **Customer complaints covered under Banking Ombudsman Scheme 2006**
  The jurisdiction of legal settlement would be within India.

10. Perceived Risks and Mitigation Measures:

The perceived risks under Mobile SMS Banking and mitigation measures are given hereunder :

Sr. No	**Risk Factor**	**Risk Mitigation**
Technology and Security Standards		
1.	Banks are required to put in place transaction limit (per transaction, daily, weekly, monthly), transaction velocity limit, fraud checks, AML checks etc. depending on the bank's own risk perception, unless otherwise mandated by the Reserve Bank.	Configuration in Mobile Banking application enables Bank to put in place measures such as Transaction Limits, Velocity limit etc. & the same will be put- in place as per outer limits prescribed by RBI. As regard fraud checks, the initiation of the mobile Banking transaction is validated using the combination of mobile number and Mobile Handset identity number (IMEI). Mobile Handset identify number is captured by the mobile Banking application, when the customer activates the application by using the secured pin (M-PIN) that is known only to the customer as the PIN mailer containing the secured PIN is given to the customer after physical identification at the branch by official concerned.
2.	Authentication of the Mobile Banking transactions	All Mobile Banking transactions will be permitted by validation using multi factor Authentication method that is a combination of Mobile number, Mobile Handset identity number and also M-PIN and login password which will be set by the customer at the time of activation of mobile Banking application.
3.	Protection of the data.	End-to-end protection of data will be done as the data will be encrypted using internationally recognized SSL encryption standards. SSL encryption ensures that a secure communication is established between the mobile handset and mobile server.

4.	System and Network security	The Mobile Banking application and database is hosted in highly secure Data Centre (DC) of the Bank. Network security and access controls at DC comply with the laid down Guidelines. Price water house has done the audit of the network and security at Data Centre. Audit of the network for the current year is in progress.
5.	Protection of the customer data	Mobile Banking application will be hosted in Bank's own domain so that entire application and data is in its control. Bank would further ensure that Mobile Banking application hosted at Bank's site is certified by an accredited external agency and also vulnerability assessment of the application is done every year.
Customer protection issues		
6.	Secrecy and Confidentiality of customer accounts	The registration for the service will be document based and physical presence of the customer at the Branch and authentication of his identity will be mandatory.
7.	Customer complaints and grievances	A helpdesk for Internet Banking is operational 24*7. The strength of the help desk team would be suitably increased and they would also be trained to enable them to manage the Help Desk for Mobile Banking also.
Disclosures of risks and liabilities		
8.	Disclosures of risks, responsibilities and liabilities of the customers on their websites and/or through printed material.	The terms and conditions applicable for availment of Mobile Banking facility as finalized by Legal and Risk Management Department(s) will be printed as part of Application for registration. The same would also be published on Bank's website before launch of the facility. The copy of terms and conditions is enclosed.

The above perceived risks and mitigation thereof have been vetted by IRM Department.

11. Review of Policy

Chairman & Mg Director, or in his absence, Executive Director shall be the competent authority to revise or amend or modify or annul any or all of the provisions contained in this policy at any time or from time to time based on the recommendations of the General Manager(IT)
In emergent situations, subject to ratification by the Chairman & Mg Director, or in his absence, Executive Director, General Manager (IT) will be the competent authority to effect necessary changes in this Policy.
The policy and operating guidelines governing the Mobile Banking Policy & Services of the Bank shall be reviewed annually.

12. References:

This policy has been drafted with reference to the guidelines issued by the Reserve Bank of India on Mobile Banking Policy.

i. DPSS.CO.No.619 /02.23.02/2008-09 - Mobile Banking Transactions in India - Operative Guidelines for Banks dated 08.10.2008
ii. DPSS.CO.No.1357/02.23.02/2009-10 - Mobile Banking Transactions in India - Operative Guidelines for Banks dated 24.12.2009
iii. DPSS.CO.No.2502/02.23.02/2010-11 - Mobile Banking Transactions in India - Operative Guidelines for Banks dated 04.05.2011
iv. DPSS.PD.CO.No.622/02.27.019/2011-2012 - Domestic Money Transfer- Relaxations dated 05.10.2011
v. DPSS.CO.PD.No.1098/02.23.02/2011-12 - Mobile Banking Transactions in India - Operative Guidelines for Banksdated 22.12.2011
vi. DPSS.CO.PD.No. 1098 / 02.23.02 / 2011-12 - Mobile Banking Transactions in India - Operative Guidelines for Banks dated 04.12.2014

13. Customer Communication

Customers can communicate with Bank's Customer Care for Mobile Banking related matters 24x7 through below mentioned channels:

Contact number: 02241561111/22
Email: admin@sawjibank.com
Letters and couriers may be addressed to: Sundarlal Sawji Urban Co-Op Bank Ltd., Jintur Tq. Jintur Dist. Parbhani 431509

Cookies Policy

COOKIES POLICY

What are cookies?

Cookies are harmless text files that web servers can store on your computer's hard drive when you visit a website. They allow the server to recognize you when you revisit. There are two main types:

- **Transient (or per-session) cookies.** These only exist for the duration of your site visit and are deleted on exit.
- **Persistent (or permanent) cookies.** These stay on your machine until they expire or are deleted
- We use both types of cookie.

We use cookies to:

- Gather customer journey information across our sites
- To map your IP Address for security purpose while providing related services
- Ensure your privacy in our secure sites
- Store login details for our secure sites
- Temporarily store input information in our calculators, tools, illustrations and demonstrations
- Store details of your marketing, product and business unit preferences to improve our targeting and enhance your journey through our sites and partner sites
- Evaluate our sites advertising and promotional effectiveness (we own the anonymous data collected and don't share it with anyone)
- We use both our own (first-party) and partner companies' (third-party) cookies to support these activities.

We do not use cookies to track your internet usage once you have left our Website, and we will not sell or distribute cookie information without your prior consent.

WHERE WE STORE YOUR INFORMATION

- The information that we collect from you may be transferred to, stored and processed by **Sundarlal Sawji Urban Co-operative Bank Ltd .**

- All information you provide to us is stored on our secure servers. Any payment transactions will be similarly secure.

Changes to this Cookie Policy:

Any changes we make to our Cookie Policy in the future will be posted on this page. Please do check our Cookie Policy from time to time to take notice of any changes made. By using the Website and/or any service offered on the Website after we have changed these terms, you agree that you are accepting these changes.

How do I disable cookies?

If you want to disable cookies you need to change your website browser settings to reject cookies. How to do this will depend on the browser you use and we provide further detail below on how to disable cookies for the most popular browsers:-

For Microsoft Internet Explorer:

1. Choose the menu “tools” then “Internet Options”
2. Click on the “privacy” tab
3. Select the setting the appropriate setting

For Mozilla Firefox:

1. Choose the menu “tools” then “Options”
2. Click on the icon “privacy”
3. Find the menu “cookie” and select the relevant options

For Opera 6.0 and further:

1. Choose the menu Files”> “Preferences”
2. Privacy

What happens if I disable cookies?

This depends on which cookies you disable, but in general the site may not operate properly if cookies are switched off. If you only disable 3rd party cookies you will not be prevented from making purchases on this site. If you disable all cookies you will be unable to complete a purchase on this site.

Contact Site www.sundarlalsawjibank.com

Privacy Policy

Sundarlal Sawji Urban Co-operative Bank Ltd. recognizes the expectations of its customers with regard to privacy, confidentiality, and security of their personal information that resides with the Bank. Keeping personal information of customers secure and using it solely for activities related to the Bank and preventing any misuse thereof is a top priority of the Bank.

This Privacy Policy has been drafted as per the rules and guidelines provided under the Information Technology Act of 2000 & Amendments.

In this policy, "personal information" means any information that relates to a natural person, which either directly or indirectly, in combination with other information available or likely to be available with the bank is capable of identifying such person.

APPLICABILITY

This Policy is applicable to personal information collected by the Bank directly from the customer or through the Bank's online portals, electronic communications as also any information collected by the Bank's server from the customer's browser.

INFORMATION

The Bank collects, retains and uses personal information only when it reasonably believes that it is for a lawful purpose and that it will help administer its business or provide products, services, and other opportunities to the visitor / customer. The Bank collects three types of information: personal, sensitive personal data or information and non-personal.

(a) Personal Information

It can be any information that relates to a natural person, which, either directly or indirectly, in combination with other information available is capable of identifying such person. Information including but not limited to name, address, telephone number, e-mail, occupation, etc.

(b) Sensitive Personal Data or Information

Sensitive personal data or information of a person means such personal information which consists of information relating to passwords, financial information such as Bank account or credit card or debit card or other payment instrument details, sexual orientation, physical physiological and mental health condition, medical records and history, biometric information, details of nominees and national identifiers including but not limited to: Adhaar card, passport number, income, PAN, etc.

For customers enrolled in services provided by the Bank, such as online RTGS/NEFT, personal information about the transaction is collected.

Any information that is freely available or accessible in public domain or furnished under the Right to Information Act, 2005 or any other law for the time being in force shall not be regarded as sensitive personal data or information for the purpose of these rules.

The information you provide online is held by the Bank business that maintains your account or is processing your application for a new product or service.

(c) Non personal information

This information includes the IP address of the device used to connect to the Bank's website along with other information such as browser details, operating system used, the name of the website that redirected the visitor to the Bank's website, etc. Also, when you browse our site or receive one of our emails, the Bank and our affiliated companies, use cookies and/or pixel tags to collect information and store your online preferences.

CHOICE

Consent will be obtained from you when your information is collected by the Bank, in a manner recognized by law. Also, you will be informed of the choices you have for providing your personal information. Only information required for legal purposes or for providing services will be collected

ACCURACY

The Bank has processes in place to ensure that the personal information residing with it is complete, accurate and current. If at any point of time, there is a reason to believe that personal information residing with the Bank is incorrect, the customer may inform the Bank in this regard. The Bank will correct the erroneous information as quickly as possible.

PURPOSE AND USAGE

The Bank uses the information collected and appropriately notifies you to manage its business and offer an enhanced, personalized online experience on its website. Further, it enables the Bank to:

- Process applications, requests and transactions
- Maintain internal records as per regulatory guidelines
- Provide services to customers, including responding to customer requests
- Comply with all applicable laws and regulations
- Recognize the customer when he conducts online banking
- Understand the needs and provide relevant product and service offers

DISCLOSURE / SHARING

The Bank does not disclose sensitive personal data or information of a customer except as directed by law or as per mandate received from the customer / applicant. No specific information about customer accounts or other personally identifiable data is shared with non-affiliated third parties unless any of the following conditions is met:

- To help complete a transaction initiated by the customer
- To perform support services through an outsourced entity provided it conforms to the Privacy Policy of the Bank
- The customer / applicant has specifically authorized it
- The disclosure is necessary for compliance of a legal obligation
- The information is shared with Government agencies mandated under law

- The information is shared with any third party by an order under the law

SECURITY

The security of personal information is a priority and is protected by maintaining physical, electronic, and procedural safeguards that meet applicable laws. Employees are trained in the proper handling of personal information. The Bank has internal corporate policy and procedures such as Grievance Redressal, Incident Management, Third Party Management, etc., which are available to our employees on Bank's intranet. When other companies are used to provide services on behalf of the Bank, it is ensured that such companies protect the confidentiality of personal information they receive in the same manner the Bank protects.

RETENTION

Information may be retained for duration of 90 days as required by regulatory clauses or as long as required to achieve the identified (and notified) purpose.

CONTACT INFORMATION

In order to address any discrepancies or grievances related to the personal information residing with the Bank, the customer may visit:

Email ID:- admin@sawjibank.com

Contact us @:-02457-237149/237330

WEBSITE USAGE TERMS And Policy

I understand and accept that **the Sundarlal Sawji Urban Co-operative Bank Ltd**. (hereinafter referred to as "Bank" or "We") maintains the website (www.sundarlalsawjibank.com) to provide visitors with information about Bank, its services and products and to facilitate communication with Bank and availing its services.

- I also accept that visitors to the Site are required to read the below terms, and use of the Site constitutes my acceptance and agreement to be bound by such terms, and the changes therein to the **Website Usage Terms** from time to time, relating to my usage of the website as communicated and made available on the Bank's website
- I am aware and accept that all information, content, materials, products (including, but not limited to text, content, photographs, graphics, video and audio content) on the website is protected by copyright in the favor of Bank under applicable **Copyright Laws** and is also protected otherwise under general Intellectual Property Law.
- I understand and accept that all information submitted by me through the Bank's website shall be deemed the property of Bank, and the Bank shall be free to use any ideas, concepts, know-how or techniques provided by me at the Site, in any manner whatsoever.
- On initiating a contact through the Bank's website I agree to being contacted by the bank or any other entities with whom the bank has entered into an arrangement
- I (user) shall not do any of the following:
    - Defame abuse, harass, stalk, threaten, or otherwise violate the legal rights (such as rights of privacy and publicity) of others.
    - Publish post, distribute or disseminate any defamatory, infringing, obscene, indecent or unlawful material or information.
    - Upload or attach files that contain software or other material protected by Intellectual Property Laws (or by rights of privacy of publicity) unless the User owns or controls the rights thereto or has received all necessary consents.

- Upload or attach files that contain viruses, corrupted files, or any other similar software or programs that may damage the operation of another's computer.
- Delete any author attributions, legal notices or proprietary designations or labels in any file that is uploaded.
- Falsify the origin or source of software or other material contained in a file that is uploaded.
- Advertise or offer to sell any goods or services, or conduct or forward surveys, contests, or chain letters.
- Download any file posted by another user of a Forum that you know, or reasonably should know, cannot be legally distributed in such manner.

- I agree that I shall not copy, reproduce, sell, redistribute, publish, enter into a database, display, perform, modify, transmit, license, create derivatives from, transfer or in any way exploit any part of any information, content, materials, services available from or through the bank website, except that which I may download for my own personal, non-commercial use.
- I agree that I will not use the bank website for any purpose that is unlawful, or prohibited by these Website Usage Terms. I also agree I will not use the bank website in any manner that could damage, disable or impair the website or interfere with any other party's use or enjoyment of the website.
- I acknowledge that the software and hardware underlying the bank Website as well as other Internet related software which are required for accessing the website are the legal property of the respective Vendors/Bank. The permission given by the Bank to access the bank website will not convey any proprietary or ownership rights in the above software / hardware. I agree that I shall not attempt to modify, translate, disassemble, decompile or reverse engineer the software / hardware underlying the bank website or create any derivative product based on the software / hardware.
- I understand and accept that not all the products and services offered on this website are available in all geographic areas and I may not be eligible for all the

products or services offered by Bank on the Site. Bank reserves the right to determine the availability and eligibility for any product or service.

- I am aware that Bank. proposes to use "cookies" (Cookies are small data files that a website stores on my computer.) for storing visitor preferences, profiling visitors and tracking visitor behavior on the bank website. By visiting the website I acknowledge, accept and expressly authorize the Bank for the placement of cookies on my computer.
- I understand and accept that Bank is not responsible for the availability of content or other services on third party sites linked from the bank website. I am aware that my access of hyperlinks to other internet sites are at my own risk and the content, accuracy, opinions expressed, and other links provided by these sites are not verified, monitored or endorsed by Bank in any way. Bank does not make any warranties, and expressly disclaims all warranties express or implied, including without limitation, those of merchantability and fitness for a particular purpose, title or non-infringement with respect to any information or services or products that are available or advertised or sold through these third party websites.
- Although Bank will take serious steps to prevent the introduction of viruses, vandals, worms, 'Trojan horses' or other destructive materials to this Site, the Bank does not guarantee or warrant that this Site or the materials that may be downloaded from this Service do not contain such destructive features. The Bank is not liable for any damages or harm attributable to such features. If you rely on this Site and any materials available through this Site, you do so solely at your own risk.
- I (user) will verify/ make my own personal inquiries before taking any action or making any final decision with respect to any matter on the website.
- The Bank shall not be liable if any transaction does not fructify or may not be completed or for any failure on part of the Bank to perform any of its obligations under these terms and conditions or those applicable specifically to its services/facilities if performance is prevented, hindered or delayed by a Force Majeure event (defined below) and in such case its obligations shall be suspended for so long as the Force Majeure event continues.

- "Force Majeure Event" means any event due to any cause beyond the reasonable control of the Bank, including without limitations, unavailability of any communication systems, breach, or virus in the processes or payment or delivery mechanism, sabotage, fire, flood, explosion, acts of god, civil commotion, strikes or industrial action of any kind, riots, insurrection, war, acts of government, computer hacking, unauthorized access to computer data and storage devices, computer crashes, malfunctioning in the computer terminal or the systems getting affected by any malicious, destructive or corrupting code or program, mechanical or technical errors/failures or power shut down, faults or failures in telecommunication etc.
- I understand and accept that Bank has the absolute discretion to amend or supplement any of the Website Usage Terms at any time Changed Terms and Conditions shall be communicated to me on the Bank's website and by other acceptable modes of communication. By using the services, I shall be deemed to have accepted the changed Website Usage Terms.
- I understand and agree that these Website Usage Terms are in addition to, and not in derogation of, the applicable Terms and Conditions relating to my usage of any other Bank's services that I may be currently availing or may in the future avail.
- I accept that the Courts in **Parbhani** alone shall have exclusive jurisdiction as regards any claims or matters arising out of dealings with Bank and all disputes will be governed by the laws of India.

TERMS AND CONDITIONS WITH LEGAL DISCLAIMER

Terms and Conditions

This document is an electronic record in terms of Information Technology Act, 2000 and amendments rules there under as applicable and the amended provisions pertaining to electronic records in various statutes as amended by the Information Technology Act, 2000. This electronic record is generated by a computer system and does not require any physical or digital signatures.

These terms and conditions set out the rights and obligations of you, the customer, and us, the Bank, in connection with your use of the Services. All the terms and conditions of this agreement are legally binding, so please read them through carefully before you agree to be bound by them. The following Terms & Conditions govern your use of **the Sundarlal Sawji Urban co-operative Bank Ltd** .(the "Bank") website- www.sundarlalsawjibank.com (herein referred to as "Website") in these Terms & Conditions.

1. Definitions

In this contract, unless the context otherwise requires,

(a) Account(s) - "Account" means Savings Bank Account or Current Bank Account or Fixed Deposit Account, Recurring Account, Loan Account or any other type of account.

(b) Affiliate - "Affiliate" means a person engaged by the Bank on any term and condition with a view to provide, facilitate, promote or excel any service by or in respect of internet banking.

(c) Bank - "Bank" means **Sundarlal Sawji Urban Co-operative Bank Ltd**. registered under the Maharashtra Co-operative Societies Act, 1960 and having its Registered Office at: APMC Market Yard, Yeldari Road, Jintur District, Parbhani-431509 and includes its successors, executors, administrators, assigns and any other person claiming through it.

(d) Home Branch - "Home Branch" means any of the branches of the Bank, with which the User has been maintaining his Account.

(e) Mailing Address - "Mailing Address" means a postal address as well as email address, registered by the User with the Bank, upon which any communication, whether in the form of document or in physical form or in an electronic form, is presumed to have been delivered and received by the User from the Bank.

(f) Password - "Password" means any word, phrase, figure or number, either assigned by the Bank or chosen by the User for the purposes of identification and for security of any Account and information, directions, instructions, advise or communication between the Bank and the User.

(g) Person - "Person" means and includes any individual, company, body corporate, association or body of persons, whether incorporated or not.

(h) Personal Information - "Personal Information" means information furnished by the User to the Bank.

(i) User - "User" means the Account holder, having attained the age of majority, that is to say completion of 18 years and having legal, valid and due authorization by the Bank to use and avail of banking facility. The term User also means and includes a Guardian, whether natural or appointed by WILL or by any competent court, in case of any Account of minor having the age below 18 years.

(j) Website - "Website" means website established, owned and maintained by the Bank.

(k) The words and expressions used herein but not defined specifically in this Agreement, but defined in the Information Technology Act, 2000 and the rules made there under, shall have the same meaning respectively assigned to them therein.

(l) The words used herein but not defined in this Agreement and in the Information Technology Act, 2000 and the rules made there under, shall with their cognate expressions and grammatical variations; have the same meaning as provided in the Indian Contract Act, Indian Evidence Act, Bankers Books Evidence Act 1891, Banking Regulation Act 1949, Reserve Bank of India Act 1934, or any other relevant law, as the case may be.

2.<u>INTERPRETATION CLAUSE:</u>

(a) Gender: Unless the contrary appears from the context, the word he/she and its derivatives are used of any person whether male or female.

(b) Numbers: Unless the contrary appears from the context, the words importing the singular number include the plural number and the words importing the plural number include the singular number.

3.APPLICABILITY OF TERMS AND CONDITIONS:

3.1 For the purposes of availing of banking facility from the Bank, the User shall apply in the Form, prescribed by the Bank, having duly and completely filled in, signed and submitted by the User to the Bank and further on having acknowledged, scrutinized, approved and accepted such application by the Bank, in writing, and informed accordingly to the User. Such application shall be submitted by the User to his home branch. Mere submission of such application by the User to the Bank, without any written communication by the Bank to the User, cannot be construed as grant of banking facility.

3.2 The User shall submit all the documents in physical form and comply with all the requirements as instructed to him by the home branch along with his application for banking facility.

3.3 Bank has and shall have an absolute discretion either to accept or reject the application, as contemplated in Clause No. (3.1) without assigning any reason

3.4 The Bank may in its absolute discretion maintain the record of all or any of the transaction/s whether in physical form or in an electronic form and the same shall be admissible in evidence in any proceeding, whether initiated by the Bank or against it.

3.5 The User is and shall always be bound to ensure that, the banking facility and/or any other related facilities and services are not used for anything, which is illegal, irregular, improper, immoral or against the interest of and sovereignty of India or against the public policy.

3.6 The User shall always strictly adhere to the security systems, security procedures, instructions and advises issued by the Bank from time to time, so as to minimize the risks involved in banking.

3.7 The User is and shall always be bound to procure and maintain, at his own cost and risk, standard, legal and licensed hardware, software and any other equipment related to the computer and proper installation thereof, with reference to the banking.

3.8 The User is at liberty to insure his hardware, software, other equipments and the banking facility or any other item, work or thing from any reputed and reliable insurance company.

3.9 Notwithstanding anything contained herein, in case the User fails to take due and reasonable care and caution in respect of banking facility and as a result of which, the User is put to any loss or damage to his data, information, software, computer hardware, telecommunication or any other equipment or any other loss in terms of money or in terms of business or reputation or otherwise; and the Bank shall not be liable or responsible for any damage or loss to the User whatsoever in such event.

4. <u>BANKING FACILITY ACCESS:</u>

4.1 The Bank shall assign or allot User ID to the User and two secret passwords- one for login and another for transaction entry at the first instance. However, the User is obliged to change such password assigned by the Bank at the earliest possible so as to maintain secrecy of his/her internet banking.

4.2 The User shall not email, transmit and disclose his password, whether assigned by the Bank at the first instance or generated by the User from time to time, or otherwise, PIN or any other vital information to any person and shall maintain absolute secrecy or confidentiality thereof. In case, the User does so for any reason

or on any occasion and as a result of which, the User is put to any loss, liability, responsibility, risk or peril of whatsoever nature, the same shall be borne, paid and suffered by the User only.

4.3 It is hereby admitted, agreed, confirmed and declared by the User and the Joint Account holders, as the case may be, that he/they has/have got himself/themselves well conversant with the practice, procedure, rules, regulations, risks and precautionary measures in banking facility and has/have voluntarily, out of his/their free will and consent, opted for availing of the internet banking. The User and/or Joint Account holders shall maintain a good rapport with the Home Branch of the bank, especially in case of any need of consultation or any contingency affecting the interest of the User and/or Joint Account holders and/or the bank.

5. BANKING FACILITY PASSWORD:

5.1 It is hereby agreed, accepted, acknowledged, represented and declared that, the password issued to the User by the Bank for access to his Account, is and shall be solely and exclusively owned by the User alone and it is his responsibility to use, preserve and maintain confidentiality of and protection to the password as well as any order, instruction, information or action, based upon the password and access to the Account of the User as well as change in the information including change of address of the User.

5.2 The User hereby authorizes the Bank for carrying out transactions and instructions on the strength of such password.

5.3 In case the User forgets or is unable to recollect the password related to his banking facility or in case of blockage of access to the internet banking, as a result of use of incorrect password, consecutively for three times, the User is bound to obtain a new password from the Bank. Such new password does not mean commencement of new contract or opening of new Account.

5.4 It is hereby agreed by and cautioned to the User that under no circumstances the User shall accept the PIN mailer, if the same is found to be tampered or damaged in any manner whatsoever and on having noticed any such tampering or damage to the PIN mailer, however slight or small, he must return such PIN mailer to the Bank immediately, failing which the User alone shall be responsible and liable for any loss or consequences arising out of the same.

6. JOINT ACCOUNTS:

6.1 In case of Joint Account held by one or more persons, banking facility can be availed off by them through one of the Account holders on the strength of User ID and the password issued to such User. In case of such Joint Account, one, who will be operating the Account, should obtain prior written and irrevocable consent of those who will not be operating the Joint Account through internet banking.

6.2 In case of dispute between or amongst the Joint Account Holders, decision of the Bank is and shall always be final, conclusive and binding on both or all of them.

6.3 It is hereby agreed that, all or any correspondence or communication by the Bank can be entered into with any of the Account holders of the Joint Account on his/their respective registered addresses with the Bank and the same shall be treated as good service.

7. CHARGES AND MINIMUM BALANCE:

7.1 The Bank has and shall always have absolute right to charge, demand and recover any amount whether on account of service or any tax, cess, fees or statutory dues or otherwise, from the User or the Joint Account holders, either jointly or severally, for providing internet banking.

7.2 The User shall always maintain a minimum credit balance in his Account as may be prescribed by the Bank from time to time.

7.3 The Bank has got an absolute right, discretion and liberty to terminate this Agreement and/or to withdraw and/or to suspend banking facility, at any time without prior notice, on the ground of breach of any of the terms and conditions contained herein or for misuse, fraud, cheating, deception, mischief, misappropriation or any other illegal or irregular action, commission or omission of act by the User, Joint Account holder or any other person in relation to the internet banking. Such action of the Bank may be in the nature of preventive or punitive remedy. In the event of action as contemplated under this clause, resulting into any loss or prejudice to the User, the Bank shall not be liable or responsible therefore in any manner whatsoever.

8. ACCURACY OF INFORMATION:

The User shall furnish true and correct information to the Bank as and when he is asked to do so including in the application seeking banking facility. In case, the User supplies false or incorrect information and in consequence of which, any loss is occurred to or suffered by the User, the Bank does not and shall not owe any liability or responsibility towards the User.

9. LIABILITY OF THE USER AND THE BANK:

9.1 The User shall not be liable for any unauthorized or fraudulent, transaction by the employee or agent of the Bank or any negligence committed by the employee of the Bank, in respect of banking facility.

9.2 The Bank, hereby assures that it has placed system integrity and security measures, password management systems, User's Account management systems, measures to handle computer virus, network communication security systems, disaster recovery and management. However, in spite of them, in case the User or any of the Joint Account holders suspect that, the User ID or password is known to any other person or notices any unauthorized transaction or interference in his/their Account/s or suspects about any hacking, cracking, tampering, damaging or any cyber crime or introducing viruses into any computer or systems, misuse of

internet domain name, cyber threats, threatening or annoying electronic mail, fraudulent credit card transactions, fraudulent application for goods and services or theft of identity or information etc., shall be immediately brought to the notice of the Bank.

9.3 User is bound as not to allow any unauthorized transaction on his account or related to his account through banking facility or otherwise and he shall not be negligent in that behalf. The User shall always maintain utmost secrecy of User ID, password and other related matters to his banking facilities and the transactions. Further, with a view to maintain such secrecy the User shall not keep any written or electronic record of his password or any other vital information regarding internet banking. The User or any other person claiming through him shall not disclose his User ID and/or password to any person including a member of the bank staff. Notwithstanding this, in case of disclosure or failure to maintain secrecy as regards the User ID and/or password or even a suspicion about the knowledge thereof, by any unconcerned person to the account of the User, the User shall as early as possible inform in writing to the bank about the same and thus, the possibility of any loss in future can be eliminated.

9.4 Under no circumstances, the bank shall be liable for any damage, loss or inconvenience (whether direct, indirect, incidental, consequential or otherwise) caused to the User and/or Joint Account holder in case the banking service is affected, disrupted or unavailable owing to mal-functioning or failure of software, hardware computer network, computer systems, computer resource, computer, disruption /failure of telecommunication systems /network, electricity, calamities/ disasters whether manmade or natural such as flood, fire, lockout, strike, riot, war, orders / directives of court/ Government/ authority or any other contingency beyond the control of the bank.

9.5 Indemnity - In consideration of the bank ,providing the User the Internet Banking, the User shall, at his own expense, indemnify and hold the bank, its directors and

employees, representatives, agents and/or the Affiliates, as the case may be, indemnified against all losses and expenses on full indemnity basis which the bank, may incur, sustain, suffer or is likely to suffer in connection with the bank, or Affiliates' execution of the User's instructions and against all actions, claims, demands, proceedings, losses, damages, costs, charges and expenses as a consequence or by reason of providing a service through banking for any action taken or omitted to be taken by the bank, and /or the Affiliates, its officers, employees or agents, on the instructions of the User. The User will pay the bank, and /or the Affiliates such amount as may be determined by the bank, and/or the Affiliates to be sufficient to indemnify it against any such, loss or expenses even though they may not have arisen or are contingent in nature.

9.6 The Bank shall not be liable for damage, loss or inconvenience owing to any virus attack in any form and in any manner that may enter into User's computer and/or computer system.

10.<u>DISCLOSURE OF INFORMATION:</u>

10.1 The Bank shall hold, possess and maintain all the personal information of the User and/or Joint Account Holders in respect of banking facility as private and confidential, even when he or they are no longer customer and shall be guided by the following principles and policies. The Bank shall not use the personal information of the User and/or Account holder for marketing purposes, unless specifically authorised by the User and/or joint Account holders. The Bank shall not reveal information or data relating to the Account of the User or Joint Account holders to anyone other than in the following exceptional cases:

a) If the Bank is required by any law to give such information.
b) If the Bank is under duty towards public to reveal such information.
c) If interest of the Bank itself requires to give such information (for example to prevent fraud).
d) If the User and/or any of the Joint Account holders directs or permits the Bank to reveal such information.

e) If the Bank is asked to give a banker's reference about to the User and/or the Joint Account holders, with the permission of the User and/or Joint Account holders.

f) If any Affiliate, Agent or Contractor of the Bank is requiring such information for the purposes of rendering any services or legal compliances or for credit rating of the recognized credit scoring agencies.

11.CHANGE OF TERMS AND CONDITIONS:

11.1 The Bank, has and shall always have an absolute right and liberty to add, insert, repeal, omit, delete, modify, amend, substitute, vary or change any of the terms and conditions mentioned herein at any time without giving any prior notice to the User and/or the Joint Account holders, whether with prospective effect or retrospective effect. Normally, such changes will have a prospective effect after giving one month notice by the Bank to the User and/or the Joint Account holders, whether through internet or otherwise. Such added, inserted, repealed, omitted, deleted, modified, amended, substituted, varied or changed term and/or condition is and shall be binding on the User and/or Joint Account holders.

11.2 The Bank may introduce, add, vary, change, suspend and terminate any of the banking services or facilities, within its absolute discretion.

12.NON TRANSFERABILITY:

12.1 The banking facilities or services are not and shall not be transferable to any other person or persons than the User, whether operating the Account individually or singly or as one of the Joint Account holders. Moreover, one of the rights, title, interest and benefit actors under this Agreement can be transferred to any other person by the User and/or Joint Account holders.

13.TERMINATION OF BANKING:

13.1 The User is entitled to quit and terminate the banking services/facilities at any time by submitting a Letter of Request to that effect to the home branch or to the Bank intimating about his intention to quit and terminate the banking service/facilities, at least fifteen clear days prior to the intended date of termination. However, it is made clear that, the User shall be responsible for whatever the transactions and dealings he has carried out till the date of actual termination of this Agreement.

13.2 Notwithstanding anything contained in this Agreement, apart from the right, to suspend, terminate, withdraw, blocking of access, as stipulated in Clause No. (7.3), of the Bank; the Bank is and shall be entitled to terminate, withdraw and/or blocking of access, in the event of death, bankruptcy, legal incompetence, legal disqualification etc. with immediate effect on having noticed the same, without giving any prior notice. The bank is also entitled to and authorised to revive any suspended withdrawn or access blocked account on any term and condition as the bank in its absolute discretion may think fit.

13.3 In the event of closure of Account, the banking facility/service shall automatically stand terminated.

14.NOTICES-

14.1 Letters, Notices or any communication by and between the bank, on the one hand and the user and/or the joint account holders, on the other, can be exchange and delivered by hand or on the registered addresses, as stipulated above, or through internet on the registered email addresses or by telex or fax or through news paper in the locality where the home branch in respect of user is situated.

15. CUSTOMER CARE CENTRE AND GRIEVANCE CALL:

15.1 Customers can communicate with Bank's Customer Care or Grievance Officer for Mobile Banking related matters 24x7 through below mentioned channels:

Grievance Officer: Manager Administration

Contact number: 02457-237149/237330

Email: admin@sawjibank.com

Letters and couriers may be addressed to:Sundarlal Sawji Urban Co-operative Bank Ltd. , APMC Market Yard, Yeldari Road, Taluka-Jintur, District- Parbhani-431509

16.JURISDICTION:

16.1 Notwithstanding anything contained in this Agreement or elsewhere, irrespective of the User and/or Joint Account holder having approached to the Customer Care Centre and Grievance Cell, which is one of the departments and internal Grievance Redressal mechanism of the bank; in the event of any dispute or difference of opinion, touching to, arising out of or in relation to this Agreement, including scope of, import of, interpretation of, rights, liabilities, obligations created or existing under this Agreement of any of the Users, Joint Account holders, Affiliates of the bank, or any person claiming through any o of them or it, shall be referred to sole Conciliator and/or sole Arbitrator, appointed, nominated, constituted and authorised by the Bank. Such Conciliator/Arbitrator shall hold and conduct all the proceedings in English and at **Parbhani** District (Maharashtra) only. Such Conciliator/Arbitrator shall have all the powers and authorities to pass any interim and final order/award by observing principles of natural justice. The Order/ Award/ Decision given by the arbitrator is and shall always be final conclusive and binding on all the parties to arbitral proceedings.

16.2 It is expressly agreed that, if permitted by law, only the courts, tribunals and forums situated at **Parbhani (Maharashtra)** only shall have exclusive jurisdiction to entertain, try and decide any legal proceeding.

17. APPLICABILITY TO FUTURE ACCOUNTS:

17.1 It is agreed that till the user opens further accounts or subscribe to any products or services of the bank or any of its affiliates to which the bank extends internal banking, the user shall be automatically bound by the terms and conditions lay down herein.

18. GENERAL:

18.1 The headings of the clauses contained in this agreement are just for the purposes of conveniences and they do not control or affect the meaning of respective clause. The user shall not assign this agreement to anybody else. However the bank may assign, sub contract or transfer any part of this contract or any work, duties, responsibilities, obligations, benefits etc. there under to any person, on any term or condition as the bank may think fit.

19. RIGHT OFF SET OFF AND LIEN:

19.1 The bank and shall always have and absolute of set off and lien irrespective of any other lien or charge, whether present or future on the deposits of any kind and nature and the credit balances there under whether in single name or joint names and/or any money, securities, bonds, assets, documents and properties held by or under the control of the bank to the extent of full outstanding dues whatsoever towards the bank arising out of or in relation to the banking services/facilities to the user.

19.2 In addition to the said right or any other right the bank is and shall be entitled to (a) combine or consolidate any of the accounts and liabilities of the user and/or the joint account holders, (b) sale any of the securities or properties of the user and/or the joint account holders by way of public or private sale without any judicial intervention and to apply the same proceeds towards the dues of the bank.

19.3 Obligations of Heirs - The user and/or the joint accounts holders, as the case may be, his/their legal heirs, legal representatives, executors, administrators and successors are and shall be bound by the terms of this agreement.

20. PROPERTIES RIGHT:

20.1 The User acknowledges that the software underlying the banking as well as other Internet related software which are required for accessing banking is the legal property of the respective vendors. The permission given by the bank to access banking facility will not convey any proprietary or ownership rights in such

software. The User shall not attempt to modify, translate, disassemble, decompile or reverse engineer the software underlying banking facility or create any derivative product based on the software.

21. COPYRIGHTS TRADEMARK AND COPYING MATERIAL:

21.1 It is hereby agreed that the name, the logo, motto etc., as appearing on the web site of the bank i.e. www.sundarlalsawjibank.com and the website itself are the exclusive properties of the bank.

21.2 The Bank has the licence for and/or all copyrights for its internet website(s) through which the User accesses the banking facility and all trademarks and other materials used on it.

22. LEGAL DISCLAIMER

The contents of this website and all on-site pages or websites ("Website") are communicated by the Bank.

- The information contained on this site is for your personal use. You may download material displayed on these pages for non-commercial use. You may not, however, distribute, reproduce, modify record, transmit, publish, reuse, report, or use the contents of these pages for public or commercial purposes, without Bank's prior written permission. Bank shall at all times be vested with all intellectual property rights contained on the materials displayed herein. The information provided herein is on an "as is" basis without warranty of any kinds. Bank specially disclaims any representations and/or warranties including without limitation any implied warranties. Access and use of the site and the facilities is entirely at your own risk. The services and products being mentioned herein are for your information only and shall not be deemed to constitute solicitation by the Bank and/ or by any of its affiliates for any such products and/or services.
- The contents, news, information, artwork, text, video, audio, picture and images on these pages are protected by Copyright laws of INDIA. The sites that are linked from

these pages are not under the control of the Bank and it does not assume any responsibility or liability for the material available on such linked sites. Access to and use of such other web sites is at your own risk and subject to the terms and conditions applicable to such access/use. These links are provided for reference and convenience only. Bank does not warranty the adequacy, accuracy or completeness of the information and/or material contained on this site or on any of the linked sites.

- Bank makes no warranty, representation or guarantee as to content, sequence, accuracy, timeliness, completeness, truthfulness and positioning of the information or the sources that the information may have been obtained from. Bank makes no warranty, representation or guarantee that the information will be uninterrupted or not-error free. Bank does not certify the performance, operation or availability of the site.
- Bank shall have no liability for any loss or injury caused either in whole or in part by acts, omissions or conditions beyond its control in procuring, compiling, delivering information or any omissions, not-errors or inaccuracies in the information or delays, interruptions in delivery of the information or any decision made, action taken or damage caused in reliance upon the information furnished herein.
- Your use of the site and any of the specific services/ products available on the site shall at all times be subject to the General Terms and Conditions and the specific terms and conditions relating to use of the site and each of these services/ products. By making use of this site you hereby agree to comply with such terms and conditions (including modifications thereto) at all times.
- The services and products available on the site are in accordance with the rules, regulations and guidelines as prescribed by Government of India and Reserve Bank of India from time to time and the Bank makes no representations that they are in accordance with the rules, regulations and guidelines of other countries governing similar services and products.
- Bank makes and has made no representation or warranty as to the quality, condition, fitness and performance of the third party products and services which

the Bank shall be distributing as a gift or reward. Further, the Bank does not warranty that any third party products/services shall be uninterrupted, timely, accurate, reliable, correct or secure; that such products/services shall be available at any particular time or location; that any defects or not-errors will be corrected. Bank shall not be liable or responsible in any manner whatsoever for any delay in delivery (or non-delivery) of such products/services or any damage costs or for any defect or variation in the quality, condition or fitness or performance of such products/services or any guarantees or warranties given by the manufacturer/dealer/seller of the product/service.

23. APPLICABLE LAW

This website and this Disclaimer shall be governed by and construed in accordance with the laws of India. All controversies or claims arising out of or in connection with this website shall be submitted to the competent Indian court in **Parbhani** city.

24. AMENDMENTS

Bank reserves the right to change and/or to renew the information provided on or via this website, including the terms of this Disclaimer, at any time. It is recommended to periodically review the information provided on or via this website, including the terms of this Disclaimer, for changes.