दि विश्वेश्वर सहकारी बँक लि., पुणे

The Vishweshwar Sahakari Bank Ltd., Pune

(Multi State Bank)

INTERNET BANKING POLICY

4TH JULY 2024

Head Office

471/472, Gultekdi, Market Yard,

Pune 411037

This is a confidential document and is meant for restricted distribution.

Every person in custody of this document has the responsibility for ensuring its confidentiality. The custodian of the document will also ensure and that the document is continually updated with amendments that may be issued from time to time. Any loss or mutilation of the document must be reported promptly to the next higher authority.

REVISION HISTORY

Sr. No.	Summary of Change	Prepared By	Approved By	Version No.	Effective Date
1	**Internet Banking Policy along with application**	**VSBL**	**Board**	**1.0**	**26.09.2022**
2	**Internet Banking Policy Change**	**VSBL**	**Board**	**1.1**	**04.07.2024**

Table of Contents

1) INTRODUCTION :

Internet Banking is a system of banking that enables customers to perform various information of customer account on a secure website via the internet. Internet Banking is basically conducted via a personal computer connected to internet. Apart from it with net banking facility one can check Bank statement, check account balance and various other deposit loan statement.

Internet Banking has become widely popular among the masses because of its wide array of benefits. All Banks offer the online banking facility for their customers now a days. In today's fast faced life, people are too much stressed out because of their work pressure and net banking offers then peace of mind as they can pay their bills, book their tickets, do online shopping, etc. from Home.

Internet Banking facility lets Customer manage his Account in the comfort of home or office as per convenience. It is a self-service channel, which is available 24 hours a day and 365 days a year in an absolutely simple, friendly but secured environment.

In Internet Banking a mere touch of a button or click of a mouse makes you accessible to a host of Banking Services, called Fingertip Banking. Customer can carry out your Banking transaction safely and with total confidentiality by enjoying online Banking without wasting time for physically going to the Branch.

2) Regulatory Guidelines - This policy has been framed considering RBI Circular no DCBR.BPD.(PCB/RCB) Cir. No. 6 /19.51.026/2015-16 dated 05th November 2015

3) Policy Statement

"To provide an efficient banking service and enrich customer banking experience, the Bank shall provide Internet Banking facility to its customers."

Objective

The objective of this policy is to establish guidelines for the Bank's Internet Banking Delivery Channel. Internet Banking is important due to the following:

1) Increased efficiency of banking services
2) Enrich banking experience of the customers
3) Demand from customers.
4) To serve as a measure for customer retention.

4) Scope Of Internet Banking Services

- Customers of the Bank who avail of Internet Banking Delivery Channel
- IT infrastructure for Internet Banking Delivery Channel

5) Services to be offered through Internet Banking

RETAIL BANKING SALIENT FEATURES:

- User can self-registered for Internet banking for non-financial services by click on get registered option.
- View account balances and statement of account.
- Backdate statement of account (as per bank policy).
- Loan A/c information, such as principal, and next payment due dates.
- Fixed Deposit details
- Password Change/Forgot Option

Other features, as may be required, shall be added from time to time to enhance service.

Procedures for Internet Banking Delivery Channel

Sr. No	Description
1.	**Ownership**

	a) IT Dept. of The Vishweshwar Sahakari Bank Ltd.,Pune shall be the Owner for the Internet Banking Delivery Channel and shall be responsible for the security of the Internet Banking services. b) The Owner shall carry out a Risk Assessment, as per the Risk Assessment Policy for Information Assets, of the service under consideration and minimize the identified risk to an acceptable level c) The Owner shall document and keep up-to-date the security requirements analysis and specifications for the Internet Banking Delivery Channel d) The Owner shall set up and implement adequate monitoring and reporting procedures.
2.	**Internet Banking Services**
	a) The Bank shall provide all types of account opening facilities through the Internet subject to the following conditions : b) The Bank shall provide banking services only to the customers who have applied to avail of this service. The Owner shall formulate and implement a legally acceptable Application Form for Customers detailing the security requirements, customer responsibility, customer acceptance etc before providing access to the Internet Banking Delivery Channel c) The Bank does not propose, at present, to provide services through the Inter-bank Gateways. d) The Bank does not propose, at present, to provide services in any foreign currency.
3.	**Technology Standards**
	a) The Owner shall designate an Information Security Officer who shall be independent from the Information Technology Department implementing the delivery channel. There should be clear segregation of duties between the Information Technology (IT) division and the Information Security (IS) division The Information Technology Division will actually implement the computer systems. There should be a separate Information Security Officer dealing exclusively with information systems security. Further, an Information Systems Auditor will audit the information systems. b) The Owner shall designate a network and database administrator with clearly defined roles. c) Logical access controls to data, systems, application software, utilities, telecommunication lines, libraries, system software, etc. should be in place. d) The Owner shall ensure that there is no direct connection between the Internet and the bank's system. e) The Owner shall have effective safeguards to prevent intrusions into the network. f) It is also recommended that all unnecessary services on the application server such as File Transfer Protocol (FTP), telnet should be disabled. The application server should be isolated from the e-mail server.

	g) All computer accesses, including messages received, should be logged. Security violations (suspected or attempted) should be recorded and follow up action taken. Banks should acquire tools for monitoring systems and the networks against intrusions and attacks. These tools should be used regularly to avoid security breaches. The banks should review their security infrastructure and security policies regularly and optimize them in the light of their own experiences and changing technologies. h) The information security officer and the information system auditor should undertake periodic penetration tests of the system, which should include: 1. Attempting to guess passwords using password-cracking tools. 2. Search for back door traps in the programs. 3. Attempt to overload the system using Distributed Denial of Service (DDoS) & Denial of Service (DoS) attacks. 4. Check if commonly known holes in the software, especially the browser and the e-mail software exist. 5. The penetration testing may also be carried out by engaging outside experts (often called 'Ethical Hackers'). i) Physical access controls should be strictly enforced. Physical security should cover all the information systems and sites where they are housed, both against internal and external threats j) The Vishweshwar Sahakari Bank Ltd.,Pune will have proper infrastructure and schedules for backing up data. The backed-up data should be periodically tested to ensure recovery without loss of transactions in a time frame as given out in the bank's security policy. Business continuity should be ensured by setting up disaster recovery sites. These facilities should also be tested periodically. k) All applications of banks should have proper record keeping facilities for legal purposes. It may be necessary to keep all received and sent messages both in encrypted and decrypted form. l) Security infrastructure should be properly tested before using the systems and applications for normal operations. The Vishweshwar Sahakari Bank Ltd.,Pune will periodically upgrade the systems to newer versions which give better security and control. m) Banks Internet banking Software provider shall provide the certificate for application integrity to the bank before implementation.
4.	**Security Standards for Internet Banking**
	a) Banks Internet banking Application shall not store Web Applications should not store sensitive information in HTML hidden fields, cookies, or any other client-side storage leading to compromise in the integrity of the data. Critical web

	Applications should enforce at least SSL v3 or Extended Validation –SSL / TLS 1.3 128 bit encryption level for all online activity.' b) Banks Internet banking System shall have EV-SSL Certificate (extended validation) for identification and encryption. c) Re-establishment of any session after interruption should require normal user identification, authentication, and authorization. Moreover, strong server side validation should be enabled. d) For carrying out critical transactions like fund transfers, the banks, shall implement robust and dynamic two-factor authentication i. through user id/password combination and second factor like (a) a digital signature (through a ii. token containing digital certificate and associated private key, preferably for corporate or iii. customers) or (b) One Time Password (OTP) to Customers Registered Mobile Number / dynamic access code through various modes e) Banks Internet banking System shall have Two Factor authentication system for transaction and Payee / beneficiary addition f) Specific OTPs for adding new payees: Each new payee should be authorized by the customer based on an OTP from a second channel which also shows payee details or the customer's handwritten signature from a manual procedure which is verified by the bank. g) Individual OTPs for all transactions (payments and fund transfers): Each value transaction or an approved list of value transactions shall require a new OTP. h) OTP time window: OTP Time Windows shall not exceed 60 seconds i) Internet banking System shall have virtual keyboard for user authentication j) In case of beneficiary addition\deletion SMS \email alerts shall be sent to Customers k) Internet banking System shall have idle session limit of 60 seconds after which it should get disconnected and back button shall be disabled and session shall stand terminated. l) Any Change in Customer Profile/ Mobile Number shall be done at Customer Home Branch only after proper identification and KYC Compliance. m) For all the transactions and profile changes SMS shall be sent to the Customer on its last registered mobile number with the bank n) For availing the Internet Banking facility Customer should have valid email id and Mobile number which should be registered with the Bank.
5.	**Internal Control System**

A. The Vishweshwar Sahakari Bank Ltd.,Pune will develop sound internal control systems before offering internet banking. This would include internal inspection / audit of system and procedures related to internet banking as also ensuring that safeguards are in place to protect the integrity of data, customer confidentiality and security of the data. The Vishweshwar Sahakari Bank Ltd.,Pune Ltd.,Pune may also consider prescribing suitable monetary limits for customers on transactions put through internet banking.

The system of internal control should cover the following:

a) Role and Responsibilities / Organizational structure: The Board of Directors and senior management are responsible for ensuring that the system of internal control operates effectively. The Audit Committee of the Board should have a designated member with requisite knowledge of information systems, related controls and audit issues.

b) Audit Policy to include IS Audit/VAPT: IS audit should be an integral part of the internal audit of the The Vishweshwar Sahakari Bank Ltd.,Pune.

c) Reporting and Follow-up: This involves having a system of reporting by the functionaries to the higher authorities. Any breach or failure of security systems and procedures will be reported to the next higher authority and to the Audit Committee. IS Auditors will prepare an audit summary memorandum providing overview of the entire audit processing from planning to audit findings, discuss the findings with auditee and obtain responses. The Vishweshwar Sahakari Bank Ltd.,Pune will have a time bound follow-up policy for compliance with audit findings. The Board of Directors need to be kept informed of serious lapses in security and procedures.

B. Application for Facilities through Internet Banking:

a) The User shall have the option of applying for facilities provided by VSBL Bank for Internet Banking. The facility to a User shall be extended to the User subject to the User complying with VSBL Bank bank's credit parameters and submitting all documents required by VSBL Bank in a physical form to VSBL Bank. VSBL Bank may in its sole discretion reject the application for the facility by the User.

b) Once CBS registration validation process completed by the Bank then after user itself by using Internet Banking application or access through Bank`s website (Internet Banking) to submit following inputs which are mandatory -

i. 15 Digit Account Number
ii. Customer Number
iii. Registered Mobile Number
iv. Registered Email ID

	Once your registration process completed then user will get access of Internet Banking. c) Not all Accounts can be accessed under the Internet Banking. d) The User authorizes VSBL Bank to add all Accounts (including joint accounts) that the User holds with VSBL Bank now or in the future, which are available to the Internet Banking.
6.	**Legal Issues**
	a) Considering the legal position prevalent, there is an obligation on the part of banks not only to establish the identity but also to make enquiries about integrity and reputation of the customer opting for internet banking. Therefore, even though request for opening account can be accepted over Internet, accounts should be opened only after proper introduction, verification of the identity of the customer and adherence to KYC guidelines. b) From a legal perspective, security procedure adopted by banks for authenticating users needs to be recognized by law as a substitute for signature. The prescriptions of the Information Technology Act, 2000, and other legal provisions need to be scrupulously adhered to while offering internet banking. c) Under Banking Regulation Act there is an obligation on banks to maintain secrecy and confidentiality of customers' accounts. In the Internet banking scenario, the risk of banks not meeting the above obligation is high on account of several factors. Despite all reasonable precautions, banks may be exposed to enhanced risk of liability to customers on account of breach of secrecy, denial of service etc., because of hacking / technological failures. The Vishweshwar Sahakari Bank Ltd.,Pune will, therefore, institute adequate risk control measures to manage such risks. d) In internet banking scenario there is very little scope for the UCBs to act on stop-payment instructions from the customers. Hence, The Vishweshwar Sahakari Bank Ltd.,Pune will clearly notify to the customers the timeframe and the circumstances in which any stop-payment instructions could be accepted. e) The Consumer Protection Act, 1986 defines the rights of consumers in India and is applicable to banking services as well. The rights and liabilities of customers availing of internet banking services shall be clearly explained to customers opting for internet banking. Considering the banking practice and rights enjoyed by customers in traditional banking, The Vishweshwar Sahakari Bank Ltd.,Pune liability to the customers on account of unauthorized transfer through hacking, denial of service on account of technological failure etc. shall be assessed and Bank shall insure themselves against such electronic and cyber risks. f) Personal data/Account information given to Bank and Bank may share data for transaction under the Digital Personal Data Protection (DPDP) Act of 2023.
7.	**Customer Liability in Unauthorized Electronic Banking Transaction**

A) Systems and Procedures

1) Bank has appropriate systems and procedures to ensure safety and security of electronic banking transactions carried out by its customers;
2) Bank has robust and dynamic fraud detection and prevention mechanism;
3) Bank has put in place mechanism to assess the risks resulting from unauthorized transactions and measure the liabilities arising out of such events.
4) Bank is continuously taking appropriate measures to mitigate the risks and protect themselves against the liabilities arising there from.
5) Bank will at regular intervals advise customers on how to protect themselves from electronic banking and payments related fraud

B) Reporting of Unauthorized Transactions

1) All the Customers of the Bank shall mandatorily register for SMS alerts and wherever available register for e-mail alerts, for electronic banking transactions.
2) Bank shall send SMS alerts mandatorily to all Customers. The customers must notify their bank of any unauthorized electronic banking transaction at the earliest after the occurrence of such transaction.
3) Customers shall report the Unauthorized Transaction on at Branches of the Bank or on website of the Bank 24x7.
4) Customers shall inform the bank immediately of the unauthorized transactions and failure to do so shall increase the liability or risk of loss to the bank/ customer.

Limited Liability of the Customer

C) Zero Liability

1) In case of Unauthorized Transaction Customer's entitlement to zero liability shall arise where the unauthorized transaction occurs in the following events:
   (i) Contributory fraud/ negligence/ deficiency on the part of the bank (irrespective of whether or not the transaction is reported by the customer).

   (ii) Third party breach where the deficiency lies neither with the bank nor with the customer but lies elsewhere in the system, and the customer notifies the bank within three working days of receiving the communication from the bank regarding the unauthorized transaction.

D) Limited Liability of the Customer

1) A customer shall be liable for the loss occurring due to unauthorized transactions in the following cases:-

(i) In cases where the loss is due to negligence by a customer, such as where he has shared the payment credentials, the customer will bear the entire loss until he reports the unauthorized transaction to the bank. Any loss occurring after the reporting of the unauthorized transaction shall be borne by the bank.

(ii) In cases where the responsibility for the unauthorized electronic banking transaction lies neither with the bank nor with the customer, but lies elsewhere in the system and when there is a delay (of four to seven working days after receiving the communication from the bank) on the part of the customer in notifying the bank of such a transaction, the per transaction liability of the customer shall be limited to the transaction value or the amount mentioned in below Table, whichever is lower.

Maximum Liability of the Customer under Para 9 (E) and RBI circular dated 6th July 2017 Para 7 (ii)		
Sr. No.	**Type of Account**	**Maximum Liability**
1	Basic Savings Account	Rs.5,000/=
2	• All other SB accounts • Pre-paid Payment Instruments and Gift Cards • Current/ Cash Credit/ Overdraft Accounts of MSMEs • Current Accounts/ Cash Credit/ Overdraft Accounts of Individuals with annual average balance (during 365 days preceding the incidence of fraud)/ limit up to Rs.25 lakh • Credit cards with limit up to Rs.5 lakh	Rs,10,000/=
3	• All other Current/ Cash Credit/ Overdraft Accounts	Rs.25,000/=

E) Summary of Customer Liability

Overall liability of the customer in third party breaches, as detailed in paragraph D and paragraph E above, where the deficiency lies neither with the bank nor with the customer but lies elsewhere in the system, is summarized in Table given below

Summary of Customers Liability

Sr. No.	Time taken to report the fraudulent transaction from the date of receiving the communication	Customers Liability
1	Within 3 working Days	Zero Liability
2	Within 4 to 7 working Days	The transaction value or the amount mentioned in Table given in E above whichever is lower
3	Beyond 7 working days	As per Banks Board Approved Policy

F) Customers Account will be credited within 10 days from the Receipt of the Complaint in above cases.

G) Reporting of the Transactions Beyond 7 working Days

In case the Customer Report the unauthorized transaction after 7 working days Customer Liability shall be 50% of the Transaction value or Rs.10, 000/- whichever is higher.

H) Reversal Timeline for Zero Liability / Limited Liability Customer (added as per RBI Circular dated 14th December 2017)

1) On being notified by the customer, the bank shall credit (shadow reversal) the amount involved in the unauthorized electronic transaction to the customer's account within 10 working days from the date of such notification by the customer (without waiting for settlement of insurance claim, if any). The credit shall be value dated to be as of the date of the unauthorized transaction.
2) Bank shall within 90 days from the date of the complaint shall resolve Customer complaint and liability of the customer, if any, established and the customer shall be compensated as per provisions of paragraphs F above.

In cases where liability is not established or customer is not compensated within 90 days from the date of complaint Customer will be compensated as per clause above immediately.

8.	**Other Issues and Disclosures**

	The existing regulatory framework over banks will be extended to Internet Banking also. In this regard, it will be ensured that: a) The products under internet banking should be restricted to account holders only. b) The services should only include local currency products. c) The Vishweshwar Sahakari Bank Ltd.,Pune will make disclosure of risks, responsibilities and liabilities of customers in doing banking through internet. d) The banks shall adhere to the KYC guidelines / AML standards and the provisions and directions issued under the PMLA 2002 while offering internet banking. e) Hyperlinks from banks' websites, often raise the issue of reputational risk. Such links should not mislead the customers into believing that banks sponsor any particular product or any business unrelated to banking. Hyperlinks from banks' websites should be confined to only those portals with which they have a payment arrangement. Hyperlinks to banks' websites from other portals are normally meant for passing on information relating to purchases made by banks' customers in the portal. Banks must follow recommended security precautions while dealing with request received from other websites, relating to customers' purchases.
9.	**System and Control Procedures for Managing the Risk**
9.1	Bank shall adopt the following risk mitigation and control procedures for Internet Banking Application ; a) IT policy implementation and management for Internet Banking b) Mandatory password length and usage of numbers, upper case and special characters. c) segregation of duties based on job description and roles. d) Identification of key business application risk that can be monitored electronically. e) Identification of key system settings that cannot be changed without authorization. f) Implementation of continuous monitoring software and /or alert management when suspicious or unauthorized activity takes place (Cyber Security Operations Centre). g) Regular updation of Anti-virus and Malware software, end point protection software and regular updation of Operation System patches, security patches, Database patches and database security patches. Monitoring security patches and alerts. h) Half Yearly Vulnerability and penetration testing of exposed applications and infrastructure.

	i) Implementation of SIEM Software, Intrusion detection / Prevention monitoring. j) Restricting Access to application modules and databases where sensitive information is accessible k) Bank shall implement Risk base transaction monitoring shall be implemented for transactions done through Internet Banking.
9.2	Bank shall have layered approach to security and follow the statutory guidelines; a) Secured hosting of Internet Banking Application. b) Implementation of Multifactor Authentication. c) Implementation of web applications to use SSL v3 or extended validation with implementation of security certificates and 128 Bit encryption for all online activity. d) Two online factor authentication for financial transactions with user id password and either digital certificate or OTP as second factor authentication. e) Masking of all critical information to stop the information leak. f) Customer will be intimated immediately through SMS and Email for the transaction initiated on his account to verify if the transaction is valid, else customer shall report to the Bank on Banks website 24x7 or Branch immediately. g) Ceiling on per day transaction limit. h) Maintain the customer behavioural pattern for log-in, password change request or any other sensitive data. i) Internet Banking Application Server and related devices should be connected to Security Operations Centre and Network Operation Centre to counter and Hacking Attempt and find vulnerabilities on continuous basis j) Bank shall implement Web Application Firewall, Anti-Virus and Anti-Malware Protection k) Multi-factor Authentication measures, Credential Confidentiality, Automatic Logout, Complex Password Format l) Customers shall get authenticated on the bank's web site through security mechanisms Extended Validation Secure Sockets Layer (EV-SSL) Certificates which will work with high security web browsers to clearly identify a Banks website's organizational identity. m) Bank shall implement measures to stop and block the man-in-the-middle attack (MITM), man-in-the browser (MITB) attack or man-in-the application attack.

	n) An authenticated session, together with its encryption protocol, should remain intact throughout the interaction with the customer. In the event of interference, the session should be terminated and the affected transactions resolved or reversed out. The customer should be promptly notified of such an incident as the session is being concluded or subsequently by email, telephone or through other means. o) Changes in mobile phone number shall be done through request by the Customer with KYC compliance at Home branch of the Customer only. p) On the Internet Banking Login Screen Virtual keyboard should be implemented. For Legal and Reputation risk management; a) Bank shall have Appropriate disclosure, Terms and Conditions for the use of internet banking services b) Privacy of customer information
9.3	For Customer awareness Bank shall :- a) Publish Regular notifications to Do's and Don'ts for using internet banking, on Banks Web site, Internet Banking Page, email b) Regular SMS shall be send to customers to not to; i) Share the user id, ii) Password and iii) OTP etc. c) Bank shall prepare the customer awareness document which will be made available at the various platforms like branches, web-site, internet banking ports, email etc. d) Customer Should be educated and made aware for 1) Never access Online Banking accounts through hyperlinks in e-mails, pop-up windows, or search engines. 2) Beware of unexpected hoax and scam e-mails with attachments and beware of suspicious web sites. 3) Never open an email attachment by unknown sender 4) Always access account by typing the web address in the address bar of the browser or by selecting the bookmark for the genuine website. 5) Install personal firewall and licensed anti-virus software and regularly update them. 6) Never leave computer unattended while logged on to Online Banking. 7) Always log out of accounts after you have finished your banking session. 8) Never give out password.

	9) Do Not use your date of birth, phone number, address, your name or name of a friend/pet/relative in password. 10) Change password regularly- every two months preferably. 11) Do Not use online banking password for anything else (ex. Email) 12) Always be cautious when using computers in public place. Do not leave screen idle for long periods or leave the computer unattended. 13) Type your Internet Banking URL. 14) Avoid using public wifi or use VPN Software. 15) Subscribe for Mobile Notification. 16) Do not use public computers to login. 17) Disconnect internet connection when not in use. 18) Keep checking saving account regularly. 19) Enable multifactor authentication. 20) Always use official Banking applications only.
10.	**Customer Guidance**
	a) The Bank has designed an Application Form for Customers. Customers who wish to avail the Internet Banking facility shall complete the form in its entirety before the facility is provided to the Customer. b) The application form details the risks of Internet Banking and provides directions and guidelines for the correct and secure use of the facility. c) The Bank shall provide adequate education / instructions and online / offline support shall be made available to the customers with emphasis on Password security. d) The Bank has setup a Helpdesk facility to provide directions on the use of the facility. The Helpdesk shall provide guidance to the Customers for the services offered. e) The bank shall handle Customer complaints with care and shall give priority for redressal of grievances.
8	**Review of Internet banking Policy**
	This policy will be reviewed at-least once in a year and whenever the business environment, Regulator guidelines and/or technology etc. changes occur.

Xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx