The Vishweshwar Sahakari Bank Ltd.,Pune

(Multi-State Scheduled Bank)

INTERNET BANKING POLICY

OCTOBER 2025

VERSION 1.3

Head Office
471/472, Gultekdi, Market Yard,
Pune - 411037

Table of Contents

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.

4. REVISION HISTORY

Sr. No.	Summary of Change	Prepared By	Approved By	Version No.	Effective Date
1	**Internet Banking Policy**	**VSBL**	**Board**	**1.0**	**Sept-2022**
2	**Internet Banking Policy Change**	**VSBL**	**Board**	**1.1**	**July-2024**
3	**Internet Banking Policy change**	**VSBL**	**Board**	**1.2**	**May-2025**
4	**Internet Banking Policy Change (Transaction Base)**	**VSBL**	**Board**	**1.3**	**Oct -2025**

5. 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, request for cheque book and various other financial transactions.

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 nowadays. 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.

1) 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

6. Policy Statement

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

7. 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.

8. Scope Of Internet Banking Services

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

9. Services to be offered through Internet Banking

a) Balance Inquiry
b) Accounts Statement
c) Funds Transfer
d) Stop Payment
e) Term Deposit/Loan Account View
f) Cheque Book Request
g) Debit Card Control
h) Any other services which Bank may add from time to time

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

10. Procedures for Internet Banking Delivery Channel

Sr.No	Description
1.	**Ownership**
	a) IT Dept. of The Vishweshwar Sahakari Bank shall be the Owner for the Internet Banking Delivery Channel and shall be responsible for provide uninterrupted 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 IT Officer from the Information Technology Department implementing the delivery channel. 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 secured 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 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 IT officer and the information system auditor should undertake penetration tests of the system twice in a year, 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 loop holes in the application. 5. The penetration testing may also be carried out by engaging outside experts auditor. i) Physical access controls should be strictly enforced. Physical security should cover all the information systems and sites where they are hosted, both against internal and external threats j) The Vishweshwar Sahakari Bank 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. k) Applications of banks should have proper record keeping facilities for legal purposes. l) Security infrastructure should be properly tested before using the systems and applications for normal operations. The Vishweshwar Sahakari Bank will upgrade the systems to newer versions as an when required, which will give better security and control.
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 TLS 1.2 128/256 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 OTP on Customers Registered Mobile Number 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. 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 120 seconds i) Internet banking System shall have virtual keyboard for user authentication j) In case of beneficiary addition\deletion SMS alerts shall be sent to Customers k) Newly added beneficiary will be available for transactions only after cooling period of 30 minutes with transaction limit of Rs.50,000/ in first 24 hours irrespective of normal limit. l) Idle session shall automatically log out customers after 15 minutes. Back-button re-entry shall remain disabled to prevent session replay. m) Any Change in Customer Profile/ Mobile Number shall be done at Customer Home Branch only after proper identification and KYC Compliance. n) For all the transactions SMS shall be sent to the Customer on its last registered mobile number with the bank o) For availing the Internet Banking facility Customer should have valid Mobile number which should be registered with the Bank.
5.	**Internal Control System**
	The Vishweshwar Sahakari Bank 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 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: IS audit should be an integral part of the internal audit of the Vishweshwar Sahakari Bank. 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 IT 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 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.
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. Vishweshwar Sahakari Bank 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, Vishweshwar Sahakari Bank 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, Vishweshwar Sahakari Bank 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) The Vishweshwar Sahakari Bank shall maintain a robust cybersecurity framework based on RBI cybersecurity guidelines, continuous monitoring and threat-intelligence systems. The Bank shall implement modern security protocols including TLS 1.2, vulnerability assessments and endpoint protection. g) The Bank shall obtain specific, informed, and freely-given consent from customers for processing personal data as required under the Digital Personal Data Protection Act, 2023. Customers shall be informed of the purpose for which

	personal data is collected. The Bank shall ensure data minimisation, secure processing and privacy-by-design principles. h) Customer data shall be stored and processed only for lawful banking purposes and shall not be shared with third parties except as required by law or with customer consent. i) Internet banking infrastructure shall be protected by a Security Operations Centre.
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 • Credit cards with limit above Rs.5 lakh	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 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.
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) ISS 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 shift duties. d) Implementation of continuous monitoring software and /or alert management when suspicious or unauthorized activity takes place (Cyber Security Operations Centre). e) Regular updation of Anti-virus and Malware software, end point protection software and regular updation of Operating System patches, security patches, Database patches and database security patches. Monitoring security patches and alerts. f) Vulnerability and penetration testing of exposed applications and infrastructure twice in a year. g) Implementation of SIEM Software, Intrusion detection / Prevention monitoring. h) Restricting Access to application modules and databases where sensitive information is accessible

9.2	Bank shall have layered approach to security and follow the statutory guidelines; a) Secured hosting of Internet Banking Application as a ASP with Finacus Solutions Pvt. Ltd. b) Implementation of Multifactor Authentication. c) Implementation of web applications to use TLS 1.2 128/256 bit encryption level with extended validation security certificates for all online activity. d) Two factor authentication for financial transactions with user id, password and OTP as second factor authentication. e) Encryption of critical information to stop the information leak. f) Customer will be intimated immediately through SMS 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 in Banking hours. g) Maintain the customer logs related to log-in, password change request or any other sensitive data. h) Internet Banking Application Server and related devices should be connected to Security Operations Centre to counter and Hacking Attempt and find vulnerabilities on continuous basis. i) Bank shall implement Firewall, Anti-Virus and Anti-Malware Protection. j) Multi-factor Authentication measures, Credential Confidentiality, Automatic Logout, Complex Password Format. k) 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. l) Bank shall implement measures to stop and block the man-in-the-middle attack (MITM) m) 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 terminated. n) Changes in mobile phone number shall be done through request by the Customer with KYC compliance at Home branch of the Customer only. o) 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. 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) Always be cautious when using computers in public place. Do not leave screen idle for long periods or leave the computer unattended. 12) Type your Internet Banking URL. 13) Avoid using public wifi or use VPN Software. 14) Subscribe for Mobile Notification. 15) Do not use public computers to login.

	16) Disconnect internet connection when not in use. 17) Keep checking saving account regularly. 18) Enable multifactor authentication. 19) 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.
11	**Customer Grievance Management**
	Resolution of Grievances :- The customers can highlight their complaints / issues vide the procedure outlined in this policy. For redressal of issues customers can email their complaint to: vsbl@vishweshwarbank.com or can lodge the compliant on the website of the Bank https://vishweshwar.bank.in Customers will receive a response within ten business days and we shall do our best to resolve the complaint to the customer's satisfaction within this period. Complex complaints which would require time for examination of issues involved, may take a longer time to resolve. However, in such cases, customers will be informed about the status of their complaint within this period. In case of unsatisfactory response from the above channel, customers can escalate the complaint to the Principal Nodal Officer of the Bank: **Mr. Rajendrakumar Sathe** The Vishweshwar Sahakari Bank Limited.,Pune 471/472, Gultekdi, Market Yard, Pune 411 037 Contact No. 9881909716 Email – r.sathe@vishweshwarbank.com

12	**Operating Procedure**

We are providing Transaction Base Internet Banking to our customers through a joint venture between Finacus Solutions Pvt. Ltd. (As a ASP) and JJIT Fintech Pvt. Ltd.

In this, the account holder can view the Balance / Statement and Details of all their Checking / Deposit / Loan accounts and can also make OWN / Within Bank / NEFT / RTGS type transactions from the Checking Account. Along with this, they can make Service Request i.e Cheque Book Request, Stop Payment, Positive Pay etc. Some necessary guidelines in this regard are as follows –

1.We are making this iNet Facility available to all account holders of both Individual and Corporate types for Savings, Current, Cash Credit, CCOD accounts. Details are as follows –

Customer Type	**Mode of Customer Type**
Individual	Single, Joint, Sole Proprietor, H.U.F. etc.
Corporate	Partnership, Trust, Pvt. Ltd. Co., LLP, Public Ltd. Co., Society etc.

2.In case of Single A/C in Individual, iNet Banking facility will be provided to the concerned Customer and in case of Proprietorship A/C, the concerned Co-Owner will be provided.

3.In case of joint accounts in individual, iNet Banking Facility will be provided to the first account holder and consent of all other joint account holders will be required.

4.In Corporate iNet Banking, the Maker / Checker must be a Partner/Director/Signatory Authority of the concerned Firm/Legal Entity and the Consent Signature of all the Partners/Directors/Signatory Authorities must be obtained. In this, a Resolution will be required in Trust, Pvt. Ltd. Co., LLP, Public Ltd. Co. and Society A/C, iNet Banking facility will be provided only to those who have been given the authority as Maker / Checker in the said Resolution.

5.For Corporate iNet Banking, the Signatory Authority as per the Operating Instructions in CBS for the account of the concerned Firm/Legal Entity along with all other Partners/Directors etc. will be applicable for Maker/Checker.

6.In Corporate iNet Banking, if there is more than one account under the Customer of the concerned Firm/Legal Entity and there are different Partner/Director/Signatory Authorities for each account, then accordingly, it will be necessary to fill a separate Application Form for each account.

7.In Corporate iNet Banking, a Partner/Director/Signatory Authority of the concerned

	Firm/Legal Entity cannot be a Maker and Checker at the same time. **Registration Process –** 1.To avail iNet Banking Facility, it is necessary to have CKYC of the concerned account holders (Joint, Firm, Partner, Director, Beneficial Owner etc.). If there is no CKYC, then first complete the CKYC process. 2.To avail iNet Banking Facility, the account holder will first have to fill the form in the prescribed format of the bank and submit it to the branch. The branch will take the form and scan it for registration. If it is an individual, save it as Br Code_I_Customer No_Name.pdf and if it is a corporate, save it as Br Code_C_Customer No_Name.pdf and send it to the IB Cell at the head office at vsbinet@vsbl.in mail ID. 3. This Application Form will be sent to the branches as per the requirement. 4. The branch should ensure that the information filled in the form by the account holder and the information in CBS as well as the information on the branch's A/C Opening Form and Profile Form are the same and then send the form to the head office as above. 5.Account holder will be registered for Internet Banking as per the form received by IB Cell and Login and Transaction Password will be sent to the concerned IB User via SMS on the Registered Mobile Number. 6.After that IB User can use Transaction Base IB service by logging in through URL- https://inet.vishweshwar.bank.in. For this purpose, a separate TAB called Internet Banking is available on the Website (Header Section). 7. The Login ID of the Internet Banking User will be his Customer ID in CBS and it cannot be changed. 8.It is mandatory for IB User to keep his/her Password as Min. 8 digit combination of Alpha numeric & special character. 9.Last 3 passwords will not be accepted in Change / Reset password. 10. If you enter the wrong password three times, the user login will be blocked for the next 24 hours. 11.Password Validity will be 60 Days. 12.IB User can set Password through ATM Card Credentials from Forgot Password Option. If ATM Card is not available, then the attached Service Request Form must be filled in the branch. 13.After the branch sends the Forgot Password Service Request Form to the H.O.-IB Cell on the mail ID vsbinet@vsbl.in, the Login / Transaction Password will be sent to the IB User's Registered Mobile Number.

14.IB User will have to create Beneficiary before making Within / NEFT / RTGS Transactions except Own Transaction and can select the said Beneficiary while making the Transaction.

15.After adding any Beneficiary, it will be activated after 30 minutes and after that, only up to Rs. 50,000/- can be sent to the said Beneficiary in the next 24 hours, after which the Regular Transaction Limit will be applicable.

16.IB User can make Cheque Book Request only till 4.00pm on Working Days.

17.Every transaction of VSB iNet User will be OTP based and OTP will be sent to that User's Registered Mobile Number. The transaction will be completed only after verifying the OTP received on the mobile.

18.The Auto Session Timeout Period of the IB User will be 15 Minutes and the User will be alerted about it within the last 30 Seconds.

13 **Transaction limit**

The ceiling on per day transaction limit as per below chart

	Savings A/C	**Current A/C**	**CC/CCOD A/C**
Self Transfer (OWN)			
Default	2 Lakh	5 Lakh	5 Lakh
Enhance upto	5 Lakh	10 Lakh	10 Lakh
Non Working hours	Full	Full	Full
Per day txn count	10	30	30
Within - VSBL to VSBL			
Default	2 Lakh	5 Lakh	5 Lakh
Enhance upto	5 Lakh	10 Lakh	10 Lakh
Non Working hours	50%	50%	50%
Per day txn count	10	30	30
Other - NEFT/RTGS			

	Default	2 Lakh	5 Lakh	5 Lakh
	Enhance upto	5 Lakh	10 Lakh	10 Lakh
	Non Working hours	50%	50%	50%
	Per day txn count	10	30	30

Business Hours - 6.00 am to 6.00 pm

Non-Businesss Hours - 6.00 pm to 6.00 am

13	**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.