Internet Banking Policy

(Version 1.2)

October 1, 2021

Uttar Pradesh Co-Operative Bank Ltd.

2- Mahatma Gandhi Marg,

Lucknow-226001

Introduction: Uttar Pradesh Co-operative Bank Limited, Lucknow established in 1944 is the apex bank of Cooperative Credit Societies in the State. Besides the State Government, 50 District Cooperative Banks and 10 Apex cooperative bodies are its members. It is a scheduled Bank. In addition, the bank also regulates the cadre authority of the secretaries/ senior managers of District Cooperative Banks and secretaries of primary agricultural credit cooperative societies. The main objective of the Bank is to exercise physical discipline over District/ Central district cooperative banks/ give them professional advice as also to play the role of a balancing center. This apex bank/ besides its own financial resources/ obtains loans on concessional interest rates from NABARD and through District Cooperative Banks extends refinance facilities for short term and medium term loans for agricultural production and other allied works. The UPCB besides agriculture products, extends financial assistance to agriculture-based large and medium processing industries like sugar factories, spinning mills, rice mills, oil mills, vegetable oil mills, solvent extraction plans, cottage industries, cold storage, handloom, agriculture, rural development banks, cooperative housing societies, marketing federation, sugar cane society, state sugar mills corporation and NAFED.

Uttar Pradesh Co-operative Bank Limited, Lucknow (herein after referred to as 'The Bank') offers various internet products to enhance access interface to our clients This is viewed as an extension of existing access mechanism to allow our clients to send payment instructions and trade related instructions to Uttar Pradesh Co-operative Bank Ltd. for processing as well as retrieving their account balance and transaction information.

While providing Internet banking services and products to its customers, the Bank shall adhere to the following policies and procedures:

1. Internet banking services will only be provided to Customers of the Uttar Pradesh Co-operative Bank Ltd. after verifying the identity of customers and completion of KYC formalities in accordance with the KYC & AML Policy & Procedures of the Bank. The Bank may receive a request for opening an account over the internet. However, accounts should only be opened after proper verification of the identity of the customer.
2. Bank shall offer Internet banking products only to its customers.
3. Bank is on CBS platform and its connectivity is Internet Protocol Version 6**(IPv6)** compliant.
4. The services will include local currency products only.
5. Bank ensures that it maintains secrecy and confidentiality of customers' accounts.
6. Bank clearly notifies its customers of the timeframe and the circumstances in which any stop-payment instructions would be accepted by it.
7. Bank shall enter into such documentation and agreements with the Customer as determined appropriate by Legal and Compliance.
8. Bank will report to RBI every breach or failure of security systems and procedure.
9. Bank complies with various guidelines issued by Reserve Bank of India as amended from time to time (including but not limited to)
   - Internet Banking in India - Guidelines dated 14.Jun.2001,
   - Internet Banking in India – Guidelines dated 20.Jul.2005
   - 'Internet Banking Facility for Customers of Cooperative Banks' vide circular DCBR.BPD.(PCB/RCB) Cir. No.6/19.51.026/2015-16 dated 05,Nov 2015
   - 'Risks and Controls in Computers and Telecommunications' vide circular DBS.CO.ITC.BC. 10/ 31.09.001/ 97-98 dated 04.Feb.1998 / UBD.No.Admn.46b/17:36:00/97-98 dated March 30, 1998.
   - Circular DBS.CO.ITC.BC.No.6/31.02.008/2010-11 dated April 29, 2011 regarding Recommendations of the Working Group on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds (Chairman: Shri G. Gopalakrishna, Executive Director)

10. All instructions of RBI relating to 'Inter- bank Payment Gateways' for settlement of e-commerce and other transactions shall be complied with.

11. Bank also has Board of Directors approved 'IT and IT Security Policy'.

12. UP CO-OPERATIVE BANK LTD. adheres to Technology and Security Standards as per RBI guidelines on 'Internet Banking Facility for Customers of Cooperative Banks' circular DCBR.BPD.(PCB/RCB) Cir. No.6/19.51.026/2015-16 dated 05,Nov 2015. The guidelines are mentioned below:

I Technology and Security Standards:

a. The Bank has Information Security policy duly approved by the Board of Directors with 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. Bank has Information Security Officer dealing exclusively with Information Systems security. Further, an Information Systems Auditor audits the Information Systems.

b. The bank has a designated 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. are in place.

d. Bank would ensure that there is no direct connection between the Internet and the bank's CBS system.

e. We have effective safeguards like (cyber security operation center, Cyber Forensics, Threat Prevention Monitoring Tools, Automatic Critical Incidents Response Mechanism on RBI Format, provision of Red Team/Blue Team concept 24*7 VAPT, Antivirus, UTM, Firewalls, IDS, IPS, DLC, Anti-Fishing, etc.) to prevent intrusions into the systems/network.

f. All unnecessary services on the Application Server such as File Transfer Protocol (FTP), Telnet are disabled. The Application Server is isolated from the e-mail server.

g. All computer accesses, including messages received, is logged. Security violations (suspected or attempted) are recorded and follow up action taken. Banks should acquire tools for monitoring Systems and networks against intrusions and attacks. These tools should be used regularly to avoid security breaches. The bank reviews its security infrastructure and security policies regularly and optimizes them in the light of their own experiences and changing technologies.

h. The Information Security officer and the Information System auditor conducts periodic penetration tests of the system, which includes:

    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 is strictly enforced. Physical security covers all the Information Systems and sites where they are housed, both against internal and external threats.

j. The Bank has proper infrastructure and schedules for backing up data. The backed-up data is

periodically tested to ensure recovery without loss of transactions in a time frame as spelt out in the Bank's security policy. Business continuity is ensured by setting up Disaster Recovery sites. These facilities should also be tested periodically.

k. All applications have proper record keeping facilities for legal purposes. It shall be necessary to keep all Received and Sent messages both in encrypted and decrypted form.

l. The Bank will have application integrity statement from the vendor/service provider, before implementing the internet banking software.

m. Security infrastructure is properly tested before using the Systems and Applications for normal operations. The Bank would periodically upgrade the Systems to newer versions which give better security and control.

n. The guidelines issued by RBI on 'Risks and Controls in Computers and Telecommunications' vide circular DBS.CO.ITC.BC. 10/ 31.09.001/ 97-98 dated 4th February 1998 / UBD.No.Admn.46b/17:36:00/97-98 dated March 30, 1998 and circular DBS.CO.ITC.BC.No.6/31.02.008/2010-11 dated April 29, 2011 regarding Recommendations of the Working Group on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds (Chairman: Shri G. Gopalakrishna, Executive Director); advising banks to comply with the same, will equally apply to Internet banking.

o. Guidelines on 'Introduction of IS Audit Policy' in NABARD circular NB.DoS.HO.POL.No. 3634/J-1/2014-15 dated February 25, 2015 will also apply.

II. Legal Issues

a. The Bank will provide Internet Banking facility to a customer only at his/her option based on specific written or authenticated electronic requisition along with a positive acknowledgement.

b. Considering the prevailing legal position, there is an obligation on the part of bank not only to establish the identity but also to make enquiries about the integrity and reputation of the customer opting for internet banking. Therefore, even though request for opening an account may be accepted over Internet, accounts should be opened only after verification of the identity of the customer and adherence to KYC guidelines.

c. From a legal perspective, security procedure adopted by bank for authenticating a user needs to be recognized by law as a substitute for signature. The provisions of the Information Technology Act, 2000, and other legal requirements need to be scrupulously adhered to while offering internet banking.

d. Under the present regime, there is an obligation on banks to maintain secrecy and confidentiality of customers' accounts/information. In the Internet banking scenario, the risk of bank 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 banks should, therefore, have in place adequate risk control measures to manage such risks.

III. Internal Control System

The bank has sound internal control systems before offering internet banking. This would include internal inspection / audit of systems and procedures related to internet banking as also ensuring that adequate safeguards are in place to protect integrity of data, customer confidentiality and security of data. Banks may also consider prescribing suitable monetary limits for customers on transactions put

through internet banking. The internal control system should cover the following:

a. **Role and Responsibilities / Organizational structure:** The Board of Directors and senior management of the Bank are responsible for ensuring that the internal control system operates effectively. 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 banks. The banks should put in place a system to ensure that a robust audit trail is generated to facilitate conduct of audit, serving as forensic evidence when required and assist in dispute resolution.

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. Bank should 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.

Banks have a communication plan for escalating/reporting to the Board/Senior Management/ RBI/NABARD to proactively notify major cyber security incidents.

13. UP CO-OPERATIVE BANK LTD. shall make mandatory disclosures of risks, responsibilities and liabilities of the customers in doing business through Internet through a disclosure template.

System and Control Procedures For Managing Risk:

13.1 Key Risks: The Internet is a wide area network of computers connected around the world to facilitate data transmission and exchange. Due to the open nature of the internet, all web-based services such as Internet Banking are inherently subject to risks such as;

- Online theft of User ID/User Name, Password
- Virus attacks
- Hacking
- Un-authorised Access
- Fraudulent Transactions
- Undetected compromise or attacks (Security Metrics)
- Loss or disclosure of sensitive or critical information assets
- Un-Authorised access, activities and fraudulent transactions are not detected on time

13.2 Potential Impact: Impact of the above mentioned risks to the bank as well as the customers are;

- Increased risk to the Bank and its reputation
- Loss of customer confidence
- Financial loss to the Bank as well as customers
- Lawsuits /Legal battles

13.3 Mitigation of Risk and control Procedures: The Bank is ready to adopt the following risk mitigation and control procedures before the Internet Banking Application is live;

- IT policy implementation and management for Internet Banking
- Mandatory password length and usage of numbers, upper case and special characters.
- Implement segregation of duties based on job description and roles.
- Identify the key business application risk that can be monitored electronically.
- Identify the key system settings that cannot be changed without authorization.
- Implement continuous monitoring software and /or alert management when suspicious or unauthorized activity takes place (Cyber Security Operations Centre).
- 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.
- Periodic vulnerability and penetration testing of exposed applications and infrastructure.
- Implement SIEM Software, Intrusion detection / Prevention monitoring.
- Restrict Access to application modules and databases where sensitive information is accessible
- A layered approach to security and follow the statutory guidelines;

    - Secured hosting of Internet Banking Application.
    - Implementation of Multifactor Authentication.
    - Enforce the web applications to use SSL v3 or extended validation with implementation of security certificates and 128 Bit encryption for all online activity.
    - Two online factor authentication for financial transactions with user id password and either digital certificate or OTP as second factor authentication.
    - Masking of all critical information to stop the information leak.
    - 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 authorities immediately.
    - Ceiling on per day transaction limit.
    - Maintain the customer behavioural pattern for log-in, password change request or any other sensitive data.
    - Setting up Security Operations Centre and Network Operation Centre to counter and Hacking Attempt and find vulnerabilities on continuous basis
    - Installation of Firewalls.
    - Anti-Virus and Anti-Malware Protection
    - Multi-factor Authentication measures
    - Credential Confidentiality
    - Automatic Logout
    - Complex Password Format

- For Legal and Reputation risk management;

    - Appropriate disclosure, Terms and Conditions for the use of internet banking services
    - Privacy of customer information

- For Customer awareness;

    - Regular notifications to Do’s and Don’ts for using internet banking, Publishing on Bank-Website, email campaign.
    - Regular SMS to customers to not to;
        - Share the user id,
        - Password
        - OTP etc.

- Bank has prepared the customer awareness document which will be made available at the various platforms like branches, web-site, internet banking ports, email etc..

13.4 Customer Awareness Documents:

- **Never** access your Online Banking accounts through hyperlinks in e-mails, pop-up windows, or search engines.
- **Beware** of unexpected hoax and scam e-mails with attachments and beware of suspicious web sites.
- **Never** open an email attachment by unknown sender
- **Always** access your account by typing the web address in the address bar of the browser or by selecting the bookmark for the genuine website.
- **Install** personal firewall and licensed anti-virus software and regularly update them.
- **Never** leave your computer unattended while logged on to Online Banking.
- **Always** log out of your accounts after you have finished your banking session.
- **Never** give out your password.
- **Do Not** use your date of birth, phone number, address, your name or name of a friend/pet/relative in your password.
- **Change** your password regularly- every two months preferably.
- **Do Not** use your online banking password for anything else (ex. Email)
- **Always** be cautious when using computers in public place. Do not leave screen idle for long periods or leave the computer unattended.
- Type your Internet Banking URL.
- **Avoid** using public wifi or use VPN Software.
- **Subscribe** for Mobile Notification.
- **Do not** use public computers to login.
- Disconnect internet connection when not in use.
- Keep checking saving account regularly.
- **Enable** multifactor authentication.
- **Always** use official Banking applications only.

13.5 The customer undertakes that he shall take all precautions including precautions as enumerated in Clause 13.4 of this policy. The precautions shall be mentioned in the application filed for availing facility of Internet Banking.

14. Customer Protection for Unauthorized Electronic Banking Transactions. This policy refers to RBI Circular reference: DBR.No.Leg.BC.78/09.07.005/2017-18 dated July 6, 2017.

UP CO-OPERATIVE BANK LTD. provides Electronic Banking to its Customers. In the event of any unauthorized transaction, Customer will be compensated for any consequential financial loss as per the below guidelines:-

(a) **Zero Liability of a Customer:-**A 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.

(b) **Limited Liability of a Customer:-** 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 user 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.

Summary of Customer's Liability

S.N.	Time taken to report the fraudulent transaction from the date of receiving the communication from the Bank	Customer's liability (Rs)
1	Within 3 working days	Zero liability
2	Within 4 to 7 working days (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)	The transaction value or 10,000, whichever is lower
3	Within 4 to 7 working days (All Other Current/ Cash credit/ Overdraft Accounts)	The transaction value or 25,000, whichever is lower
4	Beyond 7 working days	Full transaction value (Zero liability on bank)

Note: -

The number of working days shall be counted as per the working schedule of the home branch of the customer excluding the date of receiving the communication. 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). Also, the Customer service committee shall periodically review the unauthorized electronic transactions reported by customer. The credit shall be value dated to be as of the value date of the unauthorized transaction. The bank shall report the customer liability cases to Management committee. These cases will be made available to audit for review.

Further, Bank shall ensure that:-

(i) a complaint is resolved and liability of the customer, if any, established within such time, as may be specified in the bank's Board approved policy, but not exceeding 90 days from the date of receipt of the complaint, and the customer is compensated as per provisions of table above;

(ii) where it is unable to resolve the complaint or determine the customer liability, if any, within 90 days, the compensation as prescribed in table above is paid to the customer; and

(iii) the customer does not suffer loss of interest or does not bear any additional burden of interest.

Bank shall also periodically update the customer on:-

i. the risks and responsibilities involved in cases of electronic banking transactions and the customer's liability in cases of unauthorized electronic banking transactions focusing on the below
ii. the systems and procedures to ensure safety and security of electronic banking transactions carried out by customers.
iii. appropriate measures to mitigate the risks and protect themselves against the liabilities arising therefrom

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: customerhelpdesk@upcbl.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. Our focus would remain on the quality and completeness of the response, with speed of delivery being an important but not overriding factor.

In case of unsatisfactory response from the above channel, customers can escalate the complaint to the Principal Nodal Officer of the Bank:

NAME:	SHRI ASHOK KUMAR
DESIGNATION:	GENERAL MANAGER (BANKING)
CORR. ADDRESS.:	U.P. COOPERATIVE BANK LTD., 2-M.G. MARG, LUCKNOW-226001
TELEPHONE NO.:	0522-4151200/2614007, 7525006031
EMAIL ID:	customerhelpdesk@upcbl.in

Customers will receive a response within 10 business days and they will have to quote the reference number pertaining to their earlier contact with UP CO-OPERATIVE BANK LTD. Lucknow on the same issue.

Banking Ombudsman Scheme:-

If customers do not receive a response from us within one month after we have received the complaint, or if they are not satisfied with the reply given by us, they may approach the Banking Ombudsman.

UP State government is in process of establishing Ombudsman for Cooperative sector in the State. Meanwhile, Additional Commissioner and Additional Registrar (Banking), Cooperative, U.P. is looking after customer grievances for Cooperative Banks in U.P.

For the convenience of the customers, following have been displayed on our website:

- Appropriate arrangement for receiving complaints and suggestions.
- The name, address and contact number of the Principal Nodal Officer
- Contact details of Banking Ombudsman
- Code of bank's commitments to customers/Fair Practice code

The nodal officer of the UP CO-OPERATIVE BANK LTD. is kept informed on the complaints which are not redressed within one month. The details of the Banking Ombudsman

where the complainant can approach are included in the final closure letters/ emails for such cases.

15. Hyperlinks from the Bank's website shall be confined to only those portals with which UP CO-OPERATIVE BANK LTD. has a payment arrangement or sites of their subsidiaries or principals. Hyperlinks to the UP CO-OPERATIVE BANK LTD's website from other portals will be normally meant for passing on information relating to purchases made by UP CO-OPERATIVE BANK LTD.'s customers in the portal. UP CO-OPERATIVE BANK LTD. shall follow the minimum recommended security precautions while dealing with request received from other websites, relating to customers purchases.

16. The technology and security standards prescribed by RBI and recommended by the 'Working Group on Internet Banking' including the security policy will be meticulously followed by the UP CO-OPERATIVE BANK LTD.

17. Prior to offering of any banking services over the internet, UP CO-OPERATIVE BANK LTD. shall put up a note to its Management Committee stating details such as analysis of cost and benefit, operational arrangements like technology adopted, business partners as relevant, third party service providers, systems and control procedures we propose to adopt for managing risks, and any other pertinent information.

18. This policy is subject to review annually. The gap between two reviews should not be more than 12 months. It may also be reviewed as and when felt necessary by the Management Committee.

19. This policy is intended to address requirements under Indian regulations only and should be read in conjunction with applicable Firm wide policies.