INDRAPRASTHA SEHKARI BANK LIMITED
इंद्रप्रस्थ सहकारी बैंक लिमिटेड

Regd. Off.: C-2, First Floor, Wazirpur Indl. Area, Delhi-110052
+91-11-69340000-69340015
ipbank@ipbankonline.com
www.ipbankonline.com

VERSION CONTROL DOCUMENT

Policy No.	32
Policy Name	FRAUD RISK MANAGEMENT POLICY
Version No.	1.0
Board Resolution Date	25.09.2024
Board Resolution Number	12
Review Date	-
Next review date	01.10.2027 (or earlier if there are any changes)
Classification	Confidential for Internal Circulation only

Version Control Information:

Version No.	Date Issued	Author	Update Information
1.0	25.09.2024	Head Office	

INDRAPRASTHA SEHKARI BANK LIMITED
इंद्रप्रस्थ सहकारी बैंक लिमिटेड

Regd. Off.: C-2, First Floor, Wazirpur Indl. Area, Delhi-110052
+91-11-69340000-69340015
ipbank@ipbankonline.com
www.ipbankonline.com

FRAUD RISK MANAGEMENT POLICY

In terms of RBI circular No. RBI/DOS/2024-25/119 DOS.CO.FMG.SEC.No.6/23.04.001/2024-25 July 15, 2024 - Master Directions on Fraud Risk Management in Urban Cooperative Banks (UCBs) / State Cooperative Banks (StCBs) / Central Cooperative Banks (CCBs)

Background:

The Reserve Bank of India has released fresh master directions on Fraud Risk Management for Urban Cooperative Banks (UCBs) superseding the earlier directions on the subject, namely 'Master Circular - Classification & Reporting' dated July 1, 2015. These Directions are issued with a view to providing a framework to Cooperative Banks for prevention, early detection and timely reporting of incidents of fraud to Law Enforcement Agencies (LEAs), Reserve Bank of India (RBI) and NABARD and dissemination of information by RBI and matters connected therewith or incidental thereto. The revised directions mandate formulation of Board approved Policy on fraud risk management delineating roles and responsibilities of Board / Board Committees and Senior Management of the Cooperative Banks.

1.Regulatory compliance

1.1 Board approved Policy: The bank has put in place a structure of rules, practices and process in the form of a policy document on Fraud Risk Management System in terms of revised/updated directives of the RBI specifying role of the Board, Board Committees and Senior Management.

1.2 Fraud Risk Governance: The Bank has constituted a Committee of the Executives (CoE) headed by the Chief Executive Officer and two senior officers of the Bank for the purpose of performing the roles and responsibilities of 'Special Committee of the Board for Monitoring and Follow-up of cases of Frauds'(SCBMF) who shall oversee the effectiveness of the fraud risk management in the Bank.

1.2.1 The CoE shall review and monitor the incidence of frauds, including root cause analysis, and suggest mitigating measures for strengthening the internal controls, risk management framework and minimizing the incidence of frauds. The coverage shall include, among others, categories/trends of frauds, industry/sectoral/ geographical concentration of frauds, delay in detection/classification of frauds and delay in examination/conclusion of staff accountability, etc. Corresponding reviews shall be placed before the Board/Audit Committee of the Board at quarterly rests.

1.2.2 A senior official at Head Office has been designated for overall risk management functions i.e. prevention, early detection, investigation, staff accountability, monitoring, recovery, analysis and reporting of frauds etc. in terms of provisions of this policy document.

Regd. Off.: C-2, First Floor, Wazirpur Indl. Area, Delhi-110052
+91-11-69340000-69340015
ipbank@ipbankonline.com
www.ipbankonline.com

1.2.3 Whistle Blower complaints on possible fraud cases / suspicious activities in accounts shall be examined and concluded appropriately under Whistle Blower Policy.

2. Framework of Early Warning Signals and Red-flagged Accounts:

The Bank shall identify appropriate early warning indicators for monitoring credit facilities / loan accounts and other banking transactions. These indicators shall be reviewed periodically for their effectiveness. Suspicion of any fraudulent activity thrown up by the presence of one or more EWS indicators shall alert / trigger for deeper investigation from potential fraud angle and initiating preventive measures.

The tracking of EWS in loan accounts shall not be seen as an additional task but must be integrated with the credit monitoring process in the Bank so that it becomes a continuous activity and also acts as a trigger for any possible credit impairment in the loan accounts.

2.1 Early Warning Signals: Some indicative Early Warning Signals (EWS) forewarn the dealing officials about some wrongdoings in the loan accounts which may turn out to be fraudulent:

1) Default in undisputed payment to the statutory bodies as declared in the Annual report.
2) Bouncing of high value cheques
3) Frequent change in the scope of the project to be undertaken by the borrower
4) Bills remaining outstanding with the bank for a long time and tendency for bills to remain overdue.
5) Delay observed in payment of outstanding dues.
6) Frequent invocation of BGs and devolvement of LCs.
7) Under insured or over insured inventory.
8) Invoices devoid of TAN and other details.
9) Dispute on title of collateral securities.
10) Funds coming from other banks to liquidate the outstanding loan amount unless in normal course.
11) Request received from the borrower to postpone the inspection of the godown for flimsy reasons.
12) Funding of the interest by sanctioning additional facilities.
13) Exclusive collateral charged to a number of lenders without NOC of existing charge holders.
14) Concealment of certain vital documents like master agreement, insurance coverage.
15) Floating front / associate companies by investing borrowed money
16) Critical issues highlighted in the stock audit report.
17) Liabilities appearing in ROC search report, not reported by the borrower in its annual report.
18) Frequent request for general purpose loans.
19) Frequent ad hoc sanctions.
20) Not routing of sales proceeds through consortium / member bank/ lenders to the company.
21) High value RTGS payment to unrelated parties.

Regd. Off.: C-2, First Floor, Wazirpur Indl. Area, Delhi-110052
+91-11-69340000-69340015
ipbank@ipbankonline.com
www.ipbankonline.com

22) Heavy cash withdrawal in loan accounts.
23) Non production of original bills for verification upon request.
24) Significant movements in inventory, disproportionately differing vis-a-vis change in the turnover.
25) Significant movements in receivables, disproportionately differing vis-à-vis change in the turnover and/or increase in ageing of the receivables
26) Disproportionate change in other current assets
27) Significant increase in working capital borrowing as percentage of turnover
28) Increase in Fixed Assets, without corresponding increase in long term sources (when project is implemented).
29) Increase in borrowings, despite huge cash and cash equivalents in the borrower's balance sheet
30) Frequent change in accounting period and/or accounting policies
31) Costing of the project which is in wide variance with standard cost of installation of
32) Claims not acknowledged as debt high
33) Substantial increase in unbilled revenue year after year.
34) Large number of transactions with inter-connected companies and large outstanding from such companies
35) Substantial related party transactions
36) Material discrepancies in the annual report
37) Significant inconsistencies within the annual report (between various sections)
38) Poor disclosure of materially adverse information and no qualification by the statutory auditors
39) Raid by Income tax /sales tax/ central excise duty officials
40) Significant reduction in the stake of promoter /director or increase in the encumbered shares of promoter/director.
41) Resignation of the key personnel and frequent changes in the management

The Committee (CoE) shall oversee the effectiveness of the framework of EWS. Senior management shall ensure initiation of remedial action on triggers/alerts from EWS system in a timely manner and periodical review of credit sanction and monitoring processes, internal controls and systems.

2.2 EWS Framework for other banking / non-credit related transactions:

The Bank shall ensure that integrity of system is maintained, personal and financial data of customers is secure and transaction monitoring for prevention / detection of potential fraud with a minimum time lag without compromising the effectiveness of the outcome of EWS system which will broadly revolve around the very definition of fraud i.e."A deliberate act of omission or commission, by any person, carried out in the course of a Banking Transactions or in the Books of Accounts maintained manually or under Computer System in Banks, resulting into wrongful gain to any person for a temporary period or otherwise, with or without any monetary loss to the Bank". An indicative classification of Non-credit transactions is as under:

- Cash shortages – misappropriation

Regd. Off.: C-2, First Floor, Wazirpur Indl. Area, Delhi-110052
+91-11-69340000-69340015
ipbank@ipbankonline.com
www.ipbankonline.com

- Payment frauds
- Illegal gratification
- Theft of sensitive stationery
- Payment/collection of forged instruments
- ACH transactions
- Deposit related frauds
- Mis-use of Inoperative accounts
- Fraudulent discount of instruments or kite-flying
- Fraudulently taking out leaves from cheques books before/while issuing the same to customers;
- Missing sensitive inventory
- Impersonation – forging of signatures
- Swapping of ATM Cards, mis-use of PINs
- IT/Cyber incidents, Technology related frauds – Digital banking

Early Warning Signals:

- Behaviour of Staff
- Non-reconciliation of office accounts
- Non-maintenance of various books, registers, ledgers, scrolls etc.
- Non-compliance of KYC guidelines, intentionally ignoring policy guidelines
- Internal/external audit observations
- Complaints received from customers

The Bank shall extensively monitor and analyse financial transactions, including transactions carried out through digital platforms / applications, in order to identify unusual patterns and activities prompting for initiation of preventive measures towards prevention of fraudulent activities.

3. Credit facility / Loan account - Indication of fraudulent activities:

Bank shall monitor activities in credit facility / loan accounts and remain alert on activities which could potentially turn out to be fraudulent. In cases where there is a suspicion / indication of wrongdoing or fraudulent activity, it shall be subjected to internal and/or external audit for further investigation in such accounts.

The loan agreement with the borrower shall contain clauses for conduct of such audit at the behest of lender(s). In cases where the audit report submitted remains inconclusive or is delayed due to non-cooperation by the borrower, Bank shall conclude on status of the account as a fraud or otherwise based on the material available on their record and its own internal investigation / assessment in such cases.

In case an account is identified as a fraud by the Bank, the borrowal accounts of other group companies, in which one or more promoter(s) / whole-time director(s) are common shall also be subjected to examination by the Bank from fraud angle.

Regd. Off.: C-2, First Floor, Wazirpur Indl. Area, Delhi-110052
+91-11-69340000-69340015
ipbank@ipbankonline.com
www.ipbankonline.com

In cases where Law Enforcement Agencies (LEAs) have *suo moto* initiated investigation involving a borrower account, Bank shall follow the process of classification of account as fraud as per its Board approved Policy and in tune with Principles of Natural Justice as elaborated in succeeding paragraphs.

3.1 Principles of natural justice: The Bank shall ensure compliance with principles of natural justice, particularly the rule of '***audi alteram partem***' (let the other side be heard, as well) shall positively be looked into before classifying Persons / Entities as fraud, which at a minimum shall include:

- No person shall be judged without a fair hearing in which each party shall be given the opportunity to respond to the evidence against them;
- The bank shall issue a detailed Show Cause Notice (SCN) to the persons, including Third Party Service Providers and Professionals such as architects, valuers, chartered accountants, advocates etc. and also entities, their promoters/whole time and Executive Directors against whom allegation of fraud is being examined. The Bank shall consider the role of non-whole-time directors (like nominee directors and independent directors) before proceeding against them as they are normally not in charge of, or responsible to the company for the conduct of business of the company.
- The SCN shall provide complete details of transactions / actions / events basis which declaration and reporting of a fraud is being contemplated under the guidelines.
- The bank shall provide 30 days period to entities/persons, on whom the SCN served, to respond to the SCN.
- The Bank shall thoroughly examine the responses/submissions made by the persons/entities prior to declaring them as fraudulent.
- The bank shall serve a reasoned Order on the persons/entities conveying the decision of the bank regarding declaration/classification of the account as fraud or otherwise. Such Order shall contain relevant facts/circumstances relied upon, the submissions made and the reasons for classification.

3.2 Modus Operandi and Root Cause Analysis (RCA) of major frauds

The Bank shall conduct quarterly and annual review of frauds, if any, covering inter-alia adequacy of systems to detect frauds, laxity in control measures and methodology of major frauds, etc. Bank shall also carry out Root Cause Analysis (RCA) of large value frauds periodically.

For this purpose, major observations relating to Modus Operandi, Root-Cause Analysis and Major Weaknesses in Due Diligence and Monitoring Measures, as analysed by the RBI, are given hereunder to enable the branch officials to carry out reviews as required. The list is illustrative and shall be further analysed at the bank taking into account the complexities for strengthening the credit & operational risk management at the Bank. The Board / ACB /CoE shall have an oversight in the matter.

Regd. Off.: C-2, First Floor, Wazirpur Indl. Area, Delhi-110052
+91-11-69340000-69340015
ipbank@ipbankonline.com
www.ipbankonline.com

A. Modus Operandi:

Diversion of Funds – Setting up fictitious/fake entities with no apparent economic or business purpose to siphon-off loan amounts and creating fake invoices to inflate the cost of goods and services, thereby obtaining higher loan amount than needed.

Misappropriation of funds – Carrying out large-scale transactions with entities having indirect relationships with each other in a way to conceal fraudulent activities and conducting financial transactions to bypass the established terms & conditions of a Trust and Retention Agreement (TRA).

Manipulation of Books of Accounts – Routing the loan amounts in circular transactions with related parties to either inflate the sales figures or to manage working capital facilities and manipulation of financial records by eliminating or reducing or concealing the value of transactions involving related parties.

Fake Letters of Credit (LCs) – Opening of unauthorized LCs by the borrowers without proper documentation, maintenance of records and obtaining LCs for purchase of goods which either did not exist or were overvalued.

B. Major Weaknesses in Due Diligence and Monitoring Arrangements:

Inadequate Underwriting Standards / Due Diligence Process – Inadequacy of Systems & Processes at the bank for identifying and verifying counterparties while issuing LCs/BGs and inconsistencies with regard to the transactions/developments in the account vis-à-vis the financial statements of the account are not cross checked at the bank properly.

Weakness in Credit Monitoring – Submission of fake statements and book debts by the borrowers to avail credit facilities underlining weaknesses in credit monitoring process and receivables and purchases made without proper documentation with the intent to inflate drawing power.

Deficient Post-Disbursement Monitoring Mechanism – Lack of tools to focus and monitor end use of funds and to prevent misuse or diversion of funds. Further, deficiencies in monitoring mechanism at banks to check the circular transactions in loan accounts with related / inter-connected parties to ascertain end use of funds.

Inadequacy of follow-up system at the bank to ensure adherence to the sanctioned terms.

3.2.3 Independent confirmation from the third-party service providers including professionals

The Bank shall hold its third-party service providers including technology vendors and professionals such as architects, valuers, chartered accountants, advocates etc., accountable in situations, where wilful negligence / malpractice is found to be responsible for causing frauds and keep itself indemnified. Necessary insertions in this regard shall be made in all the contracts whereby the third-party service providers, their staff, agents, representatives,

Regd. Off.: C-2, First Floor, Wazirpur Indl. Area, Delhi-110052
+91-11-69340000-69340015
ipbank@ipbankonline.com
www.ipbankonline.com

consultants and/or other authorized persons shall indemnify and hold the bank and its officials harmless from and against all losses (reputational and/or financial) or damages and all action, suit, litigations or proceedings (including all costs, charges, expenses relating thereto) that the bank may incur or suffer.

3.2.4 Staff Accountability

Bank shall initiate and complete the examination of staff accountability in all fraud cases in a time-bound manner in accordance with its Staff Accountability Policy provisions.

In cases involving very senior executives of the Bank the ACB shall initiate examination of their accountability and place before the Board.

3.2.5 Penal measures for fraudulent borrowers

The Bank shall have the sole discretion to entertain or decline requests for credit facilities received from persons/entities classified and reported as fraud by cooperative banks and who are debarred from raising of funds and / or seeking additional credit facilities, for a period of 5 years from the date of full repayment of the defrauded amount/settlement amount agreed upon in case of a compromise settlement. Such requests from Entities and persons associated with such fraudulent entities may also be declined by the bank.

The Bank shall not consider restructuring or grant of additional credit facilities to borrowers who have defaulted and have also committed a fraud in the account. However, in cases of fraud/malfeasance where the existing promoters are replaced by new promoters and the borrower company is totally delinked from such erstwhile promoters/management, bank may take a view on restructuring of such accounts based on their viability, without prejudice to the continuance of criminal action against the erstwhile promoters/management.

Further, no compromise settlement involving a fraudulent borrower shall be allowed unless the conditions stipulate that the criminal complaint will be continued.

In addition to above borrower-fraudsters, third parties such as builders, warehouse/cold storage owners, motor vehicle/tractor dealers, travel agents, etc. and professionals such as architects, valuers, chartered accountants, advocates, etc. are also to be held accountable if they have played a vital role in credit sanction/disbursement or facilitated the perpetration of frauds. Bank shall report to Indian Banks Association (IBA) the details of such borrowers / third parties involved in frauds.

3.2.6 Treatment of accounts under Resolution

In case an entity classified as fraud has subsequently undergone a resolution either under IBC or under the resolution framework of RBI resulting in a change in the management and control of the entity / business enterprise, the Bank shall examine whether the entity shall continue to remain classified as fraud or the classification as fraud could be removed after implementation of the Resolution Plan under IBC or aforesaid prudential framework. This would, however, be, without prejudice to the continuance of criminal action against erstwhile

Regd. Off.: C-2, First Floor, Wazirpur Indl. Area, Delhi-110052
+91-11-69340000-69340015
ipbank@ipbankonline.com
www.ipbankonline.com

promoter(s)/ director(s)/ persons who were in charge and responsible for the management of the affairs of the entity / business enterprise.

The penal measures as detailed above shall not be applicable to entities / business enterprises after implementation of the resolution plan under IBC or aforesaid prudential framework.

However, the penal measures shall continue to apply to the erstwhile promoter(s)/ director(s)/ persons who were in charge and responsible for the management of the affairs of the entity / business enterprise.

3.2.7 Legal Audit of Title Documents in respect of Large Value Loan Accounts

Bank shall subject the title deeds and other related title documents in respect of all credit facilities of ₹1 crore and above to periodic legal audit and re-verification, till the loan is fully repaid. The scope and periodicity of legal audit shall be in accordance with the Board approved policy/Loan Manual.

4. Reporting of Incidents of Fraud to Reserve Bank of India (RBI)

To ensure uniformity and consistency while reporting incidents of fraud to RBI through Fraud Monitoring Returns (FMRs) using online portal (CIMS), bank shall choose the most appropriate category from any one of the following:

i. Misappropriation of funds and criminal breach of trust;

ii. Fraudulent encashment through forged instruments;

iii. Manipulation of books of accounts or through fictitious accounts, and conversion of property;

iv. Cheating by concealment of facts with the intention to deceive any person and cheating by impersonation;

v. Forgery with the intention to commit fraud by making any false documents/electronic records;

vi. Wilful falsification, destruction, alteration, mutilations of any book, electronic record, paper, writing, valuable security or account with intent to defraud;

vii. Fraudulent credit facilities extended for illegal gratification;

viii. Cash shortages on account of frauds;

ix. Fraudulent electronic banking / digital payment related transactions committed on the Bank; and

x. Other type of fraudulent activity not covered under any of the above.

Regd. Off.: C-2, First Floor, Wazirpur Indl. Area, Delhi-110052
+91-11-69340000-69340015
ipbank@ipbankonline.com
www.ipbankonline.com

4.1 Modalities of Reporting Incidents of Fraud to RBI

Bank shall furnish FMR in individual fraud cases, irrespective of the amount involved, immediately but not later than 14 days from the date of classification of an incident / account as fraud. The 'date of classification' shall be the date when due approval from the competent authority is obtained for such classification of fraud and a reasoned order is passed at the bank. Any further updates in such fraud cases shall be provided to RBI through FMR Update Application (FUA).

Bank shall adhere to the prescribed timeframe for reporting of fraud cases to RBI. Bank shall examine and fix staff accountability for delays in identification of fraud cases and in reporting to RBI since delay in reporting of frauds, and the consequent delay in alerting other banks, could result in similar frauds being perpetrated elsewhere.

While reporting frauds, bank shall ensure that persons / entities who / which are not involved / associated with the fraud are not reported in the FMR.

The bank may, under exceptional circumstances, withdraw FMR / remove name(s) of perpetrator(s) from FMR. Such withdrawal / removal shall, however, be made with due justification and with the approval of the Board.

4.2 Date of Occurrence and Date of Detection: The 'date of occurrence' is the date when the actual misappropriation of funds has started taking place, or the event occurred, as evidenced / reported in the audit or other findings. The 'date of detection' is the actual date when the fraud came to light in the concerned branch/audit/department, as the case may be, and not the date of approval by the competent authority of the Bank.

4.3 Closure of Fraud Cases Reported to RBI

Bank shall close fraud cases using 'Closure Module' where the actions as stated below are complete:

i. The fraud cases pending with LEAs / Court are disposed of; and

ii. The examination of staff accountability has been completed.

In all closure cases of reported frauds, bank shall maintain details of such cases for examination by auditors.

4.4 Monitoring & review: The Committee of Executives (CoE) shall monitor and ensure follow up of cases of frauds involving amounts of 1 crore and above exclusively, while the Audit Committee of the Board (ACB) may continue to monitor all the cases of frauds in general. Since retail cyber frauds and electronic banking frauds have the potential to reach large proportions, the CoE shall be briefed separately on this to keep them aware of the proportions of the fraud, modus operandi and steps taken by the Bank to mitigate them. All such cases shall be reviewed by the Board at quarterly intervals.

Regd. Off.: C-2, First Floor, Wazirpur Indl. Area, Delhi-110052
+91-11-69340000-69340015
ipbank@ipbankonline.com
www.ipbankonline.com

5. Cheque Related Frauds – Precautions to be taken and Reporting to RBI and the Police

The Bank has reviewed and strengthened the controls in the cheque presenting/passing and account monitoring processes and ensured that all procedural guidelines including preventive measures are followed meticulously by the dealing staff/officials.

Banks shall take appropriate precautionary measures to ensure that the confidential information viz., customer name / account number / signature, cheque serial numbers and other related information are neither compromised nor misused either from the bank or from the vendors' (printers, couriers etc.) side.

5.1 Reporting to LEAs / IAs and RBI – Cheque related frauds:

5.1.1 Reporting of frauds involving forged instruments in case of cheque truncation shall continue to be done by paying banker and not by the presenting banker. In such cases, the presenting bank shall immediately handover the underlying instrument to the paying bank, as and when demanded, to enable them to inform LEAs for investigation and further action under law and to report the fraud to RBI.

5.1.2 However, in the case of presentment of an instrument which is genuine but payment has been made to a person who is not the true owner; or where the amount has been credited before realization and subsequently the instrument is found to be fake / forged and returned by the paying Cooperative Bank, the presenting Bank which is defrauded or is put to loss by paying the amount before realization of the instrument shall file the fraud report with the RBI and inform the LEAs for investigation and further action under law.

6. IT/Cyber frauds, Technology related frauds – Digital banking

6.1 Cyber Security Policy: In terms of Comprehensive Cyber Security Framework for Primary Urban Cooperative Banks (UCBs), depending upon the level of complexity of its business and acceptable levels of risk, the Bank has already put in place a Board approved Cyber Security Policy, distinct from the broader IT / IS security policy. The Board of Directors is ultimately responsible for the information security of the Bank and shall play a proactive role in ensuring an effective IT (Information Technology) and IS (Information System) governance. Top management shall ensure implementing the Board approved cyber security policy, establishing necessary organisational processes for cyber security and providing necessary resources for ensuring adequate cyber security.

6.2 Citizen Financial Cyber Frauds Reporting and Management System (CFCFRMS): The Bank has onboarded on Citizen Financial Cyber Frauds Reporting and Management System (CFCFRMS), a platform developed by Indian Cyber Crime Coordination Centre(I4C), Ministry of Home Affairs where State Law Enforcement Agencies register complaints using helpline number 1930 in their respective states.

6.3 DAKSH: The Bank has also on-boarded on DAKSH, a web-based end-to-end workflow application of RBI to monitor compliance requirements in a more focussed manner. The

Regd. Off.: C-2, First Floor, Wazirpur Indl. Area, Delhi-110052
+91-11-69340000-69340015
ipbank@ipbankonline.com
www.ipbankonline.com

application will also enable seamless communication, inspection planning and execution, cyber incident reporting and analysis, and provision of various MIS reports, among others, through a platform which enables anytime-anywhere secure access. For effective utilization of all the functionalities of DAKSH in a secured and authorized manner, the Bank has outlined its policy document as per extant guidelines for implementation & proper usage of DAKSH Application. Responsibility of Nodal Officer on the portal has been entrusted to the CEO by the Board. The Bank has also a designated Chief Information Security Officer and Chief Compliance Officer as per RBI guidelines on implementation of the scheme guidelines.

6.4 Digital Intelligence Platform: The Bank has also on-boarded on the Digital Intelligence Platform (DIP) developed by the Department of Telecommunications (DoT). It is a secure and integrated platform for real time intelligence sharing, information exchange and coordination among the Telecom Service Providers, law enforcement agencies, banks and financial institutions, social media platforms, identity document issuing authorities etc. The portal also contains information regarding cases detected as misuse of telecom resources. The shared information would be useful to all stakeholders in their respective domains. It also works as backend repository for the citizen-initiated requests on the Sanchar Saathi portal for action by the stakeholders.

6.5 Regulatory Compliance:

- the Bank has applied value-based limits (per customer per day limits) on outward IMPS transactions during business and non-business hours to align with RBI guidelines;
- The Bank shall seek confirmation on Firewall status from its third-party CBS service provider and held on record.
- The CBS service provider shall also mandatorily enable logs of all their ICT systems and maintain them securely for a rolling period of 180 days and the same shall be maintained within the Indian jurisdiction. These shall be provided to CERT-In along with reporting of any incident or when ordered / directed by CERT-In.
- IT infrastructure shall be subjected to IS audit/ VAPT / System Audit & Gap Assessment with regard to Comprehensive Cyber Security Framework through a Cert-In empanelled auditing firm and ensure compliance of observations.
- Extant RBI guidelines, Advisories & Alerts shall be immediately taken up for compliance at the Bank and with our third-party CBS providers/vendors;
- Life cycle of IT assets shall be monitored;
- The Bank shall implement email security features whereby all sensitive or confidential information shall be encrypted in transmission. Further the Bank shall be able to block locked files from unknown users. Unwanted domains are also being blocked.
- The Bank shall monitor and manage cyber risks through Cyber Security Operations Centre (CSOC).

Regd. Off.: C-2, First Floor, Wazirpur Indl. Area, Delhi-110052
+91-11-69340000-69340015
ipbank@ipbankonline.com
www.ipbankonline.com

6.6 Reporting of Cyber Incidents/Frauds: The Bank has outlined its Cyber Security Incidence Reporting and Response policy in terms of revised guidelines on regulatory expectations, issued by the CSITE Group, RBI, besides defining mandatory procedures for the bank to report cyber security incidents which applies to all those agencies affiliated with the bank, including third party vendors, where an unusual cyber incident in their premise, directly or indirectly affect security of the bank. Bank shall ensure reporting and follow-up of all cyber incidents exclusively on the DAKSH portal:

- Bank shall report unusual cyber incidents to the Reserve Bank of India (RBI) positively within six hours of detection;
- Shall report all cyber incidents exclusively on the DAKSH portal;
- Report must include a clear description of the incident, time of detection, potential impact, initial action taken and any other relevant information;
- Shall respond to queries raised by the Cyber Security and IT Risk Group (CSITEG) on DAKSH portal within five working days, unless a specific timeline is mentioned.
- Initial reporting to be followed up with detailed Root Cause Analysis after investigation is completed;
- Promptly respond to follow-up queries from CSITEG;
- The responsibility for reporting cyber incidents lies with the Chief Information Security Officer (CISO) or any other competent authority
- Regular training sessions to ensure all stakeholders involved are familiar with DAKSH portal and understand the importance of timely incident reporting and response.

6.7 Fraud investigation & recovery:

The examination of a suspected fraud or an exceptional transaction or a customer dispute/alert in a bank shall be undertaken by CoE or any senior official designated for the same. In case of need, the investigating team shall seek the support of other specialised groups within the bank, such as the audit group to carry out investigations efficiently.

The Bank shall make all out efforts to recover the amount lost. The investigation team may also be able to recover some amounts during the course of their investigation. The Police may also recover some amount during their investigation. This would be deposited in Court pending final adjudication. The bank should liaise with the Police and keep track of such amounts.

6.8 Reporting of Frauds to Law Enforcement Agencies (LEAs). Bank shall immediately report the incidents of fraud to appropriate LEAs viz. State Police authorities, etc. Bank has

Regd. Off.: C-2, First Floor, Wazirpur Indl. Area, Delhi-110052
+91-11-69340000-69340015
ipbank@ipbankonline.com
www.ipbankonline.com

designated Nodal Officer and a SPOC (single point of contact) for reporting/sharing of cyber incidents of fraud to LEAs and IAs.

However, instances of phishing/vishing at customer end (not meeting the given criteria) / Accounting, clerical errors that are rectified/reversed subsequently / viruses, malwares, Trojans, vulnerabilities that are detected and handled appropriately / DoS / DDoS attack not lasting beyond 30 minutes contiguously or not impacting customer service / phishing websites, rogue apps that are monitored/brought down / branch connectivity issues / Physical tampering of ATMs/ATM sabotage are not required to be reported under unusual cyber incident.

6.9 Sharing of Information with LEAs/IAs: A Standard Operating Procedure (SOP) on sharing of requisite digital and physical information with LEAs and IAs, has been drawn by the Bank on the basis of procedural guidelines of the Central Economic Intelligence Bureau (CEIB) shared by the RBI with the Bank, for implementation by all branches/ Head Office of the Bank.

6.10 Cyber Crisis Management Plan (CCMP): The Bank has a well-defined Cyber Crisis Management Plan to analyze the scope of cyber incidents, policies, actions and responsibilities for a coordinated approach to prepare for rapid identification, information exchange, response and remediation to mitigate and recover from malicious cyber related incidents which may impact the critical business functions and processes at the Bank.

This plan takes into consideration the crisis that may occur due to cyber security incidents and breaches and presents a broad-based approach to deal with such crisis. The approach and methodology of this Cyber Crisis Management plan is derived from the 'Cyber Crisis Management Plan for countering cyber-attacks and cyber terrorism' prepared by CERT-In, MeitY, (Ministry of Electronics & Information Technology) Government of India.

7. Other Instructions

7.1 Treatment of accounts classified as Fraud and sold to other Lenders/ARCs: Bank shall complete the investigation from fraud angle & report to RBI before transferring the loan account / credit facility to other lenders / ARCs.

7.2 Role of Auditors: During the course of the audit, auditors may come across instances where the transactions in the account or the documents point to the possibility of fraudulent transactions in the account. In such a situation, the auditor shall immediately bring it to the notice of the senior management and if necessary, to the Audit Committee of the Board (ACB) of the Bank for appropriate action.

7.3 Internal Audit: Internal Audit at the Bank shall cover controls and processes involved in prevention, detection, classification, monitoring, reporting, closure and withdrawal of fraud cases, and also weaknesses including delay in reporting, non-reporting, conduct of staff accountability examination, prudential provisioning etc. observed in the critical processes in the fraud risk management framework of the Bank.

Regd. Off.: C-2, First Floor, Wazirpur Indl. Area, Delhi-110052
+91-11-69340000-69340015
ipbank@ipbankonline.com
www.ipbankonline.com

7.4 Reporting Cases of Theft, Burglary, Dacoity and Robbery

Bank shall report instances of theft, burglary, dacoity and robbery (including attempted cases), to Fraud Monitoring Group (FMG), Department of Supervision, Central Office, Reserve Bank of India, immediately (not later than seven days) from their occurrence in prescribed format 'Report on Bank Robbery, Theft, etc. (RBR) through email (available on website of RBI)

Bank shall also submit a quarterly Return (RBR) on theft, burglary, dacoity and robbery to RBI using online portal, covering all such cases during the quarter. This shall be submitted within 15 days from the end of the quarter to which it relates.

8. Annual Review of frauds:

Bank shall conduct an annual review of the frauds and place a note before the Board of Directors through Audit Committee of the Board for information. The reviews for the year-ended December may be put up to the Board before the end of March the following year. Such reviews need not be sent to RBI and are preserved for verification by the RBI inspectingofficials.

The main aspects which may be taken into account while making such a review may include the following:

a. Whether the systems in the bank are adequate to detect frauds, once they have taken place, within the shortest possible time.

b. Whether frauds are examined from staff angle.

c. Whether deterrent punishment is meted out, wherever warranted, to the persons found responsible.

d. Whether frauds have taken place because of laxity in following the systems and procedures and, if so, whether effective action has been taken to ensure that the systems and procedures are scrupulously followed by the staff concerned.

e. Whether frauds are reported to local Police.

9. Policy Review: The policy shall be reviewed every three years or earlier on receipt of revised regulatory guidelines on the subject received from RBI from time to time.

****

INDRAPRASTHA SEHKARI BANK LIMITED
इंद्रप्रस्थ सहकारी बैंक लिमिटेड

Regd. Off.: C-2, First Floor, Wazirpur
Indl. Area, Delhi-110052
+91-11-69340000-69340015
ipbank@ipbankonline.com
www.ipbankonline.com