
	Name of the Policy	Information System Security Policy
	Department	Information Technology Department (ITD)
	Year	2024-25
	Status	

1. Introduction:

- 1.1. Information System Security (ISS)/Information Security (IS) is concerned with safeguarding of information and data both in electronic and physical form, from unauthorized access, perusal or inspection resulting in misuse, disclosure, modification, recording and destruction. ISS ensures that only authorized users have access to accurate and complete information, when required.
- 1.2. IS framework being a set of policies, procedures, rules, regulations, compliance and review functions ensure smooth implementation and seamless operations to achieve the business objectives. Information Technology (IT) without doubt is a business driver and the risk management of IT is the primary area of concern for IS.
- 1.3. The three major constituents of any IS framework/architecture are people, process & technology.
 - a) First, since technology is continuously evolving, security shall move in tandem and keep pace with it. The bank will ensure that IS methods are appropriate to the IT architecture.
 - b) Secondly, the policy shall factor in the changed processes. The bank will evaluate every new process critically in the angle of security.
 - c) Thirdly, people have to understand and implement the policy. This will be ensured by capacity building. Further bank shall adhere to RBI's and other regulatory guidelines on the issue.
- 1.4. **OECD** (ORGANISATION FOR ECONOMIC COOPERATION AND DEVELOPMENT) in its guidelines for the Security of Information Systems and Networks has brought out nine principles namely Awareness, Responsibility, Response, Ethics, Democracy, Risk Assessment, Security Design & Implementation, Security Management and Reassessment.
- 1.5. Efficient IS framework is also a function of awareness, knowledge and skills.
 - a) IT Governance entails number of activities for Board & Senior Management becoming *aware* and impact of IT on a bank.
 - b) IT Security team require *skills and* processes that are effective and needed to carry out efficient operations of the Information Security policy.
 - c) The people in the business functions (users of information and information assets) require *knowledge* on day-to-day basis to use IT ie., awareness should be created on IS within bank as a part of daily operations and to ensure that all employees understand their responsibilities for maintaining IS. For example, for users at various levels in the bank, should understand their role in very simple language like Do's and Don'ts; these are derived from the policy statements.

	Name of the Policy	Information System Security Policy
	Department	Information Technology Department (ITD)
	Year	2024-25
	Status	

2. Need for the policy:

- a) The bank's business philosophy is to ensure optimum use of technology in carrying out the business, while at the same time and under any circumstances not compromising information and data security. Further, the bank is committed to conducting its business activities in such a manner that the business process is smooth, customer service is excellent and business growth is continuous.
- b) Detailed Information Security Standards and procedures are to be established and ensure compliance against such standards and procedures.
- c) Our Bank is implementing many new technologies in banking operations for the smooth conduct of its business. The bank is aware of the security and other challenges faced by it which has led the bank to draft policy guidelines to ensure that its information assets are secured & controlled.

3. Definitions:

3.1. Policy

"Policies" are management instructions indicating a course of action, guiding principles, and appropriate procedure. Policies provide general instructions, while standards provide specific technical requirements.

3.2. Procedure


"Procedures" are specific operational steps or methods that employees must follow/use to achieve goals (collection of procedures in a sequence could be called as a manual). A user manual in IS will include all rules and regulations and procedures that an employee must follow in day to day operations. It will also contain a set of do's and don'ts and a FAQ as well.

3.3. Information Owner:

A person who is responsible for data and records stored on systems is known as "Information Owner". People like business executives, business managers, and asset owners within the organization are known as Information owners.

3.3.1 Duties of Information Owner:

The owner/s may delegate ownership responsibilities to another individual, mostly personnel. While doing so the owner has to ensure that appropriate procedures are in place and followed to protect the integrity, confidentiality and security of the information used or created within his/her/their area. They can authorize access and assign custodianship of information and information asset. Specify controls and communicate the control requirements to the custodian and users of the information. Owner must promptly inform the CISO about loss or misuse of information, who will initiate appropriate actions when problems are identified. CISO has to promote education and awareness by training programs administered where appropriate.

	Name of the Policy	Information System Security Policy
	Department	Information Technology Department (ITD)
	Year	2024-25
	Status	

3.4. Business Heads

“Business Heads” are the official in-charges of various offices and functions (Heads of department in the HO and branch heads). They are responsible for enforcing the implementation of IS Policy within their control or area of operation.

3.5. Information Custodian

“Information Custodian” is the person who is generally responsible for the processing and storage of the information.

3.5.1 Responsibilities of Custodian:

- Providing and/or recommending physical safeguards.
- Providing and/or recommending procedural safeguards.
- Administering access to information.
- Evaluating the cost effectiveness of controls.
- Coordinating the maintenance of IS policy, procedures and standards as appropriate and in consultation with the CISO.
- Report promptly to the CISO the loss or misuse of any authenticated device or information.
- Initiate appropriate actions when problems are identified.

3.6. Information Users:


“Information Users” could be any employee irrespective of the level of hierarchy and will also include contractual personnel, vendors, employees of vendors, employees of service providers etc.

3.6.1 Responsibilities of Information Users:

- Access information only in line with authorized job responsibilities or roles.
- Comply with IS Policies and Standards and with all controls established by the owner and custodian.
- Adhere to all norms regarding disclosures of confidential information and refer to the authority where ever the disclosures are not defined.
- Keep authentication of devices (e.g. passwords, Secure-Cards, PINs, etc.) confidential.
- Report promptly to the IS Officer the loss or misuse of any authenticated device.
- Report promptly to the IS Officer the loss or misuse of information.
- Initiate appropriate actions when problems are identified.

3.7. Outsourcing:

“Outsourcing” means asking a third party to do a set of activities for the bank either outside the bank or inside the bank keeping in view of the confidentiality of the information which include operational, data processing, back office and third-party related activities. Bank should retain ultimate control of the outsourced activity. The

	Name of the Policy	Information System Security Policy
	Department	Information Technology Department (ITD)
	Year	2024-25
	Status	

outsourcing activities are subject to regulatory oversight.

4. Information Technology/Technology Risk:


It is a type of business risk defined as the potential for any technology failure to disrupt a business. Bank may face many types of technology risks, such as information security incidents, cyber-attacks, password theft, service outages, risk of non-compliance with data protection regulations etc., and common types of technology risks are Phishing, Malware, Data Breaches, Obsolete equipment etc.

Technology risk assessment & Management:

- a) It is driven by both, by the top as well as from the IT department, wherein regular assessments are done by way of vulnerability assessments, incident impact analysis, IT control testing and regular systems audits to ensure the appropriate technology and security practices are undertaken.
- b) Technology risk assessments are sustainable and include financial and non-financial impacts on the business operations of the Bank. Technology risks are continuously assessed to ensure the appropriate IT control mechanisms are put in place.
- c) The Risk Management process of Information Security Management consists of:
 - Identification of assets and estimation of their value including aspects like people, buildings, hardware, software, data, etc.
 - Threat assessment includes aspects like acts of nature, war, accidents, malicious acts of outsiders and insiders, etc.
 - Vulnerability assessment for each item and calculating the probability that will be exploited.
 - Incidents impact analysis.
 - Process of risk management is an ongoing one and the same should be reviewed/updated at least once a year.
 - Identifying and implementing appropriate controls mechanisms.
 - Evaluation whether the control measures provide cost effective protection.
 - Monitor the implementation of Security Policies and Standards in all Branches/ Head Office, administrative units.
 - Monitoring of ISS Policy on a continuing basis which will be carried out by the designated officials (e.g. IT Head, Administrative head, and at the grass root level, the Branch Manager).

5. IT Security and Controls in the Bank:

Our bank has introduced technology in a number of areas as mentioned above. In view of this, the implementation of processes will change along with the way we do our business. The focus will shift from branch to bank. Customers will be able to access their accounts from their home. On account of these changes, certain risks are

	Name of the Policy	Information System Security Policy
	Department	Information Technology Department (ITD)
	Year	2024-25
	Status	

foreseen in the area of security of the bank's information assets in terms of unauthorized access to bank's information and data, breakdowns in business due to technical issues or non-availability of technology support, frauds and theft in the ATMs and card business and customers facing difficulties in accessing their accounts or customers being subject to electronic threat etc. In fact, the list of vulnerable areas is large. Every one of the known vulnerability needs to be addressed if it has to be ensured that users of bank's services and banks customers have full confidence that the bank and its information systems will operate as intended without failures or problems. Bank cannot guarantee that breach of security will not happen, but it will like to minimize such possibilities. Here again bank will ensure that technology is optimally utilized and that IT enhances future growth. It is in this background that the bank is putting in place an IT security system and control mechanism to minimize the risk of security incidents involving IT usage.

6. Objective and Scope:

6.1 Objective:


"This IS Policy of The Prakasam District Cooperative Central Bank Ltd has been established with an objective of protecting all critical information and information processing assets in order to ensure secure and correct provision of services to its customers and ensure business continuity."

The objective of this is to ensure that the information assets of the bank are appropriately protected against the breach of confidentiality, failures of integrity and/or interruptions to their availability. IS is concerned with various channels like spoken, written, printed, and electronic or any other medium and also with the handling of information with reference to creation, viewing, transportation, storage or destruction. This IS Policy provides management direction and support towards IS across all relevant levels and locations within and outside the bank.

This policy mandates the IS Management at the bank. It communicates top management's commitment towards establishment and implementation of all security controls and mechanisms as given out in this and other documents lays down the structure of IS management in the bank. The IS strategy is aligned with the business objectives and legal requirements.

Specific objectives of the ISS is:

- i. **CONFIDENTIALITY:** To prevent unauthorized disclosure of information stored or processed on bank's information systems. Breaches of confidentiality may take many forms. This can be avoided by keeping the confidential data in secured places and restricting the access. (e.g., the CVV number in a credit used for operations through the internet for purchase of goods. This is vulnerable for hacking and should be protected by using the encryption techniques.)
- ii. **INTEGRITY:** To prevent the accidental or unauthorized, deliberate alteration or

	Name of the Policy	Information System Security Policy
	Department	Information Technology Department (ITD)
	Year	2024-25
	Status	

deletion of information. The data cannot be modified. It is violated when an employee modifies/alters the data accidentally or with intention to avail the benefit from the system.

- iii. AVAILABILITY: To ensure that the information is available to the authorised users as and when required. The computer system should be able to store and process the information and necessary security should be built in to secure the data. The users should be able to retrieve the data as and when required within the shortest time possible.


Critical processes are identified, and technology risk related to those processes are assessed and addressed on periodic basis. Control gap assessment is done on a periodical basis and reported to senior management for timely remedial action. The security requirements/configurations for each and every device is to be documented and reviewed annually.

To achieve the objective of Information systems security one needs to consider the information security processes. They are given below:

- a. Identification – The process of distinguishing one user from all others. The system should be able to identify the person who is accessing it, so that the accountability can be fixed (eg: User name, password, etc.).
- b. Authentication – The process of identifying the identity of the user. This is to validate that both the parties to the transaction are genuine.
- c. Authorization– Authorizing the access to data. The process of authorizing a user to access the system /data which is done through the access control privileges built in the system.
- d. Access control – It means of establishing and enforcing rights and privileges allowed to users.eg: Fixing the access rights to the users of different categories like front desk, back office, administration, etc. All modules are not given access to all the employees.
- e. Administration – The functions required to establish, manage and maintain security of a system.
- f. Audit – The process of reviewing activities that enables the reconstruction and examination of events to determine if proper procedures have been followed. This is done through the exceptional reports generated in the system.

6.2 Scope of the IS Policy:

IS policy being applicable to all information assets of the PDCCB that are electronically stored, processed, documented, transmitted, printed and/ or faxed. The policy applies to all employees and external parties which term includes suppliers, vendors, third party users, contract staff, outsourced service providers and consultants of the bank's Primary Data Centre, Disaster Recovery Centre/Cell, CBS, Department of IT as well as all other locations of the bank.

	Name of the Policy	Information System Security Policy
	Department	Information Technology Department (ITD)
	Year	2024-25
	Status	

7. Owners and Custodians:

For a policy to be effective it is imperative that each of the stakeholders understand clearly his/her as well as other's roles & responsibilities within the organizational framework. Important aspects of the role are (a) Governance, (b) Strategy, (c) Creation, implementation, operations, compliance and review of the IS policies in line with the banks broad requirements and activities.

Board of Directors of the bank is the owner of IS Policy. Chief Information Security Officer (hereafter referred to as CISO) will be the custodian of the policy.

8. Responsibilities of Board of Directors:


The Board is vested with the overall responsibility of ISS. It will develop policy guidelines to be conveyed and implemented by various layers in the organization namely people (employees and other persons entrusted with the responsibility of different business functions) at senior, middle and the grass-root levels. In doing so, the Board will keep in reckoning major objectives of the ISS. ISS policy should be such that people, when they are aware of the banks' expectations from them, are able to implement the policy in full and without any deficiency. In this regard, policies have to be clear and well enunciated.

1. Policy should be supported with standards, guidelines & procedures.
2. Policy should be statements on macro, major and organizational level issues.
3. Procedures and rules should deal with implementation of policy statements. Implementation should cover procedure, functions and technologies.
4. IS strategy have to be aligned with business objectives, indicate scope of ownership, individual & team responsibilities for the policy. These should include items such as role of IT security officer, owners of information assets, custodian and users.
5. Policy will also need the support of investment for enabling IS and such will deal with budgeting, financial outlay, reporting etc.
6. Policy must be reviewed in regular periodicity at least annually. The focus of the Policy review will be continuous improvement in IS.
7. IS governance must comply with relevant legal and regulatory requirements.

It is provided that in exceptional and emergency situations the IS Committee can approve emergency changes in the Policy which should be ratified by the Board of Management of the Bank in the meeting immediately after such changes.

9. IS Committee:

The IS Committee (ISC) of the bank is responsible for implementation of security policy and for dissemination of IS Policy across all business functions. The CHIEF EXECUTIVE OFFICER (CEO) of the bank will be the Chairman of the Committee and the CISO will be its convener. Selected Business heads of the bank will be the

	Name of the Policy	Information System Security Policy
	Department	Information Technology Department (ITD)
	Year	2024-25
	Status	

members of the committee. The committees' main focus will be supervising and oversight of IS. It will also align & integrate IT and IS strategy with business goals. The committee will meet on a regular basis to discuss implementation of IS.

- i. The committee shall be responsible for making budgets, reviewing the security procedures and compliance, as also guide people with corrective action where needed. Information Security Committee will ensure that threat & vulnerabilities are evaluated, and initiate/undertake remedial action, where ever necessary on an ongoing basis.
- ii. Risk Management Committee of the bank will also review IT security in a routine manner and will take care for promoting security throughout the bank including assisting development of IT based measures and compliance.
- iii. Bank shall ensure that technology is available for updating in a manner that efficiency and security are given paramount importance.
- iv. Lastly audit and fraud monitoring management are to be taken care of compliance.


10. Chief Information Security Officer (CISO)

The bank will nominate/appoint a CISO or entrust the exclusive responsibility of CISO to an official of the bank. Chief Information Systems Security Officer (CISO) would be responsible for the implementation, review and updating of the Information Systems Security which also reflect the Bank's requirement. He will be assisted by a team of Officers comprising both Technical and Banking Officers. CISO will be responsible for the implementation of information systems security policies in each and every one of the offices/locations of the bank.

CISO in the bank will be fully involved in various issues such as the development of the Information Systems Security Policy, updating of the Information Systems Security Guidelines on an on-going basis. In performing his/her role, the CISO will work through the existing systems and as such the banks administration department will among others, have the responsibility of the security controls and compliance with the information systems security guidelines.

The job role of CISO will include:

- a) To create, maintain and disseminate IS strategy, plans policies and procedures.
- b) To carry out assessment and review of IS risk threats and vulnerability assessment in regular periodicity.
- c) To monitor & report on a continuous basis.
- d) To obtain approval at appropriate level for IS plan, budget, resources and provide on-going support activities.
- e) To ensure that monitoring, testing and reporting of Information Security is done in an effective and efficient manner.
- f) To install effective controls to ensure compliance with IS norms.

	Name of the Policy	Information System Security Policy
	Department	Information Technology Department (ITD)
	Year	2024-25
	Status	


- g) Establish and maintain awareness and training to promote IS across the bank.

11. Coverage of the Policy:

- a) Covers all forms of electronic/print information etc. on servers, desktops, networking and communication devices, tapes, CDs, USBs and other devices. Information printed or written on paper or transmitted by facsimile or any other medium is also covered.
- b) Envisages that appropriate procedures will be created and followed at various levels of the bank to ensure absolute protection of IS. The IS objectives are set for its continual improvement.
- c) Provides directives towards IS within the Bank.
- d) Recommends appropriate security controls that have to be implemented to maintain and manage IS system in the bank.

12. To Achieve the above Objectives:

- a) The bank shall be establishing and organizing the IS governance framework so as to ensure alignment of the IS of the bank with business strategy to support growth and other organizational objectives.
- b) The bank will also be developing and maintaining an effective IS management system supported by appropriate procedures and rules in consonance with the policy.
- c) Through the CISO the bank will conduct periodic risk assessments and ensure adequate, effective and tested controls for people, processes and technology to enhance IS. Through this means the bank will ensure that critical information is protected from unauthorized access, use, disclosure, modification, and disposal, whether intentional or unintentional.
- d) The bank recognizes that this will call for deploying appropriate technology and infrastructure and training its people. The bank will particularly insist on its senior officials for monitoring, reviewing, exception reporting and taking actions thereof for improving the effectiveness of the IS management system.
- e) The bank shall provide an environment for promoting 'best practices' relative to its business, information systems and infrastructure;
- f) The bank shall ensure that all legal and contractual requirements with regard to IS are met wherever applicable and that any security incidents and infringement of the policy, actual or suspected, are reported and investigated;
- g) The bank shall organize awareness programs and training on IS to all employees as also other contractors, consultants, vendors etc.;
- h) More importantly the bank shall (a) take immediate and suitable actions for managing violation(s), if any of the IS Policy; and (b) develop a IS compliance culture in the bank.

	Name of the Policy	Information System Security Policy
	Department	Information Technology Department (ITD)
	Year	2024-25
	Status	

13. IS Review

The implementation of IS in the bank will be one of agenda items of most of the Board meeting. Further the IS Policy document shall be reviewed, by the Board periodically and at least once a year as also at the time of any major change(s) in the existing environment which will affect the policies and procedures. The reviews will cover the following:

- a) CISO report on IS and its implementation
- b) Impact on the risk profile in the bank due to changes in the information assets, technology/architecture, regulatory and legal requirements. The impact assessment will focus on effectiveness of IS policies and periodic compliance review of the policy adherence.

It is possible that as a result of the reviews there could be some need to frame additional policies or amend/update the existing policies. These additions and modifications will be incorporated into this ISS Policy document. Policies that are not relevant due to changes in the regulation etc. shall be withdrawn.

14. Applicability and Exceptions

- a. All employees and external parties are required to strictly comply with IS Policy. The bank must announce that **non-compliance to IS Policy is a ground for disciplinary action.**

b. Exceptions:

The IS Policy is a guideline and a policy pronouncement on IS requirements which is needed in the business interest of the bank. However, for smooth conduct of business exceptions against individual controls in specific policy domains shall be documented and formally approved by GM Banking in consultation with Head IT.

15. Review and modifications to the Policy:

Taking into consideration of the circulars from RBI/NABARD/NPCI and IS Cell recommendations, CHIEF EXECUTIVE OFFICER is authorized to make suitable changes to the policy from time to time. The policy to be reviewed on annual basis.

Sd/-
CHIEF EXECUTIVE OFFICER