ZILA SAHKARI BANK LTD,GARHWAL (KOTDWAR)
HEAD OFFICE - KOTDWAR

INFORMATION SYSTEM POLICY (IS POLICY)

PART - I A

1. Introduction

1.1 Banking industry uses information in every aspect of its business, from processing payments to making loan and investment decisions. Information and the supporting processes, the computer systems and the networks, and personnel (human beings) are important business assets of every Bank.

1.2 Customer confidentiality is important for all businesses but it is an USP for banking business and hence more important. In order to maintain customer confidentiality and cater to business growth information has to be fully protected from a variety of threats so as to ensure confidentiality, integrity & availability. The confidentiality, integrity and availability of information in the right place to the right person for right purposes are essential for any bank of financial institution to maintain its competitive edge, cash flow, profitability, legal compliance and reputation.

1.3 The adoption of Information Technology (IT) has brought about significant changes in the way the banking and the financial institutions create, process and store data and information. The communication networks have also played an equally catalytic role in the expansion and integration of the Information Systems, within and among the banks, facilitating data accessibility to different users.

1.4 Loss of information may lead to (a) financial losses which need to be minimized and (b) loss of reputation which must be avoided. In view of this it is important that our bank puts in place an appropriate set of controls & procedures to achieve impeccable IS (IS) to ensure that data is accessible and accessed only by authorized users of data and is completely inaccessibility to all others (unauthorized persons trying to use the system, information etc). Essentially this is an issue of data integrity and implementation of safeguards against all security threats to guarantee information and information systems security across our Bank.

1.5 As technology is evolving and ever changing it is possible that information systems in operation in banks may not have been designed to be sufficiently secure. Further, the level of security, which can be achieved through the application of technology, could be limited unless it is supported by appropriate management policies and procedures. The selection of the security controls requires careful and detailed planning. It is clear that the success of information systems security cannot be achieved except with the participation by all the employees in the Bank. It will also require support and participation from the third parties such as the suppliers, vendors, contractors and customers. This calls for our Bank to define, document, communicate, implement and audit Information and Information Systems Security.

2. Information Technology and Changing Face of Banking.

2.1 Over the last three decades banking industry in India has adopted Information and Communication Technology (ICT) which has resulted in a paradigm shift in the way banking is done in the country. Over the years, what started as a Ledger Posting Machine has moved through Total Branch Automation (TBA) to today's Core Banking Solutions (CBS) and other applications supported I T driven banking. It is seen that banking technology has not only changed the way customer perceives the bank but also the way bank drives its business. Customer is morekeen to use latest technology driven access to banking so that he/she is able to save time and effort in doing banking.

2.2 Continuous use of banking technology has enabled the banks to have a re-look into their business processes, reengineer the same to make them effective & efficient. Rapid technological up-gradation has increased the business volumes without having to increase the branch net- work. Simultaneously there is a demand for processing large amount of information within banks to enable better decision making in response to the changing business environment. The ability of technology to manage large volume of data and has resulted in IT moving from a support function to the main driver of banking business.

2.3 Thanks to the impact of IT, banks' are now able to offer Automated Teller Machine (ATM), Cards (both debit and credit), internet banking and mobile banking to its customers. The CBS gives the customer access to transact his/her account from any of the branches or from home or work place at any time. In the recent years as e-commerce has started flourishing. Banks have stepped in to complement the process as payment gateways for e-shopping, etc. Within the bank internal processes such as accounting, ledger maintaining and other processes within bank are no more manual but are more efficient due to IT driven processing of internal data/activities & back office operations.

3. IT is one of the Major Drivers of Banking Business

3.1 Over the years our bank has been making increased use of IT in business. Our bank has taken the following IT driven initiatives.

3.2 In view of this dependency of our bank on IT is fairly high. Further, IT will be central to all transaction processing. This dependence on IT is only expected to increase with time as newer technology comes into being & keeps on creating better prospects for banking business. Eventually our entire business processes will be through the use of IT.

4. Yet IT can cause Business Vulnerability

4.1. Banking technology is the use of advances in ICT for enhancing banking business. Use of technology can cause certain vulnerabilities due to possible external or internal attack, which may result in failure of the underlying information systems and compromise information assets. There is a risk for data loss due to malafide or accidental or unauthorized access, use, misappropriation, modification or destruction of information, information systems & IT. This possibility is accentuated as the number of users accessing information systems within and outside the bank is on the high side and will keep increasing. As such exercising effective control over the information will remain a

challenge. In view of the above the use of IT in banking has necessitated a completely different set of controls & processes to maintain & monitor and ensure security effectiveness. Managing vulnerability in IS cannot be manual. It is for this reason that business houses, public services and individuals manage the gap between the traditional security and controls and demand put forth by newer technologies by relying on newer technologies. Each new technology may bring in additional concerns about security.

5. I S (IS) defined

5.1 IS **(I S)** is concerned with safe guarding information and data both in electronic and physical form, from unauthorized access, perusal or inspection resulting in misuse, disclosure, modification, recording and destruction. I S ensures that only authorized users (confidentiality) have access to accurate and complete information (integrity) when required (availability)[1]. In its guidelines for the Security of Information Systems and Networks, OECD has brought out nine principles namely Awareness, Responsibility, Response, Ethics, Democracy, Risk Assessment, Security Design & Implementation, Security Management, and Reassessment.

5.2 I.S framework is a set of policies, procedures, rules, regulations, compliance and review functions ensure smooth implementation and seamless operations, to achieve the business objectives. IT is, without doubt a business driver and the risk management thereof is the area of concern for IS. The three major constituents of any I S framework/architecture are people, process & technology. First of all, since technology is continuously evolving, security has to move in tandem and keep pace with it. Our bank will ensure that IS (I S) methods are appropriate to the I T architecture. Secondly the policy has to factor in the changed processes. Our bank will evaluate every new process critically in the angle of security. Thirdly people will have to understand and implement the policy. This will be ensured by capacity building. Further our bank will adhere to RBI's and other regulatory guidelines on the issue.

5.3 Efficient IS framework is also a function of *awareness, knowledge and skills.*

- IT Governance entails number of activities for Board & Senior Management becoming *aware* and impact of IT on a bank.
- IT Security teams require *skills*, processes that are effective and needed to carry out efficient operations of the security policies.
- The people in the business functions (users of information and information assets) require *knowledge* on day-to-day basis to use IT. 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.

6. Our Bank and I T

6.1 Our bank Zila Sahkari Bank Ltd.Garhwal (Kotdwar) is using many new technologies in the banking operations. 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.

6.2 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 conduct its business activities in such a manner that business process are smooth, customer service is excellent and business growth is continuous.

7. IT Security and Controlling the Bank

7.1 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 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 a IT security system and control mechanism to minimize the risk of security incidents involving IT usage.

8. IS Policy: Objectives

8.1 The Policy.

"This IS Policy of District Cooperative bank 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. The users of technology in the bank are its employees, vendors, employees of vendors and most importantly the customers. 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.

9. Scope of the IS Policy

IS policy is applicable to all information assets of District Cooperative Bank 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.

10. Owners and Custodians

For a policy to be effective it is imperative that each 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 IS Officer (hereafter referred to as CISO) will be the custodian of the policy.

11. Responsibility

Board of Directors: Board alone can make changes in the policy. The Board is vested with the overall responsibility of IS. It will develop policy guidelines to be conveyed and implemented by various layers in the organisation 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 IS. IS 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
- Policy should be supported with standards, guidelines & procedures
- Policy should be statements on macro, major and organisational level issues.
- Procedures and rules should deal with implementation of policy statements. Implementation should cover procedure, functions and technologies
- IS strategy has to be aligned with business objectives, indicate scope of ownership and individual and team responsibilities for the policy. These should include items such role of IT security officer, owners of information assets, custodian and users
- Policy will also need the support of investment for enabling IS and such will deal with budgeting, financial outlay, reporting etc.
- Policy must be reviewed in regular periodicity at least annually. The focus of the Policy review will be continuous improvement in IS
- IS governance must comply with relevant legal and regulatory requirements

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

12. Steering Committee/ 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 Secretary/General Manager of the bank will be the Chairman of the Committee and the CISO will be its convener. Select Business heads of the bank will be 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.

- 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 Risk management Committee/function of the bank will also review IT security in a routine manned and will take care for promoting security throughout the bank including assisting development of IT based measures and compliance
- Bank shall ensure that technology is available for updating in a manner that efficiency and security are given paramount importance. Best process can be defined as Corporate IS Policy (CISP) about deployment, use and maintenance for all people as per the various levels.
- Lastly audit, fraud monitoring management to review to take care of compliance

13. Chief IS Officer (CISO)

The bank will nominate/appoint a CISO or entrust the exclusive responsibility of CISO to an official of the bank by whatever name called. CISO is responsible for ensuring that IS policies are regularly updated and reflect the bank's requirement.

- CISO will have a dedicated, skilled & adequate staff team.
- The job role of CISO will include:
    - create, maintain and disseminate IS strategy, plans policies and procedures
    - carry out assessment and review of IS risk threats and vulnerability assessment in regular periodicity,
    - monitoring & reporting on a continuous basis
    - will obtain approval at appropriate level for IS plan, budget, resources and provide on-going support activities
    - Ensure that monitoring, testing and reporting of IS done in an effective and efficient manner. Will install effective controls to ensure compliance with IS norms.
    - establish and maintain awareness and training to promote IS across the bank

14. Business Heads

Business heads are the officer- in-charge 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. It is however clearly stated that every bank Employee, officer and contractors/consultants must comply with IS Policy and protect the bank's information assets.

15. Coverage of the Policy

15.1. 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.

15.2. 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.

15.3. Provides directives towards IS within the Bank

15.4. Recommends appropriate security controls that have to be implemented to maintain and manage IS system in the bank.

16. To Achieve the above Objectives

16.1. 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.

16.2. The bank will also be developing and maintaining an effective IS management system supported by appropriate procedures and rules in consonance with the policy.

16.3. 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.

16.4. 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.

16.5. The bank will provide a environment for promoting 'best practices' relative to it's business, information systems and infrastructure;

16.6. The bank will 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;

16.7. The bank will organize awareness programs and training on IS to all Employees as also other stakeholders such as contractors, consultants, vendors etc;

16.8. More importantly the bank will (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.

17 - IS Review

17.1 The implementation of IS in the bank will be one of agenda items of all 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:

17.1.1. CISO report on IS and its implementation

17.1.2. 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.

17.1.3. 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 IS Policy document. Policies that are not relevant due to changes in the regulation etc shall be withdrawn.

18. Applicability and Exception

18.1 All employees and external parties are required to strictly comply with IS Policy. The bank has announced that **non-compliance to IS Policy is a ground for disciplinary action.** This provision will be incorporated in the Bank's disciplinary policy.

18.2 - 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 operations in consultation with Head IT.

19. Certain Terms Explained

1. Policy & Procedures how distinguished?

"Policies" are management instructions indicating a course of action, guiding principles, and appropriate procedure. Policies are mandatory and can also be thought of as the equivalent of an organization structure and governance giving responsibilities and segregation of duties for a given objective say protection of a bank's information and information assets. Policies are distinct from and considerably higher-level than "procedures" (sometimes called "standard operating procedures"). A policy statement describes an issue or an aspect or a subject only in a general way for addressing a specific problem. 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.

A standard could define how a software has to be used to perform back-ups and how to configure that software. A procedure could describe how to use the back-up software, the timing for taking back-ups, and other ways that Users interact with the back-up system. Policies drives standards and procedures and all of them require compliance. Policies provide general instructions, while standards provide specific technical requirements. Operational steps are known as procedures.

2. Who is an information owner?

Data and records stored on systems are responsibility of Information Owner, like business executive, business managers, and asset owners within the organization. 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
ducation and awareness by training programs administered where appropriate.

1. Who is an Information Custodian?

The custodian of information is the person who is generally responsible for the processing and storage of the information. Responsibilities may include:

- 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 policies, procedures and standards as appropriate and in consultation with the IS Officer.
- 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.

2. Who are information Users?

User of information could be any employee irrespective of the level of hierarchy and will also include contractual personal, vendors, employees of vendors, employees of service providers etc. They are expected to:

- 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 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.

5. What is Outsourcing?

In keeping with this international trend, it is observed, that banks in India too have extensively outsourced various activities. Outsourcing means asking a third party to do a set of activities for the bank either outside the bank or inside the bank. These activities are not

PART -I B

1. Information Systems Security Policy

Comprehensive IS policy document has to be, overall, in alignment with the business management objectives. The policy statements have to be further granulated for arriving at documented procedures.

The policy statements are provided in this Part (Part – B) of the document. Chief Information Systems Security Officer (CISO) would be responsible for the implementation, review and updating of the Information Systems Security. 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 policy's 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 role the CISO will work through the existing systems and as such the banks administration department will among others, have the responsibility of the S ecurity controls and compliance with the information systems security guidelines.

2. Environment & physical security

2.1 Purpose

Control of physical and electronic access to confidential information and computing resources is must to ensure IS. . To ensure appropriate levels of access, a variety of security measures must be instituted based on business needs and as recommended by the Chief IS Officer.

2.2 Policy Statement

Mechanisms to control access to confidential information and IT assets shall include all sites situated within the bank. The assets shall be protected against unauthorized environment and physical threats. For this purpose the bank will give clear guidelines on authority and responsibility for its employees and other authorized stake holders to access the information and IT assets. Bank employees will strictly adhere to these norms/guidelines. Detailed rules on this regard will be issued by the bank.

3. Acceptable U sage Security

3.1 Purpose

The purpose of this policy is to clarify users' rights, responsibilities, information assets and rights, to shield the organization against potential threats and liabilities. Bank assets are provided for business purpose. User of information is expected to access information only in support of authorized job responsibilities or role.
This will

- Minimize security threats by promoting awareness and good practices
- Encourage effective and positive use of information assets and resources.
- Ensure that users follow safe usage practices that do not hamper business objectives, not to bring disrepute or to attract legal liability

3.2 Policy Statement

Bank assets are l be provided for business purpose and not for the personal use of its employees or other authorized users of information and information assets. To ensure this users shall follow to safe usage practices that do not hamper business objectives, bring disrepute to or attract legal liability. Violations to the usage policy by an employer /user will attract strict action and penalties including disciplinary action.

4. Incident Management

4.1 Purpose

IS incident could be a single or a series of unwanted or unexpected IS events that have a significant probability of compromising business operations and threatening IS. IS incidents are those which impact I T security. Incident management call for plan and procedures to deal with the incidents so as to protect the information and or information assets. The purpose of this policy is to develop and implement processes for identifying and responding to IS incidents. The CISO and his/her team shall conduct reviews to identify reasons for IS incidents, evaluate the same and also develop corrective and preventive actions to manage and /or avoid recurrence of the incidents. .

It is necessary that IS events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken.

4.2 Policy Statement

Every employee and user must report such IS events (breach or attack) to his/her immediate supervisor and also to the IS department. The banks IS committee, based on the CISO recommendations define roles and responsibilities for the department heads, branch heads to identify, and manage IS incidents. Events, incidents and problems should be reported to the appropriate authority. Persons vested with the responsibility should respond promptly with a view to contain loss and damage if any and to avoid reoccurrence.

5. Asset Classification & Handling

5.1 Purpose

Bank provides the medium for the purpose of exchanging transaction details through clients/ servers. Failure to properly protect information could have serious effect on the bank. As such, they would have to be protected with stringent security controls.

Information is classified to ensure its proper protection. Immediately after information has been created, modified or acquired, information must be evaluated to determine its classification. Also it should be decided as to how it must be handled. Information asset is any asset that has value for bank & consequently needs to be suitably protected.

5.2 - Policy Statement

Every employee and authorized functionaries of the bank has responsibility in protecting the information asset from unauthorized access, generation, modification, disclosure, transmission or destruction. This is achieved by strictly following laid down procedures. In order to ensure that the security, reliability, integrity & availability of information is not compromised bank has laid down specific procedures and rules for each information activity. Bank will specify authority for appropriate asset handling. Schemes for labels shall be adapted by the bank for marking guidelines for IS.

6. Asset-Media disposal

6.1 - Purpose

Information can be compromised through careless disposal or re-use of media. Storages devices containing sensitive information should be physically destroyed or security overwritten. Rather than using the standard delete functions, all storages media should be checked prior to its disposal to ensure that sensitive data and licensed software, if any is not remained. It should be ensured that such data or software is either removed or overwritten.

6.2 - Policy Statement

Employees, users and authorized officials of the bank shall ensure that banks owned computers, devices storages media shall have all data and licensed software reliable erased from all device at the time of disposal of the media or its movement out of bank control using best practices for each type of media.

7. Anti- Virus

7.1 - Purpose

Bank must be protected against vulnerability due to virus and attack by Trojans and malicious codes. Hence IT assets of the bank must use enterprise level anti-virus solutions on the system.
Appropriate Antivirus solutions approved by the Chief IS Officer and must be deployed for protecting against virus attach and Virus checking. . Wherever possible a multi-layered approach should be used (desktops, servers, gateways, etc.) that ensures that all electronic files are appropriately scanned for viruses. Users (employees and other stake holders) are not authorized to turn off or disable virus checking.

1.6.2 - Policy Statement

Malicious codes are viruses, worms, Trojans, root kits etc. represent significant threat to performance secrecy. Bank shall ensure that these malicious codes are detected early and removed. . These guidelines shall protect IT assets of the bank against malicious code through enterprise level anti-virus solution. Bank will use an appropriate antivirus solution and keep it updated on a regular basis.

8. Networking & Internet Security

8.1 Purpose

Protecting Networking infrastructure against threats and mitigating such threats originating from external, and internal network is of prime importance of the bank. Absence of proper access control and protection can lead to internet based attack that includes unauthorized access from internet; spread of virus, worms, malware, etc. There could be unsecured transit on the network that can lead to unauthorized access leading to loss of critical & sensitive information.

It is necessary to provide secured access to the bank's network to internal and external users, provide adequate redundancy for critical IT assets & establish effective management of the networking infrastructure.

8.2 - Policy Statement

Enterprise network infrastructure shall be appropriately designed, and managed and controlled effectively in order to ensure protection of the information in the network as also of the for support infrastructure. All connections to extended network including Internet, outsourced Vendors and partners shall be authorized and provided in a secure manner. All remote access to the network shall be authenticated & provided based purely on business requirement. Network should be designed & maintained for high availability and to meet the requirement of the User.

9. - Operating Systems

9.1 - Purpose

To determine appropriate risk response options, identify performance gaps between current and desired risk level. Risk associated with IT systems whether appropriate and effectively mitigated to an acceptable level by securing Operating Systems.

9.2 - Policy Statement

Operating systems shall be installed and configured in a proper manner. Operating system shall only be accessed by authorized users (employees and others) and un-authorized will be denied by using appropriate technology and other process ensuring confidentiality, integrity and availability.

10 - Applications

10.1 Purpose

Applications are vulnerable to various kind of attacks, which are exploited by a malicious activity. Computer software owned or licensed must not be copied by users; employees and others for use at home or any other location. Exceptions to this will be specifically authorized by the Information Owner. Anyone could access information and/or data wherein security controls like Authentication mechanism can be easily bypassed. Hence, it is imperative that Security controls to protect the application are appropriate and deployed on a continuous basis.

10.2 - Policy Statement

Application deployed in bank shall have controls for secure input processing, through system, storage and output of data. Application shall be tested for security performance before deployment & for high availability. Access to application shall be restricted to authorized persons & access will be o provided on the principle of least privilege.

11. - Database

11.1 - Purpose

Bank's database contains critical and confidential business information of its constituents which have to be protected at all times. Hence, it has to be ensured that database is configured to protect client information and at the same make them available to authorized users on authentication. The organization needs to define and develop adequate controls to secure its database.

11.2 - Policy Statement

The technical team (IT department) shall implement database system configured as per best security practices. Adequate controls to maintain confidentiality, integrity and availability of database at all times shall be put in place. User access to database shall be provided as per authorization and based on authentication. Database access will be given strictly based on business, operational needs and requirement.

12. - Patch Management

12.1 Purpose

The hardware having computers and applications should be frequently patched to protect against widespread worms, malicious code that target known vulnerabilities on non-patched systems, resulting in downtime & business impact on banks.
The down time and business impact can be avoided by have effective patch management which will keep updated the IT system and applications deployed in the bank.

12.2 - Policy Statement

The bank shall be secured against known vulnerabilities in operating systems and applications software through an effective patch management process.

13. - Personnel

13.1 - Purpose

People are the key assets in creating, storing, maintaining, distributing, processing and protecting the information/data of the organization. All employees as also contractual users should adhere to all the IS security guidelines and access information purely based on job responsibilities and requirements. They should not access information for personal use. The access can be revoked or modified with changes in such responsibilities.

13.2 - Policy Statement

People are the key assets in creating, storing, and maintaining, distributing, processing protecting. All employees as also contractual users shall adhere to the Personnel Security and access based on responsibilities. The access can be revoked or modified with changes in such responsibilities

Bank shall ensure that each employee is made aware of the importance of IS and their role in ensuring IS. Also employees will be instructed to strictly adhere to various IS related instructions and not to use information for other than official purposes. Employees will be informed of their access and other rights which can be revoked in the event of role changes.

14. – Password

14.1 - Purpose

If an authorized user or a customer who is not authorized gains access to banks information and information assets, it could result into loss of confidence constituents and result in compromise with integrity of data.

Generally the user and customer gain access to information/data through user-ID and the password provided for securing transactions. Access to systems should be strictly limited for the genuine business purposes with the complement of User ID and password

14.2 - Policy Statement

Every user shall be assigned a unique User ID. Users both employees and customers shall choose/create their passwords in accordance with policy and shall protect at all times during its generation, delivery, storage and usage. The password change process shall be well calibrated. Users and Customers will be mandated to periodically change the password. Bank will educate the customer on the need for confidentiality in the password, not sharing it with others and the consequences of sharing the password.

15. - E-mail Usage and Security

15.1 - Purpose

The E-mail (FINACLE E-Mail) system for the bank is required for day-to-day function for genuine banking and operations. A lot of internal information is shared with employees and functions/function heads through email. As such appropriate controls have to be provided for security for e-mail.

15.2 - Policy Statement

E-mail ID and access shall be made available to employees purely based on business needs. Every employee shall develop a password for accessing the mail. Email activity shall be protected adequately to provide availability, exchange of information between employees of the bank and with the third parties. Bank will protect the system with appropriate technology and other means against breach or unauthorized access. Employees will not be allowed to use email for personal work. Bank has provided personalized E-Mail to each employee with excess through web mail for official use only.

16. - Change management

16.1 - Purpose

Unauthorized changes and ad-hoc changes in the IT and other electronic systems could lead to system getting interrupted and result in genuine persons and users unable to access system or information assets. It is laid down that major or minor changes to any information assets where ever necessary should be carried out with prior approvals. The changes are to be identified and monitored. The entire process will have to be documented. It is provided that changes will be implemented in test environment before taking to production.

16.2 - Policy Statement

Changes to the IT systems shall be performed in controlled manner. To ensure that the risk associated with changes are managed to an acceptable level, changes will be made only after careful

Consideration of its need, impact and proposed changes will be thoroughly tested before these are deployed.

17. Monitoring

17.1 Purpose

IT infrastructure components form a crucial part of assets of the banks. IT assets are constantly under threat from hackers and other malicious users and as a result needs to be monitored effectively on a continuous basis for identifying any abnormal activities and for the purpose of protecting the asset. The effectiveness and applicability of IS controls have to be monitored based on control testing criteria, purpose of testing and results periodically reported to the management. Security controls need to be continuously implemented on IT assets to protect them from unforeseen threats.

17.2 - Policy Statement

The bank shall establish an effective enterprise level system to centrally monitor IS controls. All access to critical applications and banks network shall be monitored for suspicious activities or security breaches. Adequate response mechanism shall be set up for controlling security breach, if any.

18. - Outsourcing/Third Party

18.1 - Purpose

There are a number of IT based activities that the bank has outsourced. These include AMC for hardware and software, maintaining ATM etc. The bank is aware of the risk of improper access to information and information assets from users of third party or outsourcing agencies which could prove detrimental to banks interests. A risk assessment exercise should be carried out to determine the specific security requirements in such cases. Contract with third parties or outsourcing agencies should be established with necessary security conditions and service levels in mind.

18.2 - Policy Statement

Bank shall ensure that access to the data processing facilities and Intellectual property rights of the bank are well protected from third party service provider's entities and controls by taking adequate measures.

19. Business Continuity

19.1 Purpose

To fulfill the bank's commitment to protect its customers and in the interest of rendering uninterrupted banking services it would be prudent for the bank to thwart all kinds of threats to its business which could have the potential to disrupt its operations. In other words bank should Ensure robust systems such that its business continuity is not threatened. In view of this, critical information systems of the bank should be planned and suitably designed to ensure continuity of operations, even in the event of a disaster. IS is one such critical aspect. Thus the purpose is to counter interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.

19.2 Policy Statement

Bank shall ensure the safeguard of its information and information assets to minimize the risk,

costs & duration of disruption to business operations. Bank will establish and maintain integration between response plans, DRP & BCP. Bank will have a plan for effective continuity of business & a well-rehearsed recovery process or a combination of these which will enable the resumption of critical business activities.

20. ATM

20.1 Purpose

The objective of this policy is to prevent misuse and minimize security risks to ATMs installed in the bank premises and at off-site locations. The ATMs being an important delivery channel offering financial and non-financial services, the security risks must be considered on top priority for prevention of frauds.

20.2 Policy Statement

A network of ATMs exists in the bank where a secret ATM operation code will be issued to the customer in the form of Personal Identification Number i.e. PIN for ATM operations. The concept of PIN prevents an unauthorized user from gaining access to the ATM network as a combination of physical card and PIN number is required for accessing the account for withdrawal of cash and/ or any other services offered by bank through card and ATM. ATMs will also be guarded suitably against theft, unauthorized access etc.

PART - II

INFORMATION SYSTEMS SECURITY POLICY POLICIES AND PROCEDURES

For all the policies stated in part I the descriptions and procedures are given below.

2. Environment and Physical Security Policy

2.1 Purpose

Control of Physical and electronic access to confidential information and computing resources is must to ensure IS. To ensure appropriate levels of access, a variety of security measures must be instituted based on business needs and as recommended by the Chief Information Security Officer (CISO).

2.2 Policy Statement

Mechanisms to control access to confidential information and IT assets shall include all sites situated within the bank. The assets shall be protected against unauthorized environment and physical threats. For this purpose the bank will give clear guidelines on authority and responsibility for its employees and other authorized stake holders to access the information and IT assets. Bank employees will strictly adhere to these norms/guidelines. Detailed rules on this regard will be issued by the bank.

2.3 **Procedures: Scope**

All sites, which house bank's critical IT assets, shall provide resistance to unauthorized physical access and have protection against environmental threats. All physical access and movement of IT assets shall be monitored and reviewed.

2.4 Access Control

2.4.1 All critical information processing facilities shall have adequate protection against unauthorized access.

2.4.2. Every employee shall be provided with name, identification/access cards consisting of banks name the details of time of arrival, duration of the activity, and reasons of access shall be recorded. In case of emergency, approval for access can be given on the phone or e-mail with a proviso that detailed request form shall be sent after activity.

2.4.5. Access to secured areas shall be allowed only after necessary approval.

2.4.6. A log book shall be maintained to track all access to critical information processing facilities.

2.4.7. An updated list of personnel who have access to critical information processing facilities shall be maintained.

2.4.8. Security guards must check IT equipment and media carried by all personnel entering or leaving information processing facilities.

2.4.9. Visitors, vendors and external people shall be accompanied by bank staff when working in critical information processing facilities.

2.4.10. An access control register shall be maintained at the entry point of Data Centre. People who are not Data Centre employees and third party (external) visitors shall make appropriate entry in the register before entering

2.5 Environmental Protection

2.5.1. There shall be adequate provisions for fire - detection, firefighting and control.

2.5.2. All personnel shall be trained for fire-fighting.

2.5.3. Air Conditioning Systems shall be implemented to ensure that the operational environment conforms to the equipment manufacturer's specifications.

2.5.4. All critical equipment such as air conditioners, gen-sets, etc. shall remain under Annual maintenance contract, at all times.

2.6 Data Centre Security

2.6.1. Critical processing area in Data Centre shall be accessed only by authorized personnel. They alone will be allowed inside/access.

2.6.2. Emergency exit shall be provided in the data center for use in emergency situation (it shall not be available as a matter of routine).

2.7 Identification of Devices

2.7.1. For easy identification, data cables and electrical cables must be properly labeled.

2.7.2. Proper labeling of racks shall also be ensured. All devices shall also be similarly numbered (as contained in the racks). Rack number shall form part of the device identification number which must be pasted on all devices.

2.8 CCTV Monitoring

2.8.1. CCTV monitoring systems shall be installed at the Data Centre and a proper monitoring system shall be put in place at entry and exit points at the Data Centre as also in area having critical IS assets. The CCTV footage shall be maintained – kept on record for a specific period – a Minimum period of 90 days.

2.9 Power at the Data Centre

2.9.1. Power Systems shall be designed and provided to ensure uninterrupted and quality power supply at the Data Centre. UPS shall be provided for backup.

2.9.2. UPS Systems shall be checked once in a quarter or as recommended by the manufacturer for its proper functioning/efficacy. Additionally, test checks shall also be carried out, on a quarterly basis.

2.9.3 A backup power system shall be provided to all access control systems, physical security systems such as fire and smoke alarms, emergency lighting systems, fire detection & suppression systems, etc.

2.9.4. The electrical power supply to the Data Centre shall be segregated from other power circuits of the building. Similarly, the power supply to the IT equipment's/assets at the Data Centre shall be segregated from all other equipment.

2.9.5 Switches shall be provided in easily accessible locations within the Data Centre and outside the Data Centre to be used to switch off the power, in case of an emergency.

2.10 Fire Prevention and Control

2.10.1 Infrastructure at the Data Center shall be erected from fire-resistant material. Automatic fire detection systems shall be installed for detection as also for alerting. Gas based fire suppression systems shall be installed to control outbreak of fire. Fire detection and suppression systems shall be capable to automatically shut off electrical power.

2.10.2 No combustible material shall be provided or stored at the Data Centre.

2.10.3 Basic training on fire-fighting techniques shall be provided to staff at the Data Centre. Periodical fire-drills shall be conducted, as per the security policy of the bank.

2.11 Environmental Safeguards

2.11.1.Temperature and humidity shall be monitored and controlled at the Data Centre.

2.11.2 Air shall be filtered and circulated to remove dust and contamination at the Data Centre.

2.11.3. Water/Moisture detectors shall be placed below the false floor in the Data Centre, if the area is prone to moisture and water seepage.

2.11.4. Raised false floor shall be erected to provide proper environment, temperature, cabling, etc.
2.11.5. The Data Centre shall always be maintained dust and dirt-free.

2.12. Preventive Maintenance

2.12.1. Preventive maintenance of all equipment, electrical installations, alarm systems, back-up power supply, UPS, etc. shall be carried out periodically.

2.12.2. Proper monitoring of such maintenance by personnel posted at the Data Centre shall be ensured.

2.13. Monitoring

2.13.1. Automatic alerting systems shall be installed at all access points to critical information processing facilities.

2.13.2. Monitoring systems shall be deployed to track any suspicious activity.

2.14 Document Security

2.14.1. Sensitive documents shall be stored in locked cabinets.

2.14.2. Fax machines and printers shall be protected against unauthorized access.

2.15 Enforcement

2.15.1. Compliance with the security policies of the bank shall be a matter of periodic review by the ISC. Any employee found to have violated this policy may be subjected to disciplinary action, up to and including termination of employment as deemed appropriate by the management of the bank.

3. Acceptable Usage Security

3.1 Purpose

The purpose of this policy is to clarify users' rights, responsibilities, information assets and rights, to shield the organization against potential threats and liabilities. Bank assets are provided for business purpose. User of information is expected to access information only in support of authorized job responsibilities or role. This will

- Minimize security threats by promoting awareness and good practices
- Encourage effective and positive use of information assets and resources.
- Ensure that users follow safe usage practices that do not hamper business objectives, not to bring disrepute or to attract legal liability

3.2 Policy Statements

Bank assets are l be provided for business purpose and not for the personal use of its employees or

other authorized users of information and information assets. To ensure this users shall follow to safe usage practices that do not hamper business objectives, bring disrepute to or attract legal liability. Violations to the usage policy by an employer /user will attract strict action and penalties including disciplinary action.

3.3 Procedures for Acceptable Users and Usage Security : Scope

Users' rights, responsibilities, information assets and rights shall be specified to shield the organization against potential threats and liabilities. Minimize security threats by promoting awareness and good practices. Encourage effective and positive use of information assets and resources.

3.4 Desktop Users

3.4.1. All desktops shall be configured by system administrators as per the secure configuration standards provided by IS Committee (ISC).

3.4.2. Users shall not install any software or applications on their desktop that is not authorized or not essential to bank's business.

3.4.3. Users shall not connect modems to their machines unless and otherwise approved by the appropriate authority.

3.4.4. Necessary measures shall be adopted by users to prevent the risk of unauthorized access.

3.4.5. Desktops as also external devices like CD, pen drives, etc. shall be configured by IT teams in accordance secured configuration by IT team be as per standards.

3.4.6. Users shall not install any software, application on their desktop that is not authorized. Users can effect changes in the desk top only through IT department.

3.4.7. Approved products only can be installed on desktops/laptops.

3.4.8. The servers shall be configured and maintained only by the I T department or authorized officials.

3.4.9. Internal LAN shall be segregated from the external Internet. User shall not connect through modems. Also for connecting to external access, network team will configure all desktops as per secure configuration.

3.4.10. User must log out of all applications when leaves; if not used, desktop shall automatically log-out for extended period of time.

3.4.11. Screen saver shall be enabled with Password. Access through pass word is essential if the PC is unattended for short time.

3.4.12. It should be ensured that there is sharing in any user's folders in desktops over network.

3.5 Laptop Users

Laptop users need to adopt the following measures

3.5.1. Ensure that laptop is configured as per the secure configuration documents provided by ISC.

3.5.2. Enable boot level password in the laptop.

3.5.3. Encryption or password protection shall be enabled for protection of data.

3.5.4. Antivirus agent with latest signatures shall be installed, before laptop is connected to the LAN.

3.5.5. All necessary patches / hot fixes for the operating system and applications installed shall be periodically updated.

3.5.6. Log off laptops when not working for extended period and enable screen saver with password for protection during short period of inactivity.

3.5.7. Backup critical files from laptop to Users' desktop or removable media like CD/Pen drives

3.5.8. User to take adequate measures for physical protection of laptop including not leaving laptops unattended in public places or while traveling.

3.5.9. If the laptop has modem / dial up facility for Internet, users shall disconnect Internet connection before connecting to the bank's LAN.

3.5.10. Loss of laptop shall be reported immediately to the department head and ISC.

3.5.11. Third party laptop connecting to the bank's network shall be restricted. Prior approval from IT head shall be taken before connecting third party laptops to bank's network.

3.5.12. Laptops Security– Configuration as per policies shall be carried out by security team.

3.5.13. Enable booting passwords and additional protection.

3.5.14 shall take precaution for physical protection by backing up critical files to central server.

3.10.15. The system shutdown option which allows users to shut down the system without logging in first, will be restricted on all servers housing sensitive information.

3.5.16. A logon banner shall appear on all information systems prior to login on to the system stating that the information system shall only be accessed by authorized users and un-authorized access is prohibited, monitored and liable for punitive actions.

3.5.17. The number of unsuccessful logon attempts will be limited to (say five) after which the system will lock that particular User ID. All unsuccessful login attempts will be recorded.

3.5.18. On completion of a successful log-on the following information will be logged: (a) date and time of the previous successful log-on (b) details of any unsuccessful log-on attempts since the last successful log-on.

3.6 Password Security

3.6.1. Users (employees and other authorized personnel) are responsible for all activities originating from their computer accounts.

3.6.2. Users shall choose passwords that are easy to remember but difficult to guess.
3.6.3. Protection
3.6.3.1. Users shall not disclose/share their passwords with anyone including colleagues and IT staff.

3.6.3.2. Users shall ensure that nobody is watching when they are entering password into the system.

3.6.3.4. User shall not keep a written copy (in paper or electronic form) of password in easily locatable places.

3.6.3.5. Users shall change their password regularly.

3.6.3.6. User shall report to the system administrator if account is locked out before 3 bad attempts.

3.7 Internet Usage

3.7.1. Internet access is provided to users for the performance and fulfillment of job responsibilities.

3.7.2. Employees shall access Internet only through the connectivity provided by the bank and shall not set up Internet access without authorization from IT department.

3.7.3. All access to Internet will be authenticated and will be restricted to business related sites.

3.7.4.. Users are responsible for protecting their Internet account and password.

3.7.5. In case misuse of Internet access is detected, bank can terminate the user Internet account and

take other disciplinary action as bank may deem fit.

3.7.6. Users shall ensure that security is enabled on the Internet browser.

3.7.5. Users shall ensure that they do not access websites by clicking on links provide in emails or in other websites.

3.7.7. Bank reserves the right to monitor and review Internet usage of users to ensure compliance to this policy.

3.8. Clear Desk

3.8.1. While users work in an online environment, at times they are required to use papers/ storage devices for information exchange. Information on important customers & sensitive business data is also available on other media like computer generated printouts, office papers, CDs, pen

drives, diskettes etc.

3.8.2. Cabins/ Desks & meeting rooms with papers piled high not only poses fire risk but also may be in legal breach for not preserving confidentiality of customer information. The act places a legal obligation on employees concerned to protect sensitive personal information.

3.8.3. To prevent such data leakage due to non-clean desks, user/ authorized personnel shall ensure that confidential documents and media files are not left unattended. Unused documents/ papers shall be destroyed using shredder machine.

4. Incident Management

4.1. Purpose

IS incident could be a single or a series of unwanted or unexpected IS events that have a significant probability of compromising business operations and threatening IS. IS incidents are those which impact IT security. Incident management call for plan and procedures to deal with the incidents so as to protect the information and or information assets. The purpose of this policy is to develop and implement processes for identifying and responding to IS incidents. The CISO and his/her team shall conduct reviews to identify reasons for IS incidents, evaluate the same and also develop corrective and preventive actions to manage and /or avoid recurrence of the incidents. It is necessary that IS events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken.

4.2. Policy Statement

Every employee and user must report such I S events (breach or attack) to his/her immediate supervisor and also to the IS department. The banks IS committee, based on the CISO recommendations define Roles and responsibilities for the department heads, branch heads to to identify, and manage IS incidents. Events, incidents and problems should be reported to the Appropriate authority. Persons vested with the responsibility should respond promptly with a view to contain loss and damage if any and to avoid reoccurrence.

4.3 Scope

Maintain processes to investigate and document incidents to be able to respond appropriately. To determine their causes, adhere to legal regulatory and organizational requirement.

4.4 Incident Identification

4.4.1. All users and administrators of IT systems shall be responsible for identifying incidents. An incident is the act of violating an explicit or implied security policy. The following actions can be classified as incidents:

i. Attempts to gain unauthorized access to a system or its data; masquerading, spoofing as authorized users.

ii. Unwanted disruption or denial of service.

iii. The unauthorized use of a system for the processing or storage of data by authorized users.

iv. Changes to system hardware, firmware or software characteristics and data without the owner's knowledge, instruction or consent.

v. Existence of stray user accounts.

4.5 Incident Reporting

4.5.1. If a user suspects that an incident has occurred, it shall be reported immediately to the branch system administrator / department head or to the helpdesk. The administrator shall do a preliminary analysis to ascertain the cause and extent of damage.

4.5.2. An incident report shall be sent to the IS Committee (ISC) containing the following details

- Description of the incident
- Possible causes
- Damages observed
- Supporting evidence
- Remedial steps taken

4.5.3. Based on data available and level of criticality of incident, ISC shall send out incident alerts to application groups and user departments which could possibly be affected by similar incidents.

4.5.4 Users of the IT system shall report security incidents identified.

4.5.5. Users are required to provide their identity and contact details while reporting incidents for effective follow up.

4.6. Incident Verification

4.6.1. The ISC shall analyze the incidents based on the data received from the administrator. The ISC shall seek more information from the system administrators, if required.

4.6.2. The ISC shall record the incident and allocate an incident number for tracking and future reference.

4.6.3. Once the incident validity has been verified, ISC shall draw up an action plan.

4.6.4. Head of IT shall be updated about the incident, impact on business and proposed action plan.

4.7. Incident Recovery

4.7.1. System personnel required for executing the recovery plan shall be contacted by the application team.

4.7.2. Additional monitoring mechanisms shall be deployed for a short duration of time after recovery to ensure that all incident related activities have ceased.

4.8. Incident Prevention

4.8.1. Based on the learning from the incident, ISC shall make necessary changes (if required) to security policies.

4.8.2. ISC shall maintain a database of incidents and recovery steps.

4.8.3.

5. Asset Classification & Handling

5.1. Purpose

Bank provides the medium for the purpose of exchanging transaction details through clients/servers. Failure to properly protect information could have serious effect on the bank. As such, they would have to be protected with stringent security controls. Information is classified to ensure its proper protection. Immediately after information has been created, modified or acquired, information

must be evaluated to determine its classification. Also it should be decided as to how it must be handled. Information asset is any asset that has value for bank & consequently needs to be suitably protected.

5.2. Policy Statement

Every employee and authorized functionaries of the bank has responsibility in protecting the information asset from unauthorized access, generation, modification, disclosure, transmission or destruction. This is achieved by strictly following laid down procedures. In order to ensure that the security, reliability, integrity & availability of information is not compromised bank has laid down specific procedures and rules for each information activity. Bank will specify authority for appropriate asset handling schemes for labels shall be adapted by the bank for marking guidelines for IS.

5.3. Scope

Information assets apply to all users of the bank housed with the institution as and/or with the outsourced/ third parties.

5.4. Accountability

5.4.1 All major information assets like application software and databases shall have a nominated Data Owner.

5.4.2. The Branch Head/ Regional Head/ Administrative Office Head will initiate measures for nominating functional owners for all major information assets of bank.

5.5. Information Classification

5.5.1. All information system assets will be classified under one of the following categories:

5.5.2. Secret Information: Secret Information is highly sensitive to internal and external exposure.

5.5.3. Confidential Information: Confidential Information is sensitive to external exposure, the unauthorized disclosure of which would cause administrative embarrassment or difficulty.

5.5.4. Corporate Confidential Information: Any confidential information of the Bank's internal affairs, which cannot be shared with employees, Branches / Regional / Administrative Offices, unless, needed for the purpose of routine operations or conducting business.

5.5.5. Branch/ Regional/ Administrative Office Confidential Information: Any confidential information, which can be shared across Branches/ Zones/ Administrative Offices, but is not intended to be shared as Public Information, will be classified as Branch/ Regional/ Administrative Office Confidential Information. Public: Public Information includes information such as various services, marketing brochures and promotional literature, advertising media and Bank web sites.

5.5.6. A given security classification cannot be downgraded to a lower category except by the Data Owner.

5.6. Document Classification

5.6.1. Appropriate security classification will be clearly stated for all hardcopy collections of documents consistent with the information classification, except for Public information. The following classification standards will be maintained.
5.7. Secret Documents: Secret documents will be marked as 'SECRET' on the first/heading page.

5.8. Confidential Documents: Confidential documents will be marked as 'CONFIDENTIAL' on the first/heading page.

5.9. General Documents: All un-labeled documents will fall into this category.

5.10. Media Handling

5.10.1. All computer media like tapes, disks, CDs pen drive etc. will be stored in a safe, secure environment, in accordance with the manufacturer's specifications.

5.10.2. Procurement, distribution and use of blank CDs, tapes, pen drive/floppies, etc. will be inventoried and controlled by the respective Administrative Head.

5.10.3. No printed output or removable media will be taken out of the office premise unless authorized in writing by the respective Administrative Head with a copy to the Gate Security In-charge, if any, wherever practical.

5.10.4. No printed output or removable media containing, Secret or Confidential data will be taken out from the Computer Room premises unless approved in writing by immediate controlling authority.

5.10.5. Personal media like tapes, disks and cassettes will not be carried and used in the office premise.

5.10.6. Inventory of software media containing system software, operating system and such other software and application utilities will be maintained.

5.11. Enforcement

5.11.1. Compliance with security policies will be a matter for periodic review by the ISC. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment as deemed appropriate by the management.

6. Asset-Media Disposal

6.1 Purpose

Information can be compromised through careless disposal or re-use of media. Storages devices containing sensitive information should be physically destroyed or security overwritten. Rather than using the standard delete functions, all storages media should be checked prior to its disposal to ensure that sensitive data and licensed software, if any is not remained. It should be ensured that such data or software is either removed or overwritten.

6.2 Policy Statement

Employees, users and authorized officials of the bank shall ensure that banks owned computers, devices storages media shall have all data and licensed software reliable erased from all device at the time of disposal of the media or its movement out of bank control using best practices for each type of media.

6.3 Scope

6.3.1. This policy is applicable to any electronic information storage or paper- based media containing internal use classification or confidential data.

6.3.2. Policy applies to all employees and third party personnel who have access to, develop, use, copy, print, exchange information, earlier internally within the organization or externally with third parties.

6.3.3. Policy applies also on all I T Assets

6.3.4. Policy also applies on the employees of the third party who are involved in the disposal procedure.

6.4. Disposal of Information Assets

Media containing sensitive information (Secret or Confidential) will be disposed of securely and safely when it is no longer required e.g. by incineration or destroyed by securely deleting. Such disposals will be authorized by the Administrative Head at the location.

6.5 Disposal of Electronic Media

6.5.1. The departmental heads are responsible for overseeing compliance with data and disk disposal in his or her area on a yearly basis.

6.5.2. Information on storage media like hard disk drives or removable media like tape drives, USB, CD drives shall be formatted or erased three times if the media is to be reused.

6.5.3. Low level formatting shall be done for hard disk drives of all desktops and laptops three times before reusing or sending them for maintenance.

6.5.4. Magnetic media like floppy disk, hard drives, zip disks, etc. shall be erased using a degaussing device or disk wiping software before being discarded.

6.5.5. Expired or corrupted storage media like floppy, CDs or tape/optical media shall be degaussed or erased prior to its disposal.

6.5.6. Optical tape drives, internal hard drives and RAID arrays shall be wiped out using department or organization's 'disk-wiping' software, since a simple delete, erase, re-format or disk command for Windows is not sufficient as there are many products which can retrieve erased data and software. Additionally, such drives shall be physically destroyed either within the organization or via an external media disposal third party service.

6.6 Disposal of Paper based Media

6.6.1. Department/Branch heads shall nominate an official from the department/branch who would be responsible for overseeing paper-based document disposal in his/her area.
6.6.2. All waste copies of sensitive information that are generated in the course of copying, printing, or faxing need to be shredded using paper shredders/incinerators or shall be placed in locked bins clearly marked as containing confidential data.
6.6.3. Confidential and restricted data and paper documents shall be destroyed using paper shredders or incinerators.
6.7. Condition for disposal of IT Assets
6.7.1. The condition of the asset and not its age shall determine its usefulness or obsolescence. The circumstances under which IT assets may be considered for disposal are –

- When no economic benefit can be derived from active use of the asset.
- When maintenance cost of an asset exceeds its replacement cost.
- Up gradation of an asset is no longer possible.
- Replacement or disposal reduces cost of operations and improves efficiency.
- Due to change in technology and market conditions, it is no longer functional.

6.7.2. Certification of usefulness or utility shall be obtained from technical expert.
6.8. Disposal of IT Asset - Procedure
Following procedure shall be followed for disposal of IT asset:
6.8.1. All proposals requesting for disposal of IT assets at departments/branches shall be submitted by the Head of the Department/branch to the IT head.
7.8.2. While disposing of IT assets, departments will ensure that necessary backup of data has been taken for future use. It should be ensured that information if any in the asset is deleted before the asset is disposed off.
6.9. Periodicity of disposal of obsolete IT Assets
Disposal process shall be carried out on a yearly basis. However, if immediate need of disposal is felt, assets can be disposed off as and when required with the approval of the IT head.
6.10. Outsourcing of Disposal of IT Assets

6.10.1. If disposal of IT assets is outsourced, external contractors responsible for general disposal arrangements, bank shall have or insist on proper security and process checks to ensure that information assets are disposed off in a secure manner. Disposal of confidential and internal items shall be logged, in order to maintain an audit trail. Disposal of confidential/restricted labelled information assets or documents shall be done securely and shall be witnessed by the custodian.
6.10.2. Non-disclosure agreement shall be signed between the bank and the external contractor while outsourcing disposal of IT assets.
Certificate of secure disposal shall be obtained from external contractor.

6.11. Enforcement

Compliance with the Security Policies will be a matter for periodic review by the ISC. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment as deemed appropriate by the management of the bank.

7. Anti-Virus

7.1. Purpose

Bank must be protected against vulnerability due to virus and attack by Trojans and malicious codes. Hence IT assets of the bank must use enterprise level anti-virus solutions on the system.
Appropriate Antivirus solutions approved by the Chief IS Officer and must be deployed for protecting against virus attach and Virus checking. Wherever possible a multi-layered approach

should be used (desktops, servers, gateways, etc.) that ensures that all electronic files are appropriately scanned for viruses. Users (employees and other stake holders) are not authorized to turn off or disable virus checking.

7.2. Policy Statement

Malicious codes are viruses, worms, Trojans, rootkits etc. represent significant threat to performance secrecy. Bank shall ensure that these malicious codes are detected early and removed. These guidelines shall protect IT assets of the bank against malicious code through enterprise level anti-virus solution. Bank will use an appropriate antivirus solution and keep it updated on a regular basis.

7.3. Scope

All desktops and server machines in the bank shall have anti-virus installed. This does not include server machines with UNIX server like operating systems where the risk of virus infection is very less.

7.4 Installation

7.4.1. Anti-virus agent installation shall be password protected.
7.4.2. Anti-virus agent shall be configured to do a full system scan at least once a day.
7.4.3. Anti-virus agent shall be configured to do a real time scan of all the files when these are accessed, copied or moved.
7.4.4. Anti-virus agent shall be configured to quarantine the infected files if they cannot be cleaned.
7.4.5. Anti-virus on the email servers shall be configured for scanning all internal and external mails.

Any change in this policy can be made only after the prior approval of the Committee of Management of the Bank.

This Information System Policy (IS Policy) of the Bank is approved vide resolution No–24(XXV) Passed in the Board of Directors meeting of the bank. Dated 01-11-2023

Deputy General Manager(Acct) **Secretary/ General Manager**