IT SECURITY POLICY

Approved by Board of Directors in Board Meeting Dated vide resolution No.-12 dated 27.06.2023

IT SECURITY POLICY

TABLE OF CONTENTS

CHAPTER-1

This chapter outlines the basic objective and scope of this IS Security Policy and some general clauses on acceptable and unacceptable usage of all IS resources.

1.1. Purpose

The policy statement that works as a preamble to the security framework contains the following framework:

- An acknowledgement of the importance of the computing resources to the business model.
- A statement of support for the information security throughout the enterprise.

- A communication to authorise and manage the definition of the lower level of standards, procedures and guidelines.
- A commitment for appropriate sanctions and rewards for the efficient implementation of information security programme.

The purpose of this policy is to safeguard Bank's Information System (IS) assets, maintain data confidentiality, integrity and availability, to fulfil organizational goals effectively and utilize resources efficiently.

This document provides the framework to ensure the protection of Allahabad Bank's assets in accordance with appropriate standards, laws and regulations

All existing policies related to Personnel, Administration, Protection of confidential information and other areas apply equally to the computerized environment

Bank has to identify its security requirements, which will facilitate to address the following:

- Risk assessment to identify the threats to information and information assets. Their vulnerability to security threats and the 'likely hood of the occurrence of such threats. The potential impact of such threats on the business reputation of the Bank.

- The legal, statutory, regulatory and contractual requirements, which the bank, its trading partners, contractors and service providers have to comply with.
- The principals, objectives and requirements, for information processing which the bank have developed to support its business operations.

1.2. Scope

This policy applies to employees, contractors, consultants and other workers at the Bank and their associates, including all personnel affiliated with third parties. This policy also applies to all applications and equipment that is owned or leased by the Bank.

1.3. General Use and Ownership

- While Allahabad Bank's network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remains the property of - -. Because of the need to protect - -'s network, management cannot guarantee the confidentiality of information stored on any network device belonging to - -.
- Employees are responsible for exercising good judgement regarding the

reasonableness of personal use. Individual Areas are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.

- Any information that the information-owner considers sensitive or vulnerable should be encrypted/password-protected in transit/storage.
- For security and network maintenance purposes, authorized individuals within - - may monitor equipment, systems and network traffic at any time, per Audit Policy.
- Allahabad Bank reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

1.4. Security and Proprietary Information

- The user interface for information contained on Internet/Intranet/ Extranet-related systems should be classified as either confidential or not confidential, as defined by data classification standards. Employees

should take all necessary steps to prevent unauthorized access to this information.

- Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts as per the password policy.
- Because information contained on portable computers is especially vulnerable, special care should be exercised. Protect laptops in accordance with the "Laptop Security policy".
- Postings by employees from a Allahabad Bank email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of - -, unless posting is in the course of business duties.
- All hosts used by the employee that are connected to the - - Internet/Intranet/Extranet, whether owned by the employee or - -, shall be continually executing approved virus-scanning software with a current virus database, unless overridden by departmental or group policy.
- Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

1.5. Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of - - authorised to engage in any activity that is illegal under local, state, or regulator's prescription while utilising - - owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities, which fall into the category of unacceptable use.

1.5.1. System and Network Activities

The following activities are strictly prohibited, with no exceptions:

- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by - -.

- Unauthorized copying of copyrighted material including, but not limited to, digitisation and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which - - or the end user does not have an active license is strictly prohibited.
- Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. This must be done only after taking prior approval.
- Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
- Revealing account password to others or allowing use of our account by others. This includes family and other household members when work is being done at home.
- Using an - - computing asset to actively engage in procuring or transmitting material that is in violation of 'sexual harassment' or 'hostile workplace' laws in the user's local jurisdiction.
- Making fraudulent offers of products, items, or services originating from any - - account.
- Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
- Effecting security breaches or disruptions of network communication.

Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

- Port scanning or security scanning is expressly prohibited except for the information system audit professionals.
- Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
- Circumventing user authentication or security of any host, network or account.

- Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
- Providing information about, or lists of, - - employees to parties outside - - in a restricted way with due permission.

1.6. Enforcement

Any violation of the policy by the employee should be deemed to be a breach of the service conditions or rules/regulations governing his /her conduct and the employee would be made liable to disciplinary action, up to and including termination of employment as per bank’s rules and policies.

1.7. Policy Ratification

The entire security policy must be ratified by the board before it is implemented. As technology is dynamic the security policy needs an on-going review to keep pace with threats arising out of the new technology.

CHAPTER – 2

This chapter proposes an ISMA while outlining the roles and responsibilities of personnel in the functional areas of administration and management involving the 3 key processes of IT, IS and ISA.

2. Organizational Structure

2.1. Information Security Management (ISM) Architecture

The following model is proposed for the Information security Management Architecture

The steering committee on Information System security, which is a top management committee, should meet once in each quarter for the following purpose.

- Review the operational/Architectural issues of the Security Policy.
- Review of the new threats and controls if any, due to implementation of new technology.
- Reassure the Bank's commitment towards Information security.
- Executive Director of the Bank should be the chairman of this Committee. General Managers in charge of Human Resources, Security, Inspection/ Audit and Information Technology should be a member of this committee.
- The security policy framework is to be approved by the Board and any changes or amendments proposed thereof in the policy are to be ratified by the Board.

IT and IS Structure

The structure of the IT Department may be designed by the Chairman of the Bank

As organisation Structure, a separate wing headed by not less than AGM Rank should be designated as Chief Information Systems Officer (CISO) for information security enforcement reporting directly to General Manger .

Information Security Steering Committee viz. the working group on Information security should comprise GM as the chairman, and Sr. Managers of other important Departments and some dedicated/qualified officers on Information Security. This working group should meet once in a quarter for the following purpose -

- Review the implementation of the security architectural policy. Fixing the operational parameter depending on the type of application.
- Appraising the committee about the plan, implementation, security lapses, new threats etc.

2.2. Roles and Responsibility

The information security architecture has the following three focussed areas:

- **Information Technology Area**
- **Information Security Area**
- **Information Security Audit Area**

The roles and responsibilities of these three focussed areas in the proposed information system architecture are as follows:

2.2.1 Information Technology Area

- IT policy and aligning IT strategy with business strategy.
- Business Technology Planning process, including the sponsorship of collaborative planning processes.
- New and existing application development for enterprise initiatives and overall co-ordination for business unit or divisional initiatives.
- IT infrastructure and architecture (e.g. computers and networks) operations and investment decisions.
- Sourcing and purchase decisions, which include make versus buy decisions relative to outsourcing versus in-house provisioning of IT services and skills.

- Establishing partnerships, including strategic relationship with Key IT suppliers and consultants.
- Technology Transfer, by providing enabling technologies that make it easier for customers and suppliers to do business with the enterprise as well as increase revenues and profitability.
- Interaction with internal and external clients to ensure continuous customer satisfaction.
- Providing training to all IT users to ensure productive use of existing and new systems.

- Implement controls.
- Manage day-to-day Security Functions.

2.2.2 Information Security Area

- Communicate with the management on the risk and controls related to Information system.
- Ensure appropriate user access and authentication controls are in place.
- Ensure that the documented security policies, standards and procedures are reviewed, updated and maintained periodically by appropriate individuals.
- Evaluate security exposures, misuse or non-compliance situations and ensure implementation of security controls to address those incidences.
- Ensure that all business unit/departmental security co-ordinators understand and execute their security responsibilities in accordance with related policies, standards and procedures.
- Organise and conduct periodic security team meetings.
- Develop and implement the security awareness program with assistance from security team members.

2.2.3 Information Security Audit Area

- Conduct reviews against established guidelines.
- Develop Audit Reports.
- Inform Management.

2.3 Management

The specific responsibility of the management is to assign the duties associated with the administration and security of the information system. The management should initiate the formation of a group that would look into the issuance, maintenance, compliance and review of policies and standards regarding the information system. Other responsibilities include:

- Assigning the necessary resources for security administration within the Bank,
- Ensuring that employee job descriptions accurately reflect their information system responsibilities,
- Determining appropriate levels of security for their information assets and/or information assets under their control and to implement the

necessary safeguards,

- Ensuring that all acquired information technology assets are compliant with the Bank's security requirements,
- Ensuring the implementation of an appropriate contingency plan,
- Promptly notifying security administrators of changes in employee status or non-enterprise relationships under their control,
- Maintaining the necessary records to permit verification of compliance with software copyright laws and licensing agreements,
- Ensuring that proper records are kept for audit purposes, and
- Performing periodic security self-assessments and supporting formulised audit and risk assessment programs.
- Conducting periodic knowledge enhancement programs and training programs for employees.

2.4 Information System - Roles and Responsibilities

The responsibilities in an information system environment are multi-layered. Job description and organisational structure charts are very relevant for all employees/ contract staff as they provide clear definitions of their job responsibilities and also define authority. Therefore it is pertinent that procedures are placed properly to have a well-defined organisational structure for exercising effective control.

Note:-

Where ever IT Officer is not posted, support for IT and IS to STC etc. will be responsibility of IT Cell of the assigned/ nearby RO as per IT's arrangement.

2.5 Administration

The administration of the information system is a specialised task and should be handled only by personnel qualified and authorised to do such tasks by the bank. The administration can be categorised into four different areas:

2.5.1 Network Administrator

The network administrator should have the technical knowledge, skills and experience to manage all aspects of the network, including designing, planning, configuration, installation, troubleshooting and maintenance.

Primary responsibilities include Network computer operations, controlling/maintaining production applications, monitoring system resources, response time, and providing first-line of support. The duties also include Intranet operations, e-mail management, troubleshooting of hardware and software problems and providing user training.

The important activities to be performed by the network administrator can be classified as follows:

2.5.1.1 Maintenance of Network

The network administrator should

- Monitor servers' power supply and the UPS;
- Monitor the backup facility/log;
- Monitor network performance;
- Perform routine virus scan/detection/removal at the entry point of the network;
- Monitor user backup activity;
- Perform routine network maintenance;
- Install, maintain, and update software and hardware;
- Maintain network applications;

- Maintain network hardware and cabling;
- Maintain disaster prevention/recovery procedures.

2.5.1.2 Change Management

The network administrator should

- Evaluate the impact of network changes and additions;
- Review and approve all planned network changes and updates;
- Documentation on changes in Network and Software items.

2.5.1.3 Disaster Prevention/Recovery

The network administrator should

- Perform network/general disaster recovery drills;
- Modify disaster prevention procedures as and when needed/necessitated;
- Schedule downtime and notify all users sufficiently in advance;
- Monitor and inform the users of the status of the network in case of downtime.

2.5.1.4 Reporting

- If any undesired/ illegal activity is noticed in the monitoring of logs, the administrator should report the matter immediately to the authorities for appropriate follow-up action.
- Apart from the above-mentioned reporting, there should be a regular monthly report made by the network administrator to the IT Management.

2.5.1.5 Miscellaneous

- Follow-up with vendors over purchases and installation of equipment;
- Verification of received material (hardware and/or software) so as to conform to the policy requirements of the bank.
- Liaise with service providers during any network downtime and ensure speedy recovery.

Note that the network administrator should never have any application or programming tasks though he is also a normal user of the information system.

2.5.2 Security administration

The security Administrator should

- Keep abreast of latest technologies.
- Be responsible for firewall/ UTM, router and intrusion detection/ prevention system administration.
- Monitor the logs of all the servers, routers, firewalls/ UTMs and intrusion detection/ prevention systems on a regular basis.
- Take action on perceivable real-time threats based on established procedures for such threats, before reporting.
- Ensure that all aspects of security including physical and logical are functioning properly.

2.5.3 System Administrator

The system administrator is responsible for maintaining a multi-user information system environment in a local area network (LAN). The responsibilities of a system administrator inter-alia include:

- Adding and configuring new workstations;

- Installing system wide software;
- Creating, issuing, deactivating, reinitialising, and monitoring user-IDs and associated passwords;
- Defining user groups and associated resource access control profiles;
- Implementing procedures to remove/prevent the spread of viruses and other unauthorised software;
- Allocating storage space for users in systems;
- Maintaining logs on individual systems;
- Ensuring the physical safety of the systems;
- Ensuring the proper storage of licenses, manuals, etc. and prompt retrieval of them;

- Sharing of administrative privileges;
- Ensuring confidentiality of both the System and Application Passwords;
- Ensuring that no unauthorised person has access to system passwords;
- Maintenance of all system passwords;
- Ensuring that an administrator equivalent password is maintained and held by another official, in case of emergency.

Note:-

The system administrator should not be involved in any security administration with the exception of physical security of the systems.

2.5.4 Database Administrator

The database administrator is primarily responsible for the proper maintenance of the databases running in the Bank. The other responsibilities include

- Performance and tuning the database.
- Creation of new database based on requirement.
- Taking periodic backup of database.
- Preventing the database from corruption.
- Archival of data;
- Checking whether there is a proper procedure for labelling back-ups;
- Checking whether all the backups are stored in a secure location or not;

- Checking whether the copy of the system backup is available off-site or not;
- Testing the integrity of backups and recovery procedures to ensure that they work whenever required. This is done in order to protect the data from corruption;
- They should take the printouts of 'fall back reports' or preserve as magnetic files without fail every day;

Note:-

Network administration and database administration is specific work areas rather than independent jobs. In the case of a centralised environment, the data centre must have a dedicated network administrator and a dedicated database

administrator. These administrators should be properly trained in contemporary technologies for effective discharge of their respective duties.

Where ever IT Officer is not posted, support for IT and IS to FGM/STC etc. will be responsibility of IT Cell of the assigned/ nearby RO as per IT's arrangement**.**

CHAPTER-3

This chapter dwells on the identification and classification of the data pertaining to the bank and the mechanisms of handling data.

3 Data Classification

23.1 Classification Analysis

The terms 'information' and 'data' are used interchangeably in the computer environment.

Information should be classified on the basis of its criticality and sensitivity vis-à-vis the business operations. The criticality of information is directly related to the criticality of the processes accessing the information.

23.2 Classification Standards

Information should be classified based on level of protection required.

- Public release -Non-sensitive information available for external release.
- Internal - Information that is generally available to employees.
- Confidential (Sensitive) -Information that is sensitive within the Bank and is intended for use only by specified groups of employees.
- Restricted (Highly Sensitive) -Information that is extremely sensitive and is Intended for use only by Named individuals

within the Bank

CLASSIFICATION

Criteria	PUBLIC	INTERNAL	CONFIDENTIAL	RESTRICTED
Description	Non-sensitive information available for external release.	Information that is only sensitive outside the Bank. Generally available to employees.	Information that is sensitive within the Bank, and is intended for business use only by specific groups of employees.	Information that is extremely sensitive, of highest value to the Bank and intended for use by named individual(s) only.
Impact of Unauthorised Disclosure	No adverse impact on unauthorized disclosure.	Limited adverse impact.	Significant adverse impact, may adversely affect the Bank, its employees, its clients or customers May destroy the confidence in the	Severe adverse impact; May cause severe financial or legal damage to the Bank; May damage the Bank's reputation.
Access Restrictions	Accessible to all the employees working in the Bank.	Access normally restricted to employees.	Access must only be granted on a business need to know. Access by external parties must be subject to a non-disclosure agreement.	Access must be limited to the specified and authorized employees only. The Information, which is very important, must not be shown to or discussed with others who are not
Storage of Information	No security is required.	Site/Department storage should be adequate to prevent casual disclosure	Here the Information is encrypted in order to provide extra protection to the data. Media must be kept in a secured environment	Information must be encrypted using some encryption technologies. Media must be locked away when not physically in the presence of the originator or
Labelling of Information	Labelling not required	Must be labelled	Each page must be marked "Confidential"	Each page must be marked "Restricted"

Disposal of Information	Removal of Directory entry for file	Removal of Directory entry for file	In addition to removing the directory entry for the file, the space used by the file must be over-written using approved means.	In addition to removing the directory entry for the file, the space used by the file must be over-written using approved means. Information must be disposed off securely using approved methods and based on retention strategies

Criteria	PUBLIC	INTERNAL	CONFIDENTIAL	RESTRICTED
Examples	Annual reports, Publications, New products.	Circulars/Memorandums, Organizational charts.	Customer information, Budgets, Staffing plans.	Strategic business plans, Cryptographic keys and materials.

23.3 Responsibility of the Data Owner

The information owner should identify and classify the information he/she is responsible for, and the classification must be based on the business requirements for:

- Confidentiality of the information (it must be protected from unauthorised disclosure)
- Integrity of the information (it must be protected from unauthorised alteration)
- Availability of the information (it must be available when required by the users)

23.4Labelling the Classified Information

- Label both physically and electronically stored information, to ensure that the information is handled according to the Bank's rules;
- Physical labelling of documents, hardware items and removable media should include security classifications;
- Electronic labelling for computer based information needs to be introduced. This could be at the folder level for sensitive and confidential information;
- Consider using password controls and / or cryptography / check-summing for highly confidential information;

- Labelling systems should not be complex, as the overhead may outweigh the value of the items being protected.

23.5 Storing and Handling Classified Information

- Highly confidential information, which has not been transported safely or destroyed securely, may be disclosed in the public domain, resulting in the loss of Bank's reputation. So, whenever the use of information/data is completed, destroy the data or save the data in a secured location;

- Confidential information may retain its original classification when it should have been re-classified to a higher level of confidentiality. This may result in loss of the information due to its storage in an inappropriate location (physical or electronic).

23.6Accepting Ownership for Classified Information

- All information or data should belong to a person who is authorized to handle that information, and that person is normally responsible for its safekeeping;
- Confidential information apparently not owned by any one person could become lost, amended or compromised resulting in potential loss or embarrassment to the bank. So the information classified as confidential should have an owner;
- Allow only authorized people to access the confidential information;
- Protect the information with the password.

23.7Securing Data

Once the data has been classified, the next step is to secure it. Classified information needs careful handling so that it does not get lost or fall into wrong hands. Bank may loose its credibility if the information is not protected. Data encryption is a good technique to secure data especially during transmission.

23.8Using Encryption technique

By encrypting or scrambling data the confidentiality and integrity are assured. Sensitive or confidential information should always be transmitted in encrypted form. Prior to transmission, consideration must always be given to the procedures to be used between the sending and recipient parties and any possible legal issues from using encryption techniques.

- Document all procedures carefully;
- Keep public / private encryption keys safe;

- The keys used to encrypt and decrypt must be held securely, but they must also be accessible when required;

- Employ large-scale encryption across entire systems only when necessary;

- Determine which information is classified as sensitive, and whether it needs to be transmitted over insecure networks, such as the Internet;
- Once the information has been encrypted, transmitted to its destination and decrypted, consider how the information should then be stored securely;
- Where necessary, seek legal opinion to confirm that the proposed encryption technique may be used between the banks and countries in question.

23.9Sharing of Information

One of the fundamental principles of information security policy is the "**Need to Know**". This principle holds that information should be disclosed only to those people who have a legitimate need for the information. The data classification scheme has been designed for the bank to support the "Need to Know" policy so that information will be protected from unauthorised disclosure, use, modification and deletion.

The requirement for the minimum baseline security control (MBSC) mechanism that should be used for each information classification. For example, for achieving the objective of identification and authentication, no security mechanism would be required for public data. While user IDs and passwords would suffice for internal data, stronger authentication techniques such as PINs / Tokens / Biometric / Smart Cards, etc. may be considered for confidential and restricted data.

Persons responsible for Human Resources Management should ensure that all employees are fully aware of their legal and corporate duties and responsibilities concerning the appropriate sharing and releasing of information, both internally within the bank and to external parties.

- A duty of care and diligence is required to protect information especially that which can be classified as 'personal';
- Based upon the sensitivity (Restricted, confidential, Internal and Public) of the information, information may be released;
- Unless the information is classified as 'Public', it should be restricted to those who have legitimate need. Such restrictions can be imposed through software and hardware Access Controls;
- Comply with the relevant legislation by ensuring that the employees are aware of their responsibilities and adequate procedural and possibly technical controls are in place to enforce it;

- Disclosure of sensitive information to others should not contravene legal regulation or possible statutory guidelines.

23.10 Maintaining Customer Information Confidentiality

Keeping customer information confidential is a legal requirement and is very essential for bank's credibility.

- The confidentiality of customer data may be compromised if it is given to an unauthorized third party. So do not give any confidential information about the customer to the third party;
- Do not allow unauthorized people to access the confidential data about the customer because the confidentiality of data may be compromised.

23.11 Deleting Data Created / Owned by Others

Data may be deleted accidentally or intentionally by others when it is shared and not protected.

- Access to data should not be given to unauthorized persons.

23.12 Password Protection

Files and documents can be additionally protected with the help of passwords. Employees/Owners should

- Always remember the password of the application/document;
- Maintain password confidentiality;
- Ensure that the choice of password and the subsequent use is tightly controlled. This should be as per the password policy.

23.13 Securing Data during Data Entry

- The first stage of ensuring data integrity is in the data entry stage itself. In respect of customer transaction accounting packages like those used in fully computerised branches, the integrity of customer master data assumes great significance;
- If master data creation is entrusted to outside agencies, the branch/office entrusting the job should make enquiries about the credentials of the agency as regards it's integrity;

- The data-entry of critical/sensitive data should be carried out in the Bank's premises only. The data or the concerned source documents should not be allowed to be taken outside Bank's premises;
- To ensure that the master data is correct, complete and consistent, branches should check the master data printouts against the source documents ;
- Branch should ensure that the errors noticed during the checking are promptly corrected in the system and after all the corrections are effected, a final printout should be taken to ensure that the corrections have been correctly made;
- The final printout should bear, on each page of the printout, round stamp/seal of the branch and the initials of the checking officials. It should be neatly bound and preserved.

23.14 Data Stores

23.14.1 On-Site Data Stores

- Ensure that data store is located within a secure area;
- Maintain tight control over media leaving and entering the secure area. Consider the use of locked boxes and dual control to protect media in transit;
- Agree formal procedures for non-routine media movements, preferably involving written managerial authorisation. Check periodically that the procedure is working;
- Ensure that the stored media is afforded due protection against environmental threats;
- Ensure that all media is adequately labelled, whether physically and / or magnetically;
- Consider taking duplicate/multiple copies of important media for added security and store them in different locations;
- Ensure that the manufacturer's guidelines with regard to the storage of the media are followed.

23.14.2 Remote (off-site) Data Stores

To protect against accidental loss of data, regular backup should always be taken and stored at a remote place i.e. offsite. This issue is further discussed under "Backups".

23.15 Transferring & exchanging data

Sufficient care has to be taken in transferring/exchanging data. Transmission of data may be through networks or through media and appropriate security measures have to be applied.

- It should be ensured that only the appropriate information is made available, or sent to, external parties and clients;
- Integrity of appropriate categories of data should be verified prior to transmission; for instance, data classified as 'Highly Confidential' or 'Proprietary' may require specific authorisation;
- The network should prevent unauthorized and illegal access to its computer resources;
- There should not be any opportunities for physical intrusion;
- Encryption of sensitive data should be considered to thwart a possible attempt at sniffing the data packets as they pass between different nodes on the network;
- The level of safeguards should be appropriate to the sensitivity of the information and its value to the bank;
- Wherever possible, applications software and the operating system's controls should support and enforce the controls required;
- Where information is to be transmitted to another bank it is essential that their Information Security safeguards are at least complementary to ours;
- It is prudent to agree and sign a mutual Non-Disclosure Agreement to demonstrate to third parties Bank's commitment to Information Security;
- To preserve the integrity of the original information, ensure that any copies, which are subsequently transmitted, are prefaced with storage, distribution, duplication and retention instructions;
- Comply with the relevant legislation by ensuring that employees are not only aware of their responsibilities, but that adequate procedures and possibly technical controls are in place to enforce it;
- Sensitive or confidential data / information, may only be transferred across networks, or copied to other media, when the confidentiality and integrity of the data can be reasonably assured e.g. by using encryption techniques.

CHAPTER - 4

This chapter outlines the access control policies including physical, logical and application access.

4 Access Control

Access control norms should define the procedures to regulate allocation of access rights to the information systems and/or services and should cover all stages in the life-cycle of user access viz. from initial registration of users to their de-registration. Privileged access rights that allow users to override the system controls should be closely monitored.

- Formal written procedures should be in force, which should define the modalities for Request, Authorisation, granting, enabling and deletion of access to the Bank's computer resources;
- All the employees, Consultants, vendors, visitors etc. should wear identification badges at all times;
- Visitors to Data Centres should sign a log register, which should contain the name, time of entry, Company/Department, and person intending to visit before granting access. Time of exit should later be recorded;
- There should also be a register (log book) maintained for the purpose of recording the entry and usage of the equipment with proper authorisation details of the person;
- The access to the server room should be closely monitored/controlled;
- Emergency access rights to systems for support/maintenance purposes should be documented and approved by the authority concerned;
- The Bank should have procedures for revoking the access rights and removal of the user accounts in the case of those on leave/retiring/resigning/absent;
- Time-out key board lock facility should be introduced to sensitive applications like financial transactions;
- Access to media and manuals like tape, disk, and documentation libraries etc should be restricted exclusively to those employees whose responsibility is the maintenance of those libraries;
- Secured doors should not be kept open under any circumstances;

- Personnel handling highly sensitive/security areas may be under pressure to reveal access codes/breach security norms and set to unauthorized/illegal tasks such as copying confidential information. The bank should take appropriate measures to safeguard against such eventualities;
- Supervisors should notify to the Administrative Manager when a user is no

longer allowed access to the facility;

- Staff should take reasonable precautions to ensure protection of systems or data available within their workspace. This includes the use of screen saver passwords, securing of confidential information, and shredding of confidential documents;
- Physical access to the data centre should be restricted to authorized personnel only;
- Suspicious activities should be escalated to the concerned authority promptly;
- The Managers should take reasonable precautions to ensure security of their area.

4.1 Logical

It is the collection of all controls used to ensure that only authorized users should have access to information/information processing facilities for which they are authorized. To identify individual users of information/information processing the following procedures should be followed.

- Assign unique user id to each individual user, maintain a record of the same in a register and take acknowledgement (signature) for the same;
- Norms should be in place to bind the users accountable for all activities performed under their user-id;
- Cancel privileges assigned to retired/resigned or transferred employees immediately;
- Suspend/cancel privileges of users who are on leave during the relevant period.

4.2 Operating system

- Automatic terminal identification should be considered to authenticate connections to specific locations and portable equipment;
- Access to information services should be through secure logon procedures and should be designed to minimise the opportunity for unauthorized access;

- All users should have unique User-IDs to ensure that all the activities can subsequently be traced/tracked to the user;
- Passwords are one of the principal means of validating a user’s authority to access system/applications. Effective usage of password should therefore enforced;
- Inactive terminals in high-risk location should be set to time out, to prevent

access by unauthorized persons.

- Machines with Windows Operating System are originally supplied with default user id as "administrator" and with no login password. Therefore, it is important to first assign a suitable password for "administrator" user id. Further, a separate user id with required rights should be crated with a proper password and the same should only be used for routine work. The administrator user id should be used restrictedly. The passwords should be maintained as per the Password Policy and in case of any necessity, the same should be available in the branch/ office.

4.3 Application

- Logical access controls (User-Id and password) should be used to control access to application systems and data;
- Many computers have one or more system utility programs, which might be capable of overriding system and application controls. It is essential therefore that the use of this (system utilities) is restricted and controlled;
- Wherever a facility is available, data and system owners should ensure that unattended terminals enforce time-out at short intervals;
- Resumption of system access should prompt revalidation of the User's identity.

4.4 Limiting sign-on attempts

In order to limit the opportunity for unauthorized attempts to sign-on to a system.

- Suspend the user-id after a maximum of **3** repeated unsuccessful log-on attempts;
- Set authentication time limit for **3** minutes;
- Terminate the session if the time limit is exceeded. Communicating to the users about the failure but not the reason;

- Authorized parties should be restricted to those functions, which have been assigned to them;
- Warning screen should be displayed, warning the user that unauthorized access will result in prosecution.

4.5 Monitoring System access and use

- Systems should be monitored to ensure conformity to access policy and standards;

- Establish elaborate fault/event access/logging system and monitor/review constantly;
- Proper audit trial mechanism should be in vogue. Important records like password changes, system breakdown, error rectification, vendor's visits etc should be maintained;
- Establish procedures for monitoring systems;
- Setting of computer clock correctly plays an important role to ensure the accuracy of audit logs, which may be required for investigations or as evidence in legal and disciplinary cases;
- There should be a mechanism by which the bank should monitor the incoming and outgoing files of the employees. It should be ensured that the employees are made aware that the bank reserves the absolute rights, to monitor incoming and outgoing files of the employees, as part of the terms and conditions of the employment and also by way of the management directives in this regard.

4.6 User Transfer or Termination Controls:

Notification to IT Department upon user termination / transfer / resignation:

For non-CBS branches, branch head of the concerned branch should be responsible to take appropriate action regarding user id of the person who has either been terminated, transfer or has put his resignation. In all above cases, user id should be deleted and subsequently to be informed to concerned ROnal head.

For CBS branches, in case of transfer, user id should be disabled temporarily in the transferred branch and should be enabled in his new branch. For termination and resignation, user id should be disabled permanently. The disabling of user id either temporarily or permanently will be done at CBS help desk for which branch head has to request for the same.

For all other offices like ROnal office, FIO, Head Office, etc. if an employee is terminated, transferred or put his resignation; his user id should be disabled. In all such cases the employee's Head of the Department should be involved for access rights. But if access to any restricted and sensitive information is concerned, DIT, HO should be taken into confidence.

Use of Network Security Monitoring tools: The Bank should deploy network security monitoring tools to verify the compliance with the network policies and generate exception reports from the system to perform quick health checks on network operations and management.

- **Implementation of network security policies:** The bank should adopt network security policies (strict controls) and IT department is responsible for implementing these policies on all network systems and host computers.

- **Change in network security policies:** Any modifications to the Logical Access policies should be made only after getting the written permission from DIT, Head Office. This change should be made with the help of Systems Administrator.

Application Specific access control policies: Following procedures should be adhered to while granting access rights to application users-

- **Creation of super user**

For all application systems running at other various locations, IT department should control the creation of super user for the application.

- **Right to control operating systems**

The department users should not be granted any rights to control the operating system privileges and tools.

- **Access to database**

Access to database tables, parameters and commands should only be restricted to respective database / systems administrators.

Access rights granted to 'Third Parties':

Access given to third parties for bank's information resources should be restricted and governed by the same principle of 'least privilege' and 'need to know basis'. The bank's employee coordinating with the respective third party consultants, engineers, vendor's representatives etc. are responsible for justifying and authorising the access rights granted to third parties.

- **Network Access Agreement:** The network access government should be entered into with the 'Third Party' before granting access to Bank's network, which would cover the responsibilities as well as the terms and conditions agreed by third party.

- **Remote connectivity:** Third party representatives should be restricted to use Bank's information resources from within the bank's network. In other words, remote connectivity from their office to the bank's network should not be allowed. However, restricted access can be provided if circumstances demand with due permission from DIT, HO. Audit trail of all such access should be taken and preserved.

- **Access rights to Helpdesk and implementation team:** Access rights to the consultants and software developers such as Helpdesk and implementation team should be formally granted and monitored. The relevant rights should be taken back once the required assignment is over. The helpdesk should primarily, be given the access to reports menu screens in the live database at the unit.

Following are the procedures for granting access to outsourced party:

- An access rights form should be completed by the outsourced party
- The outsourced party should obtain approval from controlling office / DIT, Head Office. They should communicate the approval to the System Administrator.
- On receiving information, the System Administrator should create separate IDs for outsourced parties which will be communicated to third party.
- After the Outsourced Party confirms completion of the job, the System Administrator should change the password of the said ID or delete the ID itself as the case may be after taking permission from granting authority.
- At the end of the day System Administrator should review activity logs generated at the Operating System level to monitor activities performed by the outsourced party. Such log should be made available to the controlling office / DIT / Auditor on demand.

4.7 Segregation of Duties

- Actual job titles and organizational structures may vary greatly from one organization to another, depending on the size and nature of the business. However it is important to obtain information to assess the relationship among various job functions, responsibilities and authorities in assessing adequate segregation of duties. The aggregation of duties avoids the possibility that a single person could be responsible for diverse and critical functions in such a way that errors or misappropriations could occur and not be detected in a timely manner and in the normal course of business process.
- Segregation of duties is an important means by which fraudulent and/or malicious acts can be discouraged and prevented.
- Duties that should be segregated include –

  a) Custody of the assets,
  b) Authorization
  c) Recording transaction

d) Parameter Setting

e) Access to Applications

f) Right to install utilities

- If an adequate segregation of duties does not exist, the following could occur:

  a) Misappropriation of assets.
  b) Misstated financial statements.
  c) Inaccurate financial documentation
  d) Improper allocation / transfer of funds or modification of related data could go undetected.

- When duties are segregated, access to the computer, the production data library, the production programs, the programming documentation, and the operating system and associated utilities can be limited.

- Potential damage from the action of any person is therefore reduced. Compensating controls are internal controls that are intended to reduce the risk of an existing or potential control weakness when duties can not be appropriately segregated.

- The purpose of segregation of duties is to reduce or eliminate business risks through the identification of compensatory controls. Ideally the compensatory control should be proportional to the level of business risk.

- Compensating controls for lack of segregation of duties –

  a) Audit Trails
  b) Reconciliation
  c) Exception Reporting
  d) Transaction Log
  e) Supervision Review
  f) Independent review.

CHAPTER-5

This chapter specifies the selection criteria for premises that would house IS infrastructure and the various controls that need to be set up.

5 Premises

Computer systems and related equipment should be installed/ stored in secured premises where various infrastructural facilities are in place.

5.1 Selection of Site for Computers

It is important to consider the selection of premises for installation of the computer hardware carefully at the planning stage itself as it would be difficult to make changes later once a location has been selected. The size of the area will be determined by the number of hardware to be installed. The following precautions will enable the Bank to select appropriate premises.

- Ensure that the proposed area is secured against unauthorized persons e.g. by strong fireproof doors, locks, swipe card access, security cameras, etc;
- Ensure that only authorized staff routinely enters the area and that other legitimate visitors should be formally escorted and their visits logged;
- Ensure that windows are secure against forced entry by individuals, projectiles that may be thrown or by fire within the building;
- Investigate the usage of neighbouring rooms to ensure that they do not provide an alternative entry into the secure area;
- Basement areas are to be avoided since they may be prone to flooding;
- Investigate the structure of the building to ensure that it will resist and combat fire.

5.2 Server Room policy

The branches of Allahabad Bank that are fully computerized should have a separate and secure room/partition/cabin/enclosure (and should also have proper electrical points, UPS, air-conditioning and provision for adequate security) that is designated as the Server Room, as far as possible. This room would house all the servers that are available in the LAN (and WAN) as well as the LAN (and WAN) equipment.

Location of Server Room:

The operational area and the server room should preferably not be situated on the ground floor in order to reduce risk of damage by water seepage. Further all the walls of the server room should be away from windows and should ideally be isolated from any external atmospheric influence. The IT equipment in the server room should be kept in racks.

Drainage System:

The drainage system should be such that water and drainpipes are located away from the server room.

Flooring:

The flooring should be at an ideal height of one foot from the ground and should be tiled with the anti-static material.

Switches:

Switches and sockets should all be grounded (provided with earthing) and provided with circuit breakers to avoid any untoward incidents due to faulty wiring or short circuit.

Cleanliness:

To avoid dust from entering the server room from the entrances, there should be a strict instruction on leaving the shoes outside the server room with special rubber slippers provided for the server room. Further, no food or eatables should be allowed in the server room.

Emergency Lamps:

Self-activating emergency lamps should be placed in the IT operations area and any other location as deemed necessary, as they may be required to handle abrupt power failures.

Emergency Power-Off:

Ensure the installation of emergency power off switches in strategic locations with adequate labelling and shielding to avoid accidental activation.

All ROnal Offices and other mission-critical installations should have one Server room with proper electrical points, UPS, air-conditioning and provision for

security on a 24x7 basis to safeguard the servers, routers and other networking equipment.

Note: The UPS should be preferably kept away from the server room.

- The server room should not be located in open spaces or near source of fire or near entrance or near public / customer area as far as possible.
- The server room should be accessible only to the personnel authorized by the Bank.
- Server/Switch rooms should have proper access control.
- The Server/Switch room should display a notice stating that unauthorized access is not permitted.
- A dedicated UPS with maintenance-free batteries (which should be replaced regularly depending on vendor specifications) should be maintained for server room and servers.
- The UPS should ideally reside in a dust free environment similar to that of a server room.

- There should be adequate space around the UPS for maintenance purposes.
- The UPS should be adequate to provide voltage at the same level as the regular supply and there should be no glitches in the process of the UPS taking over the electricity supply as these glitches can severely harm the machines.
- A chart showing the operational guidelines for the UPS must be prominently displayed in the room where the UPS is housed.
- Only the critical servers and the temperature control devices should be connected to the UPS to minimize the down time and service interruption.
- Visitors should not be allowed into the Server Room / Switch Room.
    - In case of vendors or support personnel entering the Server/Switch room for the sake of maintenance/support, a visitors' register should be maintained.
    - The entry of such people should always be accompanied by the entry of authorised personnel.
- Smoking and the consumption of food or drink should not be allowed in the Server/Switch rooms.
- Enhanced levels of environmental and fire protection should be installed in the Server/Switch room commensurate with the value of the systems

installed and the specific environmental needs as specified by the manufacturer and local conditions.

- Circuit breakers and shutdown mechanisms should be protected against the possibility of being accidentally set off.
- All authorized staff should be made aware of the specialized control systems installed.
- The emergency procedures should be documented and regularly tested.
- The authorized personnel and the visitors should be aware of the emergency evacuation instructions.
- The instructions manual, to be used in case of emergency, should be displayed in a very conspicuous manner.
- All the hardware devices should be numbered and labelled with a unique asset number.
- The addition/removal/relocation of hardware should be recorded and numbering and labelling done as mentioned above.
- Such modifications should be done as per "Change Management procedure".

- Should have two numbers of Power Off switches – one inside server room and another outside server room (properly protected)

5.3 Housekeeping

- The Server/Switch Room should be kept neat and clean always.
- The housekeeping staff should keep the premises clean on a regular basis.
- The doors should not be kept opened while cleaning the premises.
- A person authorised by the Bank should be supervising the cleaning work.

5.4 Physical Protection of Computer Premises/ Data Centre

Computer premises must be safeguarded against unlawful and unauthorized physical intrusion.

- Ensure that the periphery of the area has been secured against unauthorized access;
- Consider the danger posed by probable access through roof/ceiling and windows without locked grills;

- Consider the potential for access through drainage and sewage and under false floors;
- Protect external doors in the ground floor, windows and walls against forced entry;
- Consider the use of a security guard/external security agency;
- Ensure that the routine personnel access channels are designed to withstand against forcible entry by persons with ill intentions. Routine checks should be conducted on whether the doors are locked;
- Ensure that the incoming and outgoing services including communication lines are hidden from view and are adequately protected against damage;
- Consider the use of cameras with monitored screens and video recorders;
- Install an intruder alarm system;
- Install panic buttons at key locations throughout the premises;
- Ensure that Access controls are adequate to guard against opportunistic and pre-meditated unauthorized entry.

5.5 Environmental Security

5.5.1. Fire

- Smoke detectors should be installed near the equipment;

- Fire extinguishers should be kept near the equipments and employees should be trained in their proper use;
- Regular mock fire tests and evacuation exercises should be conducted.

5.5.2. Environmental failure (Heat and Air pollution)

- The premises hosting the server / network equipment / PCs, etc. should have air-conditioned facilities to prevent dust, heat and air pollution affecting IT equipment.
- The server room should have dedicated air-conditioning equipment with the temperature maintained ideally at 20 degrees Centigrade (+/- 2 degree Centigrade)
- The humidity level in the server room should not cross 50%
- The particulate dust content of the air in the server room should be maintained at below 75 mg/m3.

5.5.3. Earthquake

- Computer systems should be kept away from glass and elevated surfaces;
- In high-risk areas (earthquake-prone) computers should be secured with anti-vibration devices.

5.5.4. Lightning

- Surge suppressers should be installed;
- Backups should be stored in grounded (with proper earthing) storage media;
- Uninterruptible Power Supply (UPS) and diesel generators should be properly grounded.

5.5.5. Electrical Interruption

- UPS should be installed and tested;
- Wherever necessary line filters are to be installed to control voltage spikes;

5.5.6. Physical Access Control to Secure Areas

In view of the dangers of theft, vandalism and unauthorized use of systems, the Bank should consider restricting the number of those people who have physical access to the area where computers are housed. This requirement should be taken into account when premises are being chosen.

- All the Staff, consultants, vendors, visitors, etc. are required to wear identification badges at all times;
- Visitors to computer centres are required to sign a log which should contain the name, time of entry / exit, name of the company/department, purpose of visit and name of the person whom they want to meet in order to gain entry;
- Visitors to these areas will be provided with a temporary ID badge to be worn;
- Access to tape, disk, and documentation libraries are restricted exclusively to those employees whose responsibility is the maintenance of those libraries;
- Secured doors will not be kept open unattended at any time under any circumstances;
- Supervisors should notify the Administrative Manager when a person is no longer allowed access to the facility;

- Staff should take reasonable precautions to ensure protection of systems or data available within their workspace. This includes the use of screen saver passwords, securing of confidential information, and shredding of confidential documents;
- Physical access to Server room/ Switch room shall be restricted to authorized personnel only;
- Suspicious activity should be reported to the supervisor and/or campus police to be notified;
- Visitors who do not have an ID badge will be escorted to the front-desk and assisted with obtaining one;
- Do not allow unescorted visitors/strangers to enter the secured premises because there is chance that they may access confidential material or damage the Bank's property;
- Restrict access to secured areas.

CHAPTER - 6

This chapter outlines the policy that needs to be followed for purchase of hardware and software and other peripherals and the policy to be followed during the process of purchase and installation.

6 Hardware, Peripherals and Other Equipment

6.1 Pre-Despatch Inspection

- For all purchases of Rs. 10 lacs and above, in the case of Bulk Procurement through Advertised tendering and Discrete Procurement of Standard Items through Empanelment, Pre-Despatch Inspection of goods would be conducted before delivery to ensure the quality of the goods and their conforming to the minimum technical specifications immediately on receipt of the intimation about the readiness of the equipment. Pre-Despatch Inspection would be done by outside agency. Officers from HO, DIT and nearby ROnal office, where the factory/manufacturing unit is located may also be associated for Pre-Despatch Inspection.
- For purchases below Rs. 10 lacs, Pre-Despatch Inspection / Post Delivery Inspection may be conducted by the IT officers from Head Office DIT or nearby ROnal Office, as the case may be.
- The Report of Pre-Despatch / Post Delivery Inspection should be preserved securely by IT Department of office/branch for future reference;
  - It must be ensured that the report is signed both by the vendor and the Inspector/officer. The purpose of the vendor signing is to confirm that the Inspection has been done in the presence of the vendor.

6.2 Installation

Installation of new equipment must be properly monitored and planned to avoid unnecessary disruption and to ensure that the Information System issues are adequately covered. The equipment must be located in a suitable environment. In the case of installation of existing used hardware, care should be taken not to leave any confidential / sensitive data. The absence of an installation plan could lead to disruption to operation / systems. The installation plan should also cover adequate safeguards against increased security threats resulting from access to the systems area either accidental or intentional. The norms for hardware installation should be on the following lines:

- Adhere to the specifications and recommendations of the vendor;

- Build in adequate safeguards against fire, water, electrical failure etc.;
- Ensure that the representatives of the vendor execute a Non-Disclosure Agreement. A Non-Disclosure Agreement supports for legal redress but is not effective against actual commercial damage;
- All new systems should be configured for maximum practical security by removing unnecessary utilities;
- Ensure that all pre-installation infrastructure requirements at the premises

should be complete;

- Identify the exact location for the equipment and ensure that the power and network cables are ready;
- Anticipate events which could go wrong and consider how to minimise the risks;
- Discuss and detail the installation plan with the vendor and agree upon a detailed plan and document it;
- Allow only authorised personnel to access the systems;
- The Service Engineers should not be allowed to work unattended;
- Ensure that the safety and comfort of the users followed when locating the equipment, peripherals, and cables etc.;
- Carry out periodic monitoring of the progress;
- All new hardware installations are to be planned formally and notified to all concerned parties ahead of the proposed installation date;
- IS Security requirements for new installations are to be circulated for the information of all concerned parties, well in advance.

6.3 Acceptance Test

New hardware must be tested to ascertain if the same is working correctly. Further tests should be conducted periodically to ensure continued and effective performance functioning. Wherever new equipment is not tested for critical functions before being used, it will lead to failure and damaging both data and other linked systems. Inadequate testing will also hamper the integrity and availability of data. Testing should be therefore performed simulating live conditions so that the results of such testing can be relied upon. Adequate security procedures during testing of equipment should be built in to ensure confidentiality of data.

Taking the above risks into consideration the following guidelines for pre-installation testing for hardware needs to be followed:

- Ensure that all new installations are thoroughly tested after initial setup and before going live;
- All such tests should be in accordance with a documented test plan;
- Check the outputs of the tests to confirm the results and ensure that all key components are included in the tests;

- Devices that are known to degrade with time, e.g. printers, should be tested periodically;
- Ensure that the test plan simulates realistic work patterns;
- Ensure that Non-Disclosure Agreements have been obtained from all third parties involved in testing the equipments;
- Verify that the required security configuration and safeguards have been implemented for the new hardware;
- If live data is used in the testing process for the new hardware, ensure that it is closely monitored / controlled;
- All equipment must be fully and comprehensively tested and formally accepted by users before being transferred to the live environment.

6.4 Maintenance and Support

To ensure proper functioning / operation, hardware should be maintained clean and serviceable. Maintenance requirements vary based on the IS size and complexity. In any event, maintenance should be scheduled to closely coincide with vendor provided specification/industry standards. The guidelines for hardware maintenance and support are as follows:

- The hardware should always be covered either by warranty or by Annual Maintenance Contract (AMC). Branches / offices should take care to note and ensure renewal of AMC in time. The AMC should be on-site and comprehensive and covering all the relevant components;
- To detect and prevent systems from being infected by computer viruses, all newly acquired software coming with the hardware, should be scanned for existence of viruses before installation;
- All hard disks should be scanned for viruses on a routine basis (i.e. each time the system/PC is powered on);

- Hardware equipment should be maintained in a manner consistent with the manufacturer's recommendations;
- All hardware equipment maintenance activities should be reviewed annually in order to ensure that maintenance performed is consistent with the requirements recommended by the manufacturer;
- Hardware maintenance personnel working on equipment processing banking data or working in areas where access to such data is possible should be supervised / monitored by a knowledgeable official of the Bank who understands the implications of the actions taken;

- In instances where maintenance of equipment requires the exchange or release of components viz. tapes, disks, diskettes, memory that may contain Bank data, those components should not be released to the vendor unless the data has been rendered non-decipherable to the vendor by means of erasure or encryption techniques. Wherever these methods cannot be used, the equipment should be disposed of in a secure manner;
- Highly sensitive data must be completely obliterated (e.g. reformatting of diskettes or hard drives) and simple erasure techniques that can be recovered using software utilities are not adequate in such cases;
- The Bank should take all reasonable precautions to ensure that data maintained on the system is not compromised through the use of a remote diagnostic access;
- Computer systems including system, Application software and Hardware should be comprehensively insured;
- Alternate sources of power should be available for hardware and other equipments which are deemed essential for operations;
- System power input should be checked at least annually to ensure that it meets the manufacturer's specifications;
- System earthing should be checked at least annually, through contractor, to ensure that it meets the manufacturer's specifications;
- Where an Uninterruptible power supply (UPS) is used all hardware devices required for continued operation should be powered through the UPS.
- The UPS should shut off power to the system (file server, workstation, PC or minicomputer) in the event of fire or conditions exceeding specified environmental requirements.
- A power surge suppresser should be installed in areas that have a history of frequent significant power fluctuations.

- Where static electricity may affect the integrity and reliability of data and programs processed and stored on the equipment, anti-static devices should be installed.

6.5 Insurance

All computer hardware should be adequately insured as per the depreciated value of the asset, under the electronic equipment policy.

Insurance for software is not required.

All hardware and peripherals whose legal ownership vests with the Bank, should be insured irrespective of whether payment is made or not and/or whether full payment is made or part payment is made and / or whether such payment is debited to GL A/c Furniture and Fixtures or to GL A/c Suspense Debits or any other GL Head.

The branch should ensure that all hardware upgraded/purchased subsequent to the obtaining of insurance policy is also brought under insurance

In the event of any mishaps, prompt steps should be initiated for invoking the claim.

Ensure periodical review of adequacy of insurance coverage.

6.6 Disposal of IT Assets

The computer hardware is rendered obsolete in the shortest span of time when compared to other assets for the reason that latest versions with additional features are launched at frequent intervals. The obsolescence of hardware is further driven by the features and requirements of software, as the performance of the software is dependent on a certain level of minimum hardware configuration. At present in a period of seven years IT assets may be considered as obsolescence. The disposal of such assets will be done at the discretion of ROnal Office and Head Office. The disposal of all IT assets should be done in accordance with Hardware Procurement Policy. While taking a decision in this regard the type of the hardware, number of years used, utility value both present and future, condition of the asset, maintenance support etc. should be the factors, which are to be mainly considered.

Following safeguards are taken at the time of disposal of IT hardware assets:

- Respective ZITC / System Administrators should suggest whether to dispose an IT asset and DIT or ROnal Head should consent the approval as per Hardware Procurement Policy.

- Storage devices containing sensitive information are physically destroyed or securely overwritten/formatted in such manner that the data can not be normally recovered.

- Low level formatting is done rather than using the standard "Delete" function.

- All items of equipment containing storage media, e.g. fixed hard disks are checked to ensure that any sensitive data and licensed software is removed or overwritten prior to disposal.

- Any useful data / program, etc. should be properly backed up and should be labelled and kept safely in respective ROnal Office / Head Office before destroying or removing the same.

- Damaged storage devices containing sensitive data rechecked for data accessand then decision is taken whether to repair, discard or destroy it.

- Degaussing of data in the hard disk has to be done before the disposal of the hard disk.

6.7 Documenting Hardware Inventory

A register / database of all computer equipment used within the bank are to be established and maintained. In the absence of these the IT assets cannot be appropriately protected.

The policy for maintaining Hardware Inventory is as follows:

- Establish an inventory and implement procedures for keeping it up-to-date;
- Ensure that a documented procedure to advise the acquisition of new hardware, the disposal of old items, and any changes of location is in place;
- Periodically verify the correctness of the inventory by checking that a sample of hardware is physically present;
- Ensure periodical review of the adequacy of insurance cover;
- Establish an inventory and, in conformance with IT Plan 'ear-mark' equipment for replacement and should be planned accordingly;
- Record key information, especially hardware specifications and system software names and versions.

6.8 Hardware Equipment

6.8.1 UPS

- The UPS should be installed in a room/cabin, which should preferably be kept under lock and key;
- The UPS should be installed in a separate cabin/room and not in the same cabin/room as the servers;
- The UPS room should not be very near the server room to prevent spread of any fire resulting from a short circuit in UPS room to the server room or vice versa;
- The UPS room/cabin should have an independent access and not through the server room to obviate the need for the UPS maintenance personnel to pass through the server room;
- The room should be spacious enough to house the UPS, batteries and provide

for space for maintenance personnel to move around;

- The UPS and batteries should be provided with the recommended ambience with special attention to temperature control, humidity, dust free environment etc.;
- If the batteries are of lead acid type (e.g. tubular), the UPS room should have sufficient ventilation. An exhaust fan should also be provided to facilitate better ventilation.
- It must be ensured that the UPS is not switched off and that the power cord is properly secured to the equipment. It must be also made sure that the battery cords are properly connected;
- It must be ensured that no unauthorized person tampers with or changes the switch-settings on the UPS;
- Generally the batteries of the UPS take 8 to 12 hours for getting fully charged If the local power supply is erratic or if there is no power supply for at least 8 hours in a day, suitable arrangement for provision of a generator should be made;
- No load other than computer load should be allowed to be connected on the power supply from the UPS as it affects the quality of power supplied to the computers.

6.8.2 Modems

This usage of modems are fraught with some potential dangers arising when using Modems, ISDN links connections. These services provide an instant extension of the network but use insecure public lines and therefore considerably increasing the risk of attack of the data transmitted over such modes of connection. In view of this, the following safeguards should be followed:

- Use of modems for Internet connection from individual PCs must be strictly restricted and in so case such PC is to be connected to the network;
- Standalone systems meant as network node should not be purchased with in-built modems;
- The need for accessing the network or the corporate intranet through dial up modem should be strictly monitored and allowed on need to know basis;
- In case of need, if dial-up connection is allowed to access the corporate Intranet, a request-response mechanism should be in-built to authenticate the caller.

6.8.3 Network Hardware Equipment

The LAN equipment should be kept in the Switch/Server Room.

- Manageable hubs/switches/routers should be configured and managed by the authorized personnel only;

- The hubs/switches/routers should be properly mounted on racks meant for such equipment;
- Under no circumstance should hubs/switches/routers be kept on the floor;
- It is suggested to have 25% capacity of hubs/switches free so that they can be put to use in case of any emergency or failure.

6.8.4 Consumables

Some of the examples of consumables are printer stationery, magnetic media, toner and ribbons etc., the expenditure on which are of recurring nature. Pilfering of consumables results in increased expenditure for the Bank. Outputs/reports could also be used with the intent to defraud the bank or customers. There is also a possibility that confidential data would fall into the hands of unauthorised persons from discarded consumables.

Considering the above risks or exposure the policy for consumables should be as follows:

- Safeguard consumables against petty theft by locking cupboards, maintaining a register, insisting on verbal authorization prior to removal of items etc.;
- Take special measures to protect potentially valuable pre-printed forms and account for their usage;
- Ensure that confidential information cannot be extricated from discarded consumables, such as printer ribbons and floppy disks, by destroying them;
- Destroy or shred surplus printouts whether or not the data appears to be confidential;
- Consumables purchase should be handled only by the Division authorised by the Bank to do so, with inputs from IT division;
- Purchase of consumables should be followed with appropriate purchase procedures in place.

6.8.5 Desktops, Laptops, Notebooks and Mobile Computing Devices

This policy addresses the actions that must be taken by all - -'s personnel who have been issued by the bank or uses bank's Desktop/ Laptop/ Notebook/ Mobile Computing Device, or for those who temporarily use the same, issued/ provided to any other employee.

Users of Desktop/ Laptop/ Notebook/ Mobile Computing Device computers should follow the norms of this policy to ensure minimized risk of vulnerability of computing. The valuable data contained in Desktop/ Laptop/ Notebook/ Mobile Computing Device should be secured from theft and/or unauthorized access. Desktop/ Laptop/ Notebook/ Mobile Computing Device users and custodians should follow proper procedure to reduce the disruption caused by theft or unauthorized disclosure of information on notebooks to an acceptable level through a combination of preventive controls.

The different levels of Securities are -

A. Physical Security –

Employees of Bank using a Desktop/ Laptop/ Notebook/ Mobile Computing Device shall ensure secure storage of the Desktop/ Laptop/ Notebook/ Mobile Computing Device computer outside the office. In this respect, the points to be considered are –

- The Desktop/ Laptop/ Notebook/ Mobile Computing Device computer shall not be left unattended.

- If Desktop/ Laptop/ Notebook/ Mobile Computing Device computer is kept in a car, it should be placed out of view of casual Onlookers.
- If Desktop/ Laptop/ Notebook/ Mobile Computing Device computer is used in offices of other customer locations, the individual should ensure adequate physical security.
- In hotel rooms, Laptop/ Notepad computer shall be kept out of general view. If possible they shall be chained with physical security devices.
- In case of stationary use of Desktop/ Laptop/ Notebook/ Mobile Computing Device in Bank premises or other locations owned by Bank, they shall be secured as desktop systems during the operation. During off times, they shall be locked in a Cabinet or taken with the individual, as is applicable.
- Insurance cover shall be in place to protect all the Desktop/ Laptop/ Notebook/ Mobile Computing Device computers of Bank.

B. Logical Security of Desktop/ Laptop/ Notebook/ Mobile Computing Device –

- Each Desktop/ Laptop/ Notebook/ Mobile Computing Device Computer owned by Bank shall be provided with boot password Protection.
- Passwords shall be changed before handing over notebook computer to the user.
- All the Desktop/ Laptop/ Notebook/ Mobile Computing Device shall be enabled with the power save option, which can be activated by a specific key combination. If Notebook computer is not used for a longer break, it shall be switched off.
- When the user of a Notebook computer changes, it shall be ensured that the system shall be freshly installed and configured to prevent earlier owners

data sharing with the new user.

- Personal firewalls shall be installed in all Desktop/ Laptop/ Notebook/ Mobile Computing Device computers, which prevent the unauthorized access of data and applications when connected on the network. The rule base of firewall shall be same on all Desktop/ Laptop/ Notebook/ Mobile Computing Device computers and this shall depend on the applications and software used by the Bank employee.
- Users shall not create universally accessible shares in the Notebooks. If the shares are created they shall be restricted to only those users who are authorized to view it. It is recommended to remove the shares after specific purpose is over.
- Confidential/ restricted data/ information shall not be kept in the shared folders by notebook computer custodians/ owners.

- Incoming and outgoing data from Desktop/ Laptop/ Notebook/ Mobile Computing Device should be properly encrypted.
- Latest Antivirus should be installed on a regular basis. Updated Anti-spyware should also be installed.
- All the users of Desktop/ Laptop/ Notebook/ Mobile Computing Device should strictly follow the Password Policy.
- Important, Sensitive and Confidential information in the Desktop/ Laptop/ Notebook/ Mobile Computing Device or on any media used along with computers should be properly password protected.
- By default "Remote Desktop Connection" and "Net Meeting" features are available in windows operating systems. This feature is specifically used to remotely access and take control of the machine for troubleshooting purpose. Once permitted, the machine can be remotely controlled/ accessed later on also, until the access password is changed or the feature is disabled. This poses greater risk, as the local user of the computer may remain unaware of any unauthorized access/ changes. Therefore, remote access password should be changed and these features should be disabled by the local users, once the remote help is over. Proper noting in a register should also be made, so as to keep records of such accesses.

Data Backup –

- Regular manual backups shall be made of the data on the Notebook computers. Backup data should be preferably in encrypted form. Confidential data/ information should be in encrypted form only, with proper password management.
- Desktop/ Laptop/ Notebook/ Mobile Computing Device custodian is the owner of the machine and carries the responsibilities of data backup in the

file & printer server provided by the Bank.

- All the data on the Notebook shall be backed up and kept in a safe place before any travel.

Data Recovery –

- Recovery of the data shall be carried out as per the backup & recovery procedure.

- The original Backup should be kept back securely.

- In case of recovery of encrypted backup, the safe keeping of password of the backup should also be taken care of.

- Password should be changed, while taking new set of backup, after successful recovery and working, as per the password policy.

Control

- All Desktop/ Laptop/ Notebook/ Mobile Computing Device acquired for or on behalf of the Bank shall be deemed as Bank's property. Each employee issued with a Desktop/ Laptop/ Notebook/ Mobile Computing Device is responsible for the security of that computer and it's use, connections to permissible internet/ network connection, backup, data, OS, programs and related passwords regardless of the fact that whether the computer is used in the office, at the employee's place of residence, or in any other location such as a hotel, conference room, car or airport.

- Wherever possible, employees must avoid leaving their Desktop/ Laptop/ Notebook/ Mobile Computing Device unattended in an automobile/ train/ hotel/ office etc. The Desktop/ Laptop/ Notebook/ Mobile Computing Device should be taken care of while travelling, staying in hotel or visiting branches/ offices. The usage of computers is restricted to only authorised users for legitimate purpose.

- Desktop/ Laptop/ Notebook/ Mobile Computing Device being fragile/ sensitive and costly device, extra care should be taken that neither should it fall nor any other thing could fall on it, including any liquid/ water etc.

- It is the employee's responsibility to ensure that the anti virus and other software patches are loaded as and when required.
- The employee issued/ provided with Desktop/ Laptop/ Notebook/ Mobile Computing Device along with all the media of OS, drivers if any, for which the employee is responsible for safe custody.

While returning the Desktop/ Laptop/ Notebook, any personal data should not left on it and the same should have been properly backed up by the user on a suitable media. The contents of programs and data on the computer should be informed to the bank, at the time of return along with return its accessories/ device drivers/ OS/ programs CDs; if any.

CHAPTER-7

This chapter outlines the process and policies that need be followed with regard to the purchase, testing, installation, maintenance, storage and all the other aspects pertaining to software.

7 Software

A significant amount of Information Technology resources are normally used to develop, acquire and maintain application systems critical to the effective functioning of the key business processes. These systems in turn control critical information assets and should be considered as assets that need to be effectively managed and controlled. IT processes for managing and controlling these IT resources and other such activities, are part of a life cycle process with defined phases applicable to Business application development, deployment, maintenance etc.

7.1 Feasibility study

- Determine the strategic benefit of implementing the system either in productivity gain or for future cost avoidance;
- Identify the cost saving through the new system;
- Define the time frame upto which the solution is required;
- Determine if the existing system can correct the situation with slight or no modification;

- Determine if a ready product provides the exact solution to a requirement.

7.2 Requirement Analysis

- Identify and consult users to assess their requirements;
- Analyze requirements and determine priorities;
- Access control, regulatory requirement, Management Information needs and other interface requirement should be considered at this stage;
- Decision to acquire or develop the system should be decided at this stage.

If the decision is to buy a vendor supplied software package (ready product), then the user Division and IT Division must be actively involved in the package evaluation and selection process.

7.3 Acquisition

- Acquisition of major system and application software should be centralized at corporate office;
- The entire process of acquiring software should be structured one, starting from inviting RFP (request for proposal) till awarding the contract;
- The basic requirements for the RFP is as below:

Request for Proposal (RFP) contents

Item	Description
Product versus system requirements	The chosen vendor's product should cater to the defined requirements of the system. If the vendor's product meets all the defined requirements, the project team, especially the users, will have to decide whether to accept the shortcomings/deficiencies. Alternatively the vendor should customize the product to incorporate the necessary changes.
Customer references	Project management team should check for suitable references to validate the customer's claims about the product performance and about the competence of the vendor.

Vendor viability/financial stability	The vendor supplying or supporting the product should be reputed, profit making and preferably having an installed base and should be able to provide evidence of financial stability. New vendors pose a substantially higher risk to the bank on account of their inability to prove financial stability.
Availability of complete and reliable documentation	The bidder should be willing and able to provide a complete set of system documentation for review prior to

Item	Description
	finalization. The level of detail and precision found in the documentation is an indicator of the detail and precision of the design and programming.
Vendor support	The vendor should have a complete line of support services for the software package. This may include a 24/7 help line, onsite training during implementation, product upgrades, automatic new version notification and onsite maintenance if requested.
Source code availability	The source code should either be received from the vendor initially or there should be a provision for acquiring the source code in the event of the vendor going out of business. Usually these clauses are part of a software escrow agreement in which a third party holds the software in escrow. The acquirer should ensure that product updates and program fixes are included
Number of years of experience in offering the product	The more the number of years, the more the stability and familiarity with the product.
A list of recent or planned enhancements to the product, with dates	A short list suggests that the product is not being maintained currently.
Number of client sites using the product with a list of current users.	Larger the number implies wider the acceptance of the product in the market.

Acceptance testing of the product	This is crucial in determining whether the product really satisfies system requirements and specifications.

7.4 Installation/Implementation

Installation of new software must be properly planned to avoid unnecessary disruption and to ensure that the Information Security issues are adequately covered. The following guidelines should be followed for software Installation.

- Installation should be done either by the vendor or the user as per the agreement;
- If the installation is to be done by the vendor, then the user representative should be present along with the former and sign the successful installation report;
- The vendor should give a signed Non-Disclosure Agreement for all critical installations.
- The user manual/system manual, if any, have to be collected from the vendor;
- The supervisory password of the software, if any, has to be modified immediately after installation and kept by authorized person;
- The media of the software has to be kept in the media library as per policy and numbered;
- For system software it should be ensured that parameters are initialized properly;
- For subsequent installation of the same software at the user site i.e. either at branch /controlling offices or Central office, the request for loading software should come from the authorized user. The IT Division should arrange to load the software subject to other conditions like licensing issues etc.;
- The license of the software should be obtained from the vendor and preserved under proper custody.

7.5 Maintenance

Periodic maintenance of software is very much necessary as a preventive control for the IT systems. There should be a structured maintenance plan to ensure minimum downtime.

Pithoragarh Zila Sahkari Bank Ltd. Pithoragarh

The policy for maintenance of software is as follows:

- The vendor representative should carry identity card to establish his/her credentials.
- All software both application and system should be maintained properly for smooth functioning;

- A logbook should be maintained for entering the details of call logged with the vendor and the response time. This log should also mention the type of problem in the software so that this can be reviewed later on;
- For application software procured from outside, a on-site support maintenance agreement (contract) should be entered with the vendor for giving continuous support;
- For in-house developed application, sufficient expertise has to be developed, to support the application in-house. Efforts should be made to ensure that the application is not dependent on specific person;
- The site support maintenance contract with the vendor should inter-alia contain,
  - A non-disclosure agreement for not disclosing the data which he would have access to while maintaining the application;
  - Entry restrictions as per access control security;
  - Entry restrictions to sensitive places like data center. In case of necessity, the vendor should be accompanied by one official of the Bank.
- For easy maneuverability the software standardization should be centralized at Central office level
- In case the vendor wants to log-in to the system for maintenance, proper log-in authentication procedure with request and response should be followed;
- In case of application software both in-house and outsourced, if the maintenance involves change in the source code, then sufficient care should be taken that the changes are carried out in a test environment with sanitized data and then ported to production environment. The production executable and source code should match and also should represent the current version of the software.

7.6 Upgrades and patches

The applicability of upgrades and patches to operating systems or system software should be considered before venturing to apply them. Applicability should take into account the marketing gimmicks of the vendors to promote sales, their support system for legacy applications/software or bring some commonality in version.

Although this may sound reasonable it is important to consider the implications before making decisions. There can be more than a single aspect to consider:

- A hardware migration / upgrade;
- An operating system migration / upgrade;
- A new version of the applications software to review, test and implement;
- A possible migration of data files to the new hardware and any interfaces, which need to integrate with other systems.

These 'improvements' and 'bug-fixes' of the operating system/software should be applied to the production environment only after following the specified procedures. If applied incorrectly or directly on the production environment, the system and associated information is susceptible to the risk of information corruption or loss.

Procedures for applying upgrades/patches:

- 'Patches' to resolve software 'bugs' may only be applied, with the following precautions.
    - Verify that the patches are necessary and come from an authorized source, normally the software developers;
    - Patched versions of software should always be tested prior to release for live use. The testing and implementation of patches should not compromise software library updating procedures;
    - Apply patches only with proper authorization and system documentation.
- In case of application software operating in various branches/offices, the loading of patches need to be synchronized. The Central office - IT division should obtain the patch, test it and then vendor should install the patches/upgrades, duly tested centrally & centralized global parameters done, with due authorization of HO, DIT, ;
- In the case of application software care should be taken to keep the current source code in the production library and also in the escrow account. In fact

the first update of the source code should be done in the escrow account.

7.7 Recording and Reporting System

A software fault prevents proper and reliable use of an application or feature although reputed software and correct procedures have been used. A software incident becomes a 'fault' when the investigator has disproved other factors, such as a user error. An 'incident' is an unexpected event or result which in itself may be minor but could be symptomatic of a larger problem signaling an actual or potential security breach. All incidents must be taken seriously. Errors are compounded due to delays in fault or reporting of incidents. Insufficient data may lead to incorrect diagnosis of the fault or could camouflage a potential security breach. Where there are no procedures to monitor reported faults or to undertake trend analysis, the underlying sources of the problem may go undetected.

Therefore it is necessary to record and report such incidents/events. The policy for recording and reporting are as follows:

- Maximum errors to software could be attributed to the users. The responsibility of the CISO (Chief Information Security Officer) is to log, investigate and report security breaches and violations;
- The IS Division should submit a report to the Information Technology Division summarizing all logged security breaches and violations say monthly;
- The IS officials also should submit a report through the General Manager Information Technology Division to the Audit Committee twice a year categorizing the security breaches and violations that have occurred and the action taken in response to the breaches and violations.

7.8 Development

Design and Development Inputs: - The requirements to be met by the product must be defined and recorded, which include:

- Performance requirements from user or markets
- Applicable regulatory and legal requirements
- Requirements derived from previous similar designs and
- Any other requirement essential for design and development

These inputs should be reviewed for adequacy in order to resolve incomplete, ambiguous or conflicting requirements.

Design and Development Outputs:- The output of the design and development process are recorded in order to enable verification against input requirements

It should be verified whether the design and development output:

- Meet the design and development input requirements
- Contain or make reference to design and development acceptance criteria
- Provides input if necessary for purchasing, developing and service provision
- Define the characteristics of the product that are essential for proper use

Design and development output documents must be reviewed and approved before release.

Design and development Review:

At suitable stages of the design and development process, systematic reviews of the process should be planned and conducted to –

- Evaluate the capability to fulfill requirements for quality
- Identity problems, if any, and propose development of solutions

Participants in the design review process should include representatives of functions concerned with the design stage being reviewed. The results of the design reviews and subsequent follow-up actions must be recorded.

Design and Development Verifications:

Design and development verification should be planned and performed to ensure that the output meets the input requirements. The results of the verification and subsequent follow-up actions should be recorded.

Design and Development Validation:

Design and development validation should be performed to confirm that the resultant product is capable of meeting the particular requirements of the specific intended user. Wherever applicable, validation should be defined, planned and completed prior to the delivery of the product. Where it is impossible to undertake full validation prior to delivery, partial validation of the design or development outputs should be undertaken to the maximum extent practical. The results of the validation and subsequent follow-up actions must be recorded.

7.9 Software Code

Software code needs to be carefully controlled at all times. This includes the management of program libraries and also controlling program listings and old versions.

7.10 Program Libraries

Only designated staff should access operational program libraries. Amendments may only be made using a combination of technical access controls and robust procedures operated under dual control. Unauthorized use of software can cause disruption to the systems or fraud against the Bank. If these program libraries are not protected properly, there is chance of modification of the software and configuration files without any authorization, resulting in disruption to the system and /or other incidents.

Updating of the operational libraries should be done by the designated staff, independent of those developing software and those using the system for production. Updates should only be undertaken on receipt of a formally authorized request. Enforce standards / technical safeguards, including those within the operating system. Procedures should provide an audit trail to permit scrutiny.

Access to software should be permitted based on genuine need only and proper documentation should be done. Access should also be restricted using technical safeguards including those within the operating system, to inhibit unauthorized entry to the operational library.

7.11 Program Source Libraries

Only designated staff should access program source libraries. The codes of source and object should be preserved in a secured place and in a separate site. Absence of source code will make it difficult or impossible to maintain the systems. Unauthorized amendment of source code will also result in system failures and / or malicious damage.

The policy for managing source libraries is as follows:

- Ensure that for critical systems, the source code is available;
- Live source libraries should be updated by designated staff only;
- Ensure that such updates follow strict procedures, dual control being the minimum safeguard;

- Use technical safeguards to prevent unauthorized entry to the live source library;
- Implement procedures for updating the source library, which provide an audit trail;

- Make Backup copies of the Program Source Libraries and preserve copies off-site. Retain the last two or three historic versions of each source file to allow return to the old software version, if necessary;

- Employ checksums so that unauthorized amendments can readily be detected.

7.12 Controlling SW codes

Formal change management control procedures must be utilized for all changes to systems. All changes to programs must be properly authorized and tested before moving to the live environment. Insufficient testing of new software can often result in errors, which disrupt operational systems. Where software-coding standards have not been agreed upon, on-going maintenance can become onerous because of the inconsistent structure of the code.

The policy of controlling SW code during development is as follows:

- Set the Bank’s standards for programmers;
- Always document the code to explain the logic of the main routines;
- All codes should undergo Peer Reviews to maintain quality and standards;
- Withdraw codes that has been reviewed to prevent any further modifications;
- Benchmark testing of code must meet agreed standards. Before going 'live', software must be tested according to agreed standards;
- Errors in codes should be formally recorded and acted upon;
- During testing, source codes must be controlled and should remain unavailable to programmers.

7.13 Program listing

Control the printouts or reports, electronic or hard copy of the application source code, which makes up the programs run on our system. Loss or unavailability of a listing can result in delays in identifying the source of a system problem, the result of which could be severe. Loss or 'disappearance' of disks, tapes, etc. can

compromise the confidentiality of Bank's data. Damage to media compromises the integrity of the Bank’s corporate records. A list of programs available can be used by anyone with an intention to defraud, as it gives them the precise logic and routines for the system in question.

The policy for controlling program listing is as follows:

- Designate key individuals to monitor storage and use of removable media;

- Safeguard assets against petty theft by locking, maintaining a register etc;

- Take special measures to protect potentially valuable pre-printed forms and account for their usage and ensure that confidential information cannot be deciphered from discarded things;

- Follow the manufacturers' recommendations while handling the media;

- Take protective measures against environmental extremes like temperature, humidity, dust etc. In the case of irreplaceable data, the Bank should consider taking security copies each of which must be properly safeguarded. Ensure that all media are stored safely and securely;

- Make sure that all media are labeled clearly whether physically and/or electronically and that they can be located easily when needed. Preserve registers/printouts/floppies/CD's under lock and key;

- Old printouts should not be stacked without proper numbering as it is difficult to trace later;

- Old records should not be destroyed without proper verification before the prescribed periodicity.

7.14 Controlling Program Source Libraries

Controlling program source libraries means monitoring and investigating changes made to the program source libraries. Any unauthorized changes made to the program source libraries will lead to an error or fraud.

The following norms for controlling source libraries should be followed:

- In order to minimize the threats to the program sources libraries, the source should be kept in secure place under dual custody;

- Designate key individuals to monitor the storage and use of Program source libraries;

- Take protective measures against environmental and manual threats to the place of storage.

7.15 Old Program Versions

The application of a program code, which has been modified/ discontinued within the Bank’s system, should be controlled. If a program library has been removed or updated, the Bank may not be able to access or revert to the older version of the application in case of need. This could cause severe problems when major bugs in the newer version are reported. The old versions of programs should not be confused with the latest version, to avoid either the loss of recent enhancements or failure of other systems.

The old versions of programs should be controlled as follows:

- Do not delete/remove old versioned programs. Keep it in a secure place;
- Before deploying upgraded software on the production environment, always test it in a lab setup;
- It is necessary to keep the old/previous software versions.

7.16 Emergency amendment to Software

Emergency amendments to software are to be discouraged except in circumstances previously designated by management as 'critical'. Any such amendment should strictly follow agreed change control procedures. Emergency amendments to Software should not lead to non-adherence to agreed procedures and pave way for errors or malicious activities.

The policy for making emergency amendments to software is as follows:

- Consider the specific circumstances under which an emergency amendment had to be initiated;
- Identify the trigger(s), which will initiate the procedures. The Information Security of the Bank’s live source and object libraries should never be compromised e.g. by revealing an Administrator's password to development staff;
- Generate an audit trail and have it formally checked by competent authority as soon as possible;
- Regularize the situation at the earliest opportunity. The enhanced software or configuration file must either be added to the live libraries through the

normal procedures. Perform all deletions required under controlled conditions.

7.17 Establishing ownership for system enhancement

It is to be ensured that users recognize and accept their responsibilities for enhancements, which should always be driven by the needs of the business rather than being an IT initiative. System enhancements effected without proper study/planning could be improperly defined, poorly analyzed or inadequately tested and would prove counter productive vis-à-vis the business operations.

7.18 Approval of request

The User Department shall approve the ‘Change requirement’ form taking into account the validity of the requirement in terms of module functionality as well as MIS requirement. Based on CR form the IT department along with the respective functional department head shall conduct a feasibility analysis. Subject to the outcome of the feasibility study, the request shall be forwarded to the development team, which could be an in-house team or an outsourced party appointed for software maintenance. The roles and responsibilities of the outsourced third party or the vendor as a part of the development activity should be charted out in the agreement entered into with the third party / vendor.

A standard naming convention for each application's change requests should be adopted by the respective application teams. This naming convention should clearly bring out the respective application's name, module name and should have a distinct numbering scheme.

The development team and functional heads shall analyze the change request in terms of the following:

- Criticality and need for program change
- Exploring new ways of getting the same functionality in existing set up
- Building workarounds
- Effect on other modules / menu options / business process – Impact Analysis
- Any possible effect on existing control procedures

7.19 Intellectual property rights

For software that has been indigenously developed in-house, appropriate applications have to be submitted to the authorities concerned for getting the software patented and copyrighted. Such software, if used outside the bank, should be charged.

7.20 Outsourcing Policy

Banking Sector is a diverse sector where several parties from different sectors are involved. Because of criticality of its operations, Bank has to go for service level agreement with different parties / vendors. An SLA is a formally negotiated agreement between Allahabad Bank and any service provider(s). It should records the common understanding about services, priorities, responsibilities, guarantee, and such—collectively, the level of service. The SLA signed on behalf of the Bank should also include the entire agreement that specifies what service is to be provided, how it is supported, times, locations, costs, performance, and responsibilities of the parties involved.

Service Level Specifications / Objectives are specific measurable characteristics of the SLA such as availability, throughput, frequency, response time, or quality.

Service Level Objectives must be –

1) Attainable
2) Measurable
3) Understandable
4) Meaningful
5) Controllable
6) Affordable
7) Mutually acceptable

Service Level Objectives should generally be specified in terms of an achievement value or service level, a target measurement, a measurement period, and where and how measured.

7.21 Software License

Acquisition of software and associated licenses should preferably be planned on an annual basis to ensure that it is carried out in a controlled manner. The procurement of licenses shall be based on evaluation of current usage and formally established need for additional licenses across the organization.

Conflicts between law and policy

Where a conflict arises between national and/or local laws and the bank's policy, the law should be complied with and the GM-IT must be notified of this situation.

Compliance with Law

The respective department head should ensure full compliance with the laws and regulations relating to their information and the IT applications that process that information. The laws and regulations may include, among others:

- Prohibition of the use of illegally acquired software
- Prohibition of the use of illegally acquired data

ROnal Offices

The ROnal offices across bank will ensure that only licensed copy of software are running into the branches / offices. If any branch / office is found to be running illegal and unlicensed software then that should be uninstalled in consultation with branch / office head.

Control of Software Licenses

Software Licenses within the BANK shall be controlled and maintained to ensure protection against default or contractual and/or other limitations and liabilities.

Software License terms and conditions

Software License terms and conditions, including those applying to limited use, shall be observed at all times.

Authorisation required copying licensed products:

Products licensed to run on a specific server shall not be copied onto another server or another site without written authorisation from the vendor.

CHAPTER-8

***This chapter outlines the policy for general network sizing including the policy for cabling and housekeeping*.**

8 Networks

8.1 LAN types

The size of the LAN of the Bank branches can be categorised into 3 types.

- **Small Office**: This would ideally include all the branches that have a total number of systems that are less than 25. Such a bank branch would be served by a pair of switches/hubs.

  Note: This does not include a branch that has its LAN spread across different floors of a building.

- **Medium Office**:-Depending upon the size of the LAN, say for a branch having more than 50 systems; will require a pair of switches/hubs to provide connectivity to these systems.

- **Large Office**:-This would ideally include all branches that have a total number of systems that are greater than 50. Typically such a bank branch/office would have its LAN spread across the different floors with a floor switch in each floor and a Layer 3 switch as the backbone switch.

8.2 Cabling policy

- Structured Cabling is a must for large offices.
- The IOs should be numbered properly.
- The IOs should be properly fixed to a firm surface (preferably the wall) and should not be left dangling under any circumstances.
- In the case of a small branch office, each numbered IO should terminate on the similar numbered port of the hub/switch.
- In branches where there are floor switches the numbered IOs on each floor should terminate on the similar numbered ports of the corresponding floor switch.
- The uplink port of these switches should be taken from an IO preferably named rather than numbered.

- Test every part of a network as we install it. Even if it is brand new, it may have problems that will be difficult to isolate later.
- Stay at least 3 feet away from sources of electrical interference.
- If it is necessary to run cable across the floor, cover the cable with cable protectors.
- Label both ends of each cable.
- Use cable ties (not tape) to keep cables in the same location together.
- Data cables should not cross-electrical cables in order to avoid interference and disturbance.
- Cables should be ensured proper grounding and must not be left dangling.
- It should be ensured that rats and other rodents do not tamper with the cables.
- There should be a proper route map of the cables laid so that detection of faults is easy.
- The type of cables laid should also be properly identified in the route map.

8.3 Virtual LAN (VLAN) deployment

- VLAN deployment must be done within the LAN only.
- The criteria for VLAN deployment should be to prevent unnecessary communication between sensitive departments of the Bank and the other departments.

These sensitive Departments must be on a separate subnet of the LAN and the communication with these sensitive Departments is limited only to those

Departments who are authorised to communicate.

CHAPTER - 9

This chapter outlines the system level policies that need to be set up in case of a network operating system.

9 Network Operating System Policy

- The network operating system used by the Bank should be original and licensed;
- Sufficient number of client licenses should be available;
- The upgrades and patches to the network operating system are to be applied after due consideration and testing;
- The installation and maintenance of the network operating system should be done by the personnel authorized by the Bank;
- The software media (compact Disks/licensed floppies etc.) through which the network operating system is installed should be kept in the safe custody of the authorized personnel of the Bank.
- Physical security:
  - Lock down or disable floppy and CD-ROM drives.
  - Limit server access to only the authorised personnel by placing it in a secure location behind a locked door.
  - Keep backup media in a secure offsite location.
  - Keep manual log files for all system changes, like software and hardware upgrades.
  - Ensure that console log auditing is in place and operational on the server(s).
- Account security:
  - Passwords should be eight or more characters long and should include letters, numbers and special characters.
  - Enable intruder lockout on all user accounts and require the account to be unlocked by an administrator.

- Account time and network restrictions should be set and enforced.

- The console log files should be viewed and monitored on a regular basis.

- Configuration security:
  - Enable only the minimum necessary rights and privileges.
  - Remove or disable the "Guest" account immediately after installation.
  - Disable the services that are not required for the daily operation of the system.
  - The Remote Console option, if required should be configured appropriately and the default password should be changed. The password should also be encrypted.
- Domain security policy:
  - The operating system should allow for enforcement of security settings for the domain in which the network resides;
  - Domain controller (server) of the network should be configured to ensure the compliance of the operating system security policy settings;
  - The violations should be recorded in appropriate logs for further action.
- User Account:
  - Only the authorised users of the network should be given user accounts;
  - Each authorised user of the network should be allotted a unique user ID and initial password. The password should be changed by the user on first login;
  - The application accounts should be given only to those personnel who are required to use that application;
  - Any test accounts that may exist in the application should be removed;
  - The account lockout threshold should be set that would lock the account after the specified number of unsuccessful login attempts;
  - Account lockout duration should be set to avoid recurrence of unsuccessful attempts to login;
  - Repeated unsuccessful login attempts should result in the account being disabled or suspended;
  - User IDs should be disabled if there is found to be a prolonged or consecutive period of non-use;
  - Suspended or disabled User-IDs should not be reset without approved authorisation procedures;
  - In the case of networks where there is an option for the user to login from a remote location there should be more stringent methods of

authentication than user name and password;

- The system should generate an Exception Report for repeated unsuccessful user logins, which should be submitted to the authority concerned for appropriate actions.

- Audit:

  Audit policy is not global by default but for security purposes a global setting for the audit policy is suggested. The log files should be monitored to detect any abnormal events.

  - Audit all successful and failed logon events;
  - Audit all successful and failed user logon events;
  - Audit all successful and failed directory services events.

- Logging of events
  - In the network operating system, system logs for changes to Data and System, user access details should be provided;
  - These logs should include details of the users involved in the event, the date and time of occurrence and the details of the event;
  - These logs should be reviewed periodically and any unusual or suspicious event should be reported to the authority concerned for necessary action;
  - All security related events should be recorded in a secured audit log;
  - The secured audit log should bear the time-stamp for each event. These events should include:
    - Invalid User authentication attempts;
    - Logon and activity of privileged users;
    - Successful access to security system;
    - Access to resources beyond normal hours;
    - Changes to User security profiles;
    - Changes to access rights of resources;
    - Changes to system Security Configuration.
  - The system logs should be reviewed immediately when a user assumes a change of his role within the Bank and the access to data should be properly re-defined which should be indicative of the new role of the user concerned;
  - This change in the policy vis-à-vis new role of an employee should be done only when the procedure for such a change is formally approved by the authority concerned.

CHAPTER - 10

This chapter emphasises the necessity for appropriate change control procedures and also controls for emergency changes.

10 Change Management

To protect the integrity of the information processing systems, proper change control procedure is essential. The change control procedures should relate to hardware / software changes and those in manual procedures. The change control procedure should also address emergency changes. To prevent unauthorized changes in the production environment, a change control procedure that manages all changes regardless of the magnitude whether scheduled or emergency, should be established. The following steps should be implemented to ensure that the change control procedure, put in place, remains effective:

10.1 Schedule Change Controls

- Establish a formal change request and the authorization process thereof;
- Put in place a test and system acceptance procedure for each change;

- Allow emergency fixes only to resolve production problems;
- Verbal approvals shall be obtained by the Application Team from the respective Functional Head. This shall be immediately followed by an email confirming the same. A verbal approval for the same should be confirmed over the telephone to the IT department head.
- Functional User department representatives and the IT support personnel, in conduction with the subject matter experts (Vendors, Third parties) shall co-ordinate the process of the emergency program changes with adequate supervision.
- Once the emergency change request has been resolved, the IT department head shall ensure that all activities performed for the emergency program changes are documented for all software, existing network, hardware and application. This documentation would include the names of program files changed, reasons for change, effect on other functionality of the application, test conducted to verify accuracy of the changes, along with the user sign-off.
- Any sub-normal procedures followed during the emergency program change (e.g. giving super-user or root password to the support personnel performing trouble-shooting etc.) should be identified and restored to the original settings and configurations.
- Even in the situation of an emergency, the 'need-to-do' principle shall be followed, with appropriate restrictions on the support personnel executing program changes.
- The testing should be carried out in such a manner so as to ensure the accuracy and integrity of live data and systems.

- The documentation recommended in documenting the Changes above for normal program change procedures shall also be completed after implementing emergency program changes.
- Return to normal change procedures expeditiously and review all the emergency changes which are logged.

CHAPTER - 11

This chapter outlines the controls that need to be put in place during the process of backup. Also the types of backup, the control mechanism, retrieval mechanism are dealt with.

11 Backups

Backing up of data is most vital in any computerized environment especially in Banks. It saves the Bank from loss of data caused by accidental erasure of data, unexpected system failure, corruption of data etc. It acts as an insurance against loss of information and helps the Bank in recovering from a disaster.

11.1 Controls

- All computer systems and their associated data files should have documented backup and recovery (restore) procedures for their associated data files.
- The most recent backup tapes or disks must be stored in a secure environment, e.g. a fireproof cabinet with regular transfers to and from remote (off-site) storage.
- Backups of Operating System, Service Packs, Applications Software, Device Drivers, E-Mails, Configuration files etc should be taken, as and when there is a change or fresh installation takes place and the same should be preserved carefully.
- All data files and their associated software programs relating to core activities should be retained indefinitely and kept secure, duly labelled.
- Ensure that access to the 'old' data is available whenever required which can be achieved by archiving to optical disks/CDs.
- Periodicity of the backup should be decided depending upon the criticality of the data.

- Front office application data like that of Branch operations need to be backed

11.3 Archiving of data along with necessary related software

This is applicable to information which is not required on a day-to-day basis but which needs to be retained for a longer period and also information, which is retained in perpetuity and referred to infrequently but periodically. Such data is often removed from day-to-day processing area thereby reducing the overheads on storage and processing resources.

Weaknesses in the longevity of the media used for archives can result in a failure to restore the required data when eventually it is needed. Archived data can often be retained in a proprietary format, which is no longer supported by the present systems, thus hampering attempts at access. These are the concerns to be addressed while backing the data for archival purpose. The data along with related necessary software should be archived to avoid the above concern.
While migrating from one platform to another platform, required modalities need to be framed for retrieving the purged data/old data of previous platform for required period as per bank's policy/Banker's Book Evidence Act.

11.4 Offsite backups

To ensure the availability of and access to the Bank's data files following a disaster, copies of the files must be stored in a location separate from where the data files are normally preserved. This off-site storage is applicable to data files which are used on a regular basis in conducting business as well as those which must be retained to meet the requirements of the legislation and other regulations in force regarding retention of banking records.

Information Security and Corporate Security should review existing and potential off-site storage facilities to determine the protection, which should be provided to the data stored at such locations. This review should address environmental, physical and procedural security issues directly related to the facility and handling and the movement of media.

There should be a system for taking off-site storage of all back up media as well as entrusting the responsibility of regular preservation of off-site back up media by framing appropriate documented procedures.

11.5 Storage of backups

Finding a good way to store backups is almost as important as creating them. Backups, installation media and boot disks should be stored in a place where only authorized people have access to them. In order to make restorations simple, backups need to be well labelled. Labelling includes clearly marking the media itself as well as including a table of contents so that individual files on the tape can be located easily. In sites where several people share the responsibility of taking backups or a number of different commands are used to create backups, the label should also include the commands used to create the backup.

Most backup media are sensitive to heat, humidity, direct sunlight and dust. So it is imperative that they should be stored in a cool, dry space. Ideally, media should be stored in an environment with a temperature of 62-75 degrees Fahrenheit at 40% humidity. Keeping backups in the same room as the system may be convenient but not advocated. If the said room is struck with a disaster the backup media could also be destroyed.

11.6 Restoration testing.

- To verify the readability of backup media, mock restoration tests should be carried out, at least once in a month on the test/backup servers.
- The entire process is to be documented detailing the test plan, the activities carried out and the test results.
- Testing should never be tried in a 'live' area for it could result in loss of live data.
- It is to be ensured that the restored data is deleted from the test servers after successful completion of testing.

Use of off sites for restoration testing:

- DIT should issue guidelines for the backup restoration testing, including system privileges, and overall responsibility of the designated IT/ZITC

officers. The outsourced party and vendors should be contracted at the time of framing procedures for the restoration of data.

- The test plan is prepared in advance and essentially includes 'mock test' with the restored data. The backup media kept as 'Off-site backup' should be used for such restoration.
- Upon restoring the data on the test server, the results should be documented. Designated IT / ZITC officers at the end of the restoration exercise should verify these test results. The data restored is deleted from the test server after successful completion of the exercise.
- Any exceptions in the process mentioned above must be reported to the DIT.

Backup Solutions:

Backup and Recovery Solution should be selected based on the criticality of the application server and dependencies of business. Solutions to be considered are:

- Mirrored Back up

- Hot site (only for CBS)

11.7 Media Backup, Archival and its Retention

The Bank has the full responsibility over the data created in the course of day to day banking business. Data being very critical for Bank's operation to continue, Bank policy regarding data handling becomes highly sensitive. Data created during ongoing banking operation must be available for a reasonable amount of time to provide information either to customers, to bank or to ensure compliance with applicable regulations of government.

From time to time, Bank is asked to provide certain data by different government's department for some specific or specific group of customers. It is Bank's utmost responsibility to provide such data, based on Bank's policy.

The Bank should keep copies of the data in different media along with suitable application to extract the data. The respective departments/ data owners should develop suitable procedures for proper archival, retention and disposal/ purging of data after its expiry in consultation with DIT.

CHAPTER - 12

This chapter specifies the general policy with respect to passwords.

12 Password Policy

Appropriate controls should be ensured to control selection, usage, and recycling of passwords for the information assets in the bank. The password controls should be imposed by system to extend feasible. Application software in the bank will have to comply with minimum password standards as specified in this document.

12.1 Password Management

Confidentiality of Passwords:

User passwords should remain confidential and not shared, posted or otherwise divulged in any manner.

Password Composition:

Passwords should consist of at least eight characters which may contain alphabetic (case sensitive), numeric or special character and should not contain the user's name or user-ID. Preferably, a combination of alphanumeric (with case sensitive) and one or two special characters should be encouraged to be used. Password selection should be such that it is easy to memorize but difficult to guess or crack. Also, password to be selected should be practiced to type quickly without having to look at the keyboard to make it harder for someone to know password by someone standing in close proximity

Password Expiration:

- Passwords should expire after a maximum period of 30 calendar days. Additionally, the same password should not be repeated within a cycle of 3 password changes. After a predetermined number of failed attempts the system should not allow the user any access and a lockout must be activated.

One Time Use of Initial Passwords:

If a user is provided with an initial password by the administrator, this password should be changed immediately by the user the first time he/she logs into the system (One-time password).

User Capability to Select Passwords:

Users should be provided with the capability to change their password on the login interface (after authentication).

Password Reset:

User password resets will be performed when requested by the user, after verification of identity. The 'Password reset request' form should be filled up by the user. The new password should be a one-time password. On the individual to whom the user-ID is assigned should request for user password reset. The Head of the respective Department head/branch manager should be informed whenever a password is reset for a critical application of IT department.

Backup Passwords:

The respective branch along with IT department should identify the critical user-IDs and their passwords. These should be kept in the sealed envelope under dual custody. These sealed envelopes should be opened only when regular users are absent. The opening of envelope should be done only with the written permission of Branch Manager/Department Head and the password should be changed immediately and replaced with the new sealed envelope. Details of such activity should be entered in a separate register.

Protection of Transmitted Passwords:

Details in relation to user ID, department, password etc. should not be sent using clear text across mail systems. The same should take place only when duly approved, necessitated and documented.

The user-ID password should be authenticated as a whole. Authentication failure should provide an error message to the user that does not indicate whether the user ID is correct (e.g. "incorrect login" and not "incorrect password").

Type of Passwords:

Every user should use different layers of passwords to properly protect the Information Asset in form of Hardware, Operating System, Application, Folder, Data, Backup, E-Mail attachments etc. The following types of passwords are possible and a proper combination provides composite and stronger security through logical controls –

Super User Passwords:

All the super user passwords should be sealed in an envelope and kept under dual control in a fire proof safe. This is necessary in case the password is forgotten or the related person has left the organization without surrendering the user id and password. These sealed envelopes should be opened with the written permission of Branch Manager/Head of the Department and the password should be changed immediately and kept in a new sealed envelope. Details of such activity should be entered in the Sealed Envelope Maintenance Log Book.

Power-on Password:

Users should be encouraged to use the power-on passwords (for critical workstations and mobile computing devices).

BIOS (Basic Input Output System) Password:

Users should save the BIOS settings and access to BIOS through proper passwords, as this is very effective to have any access to Hardware itself which should be sealed in an envelope under the custody of the Branch Manager/Department Head.

OS level Password:

The user should use this password to prevent the system being accessed by unauthorized users. Many users, of different levels can be created to access the same computer, as per the need/ authority.

Application Level Password:

The user should use proper password to prevent access to application software. User should also remember to log off the application, in case he/

she is leaving the machine or application is no longer required to be running by the same user.

Screen Saver Password:

Every user should activate screen saver with password, which should be set to preferably to 5 minutes of inactivity.

File and Folder level Password:

The users should use Folder level and File level passwords (Specially in case of NTFS File System, where this feature is integrated in the System), if these are containing confidential/ sensitive information or they are shared across network/ with other users on the same computer. In case of Office documents/ Spreadsheets, the file level protection is available across all Windows OS of any type of File System (FS). It is also very important in case the files are being sent through e-mails, in which case the password should be communicated to the receiver through alternative mode and the receiver should also be advised to take proper care of the password.

Backup Level Password:

The users should use backup level encryption using proper password, if these backup files are containing confidential/ sensitive information. This backup can be on the same Hard Disk or any other Storage Device. However, proper availability of the password to legitimate user of the backup should be ensured, as with the same password the backup would not be re-storable. It is very important in case of Laptops/ Notepads/ USB Drives or any other secondary media.

Note:

All the above passwords, which can not be reset by the administrator should be kept sealed in an envelope under the custody of the Branch Manager/ Department Head. Whenever a password is opened, which was kept under a sealed envelope or the user has changed the password, it should be once again kept in a sealed envelope in the above manner. The event should be recorded in the Sealed Envelope Maintenance Log Book. Sharing of power-on passwords should not be allowed. If unavoidable, they should be maintained solely within the members of the group sharing the workstations and laptops and should be subject to the same controls as personal passwords.

Responsibility:

The System Administrators responsible for a given unit is responsible for maintaining password security controls of all data, applications and operating system on the server.

It is the responsibility of IT users at each unit to rigorously follow the password security policy. The IT users should formally intimate the System Administrator about any lapse on the password security either orally or by e-mail.

Techniques for devising effective passwords, their advantages, important Do's and Don'ts are to be known by every user in the Bank so as to reduce IS risks. From time to time, the Bank should inform its internal as well as external users through circular / guidelines on the selection, maintenance, expiry, etc. of the passwords, if there is any dynamic change in the operation of password.

12.2 Guidelines for best practices

- Critical applications like access to database in branch automation, ATM PIN generation and other applications should have a password divided into two parts with one being with the vendor and the other with the bank.
- Password must never be written down;
- Password of key role holders-such as System and Network Administrators should be preserved and held under dual control in a sealed envelope in a fire proof/resistant cabinet in a secure location so as to enable access to an authorized person in the event of an unavoidable circumstance arising out of the absence of the password holder;
- Passwords must be changed at regular intervals, and should be chosen privately by the individual users;
- Password changes must be forced in the Bank by putting in place a specific expiry period after which a user's password should not be accepted;
- After a predetermined number of failed attempts the system should not allow the user any access and a lockout must be activated.

CHAPTER - 13

This chapter outlines the controls that need to be put in place to ensure a virus-free IS environment.

13 Virus Control Policy

The bank shall develop, implement systems and procedures for protection of IT resources from all possible virus software by providing the required technical support for timely distribution of anti-virus as well as ensure prompt escalation of virus incident, reporting and management of computer virus.

13.1 Definitions :

COMPUTER VIRUS- A computer virus is an unauthorised and malicious program, which replicates itself and spreads onto various data storage media such as floppy diskette, magnetic disk, tapes and across the network. The viruses are designed to spread from one file to another, from one program to another, from one machine to another, and even from one network to another. Viruses threaten the integrity and availability of data. The symptoms of virus infection include considerably slower response time from the system, inexplicable loss of data, erroneous change in file dates, increase or decrease in file size or total failure of computer system.

VIRUS SIGNATURE- The unique pattern of virus activity is known as virus signature.

DAT FILES- These are the files, which contain the data on virus signature.

13.2 Updates of Virus 'DAT files' :

These are the files, which contain the data on virus signatures. Virus Helpdesks should update these 'DAT files'. The Helpdesk should download the data from the Internet website of vendor at given intervals. The Helpdesk should also copy these DAT files on all servers.

13.3 Updating of 'DAT files' on client computers/networked nodes:

Once the updates of virus DAT files are copied on the central host computes (servers), an operating system job should be scheduled in the network server for pushing these DAT file updates onto client computers/network nodes

connected. This job should be scheduled every week immediately after copying the DAT files on the central host computers.

13.4 Anti-Virus software upgrades :

The upgrades are the newer versions of the anti-virus software. The same should be procured and provided the newer versions/engines of Anti-virus programs in regular and timely manner and ensure a quick roll-out to all the units of CBS environment. As for non-CBS environment, products are to be finalized at DIT and ROnal Office can procure Anti-virus software and maintain the same at their end.

13.5 Virus Protection - some specific procedures :

- It should be ensured that the Anti-virus (AV) software is installed and active on every machine. Proper password protection should be there so that the Anti-virus check is not disabled by the users.

- The Anti-virus software should be run at least once in a day by each user and it should be properly scheduled, preferably during the lunch hours/non-peak hours of the office.

- Every diskette, DAT and DLT tape should be scanned for virus before use.

- Systems should be implemented to review the anti-virus software activity/logs, especially to check whether the IT users are running the AV system regularly on their desktop computers. In case the user has the AV software and does not run it for stipulated number of times, his user id should be recorded and his network account should be disabled. This should immediately be informed to Dept. Head.

- Upon encountering the virus problem, the AV software should stop the computer operations, clean the related files and the affected areas and extreme cases delete the files. The other options such as 'continue' and 'move to a directory' in AV check should not be enabled.

- Messaging and Anti-virus: The AV software for messaging system (e-mail) should be implemented. If the virus is found in mail attachment file, this file should be deleted and the sender should be informed. The recipient would get the remaining message.

- Checking the software downloaded from Internet: Software/data downloaded from outside sources such as Internet may contain a virus.

Before such software is decompressed, the users should always have virus scan active on such workstation. In order to provide more security, he should log out of all files servers and terminate all other network connections. Before executing the software, it should be screened with the approved Anti-virus package. If a virus detected, the Dept. Head and Systems Administrator should be notified immediately and no further work should be carried on the affected machine until the virus has been shown to be eradicated.

Issue an alert to all users if a particularly virulent or fast-spreading virus is discovered and take the preventive measures recommended by the vendor at critical entry points, such as the e-mail server and firewall/ UTM or proxy server, as well as the other systems that are part of the network; the user should alert the management whenever any virus is discovered on the desktop;

13.6 Virus Reporting :

Upon encountering the virus attack, the users should immediately stop using the involved computer and report it to Systems Administrator in-charge of the unit and IT personnel. For CBS branches, encountering of virus is to be reported to Help Desk at Mumbai which in turn will notify to concerned IT personnel. For non-CBS branches and other offices except HO, the same has to be reported to ZITC. The encountering of any virus attack at Head Office is invariably to be reported to DIT, head office. As the viruses have become very complex, users should not attempt to eradicate them without expert advice.

The System Administrator and IT personnel would ensure that infections which are centrally reported have been eradicated. The virus logs utility in AV check software should always be enabled and the logs should be reviewed by Systems Administrator and periodically by the IT security team. On encountering the virus, the detailed virus log should be printed and submitted to concerned department. The log should also capture the virus signature so that the IT personnel can subsequently update its software to detect new viruses as well as mutated versions of old viruses.

13.7 Preventive controls and precautions

Detection and prevention controls to protect against malicious software and appropriate user awareness procedures should be implemented. Protection against malicious software should be based on security awareness, appropriate system access and change management controls.

To protect the integrity of information and the information systems from modifications, disclosures or destruction by malicious software, the following steps should be taken:

- All systems connected to the network should have virus protection;
- Have a clean boot-up or start-up diskette / CD;
- Keep good backups of critical data and programs;
- Perform regular backups;
- Check data and software integrity by using techniques such as checksums on files or comparison of current files against backup files;
- Install fixes to known system problems as expeditiously as possible;
- Periodically review overall controls to determine weaknesses;
- Use access control facilities to limit access to information by users, consistent with their job duties and management policies;
- Use only licensed software;
- Establish procedures for checking the diskettes, pen drive, compact disk and

other such media. Any files on electronic media of uncertain or unauthorized origin or files received over non-trusted networks should be checked for viruses before use;

- Train users to scan all removable storage media, including new diskettes, pen drive, compact disk and downloaded files before using them for the first time;
- A list of approved software should be maintained and updated for virus protection;
- A Bank-wide educational and technical approach should be made to raise user awareness of virus hazards in the computing environment and to detect and purge viruses;
- Users should employ adequate anti-virus software that is updated regularly via central security control;
- Scan all content and applications for viruses before distributing them;
- Prohibit users from installing their own software on systems supporting critical information assets;
- Technical support staff should monitor anti-virus software vendor's site and public sites for information on new viruses and destructive programs;
- Issue an alert to all users if a particularly virulent or fast-spreading virus is discovered and take the preventive measures recommended by the vendor at critical entry points, such as the e-mail server and firewall or proxy server, as well as the other systems that are part of the network;
- Develop and use consistent routines for backing up data on critical systems, using a reliable backup technology and clean, functioning media that is devoid of virus content;

- Keep the virus protection software up-to-date, using the updates and patches supplied by the vendor
- The users should alert the management whenever any virus is discovered on the desktop;
- Establish a virus detection and protection procedure, to be continuously reviewed and revised, conforming to the emerging requirements and to implement the same across the Bank;
- All software acquired by the Bank should be checked by the virus detection procedure prior to installation and use;
- Conduct regular reviews of the software and data content of systems supporting critical business processes. The presence of any unapproved files or unauthorized amendments should be formally investigated;
- Establish procedures to verify all information relating to malicious software and ensure that warning bulletins are accurate and informative.
- The personnel in-charge of Information Systems Security should ensure that

qualified sources, e.g. reputed journals, reliable Internet sites or anti-virus software suppliers are used to differentiate between hoaxes and real viruses;

- The users of the information systems should be made aware of the problem of hoaxes and the action to be taken on receipt thereof.
- Purchaser should ensure that newly supplied Desktops/ PCs/ Servers are supplied free from viruses, worms, malware, Trojan, etc. A suitable clause about responsibility and appropriate labiality of the vendor should be part of the Purchase Order/ Agreement. It should also be ensured that any system that is made part of CBS network is free from viruses, worms, malware, trojan, etc. after conducting thorough scanning.

13.8 Updates and patches

The applicability of updates and patches to operating systems or system software should be considered before venturing to apply them. The hoaxes have to be differentiated from the real threats. The following points have to be taken into consideration while installing updates/patches:

- The source of the virus warning has to be verified for authenticity;
- If the system is vulnerable to the virus, only then should patching be considered;

- The source of the update/patch should be authentic;
- The updates/patches should be applied in a test environment and tested for the normal functioning of the system before being applied to the production environment;
- Apart from this, the regular updates released by the anti-virus vendor should be applied to the systems after due testing.

CHAPTER– 14

This chapter specifies the acceptable use policy for Internet usage while also specifying the controls and the operating mechanism.

14 Internet Usage Policy

14.1 Acceptable uses

- Employees given Internet access are expected to use the Internet to enhance the performance of their job responsibilities. The data and information available on the Internet provides invaluable information, which can impart the necessary skill to enhance professional competence.
- Employees given Internet access are also responsible for assisting the Bank in identifying positive organizational uses from the Internet. Beneficial uses include availability of immense work-related information / updates of licensed products, facilities of special online services / features etc.

14.2 Access Limits

- When account IDs and passwords for the Bank's Internet services are entrusted to an employee, the employee should assume the responsibility of safeguarding them from unauthorized usage;
- Account IDs and passwords must be memorized or stored in a secure location;
- When using Bank's Internet accounts, employees should remember that they are acting as agents of the Bank. Online conduct must reflect the ethics, professionalism, courtesy, and responsibility expected of the Bank employees.
- In case of internet access is provided to/ accessed by many users in a branch/ office/ department in a PC, then all such users should have internet PC login (Operating System Level) with their individual user id and password (Not with Administrative Rights) so that not only user's privacy is better enabled, but also the PC is prevented from certain type of internet threats. The users should not pass on their log-in session to other user and therefore, should invariably log-off system after the use. The administrator log-in should not be used for internet usage and it should be used only for maintenance purpose. A manual record of internet usage should also be created about timing of usage and actual user of the internet, with his/ her initials, to ascertain the actual use of the system/ facilities. The IT Asset owner of

Internet PC and facility in the respective branch/ office / department should be responsible for the above arrange to be in place. The earmarked PC for internet should be under control of proper authority to avoid unauthorized access and any unauthorized use of internet connection or internet connection device to other PC/ network should not take place. These precautions are also to be strictly ensured by other users of internet facility on stand- alone/ shared internet systems.

14.3 Handling of Information / Files

- The data sent through the Internet should be considered "public" and therefore could be “readable by anyone”. Special consideration should therefore be taken before transmitting sensitive information, including E-mail, web browser forms, etc. Encryption techniques should be utilized to reduce the risk while transmitting sensitive data;

- Data and files on the Internet should be treated as copyrighted material and therefore should not be distributed, copied or published in any form without the written permission from the originator. The liability for any copyright violation or infringement rests solely on the user/employee. The Bank would in no way be responsible for such violations;
- Supervisory permission must be obtained before downloading and installing executable files (programs) on a system. Files downloaded from the Internet should be subjected to thorough scanning by approved virus protection software before use / installation. The authority granting such permissions should verify the need for download and should also ensure that the downloaded file contains no malicious / virus programs;
- The online distribution of business related data and files through Internet should be pre-approved by an appropriate authority as per the procedures framed by the Bank with respect to such distribution and transmission of information.

14.4 Unacceptable uses

- To use the Internet for purposes that may disrupt other network uses, services or equipment. Such disruption/improper use include, but are not limited to:
    - Operating a personal business through the corporate Internet link;
    - Distributing of unsolicited advertising, junk mail or chain letters;
    - Sending or receiving sexually oriented messages or images;
    - Visiting derogatory or racially intolerant web sites;
    - Visiting sites for personal entertainment;
    - Soliciting money or advocating a religious or political cause;

-
    - Use of abusive, vulgar, or objectionable language;
    - Transmitting of any type or quantity of data that may cause disruption of services to others;
    - Propagating computer worms, viruses or other potentially malicious code;
    - Unauthorized entry to other computer or network resources.

- The Bank's networking services resources or facilities should not be used for any purposes that violate the existing laws, regulations, policies or procedures. Illegal usage will be solely attributed to the employee concerned and will warrant disciplinary actions;

- Activities that compromise network security are strictly forbidden, including the disclosure of system IDs, passwords, information etc. to allow circumventing of security controls.

- Transmitting any bank-sensitive information over the Internet, to any other party, including other employees of the bank, without the proper non-disclosure agreements in effect.

14.5 Control

- The Bank should monitor and audit Internet access for the purposes of assuring system security, proper usage, and for impact on performance. The employee has no rights of privacy in their use of the Internet;
- Failure to follow the Internet Usage Policy should lead to appropriate actions which may include reprimand, loss of Internet access, suspension, termination, or legal prosecution as the case may be.

14.6 Access Control List (ACL)

ACL filters (via router or multi-homed firewall/ UTM) should be used to deny access to all services except those needed for business.

ACL should be comprehensive and adequately documented describing how each entry in the ACL controls access to and from the internet network.

ACL's should restrict all User Datagram Protocol (UDP) based services, except those deemed essential to the operation of the firewall system/ UTM e.g., Domain Name Server (DNS). Any services that require UDP should be evaluated and approved by Network/Incharge group, DIT head before implementation.

File Transfer Protocol (FTP) services and Internet:

Both Inbound/Outbound FTP services with Internet must not be allowed, unless approved by Departmental head and Network/Incharge group, DIT. When approved, the following guidelines should apply to FTP services:

- The system administrator for the Internet servers must ensure that anonymous file transfer (Anon FTP) systems are disabled.
- All FTP sessions must be authenticated, encrypted and should be logged.
- The FTP root directory must not be at the system root level and the directory used must be "chrooted" if supported by the operating system.
- FTP sessions must be configured to disconnect after acceptable period of inactivity.
- Unsuccessful login attempts should also be disabled or disconnected.

Telnet Services:

Both Inbound/Outbound Telnet services with Internet must not be allowed.

Network News:

Accessing news resources using the bank's information systems resources should be done through an approved the bank's network news server. All news services should be provided through the firewall/ UTM.

Trivial File Transfer Protocol (TFTP):

The use of TFTP should be prohibited, unless approved by the Departmental Head and the Network/IT head.

Internet Mail:

All Internet mail should be provided through an approved mail server of the bank. All mail services must be provided through the firewall/ UTM.

SMTP traffic should be handled by a dedicated SMTP proxy (e.g., SMAP/SMAPD), and not allowed to pass through the firewall/ UTM to an internal mail server. Dangerous SMTP traffic (e.g., pipe symbols) should be rejected and logged by the proxy.

Internal host name and addresses should be hidden from mail headers. For outgoing mail messages outbound email headers should be selectively rewritten

so that all email appears as if it originated from the firewall/ UTM or external SMTP relay.

SMTP message size should be appropriately restricted to the capabilities of the mail servers.

The following configuration practices should be applied for sendmail on mail servers:

- Insecure Sendmail configuration options such as WIZ, VRFY, EXPN and DEBUG should be disabled.
- The Sendmail.cf file should allow only a minimal list of "trusted users".
- The Sendmail Aliases file should be configured securely with minimum permissions.
- The Sendmail mail queue file and mail configuration file should be configured securely, with only the minimum permissions necessary for operation."

Internet Relay Chat Services:

Internal Relay Chat Services should be prohibited.

CHAPTER - 15

This chapter specifies the policy for handling and usage of e-mails.

15 E-mail Policy

15.1 Closed User Group and External Mails

The E-Mail setup requires elaborate checks and control measures to thwart the inherent risks associated with an open system much more than in a closed user group (CUG) system.

The policy for CUG E-Mails is the same as those for Internet E-Mails vis-à-vis downloading, sending and receiving of E-Mails.

15.2 Responsibility of Users

Users of Bank's IT facilities should take all reasonable steps to prevent receipt and transmission of malicious software such as computer viruses through E-Mail. In particular, users:

- Should not transmit by E-Mail any file attachments which are known to be infected with a virus;
- Should ensure that an effective anti-virus system is operating on their computer systems which are used to access Bank's IT facilities in general and E-Mail system in particular;
- Should not open E-Mail file attachments received from unsolicited or unreliable sources.

The following activities are strictly prohibited, with no exception:

- Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email Spam).
- Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
- Unauthorized use, or forging, of email header information.
- Solicitation of email for any other emails address, other than that of the poster's account, with the intent to harass or to collect replies.

- Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
- Use of unsolicited email originating from within Bank's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Allahabad Bank or connected via Allahabad Bank's network.
- Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup Spam).

15.3 Usage of E-Mail:

Business Use Only
Email systems should be used primarily for bank's use, unless management has specifically approved the non-business use.

Incidental personal use is permissible as long as:

- It does not interfere with normal business activities or hamper employee productivity,
- It does not consume more than trivial amount of resources,
- It does not involve solicitation,
- It is not associated with any for-profit outside business activity and,
- It does not potentially embarrass the bank and its management,
- It does not result in Spam mail originating from bank's network,
- It does not result in spoofing,
- It is not unauthorised.

Procedure for Creation of new users: Employee has to put formally a request in writing to the head of department who in turn will forward such request to CBS Project Office / DIT for creating an email id. After creation of email id, user id and password will be informed to the user who has to change his password in his first login.

Blanket forwarding of e-mail: Blanket forwarding of e-mail messages is prohibited as this may clog-up the network.

Size of Mailbox and e-mails: The mailbox size for each user should be restricted to a limit depending upon user's requirement which can be increased now and then with the approval of DIT. If mail box size is increased to more than prescribed limit then purging should be done.

Wherever possible, the system should:

- Flash a warning message when a user's mailbox size reaches 90% of the prescribed limit.
- Lock out the user's e-mail account when the mailbox size exceeds prescribed limit. The user must submit a formal request to the Systems Administrator for getting his account unlocked.
- Similarly, the size of incoming and outgoing e-mails should be restricted as follows :-
  - ™ 1 MB for mails received and sent outside the bank's network
  - ™ 2 MB for mails sent within the bank.
  - ™ If in a certain case a file more than 2 MB in size is required to be sent in exigency, then permission may be obtained from System Administrator.

Retention Period:- Retention period for mail should be such that it fulfils criteria like legal, RTI act, government Compliance, IT Act (time to time), internal requirement, etc. But this period may change based on several guidelines issued either by government or the bank to fulfil compliance as on when it arises.

Confidentiality:-

Sending E-Mail via insecure public lines (e.g. the Internet) can compromise the confidentiality and integrity of the information being transmitted. Digital signatures along with encryption should be used to overcome this risk. For internal mail also digital signature along with encryption should be encouraged to use to avoid non-repudiation.

Some other points to be kept in mind while accessing the mail:-

- Make sure that signature, which include at least name, designation and department / office / branch, of the person who is sending the mail is added as the last part of the message.
- When to send cc: or bcc: messages.
- Email disclaimer is included.

- Email etiquette rules are followed.
- Attachments, if any, is properly scanned before sending and after receiving mail;

- Communication through E-mail should always be a priority among bank's employee as it is cheap and easy and there is always a proper record of such communication.

CHAPTER - 16

This chapter specifies the controls for connectivity to different networks, the policy for IP addressing, policies for administration and management of the various devices like router, firewall/ UTM and IDS. The policy for NMS is also specified.

16 Network Connectivity and Network Management System (NMS)

16.1 IP Addressing

In any TCP/IP network, IP address assumes high importance.

- Any node that is connected to the network must have a Unique IP address.
- In the Bank network, the assignment of IP addresses must be done as per the documented policy followed by the Bank.
- The physical assignment of IP addresses should be done only by the personnel authorised to carry out this activity and all the addresses that have been assigned should be documented properly for easy retrieval and perusal by the higher-ups.
- In no case should an end-user change the IP address of any node in the network.
- The procedures stated in the Change Management should be followed in case of modification of IP address.

In a DHCP (Dynamic Host Configuration Protocol) environment, the allocation of IP addresses is dynamic and involves no manual intervention except in the configuration of the DHCP server and specifying the range of IP addresses that are to be allotted.

16.2 Connectivity to INFINET

The INFINET is a Closed User Group (CUG) and the Bank is one of the CUG members. The policy for the CUG is decided by the Institute for Development and Research in Banking Technology (IDRBT) in consultation with the various

banks. All the CUG members are bound by the policy framed for the CUG by IDRBT from time to time.

16.3 Connectivity to INTERNET

In the case of the Bank branches and administrative offices (ROnal Offices) that have systems connected to the Internet through modems, the following actions/precautions should be taken.

- Those systems that are connected to the Internet should not be part of the LAN/WAN;
- Such systems should be stand-alone and should have appropriate antivirus software installed on them;
- Any business data that requires to be transferred from such systems to systems in the LAN/WAN should be thoroughly scanned for worms, virus, Trojan Horses, back door programs, etc. before transfer.
- Downloading, if necessary, should be done only from secure sites after prior permission from the authorities concerned.

16.4 Router Security Policy

The router is not only the connection point for the different networks but also acts as the first line of defence for the internal network. The points that need to be considered in the setting up and maintenance of the router are as below:

- ***Access control list***: The access control list should be configured to
    - Drop packets with invalid source address;
    - Allow only the protocols that are required to pass through.
- ***Services running on the router:***
    - All unnecessary services running on the router should be stopped;
    - Use only corporate standardized SNMP community strings.
- ***Configuration change and management of router:***
    - Once the initial configuration is done, changes in configuration should be done only when the working situation demands such a change;
    - Only the authorised personnel should be permitted to make changes to the configurations in the router;

-
    - All the changes that are done should be in accordance with the change management policy.
- ***Administrative control:***

- Only the authorised personnel should have the complete control of the router and its accessories like the TFTP server;

- o The router should be kept in a physically secure place and should be provided with adequate protection from environmental threats like fire, etc.

Apart from the above, the points that need to be considered while configuring the router are as follows:

- Local user accounts should not be configured on the router;
- The enable password on the router must be kept in a secure encrypted form;
- The router must have the enable password set to something different from the factory-enabled default password;
- Drop packets that are not intended for the internal network;
- The following options should be disallowed:
  - o IP directed broadcasts;
  - o Incoming packets at the router sourced with invalid addresses such as RFC1918 address.

16.5 Firewall/ UTM Security policy

A Firewall/ UTM is a mechanism for protecting a corporate network from external communication systems such as the Internet. The norms prescribed should prevent unauthorized use of the resources/loss of data associated with break-ins, and also to protect the confidentiality of data in the systems. Secure methods for accessing external resources should be made use of all the time.

16.5.1 The Firewall/ UTM Should

- Hide the structure of the protected network;
- Provide audit trails of all communications to or through the Firewall/ UTM system and should generate alarms when suspicious activities are detected;
- Should use a “proxy server” to provide application gateway functions through the Firewall/ UTM;
- Statically define the routes;
- Not accept session initiation from the Public Internet, except in case of internet banking;
- Defend itself against direct attack;

- Be structured so that there is no way to bypass any Firewall/ UTM component;
- Deny all in-bound and out-bound services unless specifically permitted;
- Be configured so as to log all reports on daily, weekly and monthly basis. Software tools or such utilities should be used for programmatically

summarising the log entries or the associate actions with the log file entries.

- Notify the Firewall/ UTM administrator of security alarms by e-mail, pager or other means. The alarms, among others, may relate to specified number of failed attempts to connect to any service port within a time span of specified number of minutes of consecutive failed attempts to utilise Proxy Services etc. The failed attempts should be directly logged into the Firewall/ UTM system.

16.5.2 Administration

A Firewall/ UTM, like any other network device, needs to be managed by someone and the norms for Firewall/ UTM Security should state the official is responsible for managing the Firewall/ UTM. Two Firewall/ UTM administrators should be designated and should be responsible for the upkeep of the Firewall/ UTM. The primary Administrator should make changes to the Firewall/ UTM and the secondary Administrator should only do so in the absence of the former so that there is no simultaneous or contradictory access to the Firewall/ UTM. Each Firewall/ UTM Administrator should provide their home phone number, pager number, cellular phone number and other numbers or codes in which they can be contacted for ease of maintenance/support whenever required.

16.5.3 Remote Firewall/ UTM Administration

Firewalls/ UTMs are the first line of defence against intruder. By design, Firewalls/ UTMs are generally difficult to be attacked directly, forcing the intruders to often target the administrative accounts on a Firewall/ UTM. The username/password of administrative accounts should therefore be totally protected. The most secure method of protecting against this form of intrusion is to have strong physical security around the Firewall/ UTM host and to only allow Firewall/ UTM administration from an attached terminal. However, operational concerns often dictate that some form of remote access for Firewall/ UTM administration is supported. In no case should remote access to the Firewall/ UTM be supported over untrusted/unreliable networks, which are not authenticated. In addition, to prevent eavesdropping session encryption should be used for remote Firewall/ UTM connections.

16.5.4 Physical Security

The physical security of the Firewall/ UTM should never be overlooked. If the devices are located in a non-secure area, they are susceptible to damage from intruders and at a higher risk to accidental damage. Therefore, Firewall/ UTM devices should be secured behind locked doors. The Firewall/ UTM ideally should be located in a secured environment. Another factor is the quality of the electrical and network connections and environment control. The Firewall/ UTM set-up should have backup power supplies and possibly redundant connections to external networks. Sufficient air-conditioning also is to be provided to the environment. The Firewall/ UTM should be also protected as is reasonable from natural disasters such as fire and flood. Fire extinguishers/smoke/heat alarms should be provided to the Firewall/ UTM environment.

16.5.5 Firewall/ UTM Incident Handling

Incident reporting is the process whereby certain anomalies are reported or logged on the Firewall/ UTM. A documented policy (the policy for Incident Handling) is required to determine what type of reports to log and what is to be done with the generated log report. The Firewall/ UTM should be configured to log all reports on daily, weekly, and monthly basis so that the network activity can be analysed when needed and examined periodically. The Firewall/ UTM administrator should be notified of any security alarm by email, pager or other means so that he may immediately respond to such alarm.

The Firewall/ UTM should reject any kind of probing or scanning tool that is directed to it so that the information that is being protected is not leaked out by the Firewall/ UTM.

16.5.6 User Accounts

Firewalls/ UTMs should never be used as general-purpose servers. The only user accounts on the Firewall/ UTM should be those of the Firewall/ UTM administrator and backup administrator. Only these administrators should have privileges for updating system executables or other system software. Only the Firewall/ UTM administrator and backup administrator will be given user accounts on the organisation Firewall/ UTM. Any modification of the Firewall/ UTM system software should be done by the Firewall/ UTM administrator or backup administrator and requires approval of the authority concerned.

16.5.7 Backup

To support recovery after failure or natural disaster, a Firewall/ UTM like any other network host should have a policy in place defining backup. Data files as well as system configuration files should have some backup in case of Firewall/ UTM failure.

The Firewall/ UTM must be backed at periodic intervals so that in case of system failure, data and configuration files can be recovered. Backup files should be stored securely on a read-only media so that data in storage is not over-written inadvertently and locked up so that the media is only accessible to the appropriate personnel.

An important backup alternative would be to have another Firewall/ UTM configured as the one already deployed and kept safely so that in case there is a failure of the Firewall/ UTM in use, the backup Firewall/ UTM could be utilised.

16.5.8 Restoration of Services

Once an incident has been detected, the Firewall/ UTM may need to be brought down and reconfigured. If it is necessary to bring down the Firewall/ UTM, Internet service (where configured to be available) should be disabled or the secondary Firewall/ UTM should be made operational. Internal systems should not be connected to the Internet without a Firewall/ UTM. After being reconfigured, the Firewall/ UTM must be brought back into an operational and reliable state.

Appropriate measures for restoring the Firewall/ UTM to a working state when a break-in occurs are to be in place. In case of a Firewall/ UTM failure, the Firewall/ UTM administrator(s) are responsible for reconfiguring the Firewall/ UTM and address any vulnerability that was exploited. The Firewall/ UTM shall be restored to the state it was before the failure so that the network is not left open.

16.5.9 Upgrading the Firewall/ UTM

It is often necessary that the Firewall/ UTM software and hardware components are upgraded with the necessary modules to assure optimal Firewall/ UTM performance. The Firewall/ UTM administrator should be aware of any hardware/software bugs as well as Firewall/ UTM software upgrades that may be issued by the vendor. If an upgrade of any sort is necessary, certain precautions must be taken to continue maintaining a high level of operational security.

16.5.10 Logs and Audit Trails (Audit/Event Reporting and Summaries)

Most Firewalls/ UTMs provide a wide range of capabilities for logging traffic and network events. Some security-relevant events that should be recorded on the Firewall's/ UTM's audit trail logs are:

- Hardware and disk media errors;
- Login/Logout activity;
- Connect time;
- Use of system administrator privileges;
- Inbound and Outbound e-mail traffic;
- TCP network connect attempts;
- In-bound and out-bound proxy (if configured) traffic type.

16.6 Intrusion Detection System (IDS)/ Intrusion Prevention System (IPS)

IDS/ IPS is a means of detective access control. Intrusion detection/ prevention systems should be employed by the bank to detect and notify, and in some cases, prevent unauthorized access to a networked systems or resources. The IPS/ IPS should have the following:

- The ability to react in a timely fashion to prevent substantive damage - by automatic or manual intervention.
- The ability to identify which is the precursor of more serious attacks.
- The ability to identify a perpetrator.
- The ability to discover new attack patterns.
- The ability to produce evidence.

There are two types of intrusion detection/ prevention systems, viz., Host-based Intrusion detection/ prevention system and Network based Intrusion detection/ prevention system.

Host Based Intrusion Detection/ Prevention System

Host based IPS/ IPS should be installed on each individual computer system that is to be protected. Host-based intrusion detection/ prevention is very closely integrated with the operating system it protects and has a very high level of granularity in terms of the types of threats it can detect.

Issues with Host based IPS/ IPS

- Host-based IPS/ IPSs have a negative impact on system performance - the larger the number of parameters examined by the IPS/ IPS, the greater the impact on system performance.
- Host-based IPS/ IPSs do not always notice network-based attacks, such a denial of service.
- Many host-based intrusion detection/ prevention systems have a negative impact on operating system stability.

Network Based Intrusion Detection/ prevention System

Network-based intrusion detection/ prevention systems are protocol analysers with intelligence. These devices monitor all network traffic that "passes by" on the wire, looking for "attack signatures" that indicate certain types of attacks are in progress.

Issues with Network based IPS/ IPS

- Most Network-based IPS/ IPSs miss attack signatures that are spread across multiple packets, as they do not have the capability of reassembling all fragmented network traffic.
- Network-based intrusion detection/ prevention systems cannot function

without special switch configurations (port mirroring, etc.) or hubs.

- Network-based intrusion detection/ prevention systems can be detected using tools designed to locate/ identify promiscuous mode interfaces.
- In the context of denial-of-service attacks, many IPS/ IPSs are disabled by the very events they are supposed to monitor.

The bank should go for a combination of host-based IPS/ IPS and network-based IPS/ IPS, with host-based IPS/ IPS on critical servers and network-based IDS/ IPS monitoring the flow of traffic on network segments that need to be available.

- Use a respected commercial package that is regularly updated to keep up with new vulnerabilities and attacks;

- Keep the intrusion detection/ prevention tool up-to-date by applying the latest patches and attack signatures;
- Run the absolute minimum of services on the platform hosting the intrusion detection/ prevention tool;
- Do not allow the platform's interface to be visible to the perimeter networks being monitored;
- Establish an administration and reporting network for the intrusion detection/ prevention system that is isolated from the internal network;
- Do not place too much reliance on the intrusion detection/ prevention tool and ensure other security procedures are in place.

16.7 Combating Cyber Crimes

The Bank must have security checks and controls in place to combat cyber crime directed against it.

- *Defending against internal attacks:* The Bank must provide access to information to the employees only as per the roles and requirements of that particular job.

- *Defending against third-party attacks:* The Bank must identify the access points of the network layout, and verify that the current security safeguards are operational to prevent any external entity from attacking the Information System of the Bank and causing loss to the Bank.

- *Minimising the impact of cyber-attacks:* The Bank must have contingency plans in place to reduce the impact of any attack which the Bank might have to face from either any internal entity or external entity. The chapter on Business Continuity planning throws more light in planning for contingencies.

- *Collecting of evidence:* The Bank should have logging mechanisms in place that can trace the source of intended malicious activity. These logs are the source of evidence which the Bank must use, first to trace the source of attack and later, if it decides to proceed legally against the entity that perpetrated the attack with the intention to cause loss, in any form, to the Bank.

- *Preventing Social Engineering:* The Bank must make its personnel aware of the threat posed by social engineering and should suitably instruct their personnel to follow a request-response mechanism that would identify the caller whose intentions are not known. This mechanism is absolutely essential in the Data centre where the identity of the caller should be established before any information is divulged.

- *Preventing Phishing:* Phishing is an e-mail fraud scam conducted for the purposes of information or identity theft like share passwords, credit card

numbers, etc. The messages in such e-mail may look quite authentic, featuring corporate logos and formats similar to the ones used for legitimate messages. Typically, they ask for verification of certain information, such as account numbers and passwords, allegedly for validation/ modification purpose. Since these e-mails look so official, many unsuspecting recipients may respond to them, resulting in financial losses, identity theft and other fraudulent activity against them. Sufficient user awareness, use of anti-phishing tools at user's browser etc help greatly in controlling such attacks.

16.8 Policy on NMS

NMS is a group of disciplines that designs, configures, deploys, and diagnoses, audits and projects network and application usage in a distributed environment. Making a network run requires technical expertise in managing desktops, servers, simulating networks / application loads, configuring network / infrastructure devices, drawing network topologies, processing events and performance metrics.

The Network Management solution should allow for monitoring of all networking devices required for business continuity. The five functional areas of network management that form part of the policy for network management are:

- **Fault Management** — should detect, isolate, notify, and correct faults encountered in the network.
- **Configuration Management** — should handle configuration aspects of network devices such as configuration file management, inventory management and software management.
- **Performance Management** — should monitor and measure various aspects of performance so that the overall performance can be maintained at an acceptable level.
- **Security Management** — should provide access to network devices and corporate resources to authorized individuals.
- **Accounting Management** — should provide usage information of network resources.

The network management architecture should include the following:

- Simple Network Management Protocol (SNMP) platform for fault management.
- Performance monitoring platform for long term performance management.

16.8.1 Fault Management

Faults can cause downtime or unacceptable network degradation and for this reason fault management should be implemented with highest priority among network management elements. A network management platform deployed in the Bank should manage an infrastructure that consists of multi vendor network elements. The platform receives and processes events from network elements in the network.

16.8.2 Configuration Management

The role of configuration management is to monitor network and system configuration information so that the effects on network operation vis-à-vis the various versions of hardware and software elements can be tracked and managed.

16.8.3 Performance Management

The role of performance management is to measure and make available various aspects of network performance so that inter-network performance can be maintained at an acceptable level.

16.8.4 Security Management

The role of security management is to control access to network resources according to prescribed guidelines so that the network is free from sabotages either intentionally or otherwise. A security management subsystem should monitor users logging on to a network resource and should refuse access to those who enter inappropriate access codes, etc.

16.8.5 Accounting Management

Accounting management is the process used to measure network utilization parameters so that individual or group users in the network can be regulated appropriately for the purposes of accounting or charge back.

16.8.6 Outsourcing

The following points should be borne in mind while outsourcing NMS:

- The vendor should have good and proven experience & efficiency in the field.
- The deliverables should be clearly specified.
- The location of operation should be clearly defined.
- The users of the Bank should be made aware of such an agreement between the Bank and the vendor and should extend full co-operation to the vendor in achieving the deliverables.
- The vendor should enter into a non-disclosure agreement with the Bank.

CHAPTER - 17

This chapter outlines the policy for financial services like ATM and Internet Banking.

17 Financial Services and Products

17.1 ATM Security Policy

The two main concerns of ATMs are:

- The ATM dispenses, requested functionality to a bonafide holder of a card which operates the ATM.
- The ATM should prevent an unauthorized user of the card from gaining access to the machine’s functions.

These two issues are taken care by Personal Identification Number (PIN).

17.2 ATM Switch

An ATM switch is basically an electronic device that routes traffic from Automated Teller Machine to the host processor of the Bank.

17.2.1 Desired Characteristics of ATM Switch

17.2.1.1 Functionality

- The Switch must support the Distributed Database, Clustered Database as well as Centralised Database.
- It should provide card management functionality, which a bank can use to issue all types of cards viz., ATM cards, Debit/Credit Cards and Smart Cards etc.
- It should also provide comprehensive interface support for connectivity to other networks.

Pithoragarh Zila Sahkari Bank Ltd. Pithoragarh

110

17.2.1.2 Authorization

Fault Tolerance: Zero Downtime

- The switch should support authorization both during online and offline host processing.
- The switch should be fault tolerant and should support zero percent downtime. Further it should support all the major communication protocols used for transportation of data. The system should also support ISO8583 messaging formats.

17.2.1.3 Scalability and Performance

The switch should be highly scalable and also the performance enhancement should also be high and significant.

17.2.1.4 Reliability and Availability

- The system should always provide reliable and fail-safe service to the ATM customers.
- The system should be highly scalable ensuring zero downtime.

17.2.1.5 Methods of Communication

- The system should support direct connect leased lines, TCP/IP and X.25 networks, dial-up lines and automatic switching to dial back up lines when problems with leased lines/VSAT/ISDN connectivity are required.
- Control of the communication configuration must be designed in such a way so as to allow management of Switch from disaster recovery site.
- The switch should provide communication support for multiplex and multi-drop line configuration.

17.2.1.6 Accounting and Reconciliation

The system must provide a very robust and foolproof accounting and reconciliation mechanism, which will ensure that:

- All transactions are duly logged, accounted for and record of disposal properly maintained.

- Inter branch reconciliation is done on day to day basis with mechanism to cross check the reconciliation process from the Electronic Financial

- Settlement between the bank, other institutions and interchanges/ merchant establishments is done on a day-to-day basis accurately.

17.2.1.6.1 Automatic Reconciliation

The switch should be capable of supporting automatic reconciliation on an on-going basis throughout the day.

17.2.1.6.2 Adjustment of Transaction

The system should have an automated procedure/mechanism for handling un-reconciled /disputed transactions. The mechanism should include but not limited to, entry methods, transaction creation, validation and final disposal.

17.2.1.6.3 Report Generation

The switch should also generate reports necessary for branch accounting and inter branch reconciliation automatically/compulsorily at the end of the day.

17.2.1.7 Transaction Routing

- As the switch acts as a hub for all the transactions received from its participating terminals/processors, institutions and interchanges, needed number of reliable and flexible routing schemes should be provided to handle flow of data. The routing table should allow easy, secured access to the routing information for each institution / interchange. The system should be flexible enough to allow new routing also.
- The Switch should support card prefix routing and algorithmic routing but not limited to these two only.
- When the issuer host is not available, the switch should have the ability to perform, if required Stand-in Authorization. The authorization parameters in such cases should be user definable in respect of Limit, Usage accumulation period; Negative/Positive Balance File based information etc.

17.2.1.8 Security

17.2.1.8.1 Transaction Security

- The system should support DES method of PIN (Personal Identification Number) verification. However, PIN verification may be optional for other interchange/networks. The system should support 4-12 digit variable length PIN, defined at Bank level.
- The switch should support Triple DES encryption.

- The switch should support Dynamic (master/slave) and constant key DES.

- The system should support MAC addressing – Field/Element level that adhere to ANSI X9.8 standards.

17.2.1.8.2 Operation Security

- Access Control: The switch should be accessible through passwords to ensure that only authorized users gain access to the system.
- User Rights: The system should support defining user rights on the system so that a user can perform only those tasks, which are assigned to him.
- Integrity: The switch should automatically ensure integrity of the database on an on-going basis.
- Audit-ability: The system should maintain a record of the users who have accessed the system, resources used and actions performed on an ongoing basis.
- All security violations must be logged with full details.

17.2.1.8.3 Data Security

The system must ensure complete data security. Message routing and other functions should take place in completely secured environment. All the security checks must be automatic. System should maintain a record of users and all security violations must be logged with full details.

17.2.1.9 Online Up-gradation

The system should support online up-gradation and dynamic system configuration: online database back up and maintenance, upgrade of CPU, disk etc.

The system should support multiple types of communication networks like ATM, 10/100 Ethernet, Gigabit Ethernet, SS7, Sync and Async etc.

17.2.1.10 Remote Control

The system should be able to get administered via remote console. This will ensure fault notification and diagnosis of faulty components.

17.2.1.11 Vendor Support

It should support ATM and POS devices from leading Vendors. It should support authorization both during on line and offline host processing.

17.2.1.12 Key Management

There should be separate set of keys for ATM operations like master keys for locations, terminals, pin /card verification etc. which are required to be entered at the Switch and other terminals.

Each of the above keys should be held by the Bank's officials at a senior management level. The said officials should be from a different Division other than IT Division and should not have much technical background.

It should also be ensured that the backup/duplicate keys are not stored together. As a measure of abundant precaution, while depositing the backup/duplicate security keys it should be properly documented and sealed.

17.3 Internet Banking

17.3.1 Overview

The security architecture of Internet Banking for - - is based on a multi-layered concept, on the premise that each financial transaction uses multiple layers of security and every layer adds a different technology resulting in a trusted system that is monitored at all times. The security policy for each layer is prescribed separately. Compliance of an individual layer per se does not ensure security to that layer unless all the interlinked layers are complied.

17.3.2 Layers of the Internet Banking

Internet banking as envisaged in a centralized environment has got these following basic layers:

- Browser
- Firewall/ UTM
- Web server
- Web Host
- Internet Banking Application Server
- Internet Banking database
- Middleware
- Database (Centralized Banking application)
- Data center
- Internal Network
- People
- Management

17.3.2.1 Web Browser layer

17.3.2.1.1 Risks

Active content that crashes the browser, damages the user's system, breaches the user's privacy, or merely creates an annoyance.

The misuse of personal information knowingly or unknowingly provided by the end-user.

17.3.2.1.2 Control

The controls associated with the above risks are basically in built in the design of the application.

17.3.2.1.3 Implementing SSL and Session Encryption

Review the source of HTML, JavaScript and other client-side scripting languages to ensure that these do not contain unnecessary information that could be observed and exploited by potential attackers. This might include:

- Developer names (could be used for social engineering)
- Disable functionality viz. details about Common Gateway Interface (CGI) functions and parameters, third-party tools in use, which may be vulnerable.
- Review error messages returned by the web-based application to ensure that they do not reveal undesirable information.

17.3.2.1.4 Robust logon process

Where a web-based application requires users to log on to authenticate themselves, the following factors needs consideration:

- Log-on failure messages should not indicate which of the username/password pair submitted was incorrect
- Where http basic authentication is used, there is no account lockout after successive failed attempts and applications may therefore be vulnerable to brute-force attacks.
- Where account lockout is implemented, further log-on failure messages should be carefully designed (for example, to avoid revealing when the password has been guessed correctly, even though the account is locked)
- Avoid allocating system resources for a potential user session before authentication is complete: thus reducing the scope of denial of service attacks based on initiating many log-on attempts
- **Two factor authentication:** It's opportune time to realize that the most effective way to raise the identity assurance level during authentication is to use two-factor authentication which is usually based on the traditional “something you know” form factor (e.g., password) plus another form factor that is either “what you have” (e.g., key, badge, smart card, token) or “what you are” (e.g., fingerprint, voice). Strong authentication based on two factors

is much more effective in reducing the risk associated with password attack (identity theft of fraud) and thus the chance of losing valuable business data that may very possibly lead to financial loss or damage to the image and reputation of the business. It more so required in Internet/ Mobile Banking, where password dependent financial risks are high and are always on rise.

17.3.2.1.5 Tracking session

Web-based applications often need to implement mechanisms to track transactions within a user session as the underlying http protocol cannot do this (it is stateless). When these mechanisms are designed, the following factors should be taken into account to minimize the risk of sessions being hijacked or cloned:

- Avoid using mechanisms that can lead to session IDs being unnecessarily disclosed
- Avoid session IDs that are easily predicted by including a random element.

17.3.2.1.6 Implementation of session Timeouts

Implement session timeouts for web-based applications after designated periods of inactivity if there is considered to be a risk from access to unattended browsers.

17.3.2.1.7 Session Encryption

Consider using secure session protocols such as SSL to encrypt sessions between browsers and the web server to prevent sensitive application data being intercepted.

The first layer of online financial security is the 128-bit Secure Sockets Layer (SSL) encryption between their browser and the Web Servers. SSL is the industry standard that provides secure access to online financial services from anywhere on the Internet using any current Internet browser.

SSL provides a secure channel for data transmission over the Internet. It allows for the transfer of digital signatures to authenticate users and provides message integrity, ensuring that our data cannot be altered en route. Browsers can also display a certificate to the user about the source of a secure transmission. This assures Internet users that they are communicating with the financial institution's service provider and not a third party trying to intercept the transaction on the Internet.

17.3.2.1.8 Get and Post operation

Use http POST rather than GET operations to obtain information from users that may be sensitive, personal or compromise the security of the application.

URLs requested by GET operations are stored in the browser's history file and can also be passed on to other web servers via the http Referrer field. This can lead to the disclosure of sensitive information. For example, the following GET operation could cause damaging information to be stored in insecure log files: http://www.anybank.com/scripts/login.cgi?username=xyz&password=xyzasd

17.3.2.1.9 Restriction of Hidden fields

Avoid using HTML hidden form fields to pass important or sensitive parameters from browsers to web servers.

These fields, although not displayed in web pages, can easily be viewed by users (by viewing the HTML source) and modified to cause unexpected results.

An example of the typical use of hidden form fields to avoid is shown below.

```
<INPUT TYPE="hidden" NAME="username" VALUE="allahabadbank">
<INPUT TYPE="hidden" NAME="password" VALUE="yellowsubmarine">
<INPUT TYPE="hidden" NAME="adminflag" VALUE="no">
```

17.3.2.1.10 Controlling Cookies

Where cookies are used to pass important or sensitive information between browser and web application, make sure that cookie parameters are set to avoid unnecessary disclosure of the information.

The structure of a cookie is shown below.

PARAMETER / MEANING

NAME / Arbitrary string used to identify the cookie, since a web server can send the user more than one cookie

DOMAIN / the range of hosts where the browser is permitted to transmit the cookie

PATH / the range of URLs where the browser is permitted to transmit the cookie

EXPIRES / When the browser must no longer store the cookie

SECURE / Boolean value that indicates if the browser may only send the cookie over an encrypted session

DATA / Arbitrary strings of text

Users can examine the contents of cookies stored on their PCs. Even those which expire at the end of the session can be viewed by typing: JavaScript: alert (document. cookie) into the browser URL field.

Some users prevent their browsers from accepting cookies causing problems for applications that depend on them.

17.3.2.1.11 User Input Validation

Validate data returned from browsers to check for unexpected values that could cause the application to behave in unintended ways. Particular things to check include:

- Values falling outside allowed ranges
- Volume of data returned outside expected ranges
- Special characters that could be misinterpreted by the application, for example:
- %0A new line character (in hex)
- | Pipe
- ; Semicolon
- “ Double quote
- ‘ Single quote

- <% %> VBScript terminators
- Do not rely on client-side filtering of user input (for example, using JavaScript) as this can be circumvented by the user.

17.3.2.2 Firewall/ UTM

17.3.2.2.1 Risk

In case of Internet Banking since there has to be interaction between two networks, one Internet-a public Network and Bank’s corporate Network, a private Network, there should be a Firewall/ UTM in between.

A Firewall/ UTM is a system or group of systems that enforces an access control policy between two networks. The actual means by which this is accomplished varies widely, but in principle, the Firewall/ UTM can be thought of as a pair of mechanisms: one, which exists to block traffic, and the other, which exists to permit traffic. Some Firewall/ UTMs place a greater emphasis on blocking traffic, while others emphasize permitting traffic. Probably the most important thing to recognize about a Firewall/ UTM is that it implements an access control policy. If we don't have a good idea what kind of access we want to permit or deny, or we simply permit someone or some product to configure a Firewall/ UTM based on what they or it think it should do, then they are making policy for our organization as a whole.

17.3.2.2.2 Control

The task of implementing a Firewall/ UTM should be done by going through the following steps:

17.3.2.2.3 Determine the access denial methodology to use.

It is recommended to begin with the methodology that denies all access by default. In other words, start with a gateway that routes no traffic and is effectively a brick wall with no doors in it.

17.3.2.2.4 Determine inbound access policy.

If all Internet traffic originates on the LAN this may be quite simple. A straightforward NAT router will block all inbound traffic that is not in response to requests originating from within the LAN. It is always desirable that the true IP addresses of hosts behind the Firewall/ UTM are never revealed to the outside world, making intrusion extremely difficult. Indeed, local host IP addresses in this type of configuration is usually non-public addresses, making it impossible

to route traffic to them from the Internet. Packets coming in from the Internet in response to requests from local hosts are addressed to dynamically allocated port numbers on the public side of the NAT router. These change rapidly making it difficult or impossible for an intruder to make assumptions about which port numbers to use.

If the requirements involve secure access to LAN based services from Internet based hosts, then we will need to determine the criteria to be used in deciding when a packet originating from the Internet may be allowed into the LAN. The stricter the criteria, the more secure our network will be. Ideally we will know which public IP addresses on the Internet may originate inbound traffic. By limiting inbound traffic to packets originating from these hosts, we may decrease the likelihood of hostile intrusion. We may also want to limit inbound traffic to certain protocol sets such as ftp or http. All of these techniques can be achieved with packet filtering on a NAT router. If we cannot know the IP addresses that may originate inbound traffic, and we cannot use protocol filtering then we will need more & more complex rule based model and this will involve a stateful multilayer inspection firewall.

17.3.2.2.5 Determine outbound access policy.

If our users only need access to the web, a proxy server may give a high level of security with access granted selectively to appropriate users. As mentioned, however, this type of Firewall/ UTM requires manual configuration of each web browser on each machine. Outbound protocol filtering can also be transparently achieved with packet filtering and no sacrifice in security. If we are using a NAT router with no inbound mapping of traffic originating from the Internet, then we may allow LAN users to freely access all services on the Internet with no security compromise. Naturally, the risk of employees behaving irresponsibly with email or with external hosts is a management issue and must be dealt with as such.

17.3.2.2.6 Determine if dial-in or dial-out access is required.

Dial-in requires a secure remote access PPP server that should be placed outside the Firewall/ UTM. If dial-out access is required by certain users, individual dial-out computers must be made secure in such a way that hostile access to the LAN through the dial-out connection becomes impossible. The surest way to do this is to physically isolate the computer from the LAN. Alternatively, personal firewall software may be used to isolate the LAN network interface from the remote access interface.

Decide whether to buy a complete Firewall/ UTM product, have one implemented by a systems integrator or implement one ourselves.

Once the above questions have been answered, it may be decided whether to buy a complete Firewall/ UTM product or to configure one from multipurpose routing or proxy software. This decision will depend as much on the availability of in-house expertise as on the complexity of the need. A satisfactory Firewall/ UTM may be built with little expertise if the requirements are straightforward. However, complex requirements will not necessarily entail recourse to external resources if the system administrator has sufficient grasp of the elements. Indeed, as the complexity of the security model increases, so does the need for in-house expertise and autonomy.

Depending on the Internet Banking architecture as envisaged by the Bank it is recommended to have a stateful multilayer Inspection Firewall/ UTM with redundancy.

17.3.2.3 Web server

Organizations have a wide choice of web server products ranging from commercial offerings such as Microsoft’s IIS and Netscape’s Enterprise Server (SUN iPlanet) to public domain or ‘open source’ products such as Apache. Different web servers have different security features and these should be considered in selecting an appropriate product. However, other factors will have a major influence on the choice of web server software such as:

- Choice of web host (for example, UNIX or Windows NT/2000,Linux etc.)
- Cost of purchase and support
- Skills and experience within the organization.
- The risks associated with the use of web server are generally as follows
- Web server being the first point of any Internet Banking Customer, may sometimes become the first target for the intruder
- A poorly configured web server may become a firebase for the intruder to attack to the Bank’s Network
- The open TCP&IP ports in the web server may sometimes be used by the

intruder to initiate attack

- The web server can be attacked by an insider (authorized user of the Network)-if there is no access control

17.3.2.3.1 Control

17.3.2.3.1.1 Network filtering:

Place web server(s) in a DMZ. Set Firewall/ UTM to drop connections to web server on all ports but http (port 80) or https (port 443).

17.3.2.3.1.2 Host based security:

Remove all unneeded services from web server, keeping FTP (but only if we need it) and a secure login capability such as secure shell. An unneeded service can become an avenue of attack.

Limit the number of persons having administrator or root level access.

Apply relevant security patches as soon as they are announced and tested on a pre-production system.

Disallow all remote administration unless it is done using a one-time password or an encrypted link.

If the machine must be administered remotely, require that a secure capability such as secure shell be used to make a secure connection. Do not allow telnet or non-anonymous ftp (those requiring a username and password) connections to this machine from any untrusted site. It would also be good to limit these connections only to a minimum number of secure machines and have those machines resided within Intranet.

17.3.2.3.1.3 Auditing/logging:

Log all user activity and maintain those logs either in an encrypted form on the web server or store them on a separate machine on Intranet, or write to "write-once" media.

Monitor system logs regularly for any suspicious activity.

Install some trap macros to watch for attacks on the server (such as the PHF attack).

Create macros that run every hour or so that would check the integrity of password and other critical files.

When the macros detect a change, they should send an e-mail to the system manager; write a message to logs, set off a pager, etc.

17.3.2.3.1.4 Content management:

Do all updates from Intranet. Maintain web page originals on a server on our Intranet and make all changes and updates here; then "push" these updates to the public server through an SSH or SSL connection. If we do this on an hourly basis, we can avoid having a corrupted server exposed for a long period of time.

Write a script to download HTML pages and check against a template, if changes are noted, upload the correct version.

17.3.2.3.1.5 Intrusion Detection/ prevention:

Scan web server periodically with tools like ISS, nmap or Satan to look for vulnerabilities.

Have intrusion detection/ prevention software monitor the connections to the server. Set the detector to alarm on known exploits and suspicious activities and to capture these sessions for review. This information can help us to recover from an intrusion and strengthen defenses.

17.3.2.3.1.6 Redundancy

Web server, being the first point for the customer, should have lot of redundancy in built into in terms of disk space, power supply and processor. The DNS server also can be configured to provide redundancy to the web server

17.3.2.4 WEB HOST

Web hosts are the operating systems on which the web server software works.

17.3.2.4.1 Risks

The web hosts being the primary server or domain controller can have users who can have access to this, which can pose a security threat

The capacity planning of the web host is critical to the functioning of web server

Unknown services in the operating system would pose a security threat

17.3.2.4.2 Control

17.3.2.4.2.1 Capacity Planning

Carry out a careful capacity planning exercise to ensure that the CPU, memory and disk resources of the host system are sufficient for the expected usage. Monitor actual usage of the resources over time. This will allow upgrades to be applied in advance of any serious degradation in performance.

17.3.2.4.2.2 Redundancy

Use well-tested and reliable hardware platforms with in-built redundancies geared towards the levels of availability required. For example: web hosts can be provided with redundancy in:

- Power supplies
- CPUs
- Disk drives

17.3.2.4.2.3 Physical security

- Locate web servers in a managed and secure physical environment to protect them from threats such as fire, accidental damage and vandalism.

17.3.2.4.2.4 User account Restriction

- User accounts except for the web server account(s), web master accounts and authorized administrator account should be removed
- Different root directories for the web server and server documents should be used.

17.3.2.4.2.5 Dedicated host for the web server and limited services

- Use a dedicated host for the web server and aim to disable all other services, including SMTP and FTP.
- Ensure that only a minimum set of client applications is installed. If a browser must be installed, then downloading of active content (for example, ActiveX and Java) should be disabled. Where appropriate, run multiple server instances under different IDs to provide different types of access to different users.
- Install packet filters, such as TCP wrappers, to restrict connections from known hosts or services and to log incoming service requests.
- All l sensitive files should be protected from access through the web e.g. /etc/passed, data files etc
- Use only the NT File System (NTFS).
- Disable, if possible, both the server and workstation on the host platform.
- Do not designate the server to be a domain controller. This will prevent an attacker who compromises the security of the web server from gaining

Pithoragarh Zila Sahkari Bank Ltd. Pithoragarh

domain level access.

- Rename the administrator account to an obscure name, so that an attacker would have to first guess the account name. Disable the guest account and all user accounts.

- Disable all unnecessary network services and protocols.

- Remove any bindings to NetBIOS over TCP/IP.

17.3.2.5 Internet Banking Application Server

In case of a centralized transactional Internet banking the Internet Banking application server where the Internet Banking application will reside. When the Customer clicks Internet Banking in the Website of the Bank, control will pass from the Web Server to the Internet Banking application Server.

17.3.2.5.1 Risks

Considering the functionality of the application server the following risks are perceived

- Internet Banking application server, having unrestricted access from inside the network would pose a security threat

- The operating system, on which the Internet banking application would work, if not properly configured, is a security concerns.

17.3.2.5.2 Control

17.3.2.5.2.1 Physical Location

- The Internet Banking Application server should be kept in a physical secured place inside the data centre (Physical security of the data centre is explained separately)

- It should be protected from the internal network as well as the outside network through Firewall/ UTM

17.3.2.5.2.2 Logical location

- It is always better to keep the Internet Banking Application server in a separate subnet to avoid broadcast traffic from the internal network, which is also better for security reason.

17.3.2.5.2.3 Redundancy

- Redundancy in the Internet Banking application server necessarily envisages the redundancies in all the components viz. the Hardware, software and the operating system. Since no database is supposed to be in the application server, replication or mirroring is not required, but in case of hardware or software failure there should be an automatic switch over to another system. This can be achieved by deploying the cluster for availability.

17.3.2.6 Internet Banking Database Server (Local)

Internet Banking Database Server is the place where the particulars of internet Banking customers i.e. the user profiles, the session details etc., are stored.

17.3.2.6.1 Risks

- Customer's data including their user profile are very important and can be categorized as very sensitive data. Tampering in these data has got wider ramification.
- Any disruption in this system would not allow the Internet Banking facility to the customer.

17.3.2.6.2 Control

17.3.2.6.2.1 Location-Physical

- This database server should be placed in a physically secured place inside a data centre
- Should be protected from the Internal and outside Network through Firewall/ UTM

17.3.2.6.2.2 Logical Location

- The server should be kept in a separate subnet

17.3.2.6.2.3 Redundancy

- Considering the criticality of this server, there should be a clear redundancy established in it. It would be better to have two servers in culture with mirroring facility. Bank may decide who have the internet banking local

database server on the application server itself. In such case the sizings of the application sever is of paramount importance.

17.3.2.7 Middle Ware

The Middleware is basically required to interact with the centralized database server.

17.3.2.7.1 Risks

- Its one physical interface with the Centralised-banking database makes it more sensitive. As this can be a launching pad for malicious attack

17.3.2.7.1.1 Location-Physical

- This should be placed in a physically secured place inside a data centre

17.3.2.7.1.2 Redundancy

- Considering the criticality of this server, there should be a clear redundancy established in it. It would be better to have two middleware in cluster with availability

17.3.2.8 Centralised Banking Database Server

Centralized Banking Database server is the most sensitive from the security point of view as it contains the core business data. The control needed for this is as below:

17.3.2.8.1 Location-Physical

- This should be placed in a physically secured place inside a data centre

17.3.2.8.2 Redundancy

Redundancy in the centralized database server is extremely important. The following measures should be taken for this:

- Another computer of same configuration with same IP address should be kept ready and backed up with the centralized data every one hour automatically without disrupting the business. In case of any eventualities this has to be plugged in.

- Bank should also go in for a disaster recovery site of the database in a physically different location to avoid any disaster.

- Full backup of the database should be taken at the end of the day-and the backed up media should be kept up in a physically different location.

17.3.2.9 Data Centre

17.3.2.9.1 Security and Monitoring

The Data center must be monitored around the clock by a custom security network covering every possible entry point. Entry doors should be protected by biometrics/PIN or proximity. Any failed attempts or system tampering, as well as unscheduled movement in restricted areas, glass breakage, or opening of doors will be logged and immediately reported to control staff on site. Temperature readings are taken throughout the raised floor and equipment areas, power rooms, basement, diesel fuel storage area, roof, generator, cooling towers, waiting and display areas.

It is important to note that there are police, Municipal Corporation, and fire departments all within 5/10 minutes of the Data Center.

17.3.2.9.2 Facility Access

To access any equipment in the Data Center, one should pass through a minimum of two separate security doors utilizing biometrics/PIN and/or proximity keycard access verification.

The Security Department should maintain a digital record of some important unique identification, such as a passport or driver's license, for each individual who shall be authorized to enter the facility. Should standard access verification fail, access will only be granted if the individual matches an ID, the security Department is having in the file.

If a consultant or other visitor is to be permitted temporary access, an account contact will need to pre-authorize entry at least two hours in advance, by fax, phone or in person. Security Department may require a callback to a number listed in the account contacts for final verification.

Unaccompanied access without appropriate clearance is strictly prohibited. Any such access can result in the suspension and/or termination of the account along with possible prosecution.

In case of - - as the database center is owned by third party the access control data pertaining to - - should be owned by the bank. This may be required for evidence purposes in future.

17.3.2.10 Internal Network

The internal network of the bank should not have a direct connection with the Data Center. It should always be through a Firewall/ UTM. Network IDS/ IPS should also be deployed to monitor/detect illegal activities.

17.3.2.11 People

In an Internet Banking scenario this layer consists of the internal employees those will be handling the operation. Broadly there would be three set of people who would be involved in the activities viz. Network Administrator, Database Administrators, operators.

The role of the network and the database administrator is pivotal in securing the information systems of any organization. The role extends across various job functions and any laxity in any of the functions leaves the system open for malicious purposes. A few important functions of the administrator and how they relate to or impinge on system security are discussed below:

17.3.2.11.1 Installation of software

A software (whether system or application) needs to be carefully installed as per the developer's instructions. The software system may contain bugs and security holes, which over a period are fixed through appropriate patches. It is necessary to know the latest and correct configuration of all software packages. Hackers and intruders are often aware of these bugs and may exploit known weaknesses in the software; hence, care should be taken to install only the latest versions of software with the latest patches. Further, improper installation may lead to degradation of services. Installation of pirated software is not only illegal and unethical, but may also contain Trojans and viruses, which may compromise system security. In addition, while installing software care should be taken that only necessary services are enabled on a need to use basis.

17.3.2.11.2 Access controls and user maintenance

An administrator has to create user accounts on different computer systems, and give various access permissions to the users. Setting access controls to files, objects and devices reduces intentional and unintentional security breaches. A

bank's system policy should specify access privileges and controls for the information stored on the computers. The administrators create needed user groups and assign users to the appropriate groups. The execution privilege of most system–related utilities should be limited to system administrators so that users may be prevented from making system level changes. The write / modify access permissions for all executables and binary files should be disabled. If possible, all log files should be made "append only". All sensitive data should be made more secure by using encryption. The system and database administrators are also responsible for the maintenance of users and the deletion of inactive users. Proper logs should be maintained of dates of user creation and validity period of users. There should be a frequent review to identify unnecessary users and privileges, especially of temporary users such as system maintenance personnel and system auditors.

17.3.2.11.3 Backup, recovery & business continuity

Back-up of data, documentation and software is an important function of the administrators. Both data and software should be backed up periodically. The frequency of back up should depend on the recovery needs of the application. Online/real time systems require frequent backups within a day. The backup may be incremental or complete. Automating the backup procedures is preferred to obviate operator errors and missed back-ups. Recovery and business continuity measures, based on criticality of the systems, should be in place and a documented plan with the organization and assignment of responsibilities of the key decision making personnel should exist. An off-site back up is necessary for recovery from major failures / disasters to ensure business continuity. Depending on criticality, different technologies based on back up, hot sites, warm sites or cold sites should be available for business continuity. The business continuity plan should be frequently tested.

17.3.2.11.4 System & network logging

Operating systems, database packages and even business applications produce a 'log' of various tasks performed by them. Most operating systems keep a log of all user actions. Log files are the primary record of suspicious behavior. Log files alert the administrator to carry out further investigation in case of suspicious activity and help in determining the extent of intrusion. Log files can also provide evidence in case of legal proceedings. The administrator has to select types of information to be logged, the mechanisms for logging, locations for logging, and locations where the log files are stored. The information required to be logged should include Login/Logout information, location and time of failed attempts, changes in status, status of any resource, changes in system status such as shutdowns, initializations and restart; file accesses, change to file access

control lists, mail logs, modem logs, network access logs, web server logs, etc. The log files must be protected and archived regularly and securely

17.3.2.12 Management

The security of Internet Banking is dependent on effective management practices. This section outlines the measures that should be considered in the following areas:

- Capacity planning and monitoring
- Security maintenance
- Change management
- Security monitoring
- Event logging
- Intrusion detection/ prevention
- Incident management.

17.3.2.12.1 Capacity planning and monitoring

Establish an overall capacity planning process for web site, observing the following principles:

- Ensure hardware platforms and communications links are readily scalable to respond to increases in demand without fundamental changes in architecture
- Establish monitoring processes to measure usage of the physical resources and communications bandwidth so that upgrades can be arranged before capacity overloads become problematic.

17.3.2.12.2 Security maintenance

- Identify sources of information on new security vulnerabilities in the technology being used.

- Establish a workable and reliable change control process with event logging and reporting procedures to ensure that updates are made in a safe and timely manner.

- Monitor the list of the currently available service packs and hot-fixes on the web sites of product vendors to ensure that the most recent versions are in use.

- Test hot-fixes before installation.

17.3.2.12.3 Change management

- Document the change management process and ensure that its scope is clearly understood.

- Establish a formal mechanism for identifying the security impact of changes and ensure that this is evaluated by a qualified individual.

- Implement an approval process, clearly identifying the sign-offs required for changes to take place.

- Record all controlled changes in a comprehensive and consistent manner.

- Ensure contingency plans are prepared

17.3.2.12.4 Security monitoring

- Conduct regular and frequent checks to ensure web site components continue to adhere to the agreed configuration standards required for security.

- Carry out a 'baseline review' before a web site is initially connected to the Internet and compare subsequent reviews with this baseline to detect changes.

- Check that web site components are not vulnerable to newly emerging threats.

- Conduct active 'penetration' testing to simulate external attacks on web sites.

- Use automated tools to support monitoring where possible.

17.3.2.12.5 Event logging

- Develop an audit/event logging procedure that preserves the integrity of logs by taking the following points into consideration:

- Routinely back up all logs to a directly attached device

- Keep logs (and spool directories) on dedicated disk partitions to reduce the effect of them filling up the rest of the system
- Use drop-safe logging, where the audit/event records are transmitted from the host to a dedicated PC via a serial link or to protected media such as a WORM disk
- Use the publicly available TCP wrapper software to provide detailed logs, for example of connection requests received by the bastion host
- Determine what action should be taken when the capacity of the logs has been reached: for example,

Schedule frequent checks of disk usage and automatically page the administrator when the device is approximately 90% full.

In extreme cases, it may be desirable to halt the entire system to avoid unlogged activity. However, this action will make the system vulnerable to deliberate denial of service attacks.

What Information needs logging-in

- Log-on and log-off success and failure
- Restart, shutdown and system success and failure
- Security policy changes success and failure
- User and group management success and failure
- File and object access success and failure
- Use of user rights success and failure
- Departures from 'normal' usage patterns such as: System load at different times of the day
- Number of processes running
- CPU utilisation
- Unusual successes/denials of connections
- Success and error messages from both Firewall/ UTMs
- Multiple access attempts

- Access to unusual ports.

17.3.2.12.6 Intrusion detection/ prevention

Implement an intrusion detection/ prevention process adopting the following principles:

- Use a respected commercial package that is regularly updated to keep up with new vulnerabilities and attacks

- Keep the intrusion detection/ prevention tool up-to-date by applying the latest patches and attack signatures

- Run the absolute minimum of services on the platform hosting the intrusion detection/ prevention tool

- Do not allow the platform's interface to be visible to the perimeter networks being monitored

- Establish an administration and reporting network for the intrusion detection/ prevention system that is isolated from the internal network

- Do not place too much reliance on the intrusion detection/ prevention tool and ensure other security procedures are in place.

17.3.2.12.7 Incident Management

- Incident Management for Internet Banking would be as per the policy described above.

CHAPTER - 18

This chapter outlines the mechanisms of handling incidents, classifying the severity of incidents, the reporting and the response mechanisms.

18 Incident handling

The Bank should have in place a strong Information Security set up which should monitor the implementation of the various Information Security norms and guidelines on a regular basis. There should be periodic analysis of the various logs to detect deviations, if any, and to look for possible breaches /

Pithoragarh Zila Sahkari Bank Ltd. Pithoragarh

violations.

18.1 Incident

A computer security incident is defined as: "A real or potential violation of an explicit or implied security policy." An incident may relate to any one of the following:

- Suspected hacking attempts
- Successful hacking attempts
- Loss of information due to unknown reasons
- Hardware resources and components lost/stolen
- Virus incidents regarding e-mail, Internet, CD, diskette and others
- Threat to Physical Safety of human beings.
- Attacks originating from Bank's network.
- Threats, harassment, and other criminal offences involving individual user accounts.
- Compromise of individual user accounts on multi-user systems.
- Forgery and misrepresentation, and other security-related violations of local rules and regulations.
- Compromise of Desktop Systems.

The incidents can be categorized into five types based on the results of the incident:

- Increased access
- Disclosure of information
- Corruption of information
- Denial of service
- Theft of resources

In practice, actual incidents often fall into multiple categories. For example, web site defacement involves (at least) increased access and corruption of information; a system compromise involves (at least) increased access, disclosure of information, and theft of resources. The purpose of incident response is risk mitigation; at the point that an incident or potential incident is identified; these actions are intended to minimize damage and exposure, and facilitate an effective recovery. Within the risk mitigation goal, incident response has a hierarchy of priorities:

1. Human life and safety
2. Sensitive or mission-critical systems and data
3. Other systems and data
4. Damage to systems or data
5. Disruption of access or services

18.2 Documentation and formal reporting:

A person designated by department head should maintain the central database of all such incidents. The person so designated, after analysing the extent of exceptions and facts of the incident, should appraise the related IT department personnel. A detailed risk and impact analysis for the incident should be carried out by the IT team. The IT department should ensure that all incidents are categorised based on the nature of each incident and are held in a database created for the purpose. The database should be able to provide information on demand and should have the capability to perform analysis on the data contained within. The bank's employees encountering incidents would thus be able to access the incident database and possible find solutions if the incident had occurred before. Frequently asked questions should also be incorporated into the database to assist the user in finding solutions to incidents encountered; such incidents should also be reported.

All the incidents should be reported through branch/ office head to immediately higher office, having ZISO/ ISA/ CISO and in turn it has to be forwarded to IS Cell, HO. The classification of Incidents as per IS Cell, HO should be the final in all cases and a database should be maintained there, to refer the cases at any point of time. All critical nature of incidents should be escalated simultaneously to CISO to ensure effective monitoring, immediate attendance and for avoidance of the spread of the same incident to other systems.

18.3 Monitoring:

All the major incidents should be reviewed and monitored by the Security Administrator and discussed in the Technology Committee meeting every month. The magnitude and critically of the incidents may prompt the GM-IT to discuss and take action on the incidents immediately instead of at fixed intervals.

18.4 Development of corrective action plan:

The IT department, in consultation with effected System Administrator or any other person it deems fit should prepare the corrective action plan for the incident. The action plan, though specific to each case, should typically cover the following:

- Facts and explanation/reasons for the incidents
- Corrective action to be taken
- Estimated cost of implementing the corrective action
- Estimated time frame, start date and end date
- Personnel responsible for taking the action.

18.5 Information exchange with other Incident Handling teams:

The IT department can share information with other incident management teams and general public. The following information will not be released for general public:

- Private user information about particular users, or in some cases, particular applications, which should be considered confidential for legal, contractual, and/or ethical reasons. However, if the identity of the user is disguised, then the information can be released freely (for example to show a sample, cshrc file as modified by an intruder, or to demonstrate a particular social engineering attack).

- Intruder information is similar to private user information, but concerns intruders. While intruder information, and in particular identifying information, will not be released to the public (unless it becomes a matter of public record, for example because criminal charges have been laid), it will be exchanged free with system administrators and tracking an incident.
- Private site information of the technical nature except with explicit permission of the site in question.
- Embarrassing information includes the statement that an incident has occurred, and information about its extent or severity.
- Any information that has been classified as confidential or restricted.

18.6 Classification of incidents

Depending on the impact of the incidents on the business processes/ IT Assets or reputation of Bank or it' staff/ associates/ customers, the incidents can be classified as Major, Minor and Ignorable.

18.6.1 Major

- Deliberate violation of Information System Security Policy

- Any violation which has impact on customer service

- Violation by the third Party
- Violation resulting in financial loss
- Violation which has either resulted in the loss of reputation or has the potential for reputation loss risk.
- Violation by staff/officers of IT Department/Data Centres
- Violations having legal/regulatory implication
- Affecting the critical assets
- Any type of loss/ damage/ disappearance/ stealing/ unauthorized access, usage or alteration (addition/ modification/ deletion) to Bank's IT Assets or in IT Assets kept in Bank's premises with Bank's proper consent.

- Any sort of security attack or IS Incident of this nature in Bank's network or in IT Assets.
- Unauthorized use of other's user-ID and password.
- Careless handling of Bank's confidential and sensitive data/ systems or spreading/ leakage of the same to unauthorized/ unintended persons.
- Incidents occurred due to software/ hardware limitation.
- Incidents caused due to lack of knowledge/ human errors leading to reputation loss.
- Not reporting an incident.

The bank may include other incidents depending on the need and the evolving scenario.

18.6.2 Minor

Incidents of the following nature, which may not be classified in other two categories of Incidents i.e. 'Major' and 'Ignorable' –

- The first time violations
- Violations in standalone system not falling in Major Category

Any other incident as described by the bank from time to time.

18.6.3 Ignorable

- First time violation not resulting in financial or monetary loss.
- Violation in the stand-alone system not resulting in financial or reputation loss.

Any other incident as described by the bank from time to time.

18.7 Incident response process

- All the incidents should be reported to the appropriate officials in the prescribed format.
- The first hand reporting should be done from the source by the user/ person who notice it.

- Failure to report an incident is itself an incident and categorised as major security breach.
- At Branch/ Office level, the incident should be reported to the Branch Manager/ Office Head, who in turn will report it to the CISO at IS Cell, Head Office through respective ZISO/ ISA.
- At Controlling Offices, the incidents should be reported to CISO at IS Cell, Head Office respective ZISO/ ISA.
- The Incidents at Head Office/Data Centre should be directly reported to CISO.
- The Incidents which are categorised, as "Ignorable" should not be reported to CISO but a monthly statement of Ignorable incidents should be reported to CISO. In case the incidents are not categorised at the source it should be sent to CISO.
- CISO will finally categorise the incidents as Major/Minor/Ignorable and initiate actions as appropriate.
- If required the Incidents can only be escalated to third parties by the CISO.
- CISO should maintain a database of Incidents reported and action taken for future reference.
- The original evidences of the incidents would be stored at the source and the copy at the IS Cell, Head office .The period of storage etc. would be decided as required from time to time.

18.8 Levels of Escalation:

Level One

Escalation Level One is the initial level for all incidents. The contacts at this level should have the ability to call at the earliest to action engineers and to escalate to management as required, to resolve all categories and severity of incidents.

Level Two

Escalation Level Two represents the next level of management. Escalation to this level is appropriate only when Level One interaction has failed to result in resolution and further action transcends the authority of Level-One staff.

Level Three

Escalation Level Three represents senior management with authority to take actions that fall outside the standard operating policies of the concerned organizations. Escalation to Level Three is appropriate in cases where Level-One and Level-Two interactions have been unsuccessful in resolving an operational issue.

Points of Contact:

Point-of-contact information is required for each escalation level defined above. Telephone numbers and email addresses are required for each level. Information regarding appropriate protocols and methods for reliably making contact with each level should also be provided by the concerned organizations, including mobile numbers, primary and alternate contacts, and information regarding preferred time windows, as appropriate.

The contact information will be shared only among those providers who are members of Computer Incident Response Team and who have subscribed to the process documented herein.

CHAPTER - 19

This chapter outlines the mechanism of establishing business continuity and the planning for Disaster recovery.

19 Business Continuity and Disaster Recovery Plan

One of the main reasons for having a Contingency Plan is self-preservation of the organisation. With the large complex computer infrastructures of today's information systems, it is simply a matter of time before they will experience some kind of disruption event. Whether it is a disruption due to natural, technological, or human causes, pulling out a management-approved plan that outlines actions to be taken makes managing the event easier. As a result, many organisations focus time and effort on trying to predict when these types of events will occur and how to manage them, thus generating a Contingency Plan.

The three hierarchical functions to Contingency Planning are Business Continuity Planning, Disaster Recovery Planning, and Emergency Management Planning. The break-down of these functions is based on the role they play within Contingency Planning. Although most organisations address all three functions in one plan or document, it is important to recognise that each serves a different function. In order for a Contingency Plan to be complete, all three functions must be addressed.

"Business Continuity Planning is a function of the entire organisation". In the event of a complete disaster, this function provides for the survival of the organisation by outlining the thought process and overall goals of the entire organisation's Contingency Plan. It is used to help identify critical large-scale or corporate-wide vulnerabilities and to help determine how to mitigate and resume business operations.

While the Business Continuity Planning function serves to define actions and goals in a broad setting, the Disaster Recovery Planning function defines the actions and goals of each business unit or department. By having each business unit or department focus on its specific needs in preparation for and during a disaster, the recovery process can be achieved more efficiently. For example, the IT department will need servers and tape drives rather than the keys, security logs, and access cards and other supplies needed by the Facilities and Security department, all of which is critical to the return of normal business operation. It is the responsibility of each department to define the critical materials necessary to continue operation, and the responsibility of management to ensure that all of the departments' needs and concerns have been addressed.

Emergency Management Planning is the function of preparing for, mitigating, responding to and recovering from an emergency. In other words, this is the action plan. To accomplish the goals of the Business Continuity and Disaster Recovery Plan, a process must be built upon the internal level of emergency management capabilities within the organisation, and address all types of disasters, phases of management, and necessary participants (the who, what, where, and how of the plan).

A business continuity management process should be implemented to reduce the disruption caused by disasters and security failures to an acceptable level through a combination of preventive and recovery controls. The consequences of disasters, security failures and loss of service should be analysed. Contingency plans should be developed and implemented to ensure that business processes can be restored within the required time frame.

Bank should have Business Continuity Plans taking into consideration the following points:

- The conditions for activating the plans which describe the process to be followed (how to assess the situation, who is to be involved, etc.) before each plan is activated;
- Emergency procedures, which describe the actions to be taken following an incident, which jeopardises business operations and/or human life. This should include arrangements for public relations management and for effective liaison with appropriate public authorities e.g. police, fire service and local government;
- Fall back procedures which describe the actions to be taken to move essential business activities or support services to alternative temporary locations and to bring business processes back into operation in the required time-scales;
- Resumption procedures which describe the actions to be taken to return to normal business operations;
- A maintenance schedule which specifies how and when the plan will be tested and the process for maintaining the plan;
- Awareness and education activities which are designed to create understanding of the business continuity processes and ensure that the processes continue to be effective;
- The responsibilities of the individuals, describing who is responsible for executing which component of the plan. Alternatives should be nominated as required.

19.1 Business Continuity Management Process

There should be a managed process in place for developing and maintaining business continuity throughout the organisation. It should bring together the following key elements of business continuity management.

- Understanding the risks the organisation is facing in terms of their likelihood and their impact, including an identification and prioritisation of critical business processes;
- Understanding the impact which interruptions are likely to have on the business (it is important that solutions are found that will handle smaller

incidents as well as serious incidents that could threaten the viability of the organisation) and establishing the business objectives of the information processing facilities;

- Considering the purchase of suitable insurance which may form part of the business continuity process;
- Formulating and documenting a business continuity strategy consistent with the agreed business objectives and priorities;
- Formulating and documenting business continuity plans in line with the agreed strategy;

Business continuity should begin by identifying the events that can cause interruptions to business processes e.g. equipment failure, flood and fire. This should be followed by a risk assessment to determine the impact of those interruptions (both in terms of damage scale and recovery period). Both of these activities should be carried out with full involvement from owners of business resources and processes. This assessment considers all business processes and is not limited to the information processing facilities. Depending on the results of the risk assessment, a strategic plan should be developed to determine the overall approach to business continuity.

19.2 Considerations of What to Include in a Contingency Plan

Starting a plan can be difficult, but it is helpful to keep the following things in mind (this is just a list to start the thought process; other items can be added):

19.2.1 Purpose of the Plan

States the purpose of having a Contingency Plan and how it fits into the normal operations of the organization.

19.2.2 Priority of Life Statement

Includes a Priority of Life statement. Safety and wellbeing of the employees are the most important aspects of the organization.

19.2.3 The Hazard or Disaster Identification

Provides for identification of the potential hazards that could affect the organization. If an office is located in the Sahara Desert, then planning for flooding isn’t as critical as contamination of the water supply.

19.2.4 Business Impact Analysis

Outlines the potential financial, data, and communication losses that will occur if the network is down for 24 hours, 48 hours, and 72 hours. This shows management the "bottom-line" impact of these losses and how planning can reduce these costs. Indirect costs should not be ignored.

19.2.5 Prevention Strategies

Outlines the policies and procedures to be followed to prevent normal events from jeopardising the ability of the organization to perform its mission.

19.2.6 Critical Applications and Structure of the Network

Provides information on the why, what, and where of the organisation’s network. The areas addressed will be why the network is important, what the main purposes of the network are, and how the network is physically structured.

Identifies all applications that are critical for the organization to perform its mission, as well as applications that are critical for data recovery.

19.2.7 Responsibility, Notification, Authority, And Approval Of Funds

Provides detail information on whom of the plan. Answers questions such as: Who is responsible for the action that need to occur; who is going to notify everyone in the organization; and who has the authority to declare a disaster or disperse funds for emergency operation.

19.2.8 Writing and Implementing Business Continuity Plan

Outlines the policies and procedures to be followed in case an event occurs which jeopardizes the ability of the organization to perform its mission.

Plans should be developed to maintain or restore business operations in the required time scales following interruption to, or failure of, critical business processes. The business continuity planning process should consider the following:

- Identification and agreement of all responsibilities and emergency procedures;
- Implementation of the emergency procedures to allow recovery and restoration in required time-scales. Particular attention needs to be given to the assessment of the external business dependencies and the contracts in place;
- Documentation of the agreed procedures and processes ;
- Appropriate education of staff in the agreed emergency procedures and processes including crisis management;
- Testing and updating of the plans.

19.2.9 Testing the Plans

Outlines the testing of the plan, the policies and procedures to be followed, the purpose and scope of the testing, and the frequency of the tests to be conducted.

Business continuity plans may fail on being tested, often because of incorrect assumptions, oversights or changes in equipment or personnel. They should, therefore, be tested regularly to ensure that they are up to date and effective. Such tests should also ensure that all members of the recovery team and other relevant staff are aware of the plans. The test schedule for business continuity plans(s) should indicate how and when each component of the plan should be tested. It is recommended to test the individual components of the plans(s) frequently. A variety of techniques should be used in order to provide assurance that the plan(s) will operate in real life. These should include:

- Table-top testing for various scenarios (discussing the business recovery arrangements using example interruptions) ;
- Simulations (particularly for training people in their post-incident/crisis management roles);

- Technical recovery testing (ensuring information systems can be restored effectively);
- Testing recovery at an alternate site (running business processes in parallel with recovery operations away from the main site) ;
- Tests of supplier facilities and services (ensuring externally provided services and products will meet the contracted commitment); and
- Complete rehearsals (testing that the organization, personnel, equipment, facilities and processes can cope with interruptions).

19.2.10 Maintenance and Re-assessment of the Plans

Addresses how revisions, updates, and maintenance of the plan occur. Once developed, the plan should be a living, breathing entity, which is under constant review and updates. If the maintenance falls short, the plan will be ineffective and obsolete.

Business continuity plans should be maintained by regular reviews and updates to ensure their continuing effectiveness. Responsibility should be assigned for regular reviews of each business continuity plan. The identification of changes in business arrangements, not yet reflected in the business continuity plans, should be followed by an appropriate update of the plan. This formal change control process should ensure that the updated plans are distributed and reinforced by regular reviews of the complete plan. Consideration should be given to the possibility of degradation of media used for storage of records. Storage and handling procedures should be implemented in accordance with manufacturer's recommendations.

19.2.11 Training

Includes policies and procedures for training organisations employees, managers, vendors, and emergency response personnel. The frequency of training and retraining, the degree of information needed, and the methodology used will all be covered.

19.2.12 Appendices

Includes appendices that should be indexed and cross-referenced, with the use of graphics and flow charts encouraged when possible. All lists should be updated with current information on a regular schedule. This would include the inventory of people.

CHAPTER– 20

20 Security Awareness and Training

- Delivering awareness programme to permanent staff
- Third Party Contractor: Awareness Program
- Providing regular Information updates to staff

20.1 Delivering Awareness Programme to Permanent Staff

Permanent staff is to be provided with Information security awareness tools to enhance awareness and educate them regarding the range of threats and the appropriate safeguards

Information security issues to be considered when implementing the policy include the following

- Sensitive data may be acquired unlawfully, damaged or modified because staff have become complacent
- Sensitive data may be compromised by staff assuming new duties without specific Information security Training.

20.2 Third Party Contractor: Awareness Program

An appropriate summary of the Information security policy must be formally delivered to any such contractor prior to any supply of services.

20.3 Delivering Awareness Programme to Temporary Staff

An appropriate summary of the Information security Policies must be formally delivered to, and accepted by, all temporary staff, prior to their starting any work for the organization.

20.4 Providing Regular Information Updates to staff

The organization must provide regular and relevant Information security awareness communications to all staff by various means, such as electronic updates through Intranet, briefing, Newsletters etc.

20.5 Training

- Information security Training on new systems
- Information security Officer Training
- User Information Security Training
- Technical staff Information Security Training
- Training new recruits in Information security
- Training for Information system auditors

20.5.1 Information Security Training on new systems

The organization must provide training to all users of new systems to ensure that their use is both efficient and does not compromise Information security

The Information security Issues to be considered when implementing the policy include the following

- Confidential data may be lost, damaged or compromised by staffs that are unfamiliar with the new systems.
- Data may be lost because the new Information security systems are installed incorrectly, a and their alarms and messages are misinterpreted

20.5.2 Information Security Officer: Training

Periodic Training of officers posted in the Information security Department must be priories to educate and train them in the latest threats and Information security techniques.

The security issues to be considered when implementing the policy are as follows:

- Organization's Information security measures can be compromised by new virus software or techniques unknown to Information security team
- Essential data may be lost or compromised because the Information security

team implements inappropriate measures.

20.5.3 User-Information security Training

Individual training in Information security is mandatory, with any technical training being appropriate to the responsibilities of the user's job functions. Where staff change jobs, their information security needs must be re-assessed and new training provided as a priority.

20.5.4 Technical staff: Information Security Training:

Training in information security threats and safeguards is mandatory, with the extent of technical training to reflect the jobholder's individual responsibility for configuring and maintaining Information security safeguards. Where IT staff change jobs, their Information security needs must be re-assessed and any new training provided as a priority

20.5.5 Training new recruits in Information security:

All new staff /recruits must receive mandatory Information security awareness training as part of induction.

20.5.6 Support/ Help Desk:

The primary purpose of the help desk is to service the user. The help desk personnel must ensure that all hardware or software problems that arise are fully documented and escalated based on the priorities established by procedure

The basic function of the help desk is to perform the following –

- Document problems that arise from users and initiate problem resolution.
- Prioritize the issues, and forward them to the appropriate managers, accordingly.
- Follow up on unresolved problems.
- Close out resolved problems noting proper authorization to close out the problem by the user.
- Determine whether the number of personnel assigned to each shift is adequate to support the workload.

20.6 Desktop Policy:

Desktop screen should contain minimum required folders, files and shortcuts so that desktop screen is clearly visible and icons are not cluttered. After completing work on folders/ files or shortcuts, kept on the desktop, the same should be moved to appropriate folders so that again enough free space is created on the desktop to accommodate fresh set of urgent folders/ files/ shortcuts.

- There should be only required papers on the desk and tables neat & clean.
- There should not be any writing/ pasting on table tops, counter panel regarding user id and password, any other confidential information which may breach security, guidelines etc.
- Wall paper and screen savers used should be tested to be free from virus/ Trojan horse/ spyware etc., decent and should be preferably supplied along with the operating system/ or provided by the Bank.
- Users should take good care of systems, media, facilities and peripherals provided by the Bank and should strictly observe security guidelines in this regards.
- Information available through desktop computers/ attached media or peripherals to any user should be only on the basis of need to know.

CHAPTER - 21

This chapter specifies the controls related to Intellectual Property Rights.

21 Intellectual Property Rights

To minimize concerns over the intellectual property rights to software, a written policy on Intellectual property rights should be adopted. The employees and the contractors involved in the development of the software should be made aware of this policy.

21.1 Copyright

Appropriate procedures should be implemented to ensure compliance with legal restriction on the use of material in respect of which there may be intellectual property rights such as copy right, design rights or trade mark. Copyright infringement can lead to legal action, which may involve criminal proceedings. Legislative, regulatory and contractual requirement may place restrictions on the copying of proprietary material. In particular, they may require that only material that is developed by the organization or that is licensed or provided by the developer to the organization can be used.

21.1.1 Software Copyright:

Proprietary software products are usually supplied under a license agreement that limits the use of the products to be specified machines and may limit copying to the creation of back-up copies only. The following controls should be considered.

- Issuing standards for the procedures for acquisition of software products
- Maintaining awareness of the software copyright and acquisition policies and giving notice of the intent to take disciplinary action against staff that breaches them.
- Maintaining appropriate asset register
- Maintaining proof and evidence of ownership of licenses, master disks, manuals etc.

- Implementing controls to ensure that any maximum number of users permitted for using the software is not exceeded
- Carrying out checks that only authorized software and licensed products are installed
- Providing a policy for maintaining appropriate license conditions
- Providing a policy for disposing of or transferring software to others
- Using appropriate audit tools;
- Complying with terms and conditions for software and information obtained from software vendors and public networks and
- Network management software or server management software should be used to detect unauthorized software in the network

CHAPTER - 22

This chapter specifies the policies related to IS Audit.

22 Information System Audit

22.1 Need for Information system Audit

Assets safeguarding, data integrity, system effectiveness and system efficiency can be achieved only if an organization's management sets up a system of internal control. While the traditional components of internal control viz. separation of duties, clear delegation of authority and responsibility, recruitment and training of high-quality personnel, a system authorisation, Independent check on performance have to be present in an Information system –may be in a different way-there must be an on going process in the organisation by which an independent individual/department accumulates and evaluates evidence…for the purpose of reporting between quantifiable information and established criteria. Hence there is a need for Information system audit.

22.2 Audit Charter

The responsibility, authority and accountability of the Information system audit function should be well defined. Both internal and external audit, require to be appropriately documented in an audit charter or engagement letter, defining the responsibility, authority and accountability of the IS Audit function. The IS auditor will have to determine how to achieve the implementation of the applicable IS Audit standards, use professional judgement in their application and be prepared to justify any departures there-from.

22.2.1 Contents of the Audit Charter

The audit charter should clearly address the three aspects of responsibility, authority and accountability of the IS auditors.

22.2.2 Who should conduct the IS Audit

The Top Management's document should clearly state about who should conduct the IS Audit. As the conduct of IS Audit is a specialised job and the bank do not have sufficient CISA / CISSP professionals in-house, to start with the IS audit function should be conducted by an outside agency having CISA / CISSP professionals along with Bank's internal Auditors till the in-house staff equip

themselves with requisite qualifications / experience. The prescription of the regulators should be strictly followed in deciding about who should conduct the IS Audit. In any case Auditor should be independent of the auditee.

22.2.3 Periodicity of the Audit

The periodicity of the audit should be based on the riskiness of the area/branch/process. Usually in fully computerized branches it should be once in a year .The Network penetration test etc should be done in more frequent intervals. The risk should be classified into High risk, Medium risk and Low risk. The High risk branches should be audited frequently i.e., at least once in Nine months, Medium risk branches at least once in a year and Low risk branches at least once in Fifteen months.

When a branch is computerized from manual system, migrates from one platform to another platform or one software to another software, the IS Audit should be conducted within Six months.

22.2.4 Independence

In all matters related to auditing, the information systems auditor is to be independent of the auditee in attitude and appearance.

22.2.5 Organizational Relationship

The information systems audit function is to be sufficiently independent of the area being audited to permit objective completion of the audit.

22.2.6 Competence

22.2.6.1 Skills and Knowledge

The information systems auditor is to be technically competent, having the skills and knowledge necessary to perform the auditor's work. The knowledge of these auditors needs to be updated regularly. The bank should provide adequate training facilities to the IS Audit team to conduct audits effectively. The IS Auditors should exchange their views and share their experiences internally.

22.2.6.2 Continuing Professional Education

The IS auditor is to maintain technical competence through appropriate continuing professional education. - - should encourage officers in IS Audit department to acquire professional qualifications viz. CISA and CISSP by reimbursing course fee, annual maintenance fee, Registration fee, Examination fee and paying honorarium.

22.2.7 Planning

22.2.7.1 Audit Planning

The information systems auditor is to plan the information systems audit work to address the audit objectives and to comply with applicable professional auditing standards.

22.2.8 Performance of Audit Work

22.2.8.1 Supervision

Information systems audit staff are to be appropriately supervised to provide assurance that audit objectives are accomplished and applicable professional auditing standards are met.

22.2.9 Evidence

During the course of the audit, the information systems auditor is to obtain sufficient, reliable, relevant and useful evidence to achieve the audit objectives effectively. The audit findings and conclusions are to be supported by appropriate analysis and interpretation of this evidence.

22.2.10 Reporting

22.2.10.1 Report Content and Form

The information systems auditor is to provide a report, in an appropriate form, to intended recipients upon the completion of audit work. The audit report is to state the scope, objectives, period of coverage, and the nature and extent of the audit work performed. The report is to identify the organization, the intended recipients and any restrictions on circulation. The report is to state the findings, conclusions and recommendations and any reservations or qualifications that the auditor has with respect to the audit.

22.2.11 follow-up Activities

22.2.11.1 follow-up

The information systems auditor is to request and evaluate appropriate information on previous relevant findings, conclusions and recommendations to determine whether appropriate actions have been implemented in a timely manner.

22.2.12 Compliance Audit

An organization’s operations are subject to a variety of laws and regulations. Violation of these laws and regulations would result in imposition of huge fines and penalties. Compliance with these laws and regulations is monitored by the regulatory authorities through Compliance Audit.

Compliance of audit (viz. IS Audit) of the computerised environment is a difficult and complicated task. There has to be a systematic examination of the environment/ programs/ networks/ data/ transactions etc, at least a reasonable sample thereof, to understand the various issues involved. A complex maze of laws, regulations and audit rules will require to be considered under Compliance Audit. Any version change or change of application and data migration should also be subject to Audit.

IS Audit Compliance follows a three-phase-audit route –

1. **In the planning phase or the first phase of Compliance Audit**, the various

applicable rules, regulations, laws, regulatory fiats etc. will require to be studied and noted down. Appropriate tests, which may verify compliance with these rules, regulations, laws and regulatory fiats, will require to be decided and planned.

2. **In the test/control phase or the second phase of Compliance Audit**, the tests, as planned in the first phase, will require to be carried out and the compliance therewith observed. Variations/exceptions/violations will require to be noted down for mention in the audit report.

3. **In the last phase of Compliance Audit**, a sample of transactions should be tested in detail for compliance.

Compliance with various statutory guidelines, legal and regulatory guidelines and adherence to trade practices and conventions require to be thoroughly tested under Compliance Audit.

CHAPTER – 23

This chapter specifies the mechanism of policy review.

23 Policy Review

Technology is dynamic so also the vulnerabilities and threats so it is always desirable for the Management to review the security document annually or as and when there is deployment of new technology having different risk perception.

In any case, the IT security policy needs to be reviewed periodically, say, once a year, or if necessitated, by the working group on Information Security (to be set-up by the Bank). Some of the major factors that can influence the review of the policy are as follows:

- Emergence of new technology and its applicability to the Banking requirements;
- Vulnerabilities discovered in the existing technology;

- Any regulatory requirement;

- Any legal requirement.