Rajasthan Marudhara Gramin Bank

Information Technology Service Department
Head Office, Jodhpur

87

Information Technology (IT) Policy
Standards and Procedures

Version	**7.0**
Date of Adoption	22 OCT 2024
Renewal Frequency	**Annually**
Last Review Date	**29.12.2023**

Rajasthan Marudhara Gramin Bank

ITSD

A. Objective of IT Policy

The objective of the IT Policy is to set the guiding principles for establishing IT operational procedures and at the same time to achieve Confidentiality, Integrity and Availability of the information and information systems used by those IT Operations.

B. Document Distribution

This document is owned by RMGB's General Manager (IT).

C. Primary recipients

All Employees of the Bank

D. Authority

IT Policy & Standards shall be reviewed at least annually by the GM and any amendments to the plan shall be approved by the Board of the Bank.

E. Standards & Procedures

Standards are detailed requirements that need to be met for complying with the IT Policy & IS Security policies. Separate set of standards have been developed for each policy statement. Standards include measures that need to be taken for mitigating all risks associated with the respective domain covered by the policy statements. Procedures are detailed guidelines of how to implement the measures and who should be responsible for the implementation.

F. Objective

The key objectives of developing Standards and Procedures are:

F.1. To ensure that IT Policy is interpreted correctly and uniformly across the Bank.

F.2. To provide guidelines for implementation of the policies.

F.3. To create awareness about policies and assist in policy compliance.

G. Scope

These policies & security standards are applicable to all locations of BANK within India

including all IT assets, all IT processes, all business processes supported by IT and all employees of the Bank.

H. Management of IT Policy

GM shall review and approve the IT Policy and Standards for further approval of Board of the Bank. GM shall assist ITSD in framing, review of the policy, dissemination and enforcing of approved IT Policy & Standards and related activities in the Bank. IT Policy & Standards shall be reviewed at least annually by the GM and any amendments to the plan shall be approved by the Board of the Bank. ITSD shall assist GM-IT in performing his responsibilities towards IT subcommittee and Information Security.

I. Responsibilities

I.1. The IT Sub Committee of Bank is responsible for approving the standards and procedures and approving any subsequent modifications for achieving desired level of information system security in line with Business Requirements.

I.2. The IT Sub Committee is responsible for ensuring that standards and procedures are current and reflect the requirements of the Bank with the help of ITSD.

I.3. Controllers/Application Owners/Dept. Heads/Heads of all branches are responsible for implementing and enforcing the relevant portions of the standards and procedures within their jurisdiction.

I.4. ITSD is also responsible for dissemination of the standards and procedures.

I.5. Inspection & Management Audit Dept. is responsible for auditing the level of compliance with the standards and procedures.

J. Compliance

The Bank expects all employees and authorized external personnel including vendors to comply with these standards and procedures. Failure by any employee of the Bank to conform to applicable standards & procedures may result in disciplinary action. Vendors shall be dealt with according to the contracted covenant.

K. Exception

Exceptions or deviations from the policy, standards, procedures & guidelines will be processed as follows:

Approving Authority: CISO

Exception Criteria: The following criteria will be used

a) Existence of a genuine need for exception
b) Adequacy of compensating controls

Workflow: Head– IT will assess and submit all requests with his recommendations to the CISO.

Registration & Tracking: All such requests will be registered, tracked and submitted for subsequent review to CISO through IT Head.

Duration, Expiry & Review: All Exceptions or Deviations, when approved, should be for a minimum period and the period should not exceed ONE YEAR in any case in one instance. Any extension requests should be reviewed and assessed again before expiry of the approved period as per the same workflow & criteria mentioned above.

L. Review

ITSD will review this policy and standards and procedures every year, based on user inputs, independent review reports, compliance reports or new risk exposure and propose changes wherever required. ITSD will also review and propose changes to the standards and procedures when significant security breaches / incidents occur in the Bank and based on applicable legal and regulatory requirements.

IT Policy

Table of Contents

1 Software Development

1.1 Policy Statement

1. 1. 1 All software developed or customized for use by the Bank should follow a standard development process to ensure it meets functional, security and performance requirements. Adequate controls in software development process should be built to address risks in meeting functional and security requirements of the Bank, in regulatory compliance, in timely completion and in meeting performance requirements.

Standards and Procedures

1.2 Applicability

1. 2. 1 This policy applies to software development under the following categories-

- New product development
- Customization of a product in terms of adding new functionality or changing its functionality
- Integrating new modules to existing product

1. 2. 2 Customization of existing report formats or generating new report formats, or any other minor customization to existing product may follow only the maintenance section of this policy.

1. 2. 3 While procuring software or outsourcing its development, relevant portions of this policy will be applicable.

1.2.4 All CBS existing products to be reviewed periodically and old and redundant products to be deleted/ blocked.

1.2.5 In house development of Non CBS software for deployment in RRB to be encouraged and reviewed periodically.

1.3 Identification and Feasibility study

1. 3. 1. Any software development request should be based on the genuine business requirement and should be put forth by the departments of the bank like CM(P&D), CM(CREDIT), CM(Recovery), CM(FI), CM(ACCOUNTS), CM(I&A) etc. The requestor shall submit a formal proposal providing the objectives to be met and expected benefits obtained by the solution.

1. 3. 2 On receiving the request, CM IT department will conduct a feasibility study. The feasibility study should include:

1.3.2.1 Current deficiencies, expected benefits and functional requirements to be provided by the software solutions in terms of what will be the input and output solutions user base, Interdependency with other systems and performance indicators. Further the available applications are to be critically examined whether they can be customized to meet the new request or any alternate readymade products is available in the market, including the estimated cost.

1.3.2.2 After making a careful cost benefit analysis, a decision may be taken to outsource the software development.

1.3.2.3 In case the decision is to buy any product, the user request and the feasibility study report will be the input to procurement committee (as per IT Procurement Policy).

1.3.2.4 In case of outsourced software development or direct software product procurement the requirements of this policy should be applied as relevant.

1.3.2.5 Based on the study the ITS Department should recommend on outsourcing to the sanctioning authority for principle approval.

1.3.2.6 Security Evaluation should be carried out before and after deployment of all applications. In addition to this, code review of critical applications should be conducted by Application Owner in consultation with Information Technology Service Department.

1.3.2.7 The project development team should simulate the target environment. The simulation should be done is such a way that the only difference between the test environment and live environment should be in the fact that the non- production data is used. In cases where exact simulation is not possible, the limitations of the testing should be documented.

1.3.2.8 The Project development team should organize the developed/customized software to be tested by end user(s) for acceptance. The user group representative should be involved in planning test cases for user acceptance testing (UAT).

1.3.2.9 UAT should cover

- Adequacy of the implementation for the requirements specified

- Any changes in the mode of operations after the requirement analysis phase
- Any changes in the statutory/regulatory requirements
- Adequacy of the security controls

1.3.2.10 The Project development team should verify that the latest and tested product components are delivered. This should include compiling the sources with the latest components.

1.4 Post Deployment Review

1.4.2 IT departments should organize a post deployment review within six months of deployment.

1.4.2 Appropriate control measures should be established to ensure that the Intellectual property rights of the software is not comprised/mis-used.

2 IT Outsourcing

2.1 Policy Statement

The risks associated with outsourcing of IT services, software development & business processes must be assessed and managed to an acceptable level and adequate controls should be built to ensure that business requirements of the Bank are met by the outsourced vendor. All outsourcing contracts will detail security requirements and vendor should be able to demonstrate compliance with such requirements.

Standards and Procedures

2.2 Applicability

2.2.1 This policy applies to outsourcing of IT services, software development and business processes. For the purpose of this policy, such activities will be considered as outsourcing if they are of long-term duration (more than six months). Contracting of services for shorter durations (e.g. Product implementation, audits, UAT, IT consultancy and hardware installation), routine activities and annual maintenance contract for hardware/software are not considered as outsourcing.

2. 2. 2 As per RBI Guidelines, all IT Outsourcing have been identified as Material Outsourcing.

2.3 Feasibility study, Materiality Criteria & Risk Evaluation

2. 3. 1 All major outsourcing projects which have Bank-wide usage or impact, shall be taken up by the IT Departments i.e. reporting GM(IT).

2. 3. 2 The Feasibility study should be under taken by the IT Department to analyze the requirements of the departments, the set of activities to be outsourced, the in house capabilities in performing the activity vis-à-vis outsourced vendor in terms of the following:

2.3.2.1 Technical skills – The current in-house skills, the ability to build up skills as well as the future requirement of skills need to be assessed. Certain technology areas might require people to continuously skill up to meet the business requirements. This might involve cost to Bank in terms of Employee training and retention.

There are also technology areas that are sufficiently mature and need only standardized skills for operations and maintenance.

2.3.2.2 Infrastructure– There could be additional infrastructure requirements for delivering the particular activity. It should be analyzed if these investments are in-line with the Bank's long-term strategy or it is better to outsource.

2.3.2.3 Management resources – Domain experts with management skills and experience might be required to manage the IT delivery. It needs to be considered if such talent is available within the Bank and whether developing these skills in-house will provide strategic advantage

2.3.2.4 Financial considerations - The overall cost of outsourcing the solution compared to performing the activity in-house

2. 3. 3 The study should analyze the extent of strategic advantage provided by outsourcing. Some of these can be-

2.3.3.1 Reduce the time to market for any customer service due to faster execution through outsourcing

2.3.3.2 Improved service level or quality of service due to better process/ methodologies available with vendor

2.3.3.3 Increased access to new technology in future and reduced risk of technology obsolescence

2.3.3.4 Flexibility in amount of service depending on uncertainties in future growth

2. 3. 4 The study should consider the broad security risks of outsourcing and assess whether such risks can be controlled or they can be potentially insurmountable. The exact methodologies for mitigating the risks may be worked out later during development of the outsourcing plan. It should also be assessed whether outsourcing the activities creates any reputation risk for the Bank.

2. 3. 5 Risk Evaluation and Measurement

2.3.5.1 Risk evaluation should be performed prior to entering into an outsourcing agreement and reviewed periodically in the light of known and expected changes, as part of the strategic planning or review processes.

2.3.6 Based on the study, the team should provide its recommendation on outsourcing

to the sanctioning authority for in-principle approval. For complex or high value projects, such approval should be given by Competent Authority.

2.3.7 Before outsourcing any activity, Bank should consider level of concentration of outsourced activities with a single service provider and over-dependency due to same, and capabilities of that service provider to deliver the services up to desired level.

2.4 Outsourcing Plan

Once outsourcing has been approved, the Project Sponsor should create an outsourcing plan.

2. 4. 1 The plan should state the objective to be achieved with outsourcing and the expected deliverables, as outlined in the feasibility report.

2. 4. 2 The plan should have a clearly defined scope including key milestones for measuring progress periodically and service levels to be met by the vendor. It should be ensured that management of service levels in outsourced activities and key decision making controls are retained by the Bank in any outsourcing scope.

2. 4. 3 The intended timeframe for outsourcing should be defined. The time frame will influence the procurement procedure in terms of evaluating the financial & operational stability of the vendor.

2. 4. 4 The plan should include the key security controls regarding data viz., confidentiality and availability that need to be considered by procurement committee when choosing the vendor. ITSD should be consulted for determining the security requirements.

2. 4. 5 The plan should cover the necessary steps to be taken for transition of responsibilities from the Bank to the vendor. This will include processes to be mapped, data & system conversion requirements, staffing of personnel and their training requirements.

2. 4. 6 The plan should outline scenarios post the time frame of outsourcing, i.e. how the activities will be transitioned back to the Bank or other vendor in future-

2.4.6.1 From vendor to the Bank-If the services are being transitioned to the internal team, necessary steps should be taken in advance to ensure that the necessary

skills sets are available.

2.4.6.2 To a different vendor- Necessary documentation and handover training needs to be planned in advance.

2.4.7 The plan should be approved by the GM, IT and passed to the procurement committee.

2.5 Vendor Selection

2.5.1 The procurement of outsourcing services will be as per IT Policy of the Bank. The outsourcing plan becomes input for the procurement committee in determining the scope, deliverable, service level and risk controls requirements.

2.5.2 For outsourced software development, the software vendor should be SEI-CMM/ISO 9000 certified

2.5.3 The Bank can consider auditing the operation policies & procedures relevant to outsourced activities of the final short-listed vendors. This can be external third party audit or internal audit by vendor or onsite visit by the Bank's own team. The objective will be to ascertain that operational controls are strong to deliver reliable & accurate service.

2.5.4 The Bank may also consider auditing the security controls of the final short-listed vendors for the risks identified from outsourcing plan. It can be through external parties, vendor's internal Audit report/ assurance or by ITSD.

2.6 Transitional Risks

2.6.1 When activity is being transitioned from the Bank to vendor, the following should be addressed-

2.6.1.1 Vendor has established process & methodologies for performing the service and it has been adequately matched with existing process within the Bank. Outsourced vendor may have superior process for delivery so while mapping the internal process to that of vendor only the key aspects of process should be matched.

2.6.1.2 In case of any ownership of software, hardware, personnel or documents to be assigned to the vendor, it should be documented in the contract and vendor should have processes to execute his custodial responsibilities.

2. 6. 2 When the activity is being transitioned from the vendor to the Bank, following should be addressed-

2.6.2.1 Steps should be taken to ensure adequate knowledge transfer. This will include transfer of skills and operating processes and procedures. This can be achieved through focused training sessions for specific user and System Official groups and detailed documentation.

2.6.2.2 To ensure continuity of service, there needs to be contract with the original vendor for support after transition. It can include technical support on queries; support on process implementation or in case of software a provision for future upgrades.

2.6.2.3 All data relating to the Bank and its customers that are stored at vendor site needs to be transferred. This could include data and documents that have been collected from the Bank and its customers for performing the activity. Archived data that is stored at vendor premises should also be transferred.

2.6.2.4 Access privileges of the vendor to the Bank systems should be removed on transition.

2. 6. 3 In case of outsourced software development, the following should be delivered to the Bank by the vendor

2.6.3.1 All product components

2.6.3.2 Dependent and/or external modules

2.6.3.3 Base documents, which includes, user manual, installation manual, operations manuals, technical manuals, test procedure.

2.7 Security

2. 7. 1 All vendors servicing the Bank should comply with the Bank's IS Security policies in key concern areas relevant to the activity being outsourced. ITSD needs to evaluate the vendor's current policies and practices to understand the level of compliance with the Bank's policies. If there are additional policy areas that are relevant to the activity being outsourced, but not covered by the Bank's policies, ITSD should evaluate the level of security achieved by vendors.

2. 7. 2 Vendor's ability to maintain continuity of services should be assessed against

the level of availability required by the Bank. For lower scale of availability, back up & recovery procedures need to be assessed. For higher levels, the vendor should have business continuity and disaster recovery provisions.

2.7.3 In the case of outsourced software development, following measures need to be taken-

2.7.3.1 Vendor should follow the Software Development Policy of the Bank or vendor has equivalent process to meet the requirements of the Bank's policy

2.7.3.2 Application should meet the security requirements as defined in application security policy of the Bank.

2.7.3.3 As far as possible, the Bank retains the ownership rights of the software including source code. In case this is not possible, adequate measures including software escrow or first right to buy need to be taken to ensure that application software code is available in the event of vendor failure.

2.7.4 While ownership of software, hardware and other assets can reside with the vendor, data ownership should be retained by the Bank and assigned to the Bank personnel.

2.8 Performance

2.8.1 Outsourced activities should have a service level agreement that defines the milestones of delivery, quality & cost metrics of delivery, staffing of personnel and uptime of the service.

2.8.2 The Application Owner will be responsible for controlling and monitoring vendor performance. The performance should be tracked against project milestones and contracted service levels.

2.8.3 For software development outsourcing, the following delivery checks should be carried out before software acceptance. Project Sponsor should designate a team for software acceptance.

2.8.3.1 Application should be tested and certified for security requirements by the team or any other entity independent of the outsourced vendor

2.8.3.2 Load testing of application should be carried out by the team. Alternatively software vendor should produce test results corresponding to production requirements on final version of software

2.8.3.3 User Acceptance testing should be carried out by the team with involvement of user department

2.8.3.4 All project documentation including user manual, operations manuals, technical manuals and test records are received.

2. 8. 4 Periodic formal review of vendor performance against the service level agreement needs to be conducted by the Bank. Review period will depend on length of the contract and criticality of the service. Relevant matrix of the service performed should be generated and for any slippage in service, vendor should initiate action plan for improvement.

2.9 Contractual Terms

2. 9.1 Contracts should be clearly written and sufficiently detailed to provide assurances for performance, reliability, security, protection of Intellectual Property Rights and reporting. Management should consider whether the contract is flexible enough to allow for changes in technology and the Bank's operations. The following key areas need to be addressed in contracts.

2. 9. 2 Legal Aspects:

- Contract should be vetted by Bank's legal Dept. on their legal effect and enforceability. Every such agreement should address the risks and risk mitigation strategies.
- The contract should mention time-frame for support and receiving of required information from service providers, in case of Customer Grievance/Complaints to avoid any legal/ regulatory issues.

2. 9. 3 Scope of Service

2.9.3.1 The contract should clearly describe the rights and responsibilities of parties to the contract including timeframes and activities for implementation.

2.9.3.2 The contracting parties' rights in modifying existing services performed under the contract

2.9.3.3 Guidelines for adding new or different services and for contract re- negotiation

2. 9. 4 Duration

2.9.4.1 The Bank should consider the type of technology and current state of the industry when negotiating the appropriate length of the contract and its renewal periods. While there can be benefits to long-term technology contracts, certain technologies may be subject to rapid change and a shorter-term contract may prove beneficial.

2. 9. 5 Security

2.9.5.1 The contract should document all security requirements identified and agreed upon during evaluation phase for hardware and software services

2.9.5.2 The vendor should report to the Bank when material intrusions occur, the effect of the intrusion on the Bank, and corrective action to respond to the intrusion.

2.9.5.3 The contract should address the vendor's responsibility for backup and record protection, including equipment, program and data files, and maintenance of disaster recovery and contingency plans.

2.9.5.4 The vendor should provide the Bank with operating procedures the vendor and the Bank are to implement in the event of disaster, including recovery and contingency plans.

2.9.5.5 Contracts should include specific provisions for business recovery time frames that meet the Bank's business requirements.

2.9.5.6 The Bank should ensure that the contract does not contain any provisions that would excuse the vendor from implementing its contingency plans.

2. 9. 6 The contract should include provisions for addressing control over operations such as:

2.9.6.1 Internal controls to be maintained by the vendor

2.9.6.2 Compliance with applicable regulatory requirements.

2.9.6.3 Compliance with IPR of software / modules used and indemnity to the Bank for IPR violations.

2.9.6.4 Records to be maintained by the vendor and the Bank's access to these records

2. 9. 7 Audit

2.9.7.1 The Bank should generally include in the contract the types of audit reports the Bank is entitled to receive (e.g., financial, internal control and security reviews).

2.9.7.2 The contract may also specify rights to obtain documentation regarding the resolution of audit disclosed deficiencies and inspect the processing facilities and operating practices of the vendor.

2.9.7.3 The Bank should consider the degree to which internal audits completed by vendor audit staff can be used and the need for external audits and reviews. For services involving access to open networks, such as Internet- related services, special attention should be paid to security.

2.9.7.4 The Bank may wish to include contract terms requiring periodic security audits to be performed by an in-house Bank team or by an independent party with sufficient expertise. These audits may include penetration testing, intrusion detection, and firewall configuration.

2. 9. 8 Sub-contracting

2.9.8.1 The Bank may consider if sub-contracting should be expressly prohibited

2.9.8.2 Certain vendors may contract with third parties in providing services to the Bank. Prior written approval should be obtained from the Bank before any subcontracting. The Bank should evaluate all subcontractors before giving approval.

2. 9. 9 Cost

2.9.9.1 The contract should fully describe fees and calculations for base services, including any development, conversion, and recurring services, as well as any charges based upon volume of activity and for special requests.

2. 9. 10 Ownership and License

2.9.10.1 The contract should address ownership and allowable use by the vendor of the Bank's data, equipment/hardware, system documentation, system and application software, and other Intellectual Property Rights.

2. 9. 11 Performance

2.9.11.1 The Bank should include performance standards defining minimum service level agreements (SLA) and remedies for failure to meet standards in the

contract. The bank should consider including in the contract a provision for a dispute resolution process that attempts to resolve problems in an expeditious manner as well as provided for continuation of services during the dispute resolution period.

2. 9. 12 Limitation of Liability

2.9.12.1 Contract should identify situations in which the Bank may be liable for claims arising as a result of non-performance of vendor or resulting out of security breaches and specify indemnification of Bank by the vendor.

2. 9. 13 Termination

2.9.13.1 Termination rights may be sought for a variety of conditions including change in control (e.g., acquisitions and mergers), convenience, and substantial increase in cost, repeated failure to meet service levels, failure to provide critical services, Bankruptcy, company closure, and insolvency.

2.9.13.2 Contract should include provision for arbitration.

2.10 Re-evaluation

2. 10. 1 If the contract is granted for more than a year, there should be an annual review to ensure that the vendor still meets all the necessary criteria. The evaluation should be done by the Project Sponsor based on the same criteria used by procurement committee to choose the vendor.

2. 10. 2 The objective of re-evaluation of vendor is to obtain consistent performance as well as to ensure that all the risks identified in outsourcing plan are still being mitigated.

3 IT Procurement

3.1 Policy Statement

Procurement process for IT hardware, software and services should ensure that procurement is carried out on the best possible terms of business benefits, quality and cost in a transparent manner that make economic and efficient use of the Bank's resources. Information security requirements in hardware, software and services being procured, should be identified, and included in the specifications during procurement. Major procurements should be evaluated to determine the resultant extent of business benefits achieved from procurement.

Standards and Procedures

3.2 Applicability

3. 2. 1 This policy deals with the standards and procedures for technical evaluation of different IT products/solutions/service offerings, criteria for evaluation of vendors /service providers, during procurement and in the post implementation phase. The financial discretion for the purchase of the products/solutions/or services will be as laid down in the Bank's Scheme of Delegation of Financial Powers.

3. 2. 2 This policy applies to the procurement of IT hardware, software and services as under:

3.2.2.1 Hardware (e.g.- computer equipment such as Servers, PCs, terminals, Laptops, tablet PCs, Notebook PCs; all communication and networking equipments; Video conferencing equipments; MICR Cheque Processing equipments; Computer peripherals & spares; ATMs Cash Dispensers, ATM accessories such as Video surveillance systems, etc.); Physical Access and Monitoring devices i.e. Biometric access system, CCTV cameras etc.

3.2.2.2 Software (e.g.- Operating system, database, business applications, middleware, firmware, utilities, testing tools, security products, office automation etc.)

3.2.2.3 Services related to IT (e.g. Professional services such as project implementation, software customization, maintenance services, monitoring & testing, facilities management, etc.)

3.2.2.4 IT Consultancy Services (e.g. Specialized Professional services such as System integration of high value projects, Project Management, Technology Plan, IT strategy, IS Security, IS Audit, Certifications, etc.)

3.3 Procurement Initiation

3.3.1 Procurement for all major IT projects/IT consultancy including outsourcings which have Bank-wide usage or impact shall be initiated by IT Department.

3.3.2 Routine purchases (purchase of standard off-the-shelf computer Hardware and Software, software for localized or departmental use, standard communication and networking equipments, Servers/PCs/Terminals, upgradation of PCs/Servers) can be initiated by IT department. All purchases should be governed by an annual budget.

3.3.3 The extent of benefit and value provided to business should be analyzed against the cost of solution while making the decision to procure a product or service.

3.3.4 The procurement shall be under taken as per CVC guidelines. If procurement committee is required as per CVC guidelines for the specified amount the procurement shall be under taken through a procurement committee as constituted below: -

i. General Manager, IT (Chairman of Committee)
ii. Chief Manager, IT (Member)
iii. Chief Manager, OAD (Member)
iv. Chief Manager, FI (Member)
v. Chief Manager, Accounts (Member)
vi. Chief Manager, Loans (Member)
vii. Chief Manager, Planning & Development (Member)
viii. Chief Manager, Asset Management (Member)
ix. Officer, Technical Cadre (Member)

Any two chief Manager, along with Officer of technical cadre, Chief Manager, IT and General Manager, IT is required for procurement committee quorum.

3.3.5 The procurement from sponsor bank empaneled vendors to be initiated where ever possible

3.3.6 The L1 prices arrived at by sponsor bank IT Procurement RFP to be utilized to reap the advantages of scale in reducing prices.

3.4 Approach to Procurement

3.4.1 The procurement procedure should be in conformity with CVC guidelines, issued from time to time, and follow the two-bid system viz. the technical bid and the commercial bid. The following guidelines are issued to assist the procurement committee in technical evaluation of vendors and solutions, arriving at criteria for technical short listing and determining important contractual provisions.

3.4.2 Competitive bidding is necessary to obtain the best price performance advantage. Procurement can be through 3.4.3.1 Expression of Interest (EOI) /

Request for Proposal (RFP) procedure or competitive direct quotations (Request for Quotations-RFQ) in case of empanelled suppliers. Process selected and the number of vendors involved should balance the cost of procurement and efficiency of the procurement process.

3. 4. 3 Request for Proposal (RFP): Direct RFP can be called without EOI where requirements are known in fair detail and specifications of solution and techno-commercial competence of vendors is well known. (e.g. Procurement of hardware where the product specifications are known)

3.4.3.1 EOI / RFP should be released on the Bank's website and depending on the value of the procurement a small newspaper advertisement may be placed in national newspapers.

3.4.3.2 Direct competitive quotations (RFQ) can be called without going for EOI/RFP when product features are well known and the vendors have already been empanelled.

3.4.3.3 Vendor pre-qualification (empanelment) should be done to ensure fair bidding, for standardized products / configuration, such as Branch Servers, PCs, etc. by IT Dept. and should be reviewed at least once in 2 years.

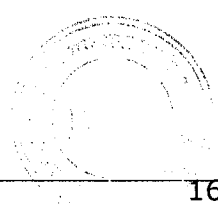
3. 4. 4 The EOI will call for a profile of the company, comprising information on the company's corporate structure, operations, financial statements, quality standards, support personnel and their distribution, client information, summary of previous projects of similar nature etc. Minimum eligibility criteria for responding to the EOI (e.g. minimum annual turnover, availability of direct support services at select cities etc.) should be decided by the Procurement Committee and specified in the EOI.

3. 4. 5 RFP should be prepared in a detailed structured format for clarity and completeness of the response. The RFP should contain two distinct structured formats, viz., the Technical Bid format and the Commercial Bid format

3. 4. 6 RFP- technical bid should clearly spell out the technical requirements with regard to

3.4.6.1 Product features or scope of service

3.4.6.2 Time frame for delivery and period of contract



3.4.6.3 Licensing terms and conditions

3.4.6.4 Acceptance testing methods

3.4.6.5 Terms for pilot testing (if required)

3.4.6.6 Terms of payment

3.4.6.7 Warranty/AMC terms & conditions - Support expected, committed maintenance support for the number of years required, etc.

3. 4. 7 RFP- Commercial bid should call for specific price information of various components/services for a period of at least three years including the following:

- One time purchase cost
- Cost of installation or customization
- Recurring cost (Maintenance and updates/upgrades)
- Cost of training

If precise quantities or bill of materials cannot be given, approximate estimates can be given, for the purposes of arriving at L1 Vendor, and indicated in the Commercial bid format. Commercial bid format should not provide for multiple options, which may introduce ambiguity in the determination of L1. If this becomes necessary due to existence of variable options, the Procurement Committee should record a note for the basis on which L1 vendor will be chosen, prior to opening of commercial bids. Technical bids should be accompanied by a template of the commercial bid without price information and any terms/conditions introduced by the vendors should be discussed and clarified before proceeding to open commercial bids.

3. 4. 8 Consultants recommending solutions for projects can be disqualified from bidding for supply of goods and services for the same project. Subsidiaries and associates of same vendor may be prevented from bidding separately for the same project

3. 4. 9 All vendors meeting the technical requirements, in the technical round will be considered equal and commercial quotes of vendors qualifying in the technical round will be opened. The vendor whose quotation is the lowest (L1) will be selected for price negotiation.

3.5 Evaluation Criteria

3.5.1 Procurement committee should evaluate technical bids received in response to RFP and short list the vendors based on clearly defined parameters and scoring methods. Following are the guidelines for vendor selection:

3.5.1.1 Stability, in terms of financial strength, market leadership and number of years in the business. Stability has to be judged against the maturity of the technology being procured. Newer technology or services will have to be carefully judged for stability and sustained performance.

3.5.1.2 Management composition of the organization to be verified to determine the top management experience and expertise in the business line.

3.5.1.3 The quality of delivery processes and project management methods should be considered in evaluation of vendor. This will include in-house infrastructure, geographic reach and number of people.

3.5.1.4 For strategic and high value orders, the selected vendor should preferably be certified in quality standards like CMM/ ISO 9000.

3.5.1.5 Past performance records for delivery of goods and services to the Bank.

3.5.2 Procurement committee should create an evaluation form. An evaluation form should have parameters corresponding to the procurement being made. Evaluation form should be used to rate vendors/solutions against the parameters during the selection process.

3.5.3 Additional evaluation guidelines for hardware procurement

Hardware Vendor

3.5.3.1 Deployment and implementation skills of the vendor for the solution being provided in order to ensure timely and quick implementation.

Relevant skills in troubleshooting and problem solving should also be considered.

3.5.3.2 Both principal & reseller should comply with quality assurance standards.

3.5.3.3 Customer base across business lines, especially customers with similar requirements like the Bank should be considered.

3.5.3.4 Geographical presence of the vendor that will enable support & hardware service across a larger geographical area.

3.5.3.5 Other support requirements should take into account the following-

delivery terms, warranty, skilled personnel, principal capacity, multi-location support, spares & replacement.

3.5.3.6 To guard against the risks of the vendors supplying counterfeit/non- original equipments and not providing proper license certificate for operating systems/ software, an undertaking, as per Annexure, should be obtained from the OEM/Vendor.

(Annexure)

Specimen Undertaking

With reference to your Request for Proposal (RFP) for (name of the Hardware like Desktop, Server, Hard disk etc.) dated ----------we hereby confirm that all the components /parts/assembly/software used in the (name of the Hardware like Desk Top, Server, Hard disk etc.) to be supplied shall be original new components / parts / assembly / softwares from Original Equipment Manufacturer and that no refurbished/duplicate/second hand components/parts/ assembly/ softwares shall be supplied or shall be used. We shall also produce certificate from the Original Equipment Manufacturers in support of the above statement.

We also confirm that in respect of licensed operating systems and other software utilities to be supplied, the same will be procured from authorized sources and supplied with Authorized License Certificate such as Paper Licenses, Product Keys etc.

In case the Bank finds that the above conditions are not complied with, we agree to take back the Hardware etc. supplied as above and return the money paid by you, in full within seven days of intimation of the same by the Bank, without demur or any reference to a third party and without prejudice to any remedies Bank may deem fit.

Authorized Signatory

Name and Designation

3.6 Price Negotiation

3.6.1 Price negotiation should follow CVC guidelines.

3.7 Confidentiality and Probity

3.7.1 Once the first proposals have been received from the bidders, procurement committee members should keep the content of all proposals, discussions or vendor correspondence confidential and take due care to prevent disclosure of any bidder's proposal information to another bidder.

3.7.2 Procurement committee should ensure that NDA has been signed with bidders in case the information revealed for bidding by the Bank is confidential in nature.

3.7.3 All prospective bidders will be provided the same information, and will be assured of equal opportunities to obtain additional information on a timely basis.

3.7.4 The procurement committee can make the broad parameters of the selection process and evaluation criteria known to prospective bidders.

3.7.5 High standard of ethics must be observed during the procurement and execution of contracts.

3.7.5.1 Bank will declare a firm ineligible, either indefinitely or for a stated period of time, if it at any time determines that the firm has engaged in corrupt or fraudulent practices in competing for, or in executing the contract.

3.7.5.2 Bank will reject a proposal for award if it determines that the bidder recommended for award has engaged in corrupt or fraudulent practices in competing for the contract in question.

3.7.6 Procurement committee members will ensure that they are not, or are not perceived to be in a conflict of interest with any vendor. Members should report any conflict of interest to their supervisor and discuss whether they should exclude themselves from any role in the procurement.

4 SLA Management

4.1 Policy Statement

Business critical IT services should have well defined service level agreements that specify performance requirements and establish accountability of service providers. Service levels should be monitored, recorded and reviewed against the defined performance requirements to ensure continuous availability of such services.

Standards and Procedures

4.2 Define Requirements

4. 2. 1 Service Level Agreements (SLA) should be entered into with external vendors for providing services related to management of applications, servers/desktops, networks or data processing. SLA should specify availability and performance requirements (e.g. availability of IT components/applications, response time of applications, restore time for problems, accuracy and integrity of data, expected throughput/output of work etc.) and establish vendor accountability.

4. 2. 2 The IT department should formulate or appoint a person knowledgeable in the concerned area for formulating the Service Level Agreement (SLA) requirements. SLA agreement should cover all the related requirements mentioned in the IT Outsourcing Policy.

4. 2. 3 All the user requirements should be taken into consideration while designing the SLA. This should include the following:

4.2.3.1 A description, from the Bank's perspective, of functions to be provided by the service provider

4.2.3.2 Times, days and locations on which the service must be available

4.2.3.3 Accuracy, Integrity and Service continuity requirements with tolerance limits for downtimes

4.2.3.4 IT resources needed to provide the service

4.2.3.5 References to the current operational methods or quality standards to be considered when defining the service

4.2.4 SLA should address all the important aspects for providing a good service. The SLA should be defined such that the commitments are realistic and measurable. This should cover the following:

- What the vendor is promising
- How the vendor will deliver the services
- How service delivery will be measured and by whom
- What actions to be taken if the vendor fails to deliver as per the agreement
- How the SLA will change over time
- Ensuring separation of arrangements to deliver services for more than one project in case of single vendor. In case vendor fails to provide alternate arrangements, provision of cost recovery by Bank should be in place to the extent of loss incurred by the Bank due to such failure.

4.2.5 Typical SLA will include the following components

4.2.5.1 Service objective defining what is the overall objective for establishing the SLA. Service objective generally is a measure of the quality, speed, availability, capacity, reliability, user-friendliness, timeliness, conformity, efficiency or effectiveness of services.

4.2.5.2 Scope of services including definition of service provided, specifications on number of hours and days that service will be offered, including maintenance and upgrades, specification of the number and locations of users and/or hardware/software for which the service will be offered.

4.2.5.3 Measurement metrics - Metrics are used to measure and confirm that the necessary service level objectives have been achieved. Metrics should measure the level of performance the vendor is giving to the Bank, and not to be based on the performance level, the vendor is delivering in aggregate to all its customers. Each measurement should logically support a requirement that is linked to objectives.

4.2.5.4 Acceptable range of service levels – For each of the metrics, the levels of service acceptable to the Bank should be defined. Some of the measurement metrics and their acceptable range can be as below

4.2.5.4.1 Specific requirement for system uptime against total time for which service is required and minimum level of service (e.g. 99.9% over a period of 1 year). Acceptable mean time between failures (MTBF) should also be considered.

4.2.5.4.2 Specific requirement for maximum downtime due to individual outage (e.g. no more than 1 hour of continuous downtime)

4.2.5.4.3 Specific requirement for availability of services and penalty for outage during peak business hours.

4.2.5.4.4 Specific requirement or parameters for capacity/load (e.g., 1000 transactions processed per minute).

4.2.5.4.5 Application response time (e.g. 95% of users get response within 2 seconds)

4.2.5.4.6 Accuracy level (e.g. 1 error in 1000 data entries)

4.2.5.4.7 Network latency (e.g. average round-trip latency from branch to Data Centre to be less than 300 milliseconds)

4.2.5.4.8 Specific Response time for problems (e.g. High Priority problem will be responded within 30 minutes, normal priority within 4 hours and low priority within 1 day)

4.2.5.4.9 Specific Resolution time for problems (e.g. High Priority problem will be resolved within 2 hours, normal priority within 1 day and low priority within 3 days)

4.2.5.5 Formula for calculating the measurement – SLA should define the method for calculating the acceptable ranges of metrics. It should consider the following:

4.2.5.5.1 Exception conditions like failure of hardware/ software at customer site not managed by the vendor, service dependencies with third parties, scheduled & emergency maintenance, force majeure.

4.2.5.5.2 Scheduled events that impact service availability (like scheduled maintenance, enhancements)

4.2.5.6 As per IT Outsourcing Policy, Bank reserves the right to audit the Vendors / third –party and activities performed by them as per the

agreement. This can be done by Bank's own team or regulatory authorities like RBI or external third party authorized for the same. SLA should mention the Bank's right to audit in above lines, and should ensure that Security Review/ Audit report findings are closed by vendor/third- party as per the SLA.

4.2.5.7 Penalties for non-performance – Penalties can range from extension of service period, reduction in charges, reduction in charges plus additional compensation and corrective action plan. Penalties should match the severity of the consequences to the Bank if the key performance measures are not met.

4.2.5.8 A cap on the maximum penalty chargeable to the vendor should be specified in the SLA and it should be ensured that the charges due to the vendor are sufficient to recover maximum penalty amount. SLA should also define conditions which amount to continued unsatisfactory service levels or result in repeated levy of penalties, which can lead to termination of the contract.

4.2.5.9 Reports - The SLA should require the service provider to make available clear, useful and timely reports on performance for each measurement period. The SLA should also define precisely what information will appear on the reports, such as exception reports for missed service levels and trend reports for key service levels. The SLA should also require the vendor to conduct a root-cause analysis of service level failures and report the results to the Bank.

4.3 Monitoring the SLA

4.3.1 The IT Department should monitor or designate a person responsible for monitoring vendor performance. The main responsibilities should include-

4.3.1.1 Setup systems for calculating the performance metrics

4.3.1.2 Measure service activity results against defined service levels.

4.3.1.3 Examine measured results to identify problems and determine causes.

4.3.1.4 Take appropriate action to correct failed activities, functions, and/or processes including administering of penalties under SLA.

4.3.1.5 Continuously guide vendors through feedback sessions based on

measured performance metrics.

4.3.1.6 Deterrent penalties to be imposed for performance failure in a way to recover the financial /reputational losses caused to the bank.

4.4 Reporting

4.4.1 The SLA reports should be provided by the vendor at pre-defined intervals. Reports should compare the agreed service levels and the service levels actually measured.

4.4.2 It should be ensured to consolidate the SLA reports by IT Department and put up for review to one level higher authority, on quarterly/half-yearly basis depending upon the criticality of related information system or services.

4.4.3 If the service levels do not meet agreed SLA, then actions should be taken for improvement.

5 Third Party Access

5.1 Policy Statement

5.1.1 Access *by* third parties to any IT asset must be strictly limited and controlled. An assessment of third party access risks must be made and controls appropriate to producing an acceptable level of residual risk should be put in place. Third party contracts should include specification of responsibilities and consequences for unauthorized access to information systems of the Bank.

Standards and Procedures

5.2 Access Request and Approval

5.2.1 Access to information or other system resources of the Bank should be provided to third parties having a business need for the same. The requirements could include the following.

5.2.1.1 Service-provider/vendor network having dedicated connectivity to the Bank's network for managing or monitoring resources. (e.g. Network integrator, Managed services vendors).

5.2.1.2 Hardware/software vendor needs intermittent access to the Bank's IT systems for managing or for troubleshooting.

5.2.1.3 External IT consultant/service-providers/vendor employees working in the Bank's premises requiring LAN connectivity and application access.

5.2.1.4 External IT consultant requiring access to the Bank's documents.

5.2.1.5 Connection with other Banks or financial service providers.

5.3 Third Party Access Assessment

5.3.1 While providing access to third-party user, following assessment should be conducted to identify the risk involved and controls sufficiency:

5.3.1.1 The criticality and sensitivity level of asset proposed for access.

5.3.1.2 Type of third party users (general user or privileged user and on-site or off-site)

5.3.1.3 Functions to be carried out by the third party user

5.3.1.4 Type of access controls already in place. Any additional controls, required, if any.

5.3.1.5 Access privilege level required.

5.3.1.6 Need of encryption of data during transmission

5.3.1.7 Legal/ Statutory requirements while providing such access

5. 3. 2 Application Owner will decide on criticality level, type of physical and logical access that is required. All critical access to third party personnel should be provided by the Application Owner based on the approval given by the appropriate authority. Any non-critical or regular access may be assessed and approved by Application Owner. The access approval should contain the duration of access and also the necessary privileges. This will include the following types of access.

5.3.2.1 Desktop/Laptop connectivity in LAN

5.3.2.2 Email Account in the Bank's mail system

5.3.2.3 Internet access

5.3.2.4 Application access

5.3.2.5 Approved Communication link like Leased line connectivity to the Bank's network.

5.3.2.6 Dial-in connection to the Bank's network.

5.3.2.7 Access to documents

5.3.2.8 Access to system room/Data Centre

5.3.2.9 Administrator login on servers and desktops

5.3.2.10 Duration including dates for removal/disable of access

5. 3. 3 Access to external auditors should be restricted based on "need-to-know" basis. For example evidences should be shown to external auditor based on scope of audit. Any other access like user IDs etc should be avoided unless explicitly required for conducting audit and approved by respective controller.

5. 3. 4 It should be ensured that such third-party access is disabled/ removed after approved duration or when the need is over, whichever is earlier.

5.4 Privilege allocation and monitoring

5. 4. 1 Access privileges should be provided by respective System Officials based on the approval. Authorization process followed for internal user creation should be followed for third party users also.

5.4.1.1 All application accounts including Email accounts and Internet access accounts of the third party personnel should be differentiated by using a different naming convention.

5.4.1.2 Unique user id should be created if there are multiple people requiring access from same external agency.

5.4.1.3 Access should be provided on the principle of need to know and need to have basis.

5.4.1.4 Wherever technically feasible, create user account with specific end-date so that it is automatically disabled after required time.

5.4.1.5 For outsourced vendors, who may need to access Bank's systems for remote troubleshooting, access should be provided using one-time user- ids and passwords, every time such access is required.

5. 4. 2 Application Owners are responsible for disabling the access after requested time. If the access requirements end before the date mentioned in the request form or if there is need for extension, it is responsibility of the Application Owner to arrange accordingly.

5.4.2.1 If existing user-id/password has to be shared with the third-party personnel for troubleshooting, these should be changed by respective users/System Officials soon after use.

5.4.2.2 Third party personnel should be accompanied at all times by the Bank staff if they are working in sensitive areas like system room or Data Centre.

5.4.2.3 Third party personnel should be supervised, by Bank staff at branches/offices, if they have been provided physical access to system room for any troubleshooting.

5.4.2.4 Users/System Officials should ensure that all media that is brought by third-party should be scanned for virus before being used.

5.5 Connection on internal network

5. 5. 1 Third-party laptops or notepads should not be allowed to connect on LAN network. Only in exceptional cases, such connections may be allowed after ensuring the following.

5. 5. 2 If third party personnel need to have connectivity to the internal network, it can be done either through their laptops or via desktops provided by the Bank. If it is a desktop provided by the Bank, these should be built as per secure configuration document (SCD) for desktop. It should be ensured that only software needed for the job is installed. If access is provided via third party personnel's laptop then necessary approval by the Application Owners/Head of the Unit should be obtained before allowing such access. Application Owners should maintain an approved list of third party Vendors for accessing applications. Indemnities should be obtained from approved vendors for accessing our network. Only approved vendors should be allowed to connect to our network by the Application Owners by a separate approval on case to case basis. ITSD will provide a checklist which should be filled and signed by the vendor for seeking approval for connectivity to our systems. It should be ensured that anti-virus protection is enabled with latest virus definition and all necessary security patches are installed and media brought in by the third party personnel is scanned for viruses before use.

5.5.2.1 If the connection is required for more than 1 week, the third party personnel's laptop should be installed with the anti-virus solution used by the Bank to ensure timely updates and to facilitate monitoring.

5.5.2.2 Application Owners should ensure that third party personnel are made aware about the Bank's acceptable usage policy. Third party personnel should agree to abide by these requirements as part of contractual terms.

5. 5. 3 A NDA along with access request, should be signed by individual employees of third party entering/ accessing Bank's critical locations/resources. The NDA format for such access request should be as follows:

USER UNDERTAKING

1. I.....working as.....with .....have been designated to work as..... At, BANK (RRB) .....

2. I confirm that I have been told/made aware of Bank's "Acceptable Usage" Policy and I agree to abide by Banks "Acceptable Usage Policy".

I undertake to

- Keep all relevant data of the Bank as confidential
- Access only the relevant data that is required for the job
- Follow the "Acceptable Usage" policy of the Bank
- Perform the security responsibilities and comply with the requirements specified in the "Acceptable usage policy"

3. I understand the importance of information security and agree to take all reasonable precautions, to protect the information assets of the Bank. I also understand that non-compliance with the "Acceptable usage policy" by me can lead to

- Suspension of access privileges
- Change of personnel assigned to the job
- Financial liability for actual, consequential or incidental damages
- Termination of the contract.

Signature of the employee:

Employee Name:

Employee ID/Employee Number:

Company Name:

Date:

5.6 Remote Network Access

5. 6. 1 External networks that are permanently connected to the Bank should be separated by Firewall. These connections will be provided via private leased lines and are required either for IT service providers or financial service provider networks.

5. 6. 2 Firewall should restrict access to essential IP addresses/Ports. All access should be provided on a need to know and need to have basis.

5. 6. 3 Third party personnel could require access to specific resources in the Bank's network on temporary basis. These connections will be provided either by connecting over the Internet or via providing direct dial-in access to the specific device. This is normally required for providing technical support for servers/devices that are in production.

5.6.3.1 If the connection is via the Internet the remote user should be authenticated before allowing access. All data transfer over Internet should be encrypted. All access should be restricted to essential IP- addresses/ports. This can be achieved by setting up a VPN server at the Internet gateway for authenticating and encrypting remote connections.

5.6.3.2 If the third party access is being provided via direct dialup to the device, the dialup facility should be disabled soon after the specified activity is over. Direct dialup to devices bypasses all existing security controls. Hence, if feasible the device to which the access is provided should be disconnected from the rest of the network during this period.

5.7 Non-disclosure agreements

5. 7. 1 The third party should sign non-disclosure agreements with the Bank to prohibit the third party and its agents from using or disclosing the Bank's information. This should be covered as part of contract with the third party.

5.8 Third-Party Responsibilities

5. 8. 1 The agreement with third party should cover the responsibilities to be ensured by third party including:

5.8.1.1 Third party should maintain and advise the Bank, a list of their personnel authorized for such access.

5.8.1.2 The third Party should inform the Bank in writing for changes in their personnel deployed in case of rotation and resignation of staff etc, so that the Bank can disable user ids and remove / change passwords in order to secure its resources.

5.8.1.3 Where the third Party has direct or indirect access to data or information owned by the Bank this information must not be copied, divulged or distributed to any other party or shared with any unauthorized person.

5.8.1.4 On the completion of agreement, third Party must return or permanently delete or destroy all assets belonging to Bank, which are acquired during the course of agreement.

5.8.1.5 Third-party shall be liable for all the activities performed by user-ids / access provided to them.

5.8.1.6 In case of undesired/inappropriate behavior or misrepresentation by the third-party employee/representative, Bank has right for full compensation from third-party.

5.8.1.7 Third-party should inform and take permission from Bank, before sub-contracting or engaging external agencies for activities covered under agreement with Bank.

5.8.1.8 Third-party should ensure and submit confirmation of compliance of all requirements as per agreement with Bank, before sub-contracting or engaging any external agencies.

5.8.1.9 Third-party should provide a common contact number to verify the identity of the support engineers who assigned for troubleshooting activity for Bank (branch/office/unit).

5.9 Penalties

5. 9.1 Failure to comply with contractual obligations relating to responsible usage of IT infrastructure of the Bank can lead to penalties including-

5.9.1.1 Suspension of access privileges

5.9.1.2 Change of personnel assigned to the job

5.9.1.3 Financial liability for actual, consequential or incidental damages

5.9.1.4 Termination of contract

5.9.1.5 Deterrent penalties to be imposed for performance failure in a way to recover the financial /reputational losses caused to the bank.

6 Data Centre Management

6.1 Policy Statement

6.1.1 Data Centre will have adequate physical and logical protection for the IT assets housed within and secure processes must be followed for server deployment, administration and monitoring within the Data Centre.

Standards and Procedures

6.2 Data Centre Manager

6.2.1 The responsibility to maintain the data center lies with the ASP for CBS and CBS plus services as the bank does not have its own data center.

6.3 Data Centre Teams Centre

6.3.1 Data Centre should have following teams for management of physical and logical protection of data Centre infrastructure respectively:

6.3.1.1 Data Centre Management Team: This team should manage the infrastructure facilities on 24x7 basis. The team shall be responsible for physical and environmental security of Data Centre and ensuring the high availability of infrastructure to applications hosted on.

6.3.1.2 Data Centre IT Operations Team: Every Application Owner should have a representative at Data Centre

6.3.2 Data Centre IT operations team should support the operations on a 24x7 basis. The responsibilities of the team will include the following:

6.3.2.1 Management of Data Centre desktops

6.3.2.2 Emergency response and incident handling for any incidents including virus/worm outbreaks or system compromise in consultation with ITSD.

6.4 Management LAN

6.4.1 A management LAN should be setup for administering and monitoring the servers from within the Data Centre. This network should have desktops, which will be used by person designated as administrator of applications hosted in the Data Centre and Data Centre IT operations team for accessing the servers for administration purposes. If network backups are being taken the backup server should be located in management LAN. The machines located in this network should not have external network excess including across to

Internet.

6.5 Firewall

6. 5. 1 Application Owners and IT-Networking Team should co-ordinate with ITSD to ensure that systems with different risk levels are segregated into different segments by a firewall. The firewall segments should be designed in consultation with ITSD.

6.6 Anti-virus

6. 6. 1 The Data Centre IT operations team should ensure that anti-virus software is installed and signatures updated on all the devices in the management LAN.

6.7 Physical Access Control

6. 7. 1 All entry points to the Data Centre should have access control facility for both entry and exit. There should be technology based access control solutions like biometrics or access cards.

6.7.1.1 Access control cards with photo-identity should be provided to all users who need to access Data Centre on full-time or near full-time basis. Access should be provided on a need to have basis.

6.7.1.2 Temporary access cards may be issued to visitors.

6.7.1.3 All the entry points to the Data Centre and movement within the Data Centre should be monitored by CCTV. It must be ensured that there are no other physical access/entry points which are not being monitored.

6. 7. 2 Photographing and Video shooting in Data Centre should be prohibited except for the purposes of monitoring movement of people and assets. Devices with facility of photography or video shooting should also be prohibited.

6. 7. 3 Emergency exits should be provided. Emergency exits/Panic doors should be provided. This exit should always be locked for access from outside. Burglar alarm shall be provided at the emergency exit.

6.7.4 Application Owner should inform the DCM in advance about any person (employee/vendor) requiring physical entry to Data Centre.

6. 7. 5 Employees requiring access to Data Centre should have identity card. Vendor, third Party support personnel should provide an acceptable identity proof and a letter on the company letterhead stating that the person is an employee of

the company and assigned to work with the Bank.

6. 7. 6 The server area should be physically separated from the rest of the Data Centre. Strict physical security controls should be in place to restrict access to server area. Access to this area should be limited to Data Centre IT operations team. Any external person, who needs to access the server area, should be accompanied by a member of the Data Centre IT operations team.

6. 7. 7 CCTV should be deployed to monitor movement of personnel inside and peripheral data Centre area. There should not be any area out of sight and sufficient light/emergency light must be ensured in this case.

6. 7. 8 All racks in the server room should be locked, wherever feasible. Access to these racks should be restricted to authorized personnel.

6. 7. 9 Security guards should ensure that there is no unauthorized movement of IT equipment into or out of Data Centre. All personnel entering the premises should declare, if they are carrying any IT equipment like storage media or mobile portable device. If anything needs to be taken out that should be informed in advance to the guards by respective authority.

6.7. 10 An access control register should be maintained at the entry point of Data Centre. All non-Data Centre employees and external visitors should make an entry in the register before entering the Data Centre.

6. 7. 11 Server area should be protected by minimum two levels of protection before providing physical access.

6.8 Environmental Safety

6. 8. 1 Power systems should be designed to provide power, at appropriate levels and quality, without interruption. There should be adequate redundancy for power sources and no single points of failure. All IT equipment within Data Centre should have power supplied from two sources of UPS (uninterrupted power supply) for reliability except modems where base power is supplied from service provider exchange. Arrangements should also be made for supply of power from a back-up generator which should be located at raised height.

6.8.1.1 Separate Power supply with backup power should be provided for access control systems and other physical security systems such as alarms, fire detection and suppression systems, emergency lights etc.

6.8.1.2 The electrical power supply to the Data Centre should be isolated from other circuits of the building. Within the Data Centre the electrical power supply to the IT equipment should be isolated from other equipment.

6. 8. 2 Emergency power off switches should be provided ineasily accessible locations within the Data Centre.

6. 8. 3 Fire detection and alarm system should be placed at identified locations inside data Centre.

6. 8. 4 Fire resistant material should be used for building Data Centre infrastructure.

6. 8. 5 Combustible materials should be avoided in the Data Centre.

6.8.6 All personnel in the Data Centre should be trained in basic fire fighting techniques. Fire drills should be conducted periodically to check preparedness of the personnel.

6.8.7 Air conditioning mechanisms should be implemented to ensure that the operational environment conforms to the equipment manufacturer's specifications.

6.8.7.1 The temperature and humidity must be monitored and controlled

6. 8. 8 Air should be circulated & filtered to remove dust & contaminants.

6. 8.9 Raised false floor should be used since it provides the flexibility in wiring, equipment siting and air conditioning.

6.8.10 False ceiling is recommended for flexibility in electric wiring, lighting, concealing AC ducts and protection against water seepage.

6.8.11 Eatables should not be permitted within the Data Centre. Smoking is prohibited in and around Data Centre area.

6. 8. 12 Data Centre premises should be kept clean and free from dust and dirt.

6. 8. 13 Pest Control and Rodent Control should be carried out periodically.

6. 8. 14 Locations for Data Centre and Disaster Recovery Centre should be identified so they both should not be located under common seismic zone.

6.9 Maintenance

6. 9.1 There should be a schedule drawn up for preventive maintenance of equipment used to control environmental threats including air-conditioning, power and fire control systems.

6. 9. 2 Periodic testing should be carried out for the following to ensure that such equipment function when needed.

6.9.2.1 Fire control systems including sprinklers, water pipes etc, if feasible.

6.9.2.2 Backup power supplies like generator, UPS etc.

6.9.2.3 Alarm systems like physical intruder alarms

6.10 Monitoring

6. 10. 1 DCM is responsible for monitoring the safe and secure operations of the Data Centre including the following

6.10.1.1 Ambient temperature and humidity are within acceptable range

6.10.1.2 Physical movement of personnel and equipments.

6.11 Documentation

6. 11. 1 The DCM should maintain documentation for the following.

6.11.1.1 Network architecture of the Data Centre. This should include the following details:

- Firewall segments and servers.
- IP addresses

6.11.1.2 Physical layout of the Data Centre. This should include the following details:

- Floor plan
- Rack Plan
- Power Supply Plan
- Data cabling
- Electrical cabling

6. 11. 2 All details regarding servers and other devices deployed in the Data Centre should be maintained by the DCM. A separate folder can be maintained for each application groups. The details should include the following

6.11.2.1 New device commissioning and De-commissioning requests

6.11.2.2 Requests for access to support personnel

6.11.2.3 Device inventory (Device Identification numbers, IP address, Operating

System and Application name)

6.11.2.4 Name and contact number of persons designated as System official/ Application Owner

6.11.2.5 Records/Logs of Access Card, CCTV. Data Centre Management team should devise backup procedures and retention period for the same which should not be less than 3 months.

6.12 Incident reporting

6. 12.1 In case of outsourced data Centre facilities, Outsourcing Agreement and Service Level Agreement should be ensured for compliance of applicable clause of IT and IS Security Policy including Data Centre Management Policy.

6. 12. 2 In case of outsourced data center, same should not be less than of Tier 3 of global industry standard TIA-942 and should have best industry infrastructure and practices.

7 Configuration Management

7.1 Policy Statement

7.1. 1 Bank's systems should be configured for high security, reliability and stability and all such configuration should be documented. Systems should follow standard naming conventions for efficient identification in configuring and in problem resolution.

Notes:

- Branches should ensure that the server, desktops and network devices are securely configured.
- Branches should securely preserve the authority letters carried by project officers for implementing/changing configuration setting for future reference.
- Branches should ensure that the reports submitted by project officers after implementing/changing configuration settings are securely preserved for future reference.

8 Anti-Virus

8.1 Policy Statement

8.1.1 All servers, desktops and access points to Bank's network must be protected against malicious code with anti-virus software and processes must ensure early detection, efficient containment and eradication of malicious code within the network of the Bank.

Standards and Procedures

8.2 Installation

8.2.1 All servers, desktops, laptops and other portable devices should have anti-virus agent installed. Official in-charge of system in branch/offices should ensure that all new systems including desktops, laptops and servers have anti-virus agent installed and configured as soon as they are connected to the network.

8.2.2 Anti-virus agent installation should be password protected to ensure that end users cannot uninstall the agent. The anti-virus agent should be configured in such a way that end users will not have privileges to change any settings or to disable the agent.

8.2.3 Anti-virus agent should be configured to scan the machine at least once per day. The time of scanning can be either when the system boots up or during non- peak usage hours.

8.3 Functionality provided by Anti-virus solution/Agent

8.3.1 Anti-virus agent should be configured to do a real time scan of all the files when they are accessed, copied or moved. This will ensure that all viruses are detected before they get activated.

8.3.2 The anti-virus solution should ensure that Anti-virus scanning process resumes if system reboots in-between scanning process.

8.3.3 The solution should allow the On-Demand scanning. Agent should be able to recognize the last scanned file and resume scanning from the file if an "On- Demand Scan" is interrupted.

8. 3. 4 Anti-virus agent should be configured to quarantine virus infected files if they cannot be cleaned.

8. 3. 5 Anti-virus agent should automatically scan any externally connected storage media like Pen drive, CD Drive etc., immediately on connection.

8. 3. 6 If any desktop is found infected, same should be scanned with anti-virus client with updated virus definitions.

8. 3. 7 Anti-virus software should be installed on Email servers including SMTP gateway systems that transact email with the external world. Anti-virus software should be configured to scan attachments in all Emails. If a virus is found in an incoming SMTP mail then the following actions should be taken:

8.3.7.1 Infected attachment should be deleted.

8.3.7.2 A notification sent to the recipient informing him/her that a virus was detected in the attachment along with the rest of the mail.

8. 3. 8 Anti-virus software should be installed on the Internet proxy server and configured for the following.

8.3.8.1 Whenever a user downloads/uploads a file, it should be scanned for viruses.

8.3.8.2 If a virus is found, then the download/upload should terminate and the user informed on the status.

8. 3. 9 If feasible, the anti-virus agent should be configured to accept updates from a backup anti-virus server, incase the primary server fails.

8. 3. 10 The solution must scan and remove all malwares, spywares, viruses etc from the system without causing any system degradation.

8. 3. 11 The solution should scan all types of traffics including HTTP, SMTP for viruses, malwares, spywares etc. The solution should have proactive scanning to protect against known and unknown threats.

8. 3. 12 Anti-Virus solution should provide Endpoint protection like denial controls and data leakage prevention.

8. 3. 13 The solution should support Multi-threaded scanning for high degree of accuracy without leveraging on system resources.

8. 3. 14 The solution should provide protection against mobile code by:

8.3.14.1 blocking any use of mobile code;

8.3.14.2 blocking receipt of mobile code;

8.3.14.3 controlling the resources available to mobile code access;

8.4 Anti-Virus Support Team

The ASP is responsible for anti-virus administration and security patch distribution. The System officials at ITCELL will coordinate with ASP to assist the branch officials in addition to managing anti-virus/patches in their respective offices.

8.5 Anti-Virus Signature Update

8.5.1 New signatures should be applied to all systems as soon as these are released by anti-virus vendor. Anti-virus application architecture should ensure that all systems across the bank are updated within 24 hours.

8.5.2 All systems in the LAN network should be configured to get the signature updates from the nearest anti-virus server. ASP is responsible for ensuring that all systems in the LAN are updated with the latest signature pattern files.

8.5.3 The primary server should be configured to pick up the signature pattern from the vendor site. Periodically ASP should manually check with the anti-virus-vendor site to ensure that the latest signatures are getting updated on the primary server

8.5.4 All standalone systems including laptops shouldalso have anti-virus protection with regular updates.

8.5.5 These reports should be sent to the ITCELL on a monthly basis. The Senior manager IT should be responsible for analyzing the reports and ensuring that the branches are updated with latest signature patterns.

8.6 Server security

8.6.1 Server operating system and anti-virus application should be setup as per the secure configuration document.

8.7 Performance Monitoring

8.7.1 Logging should be enabled for operating system as well as for the anti-virus application on anti-virus servers. ASP is responsible for monitoring the logs.

The log reports should be sent periodically to IT Dept. These logs should be analyzed for:

8.7.1.1 Failed administrative logins

8.7.1.2 Start and stop of services

8.7.1.3 Modification of user privileges

8.7.1.4 Denial of Service attempts

8.8 Tracking New Vulnerabilities

8.8.1 ASP should be responsible for keeping track of any new vulnerability that could lead to a worm or virus attack.

8.8.2 When a new vulnerability is published, ASP should identify the steps that need to be taken to ensure that the associated risks are mitigated.

8.9 Documentation

8.9.1 Documents for the following should be maintained and updated by ASP.

8.9.1.1 Anti-virus server installation procedure. This should include OS/Application configuration documents and operating procedures for the following.

- Server monitoring
- Backup and recovery
- Report generation

8.9.1.2 Anti-Virus agent installation procedure.

8.9.1.3 Troubleshooting FAQs for server and agents.

8.9.1.4 Anti-virus related task list for system officials.

8.9.2 ASP is responsible for distributing the relevant documents to designated System officials in IT Department.

8.10 Backup and Redundancy

8.10.1 ASP should be responsible for the backup operations of critical anti-virus servers. Following components should be backed up.

- Operating system files
- Anti-Virus application files

- Configuration settings.
- OS and application log files

8.10.2 There should be redundancy provisions made for the critical anti-virus servers.

8.10.3 Recovery testing should be done periodically.

8.11 Change Management

8.11.1 All critical changes to the anti-virus infrastructure including the following should adhere to change management process. This will include the following:

- OS /Antivirus Application upgrade
- Changes in anti-virus architecture or update schedule
- Addition/Removal of an Anti-virus server/ Component

8.12 Vendor Support

8.12.1 The Service Level Agreement with anti-virus vendor should include the following provisions

8.12.1.1 Providing signature updates and newer versions of the software.

8.12.1.2 Providing technical support including onsite support within specified time frames

8.12.1.3 Contact persons and response times for technical escalations

9 Network Security Device Management

9.1 Policy Statement

All critical applications should be protected by network security devices viz. Firewall, VPN, IDS, IPS from both external users and internal users of the Bank. The network security devices should be protected by secure configuration and management practices to ensure access and availability to authorized users/applications/processes only.

Standards and Procedures

9.2 Network Security Device management

9. 2. 1 The network security devices should be configured and managed to limit the access of data only to authorized users. Logical position of firewall in network architecture should ensure that firewall is not bypassed.

9. 2. 2 Network based Intrusion Detection System (NIDS) should be deployed to monitor the traffic to critical systems including application servers, web server, database servers, network and security devices by the ASP.

9.2.2.1 NIDS will not be able to track all attacks happening on the network. This is true for systems that are accessed through encrypted channels (for e.g. over SSL, SSH). In these cases the ASP shall ensure that Host Based IDS (HIDS) can be installed on these systems to detect the attacks.

9. 2. 3 ASP shall be responsible for Risk assessment, approvals to ACLS of firewall, access controls of VPN, configuring alerts of IDS/IPS, and their monitoring, and review.

9.2.4 ASP shall be responsible for procurement, installation, configuration, signature Updation of IDS/IPS and maintenance of network security devices.

9.3 Firewall rule base creation

9. 3. 1 ASP should be responsible for designing and testing the firewall rule base before deployment. Configuration Management Policy should be referred for testing procedures in this regard. The teams should get the required inputs from the respective Application Owner for designing the rule base.

9. 3. 2 All firewalls should be configured as stateful inspection firewall. Firewall rule base should restrict access to required ports on the target machine. The Source field in the rule base should be restricted to specific IP addresses/Subnet addresses except for the applications required to be accessed from internet for business purpose. . In the case of applications where the number of individual IP addresses/subnets is very large the source address can be made generic to make the rule base more manageable. Firewall should have a rule to deny all access(s) that are not explicitly allowed.

9. 3. 3 Access to administrative ports including SSH and Microsoft Windows Terminal services on protected servers should have user ID based authentication at the firewall in addition to source IP address. User authentication provides additional security and also provides facility for authenticating roaming users.

9.3.4 Firewall user-database, needed for rules that are configured for user-authentication, can be stored either locally on the firewall or in an external directory server. Enforce password policy for these user accounts including password expiry, password history, and password complexity. Account lockout should be configured to prevent password cracking attempts. It should be ensured that these user credentials are transmitted in encrypted format from the user desktop to the firewall.

9. 3.5 The rule base should be approved by both source and destination Application Owners and ITSD prior to deployment. ITSD should give a copy of the approved rule base pertaining to the application to the respective Application Owners. This will ensure that Application Owners are aware of the services that will be allowed through the firewall prior to deployment. This will also help in reducing troubleshooting efforts when the firewall goes into production.

9. 3. 6 If there are applications that require large number of dynamic ports and access cannot be restricted to specific ports at the firewall, then these servers should be separated out into a new segment.

9.4 Firewall rule base change

9. 4. 1 After the firewall goes into production, all changes to the rulebase should be done after proper authorization, to ensure that the security level is maintained.

9.5 Firewall rule base review

9. 5. 1 A periodic review should be conducted by Application Owner on respective firewall rule base to ensure that all access permissions provided through firewall, are current and updated w.r.t. business requirements.

9. 5. 2 Application Owner should ensure that all temporary rules areremoved/ disabled once the need is over.

9.6 IDS/IPS

9. 6. 1 All access to critical systems including application servers, web server, database servers, network and security devices should be monitored continuously by ASP for malicious activity. Network based Intrusion Detection System (NIDS) should be deployed to monitor the traffic to following systems

9.6.1.1 Systems accessed by external networks → All systems that are accessed by external sources should be monitored by NIDS.

9.6.1.2 Critical internal application servers → Critical application server (e.g. the critical Server which is accessed by the internal users at the branches) should be monitored by a NIDS.

9.7 Administrative Access

9.7.1 Administrative access to security devices is required for activities including ACL modification/signature Updation, device-user account management, device-administrator account management and log monitoring. Access Privileges should be provided to members of the ITSD and other authorized users (approved by ITSD) on a need to have and need to do basis.

9. 7. 2 Administrator accounts on the devices should have password policy and account lockout configured as per User Access and Password Management Policy.

9. 7. 3 Access to device administration programs should be through encrypted channels. If the device software itself does not provide this facility, then additional mechanisms like IPSEC should be used for this purpose.

9. 7. 4 Logical access to the network security devices should be limited to the ISD and Networking Teams and authorized users (approved by ITNW). Local System Officials should not have access to device application. Device should have access

permission rules based on required network segment IP addresses only.

9.8 Logging

9.8.1 Logging needs to be enabled to ensure that all critical access is tracked. Logging should be enabled for rules enabling administrative access (e.g. SSH access to Bank's web server). Logging may not be enabled for normal user access (e.g. HTTP access to Bank's web server).

9.8.2 Logging should be enabled for the first rule that blocks all direct communication with firewall itself from unauthorized networks/hosts.

9.8.3 Logging should be enabled for the last rule that blocks all access that is not explicitly allowed by the other rules..

9.8.4 Logging should be enabled to track any changes done to device configuration including changes to ACLS in case of Firewall, Access controls in case of VPNs, signature Updation in case of IDS/IPS. This will ensure that all changes can be tracked for trouble shooting as well as for audit purposes.

10 Incident Management

10.1 Policy Statement

All security breaches or attempts to breach and all discovered security weaknesses in information systems must be reported. Incident management process must ensure that all reported security breaches or weaknesses are responded to promptly and action taken to prevent recurrence.

Standards and Procedures

10.2 Incident Identification

10. 2. 1 An incident is the act of violating an explicit or implied security policy and discovery of security weaknesses in system. The following actions can be classified as incidents:

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

10.2.1.2 Unwanted disruption or denial of service

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

10.2.1.4 Changes to system hardware, firmware or software characteristics and data without the Application Owner's knowledge.

10.2.1.5 Existence of unknown user accounts

10. 2. 2 Incidents could result in un-authorized access, disclosure of information, corruption of information or denial of service. Users and System Officials should follow these guidelines in identifying an incident:

10.2.2.1 Abnormal system resource usage → If the CPU, memory utilization on a system is very high, the system could have been compromised. Attackers use compromised systems for spreading viruses or attacking other machines leading to high resource utilization. System Officials need to track resource utilization and analyze reasons for any abnormal usage.

10.2.2.2 Users experience slow response → End users could experience slow response times if the application servers or the network has been compromised and is being used for malicious purposes. Virus or worm

outbreak could lead to network congestion that would in-turn cause application responses to be slow and unstable. End users should report any drastic drop in application response or system stability to System Officials.

10.2.2.3 Data corruption → Unauthorized modification or deletion of data or inability to retrieve data in correct format or web site defacement.

10.2.2.4 Changes in passwords and user-id → System users should report to System Officials if they find the passwords do not work. Any changes in user passwords, addition/deletion of user accounts could be indications of system compromise.

10.2.2.5 Unauthorized activation of suspended / deleted user accounts

10.2.2.6 Traffic on non-essential ports → If there is network traffic on ports that are not used by any of the internal applications this could be signs of a backdoor application in the network. The traffic should be tracked and reported by the monitoring team. If the backdoor application tries to traverse the firewall, these would be tracked by the firewall logs.

10.2.2.7 Existence of unknown user accounts → Normally attackers create new accounts on the systems after they are compromised. Existence of unknown user accounts, especially those with administrative privileges, could indicate that system has been attacked.

10.3 Incident Reporting

10.3.1 If an user, either Bank's employee, vendor, contractor orthird party personnel etc., suspects that an incident has occurred, it should be reported immediately to system official or the designated official responsible for the application/system. He/she should not attempt to check/test/prove the suspected weakness which may damage the service / system.

10.3.2 Branches / offices should report the incidents to their respective controllers. Designated Controllers/ IT Officer should do a preliminary analysis of the incident before reporting to the IT Department (ITSD).

10. 3. 3 The report should contain the following details.

10.3.3.1 Description of the incident → Details regarding the logical and physical events regarding the incident, date and time of incident, reporting person.

10.3.3.2 Possible causes → Based on the damages observed and other evidence available System Officials should include the possible causes of incident. This could include worm/virus attacks, password compromise or social engineering.

10.3.3.3 Damages observed → All loss of data, system downtime, system instability, slow response times should be included.

10.3.3.4 Supporting evidence → All evidence regarding the incident including system or application logs files, alerts and logs of security devices including firewalls and intrusion detection systems should be included in the report.

10.3.3.5 Remedial steps taken → Any preventive measures taken like disconnecting system from network, changing administrative password or applying a new patch.

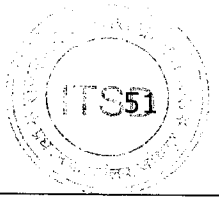
10. 3. 4 All data related to the incident should be secured and preserved properly, because such materials will be required as evidence during investigation.

10. 3. 5 All information security incidents can be reported through service desk or through email in format provided by ITSD.

10. 3. 6 If ITSD is convinced about the authenticity of the incident, an incident alert should be sent to all application groups and user departments who are using similar IT systems or could potentially be affected by the same incident. The incident alert should contain details on how to identify the incident and steps to be taken to recover from incident.

10.4 Evidence Collection for Incident

10. 4. 1 All evidences and audit trails related to incident should be collected and preserved in secure manner ensuring its authenticity, accuracy and completeness.



10. 4. 2 Depending on the nature of security incident and feasibility, a full backup of the system/data should be taken and preserved (sealed) in the custody of the authorized persons by ensuring chain of custody.

10.5 Incident Response

10. 5. 1 ITSD should analyze the incident based on the data available in the incident report. If more data related to the incident needs to be collected, ITSD should get it from the respective application groups.

10. 5. 2 Incident should be categorized as High/ Medium/ Low risk based on past experience / likely impact.

10. 5. 3 Incident should be escalated to appropriate authorities immediately. For responding to the incidents time is of essence and response should be with utmost promptitude.

10.5.4 Once the incident has been verified, ITSD should ensure recording the incident in the incident register in electronic form. An incident number is allocated that will be used for incident tracking and future reference. The incident register should contain the following details:

- Incident reporter name
- Incident reporter branch/Dept. information
- Date and Time of reporting
- Incident Risk Category (High, Medium and Low)
- Reason of Incident
- Action taken
- Impact of Incident
- Status
- Date of closure
- Comments

10. 5. 5 All collected evidence and incident details should be provided to respective Application Owner for recovery and risk mitigation.

10. 5. 6 Based on the nature of incident and collected evidence, respective Application Owner should initiate action for incident recovery and risk mitigation in consultation with ITSD. Chairman should be updated about the incident and action

taken, in case of incidents categorized as High.

10.6 Incident Recovery

10. 6. 1 Depending on the nature of the incident and based on the action plan drawn up by Application Owner, all system personnel and security professionals required to recover from the incident should be contacted. Recovery will involve identifying and eliminating the cause of the incident. This could involve a series of activities including implementing additional security controls, installation of new patches, recovery of systems backups, and reconfiguration of security devices including Firewall rule base and intrusion detection system alerts.

10. 6. 2 Once the recovery has been done, additional security monitoring devices should be configured to ensure that the incident activity has ceased. This could involve a series of activities including deployment of additional intrusion detection systems, frequent monitoring of system and application logs of affected systems.

10. 6. 3 During Incident Recovery process, it should be ensured that integrity of affected systems and controls is confirmed with minimal delay.

All emergency actions taken by Application Owner for incident recovery should be documented in detail and should be reported to CISO.

10.7 Incident Prevention

10. 7. 1 The final step of incident handling process is to conduct a detailed analysis to identify the strong and weak points in the existing IT infrastructure and policies. If needed, IT Department should make recommendations for necessary changes to security policies, standards and procedures.

10. 7. 2 ITSD should maintain a database of incidents and solutions. This will help in providing quicker solutions if the same or similar incident happens again.

10. 7. 3 Based on the learning from the incident, incidents should be analyzed based on nature and impact, and ITSD should make recommendations to the Chairman for procuring additional security services and solutions (if required) for improving security.

11 Email

11.1 Policy Statement

Email application will be protected against risks of malicious code, spams and unauthorized access and should be managed to ensure high availability. Email accounts will be provided to users with business requirement after due authorization.

Standards and Procedures

11.2 Email Support Team

11.2.1 A dedicated email support team Central Email Team (CET) headed by SM(IT) should be formed for managing and supporting the Email infrastructure. CET should be responsible for installation, configuration, administration and security of all email server components. CET will report to the Head of IT-Dept.

11.3 Email Account Creation

11.3.1 Email IDs should be provided only for users having a business need for the same. Email account should be created only after approval and authorization from the branch manager, Dept Head or other competent authority. HRMS application should be enabled and utilized to initiate creation of new e-mail accounts.

11.3.2 All e-mail accounts should be protected by a user-id/password.

11.3.3 Personal email ID should be created based on the naming standard. Ideal naming standard can be in the form of 'firstname.lastname@BANK(RRB)ank.in'.

11.3.4 Designation based email IDs should be created only after an authorization from competent authority. The naming standard can be in the form of 'designation.department.location@BANK(RRB)ank.in'.

11.3.5 Email IDs for branches should be created based on naming convention BANK(RRB).branchcode@BANK(RRB)ank.in and Email IDs administrative offices/ departments can be created with mention of location like Email ID for accounts section of Head Office can be accounts.headoffice@BANK(RRB)ank.in.

11. 3. 7 Any mails to be sent for mass mailing like marketing, product promotions, customer education etc. should be sent through a common ID. Mail IDs should be provided to departments on need basis. The user/ Dept. Head should report any misuse of email IDs.

11. 3. 9 For a change in ownership for designation based email accounts the Dept. Head or controller should inform CET who will also reset the password on receiving this information.

11. 3. 10 CET will provide a facility on service desk for password reset requests. Users should contact service desk to reset their passwords. In case direct communication is not possible with service desk, Dept. Head should send the mail for password reset.

11. 3. 11 Designated Official responsible for configuration of Email IDs on user desktops, should ensure that data file of email id is configured on separate drive other than drive where OS is installed.

11.3.12 Emails clients which are authorized by the ITSD should only be used.

11.4 Deactivation / Deletion Of Email Accounts

11.4.1 An email account should be deleted as soon as the need for the same is over.

11. 4. 2 For employee e-mail IDs, termination of email IDs could be due to employee leaving the organization, or employee getting retired or demise or dismissal/removal. HRMS and Branch/Office Head should report to ITSD about employees leaving the organization at least three months in advance in case of retirement. For others, the same may be intimated at the earliest. The respective Dept. Heads/ Branch Managers should inform the ITSD for terminating the email accounts.

11. 4. 3 The email administrator should delete the account and update the user's Dept. Head.

11. 4. 4 It should be ensured that the deleted e-mail IDs are not re-allotted to any other user in the organization.

11. 4. 5 In case personal email-IDs are not used for 180 days should be disabled .

11.5 Size of Mailbox and Emails

11. 5. 1 Mailbox size and e-mail attachment size for sending will be decided by ITSD based on business needs. For larger storage space the user would need to

submit a request to ITSD, which has to be authorized by the Dept Head/Branch Manager in accordance with guidelines provided by ITSD.

11.6 Server Security

11.6.1 Central Email Team is responsible for ensuring the security of the email servers. Central Email Team should setup the Email application and the underlying operating system as per secure configuration document.

11.6.2 Selected set of Email servers will need access to/from Internet for transacting with external domains and for remote mailbox access. These servers should be protected from Internet using a Firewall. The Firewall should be configured to ensure that only required ports are opened to/from Internet. The ports that need to be allowed should include secure SMTP ports for mail transfer, secure POP3, IMAP/NRPC/secure LDAP/ for downloading mails and Secure HTTP for web-mail access.

11.6.3 Email servers including SMTP relay server and user web-mail access server that directly interact with the Internet should not host any mailboxes. This is to ensure that in the event of compromise of these servers, user mails are not at risk.

11.6.4 Content filtering rules should be documented and applied at gateway server to remove email communication of harmful contents or attachments through emails.

11.6.5 Adequate steps should be taken to protect the users from SPAM mail. Anti-SPAM software should have the capability to reject mails sent from well-known open relay servers.

11.6.6 All communication between email client and server should be encrypted. Secure POP3, Secure SMTP, Secure IMAP, Secure LDAP, NRPC and Secure HTTP protocols should be enabled on the server. Necessary configuration steps should be taken on the server to ensure that users cannot use clear text protocols to connect to the server.

11.6.6.1 On intranet, all mail based services should be available to the email users.

11.6.6.2 On internet, only secure HTTP or NRPC protocols should be allowed.

11.6.7 The emails accessed through the internet using a browser should have session

timeout enabled in case the user is not accessing the mail for a specified time. Session time-out should be set to 5 minutes or less.

11. 6. 8 Anti-virus software installed on the Email server should be configured to check all internal and external mails.

11. 6. 9 Anti-virus software should be installed on Email servers including SMTP gateway systems and other related product servers that transact email with the external world. Anti-virus software should be configured to scan attachments in all Emails. If a virus is found in an incoming SMTP mail then the following actions should be taken:

11.6.9.1 Infected attachment should be deleted.

11.6.9.2 A notification sent to the recipient informing him/her that a virus was detected in the attachment along with the rest of the mail.

11. 6. 10 Email servers should be configured to attach a disclaimer to all outbound external mails. The following disclaimer can be used "The information in this mail is confidential and is intended solely for the addressee. Access to this mail by anyone else is unauthorized. Copying or further distribution beyond the original recipient may be unlawful. Any opinion expressed in this mail is that of the sender and does not necessarily reflect that of BANK(RRB)."

11. 6. 11 Mechanisms should be implemented to allow the user to access spam mails for a limited period of minimum 7 days.

11.7 Email Usage

11. 7. 1 Email sent by employees using Bank's email system would be equivalent to signed official communication sent by the respective individuals. Similarly incoming emails would also be treated as inward official communication received by the respective users.

11. 7. 2 Digital Signature can be considered for email communication based on sensitivity of content being sent and business requirements.

11. 7. 3 All official email communication should include following details:

11.7.3.1 The subject column of Email should have the brief of the text to be sent/ communicated. It should not be left blank.

11.7.3.2 All official emails should contain name of sender. Emails should not be sent Anonymous or using generic names like Designation or Dept Name only.

11.7.3.3 A signature must be used while sending emails, having details of Sender Name along with Designation, Dept and Contact Number.

11.7.3.4 Tag line or messages should not be used below signature.

11.7.4 Users should also refer to the Acceptable Usage Policy – E-mail usage for compliance.

11.7.5 Users should only use their own / designated email IDs for sending and receiving mails.

11.7.6 Any mass mailing like promotional or advertisement mails sent by the Bank should have an option for a user to opt out of receiving such emails. These e-mails should be discontinued, on receipt of such response.

11.7.7 All e-mail accounts should have a strong password. All Emails stored locally on the user's desktop should be protected by a strong password.

11.7.8 Users should promptly report all suspectedsecurity vulnerabilities or problems that they notice with the email system to the CET.

11.8 Monitoring

11.8.1 All email messages sent and received by the users of the Bank are considered as the property of the Bank. Bank reserves the right to examine all e-mail messages, files, directories, and other information stored on the Bank's computers at any time and without prior notice. E-mail messages may be monitored for any of the following reasons:

11.8.1.1 Ensuring internal policy compliance.

11.8.1.2 To support internal investigations for suspected criminal activity.

11.8.1.3 To assist with the management of information systems of the Bank.

11.8.1.4 Illegal activities or unlawful acts associated with the use of an e-mail service.

11.8.2 Bank has the right to disclose any suspicious e-mail messages sent or received by users of the Bank, to the law enforcement officials without prior notice to the employee who may have sent or received such messages. Users should therefore restrict their communications to business matters in recognition of this electronic monitoring.

11.8.3 The Bank will implement journaling for all mails, internal as well as external.

11.8.4 If the user wants to retrieve emails, the user should approach CET through

Dept. Head or other competent authority

11.9 Change Management

11.9.1 ITSD should be responsible for implementing changes to the Email server.

12 Backup

12.1 Policy Statement

Data and software essential to the continued operations of the Bank will be backed up and periodically tested for recovery by ASP. The security controls over the backup data and media should be stringent.

Standards and Procedures

12.2 Backup Process

12. 2. 1 ASP is responsible for Project Management , Data back up and maintenance .Backup should be taken regularly to ensure that data is available in the event of system failure or for recovering old transactions.

12.2. 2 ITSD should decide the scope of Backup process based on following requirements:

a. Business requirements

b. Legal/regulatory/statutory requirements

c. Criticality of the information

d. Restoration time constraints

12. 2. 3 Based on the scope, the ITSD should identify the essential components that need to be backed up for the respective application including

a. Operating system files

b. Application files

c. Data files

d. Configuration files

e. Database

f. Log files including operating system logs, application logs and security logs

12. 2. 4 Backup scheduling

12.2.4.1 Backup should be scheduled during non-peak usage hours.

12.2.4.2 Backup should be taken before and soon after execution of a critical process e.g. month end processing, annual closing

12.2. 5 Full backup should be taken before and soon after any major changes to hardware, OS, application or configuration including the following:

a. Upgrade of operating system.

b. Installing a new application component

12.2. 6 Type (Full, Incremental, Differential or Mirror backup etc.) and frequency of backup (Daily, Weekly etc.) and type of backup media to be used for each application should be decided by Application Owner taking into consideration the following parameters.

- Volume of transactions.
- Criticality of the data.
- Recovery time constraints

12. 2. 7 The backup media should be chosen based on the amount of data that needs to be backed up and the speed of backup device.

12. 2. 8 ITSD should define the retention period for all data handled bythe application.

12.2. 9 ITSD should determine the media expiry date when a new backup media is being introduced. This date is calculated considering the following parameters

a. Physical life of the media

b. Number of backups that will be taken

12. 2. 10 Responsibility for backup operations should be assigned to ASP.

13.2.10.1 For the applications deployed across the branches/ offices/Head Office,The Branch Manager/ IT Officer / System Officer respectively should be responsible for the backup operations.

12. 2. 11 A register should be maintained to track the backup operations. The register should have following details.

a. Serial Number to backup media

b. Application name

c. System Official name

d. Date of backup

e. Type of Backup data (Full, Incremental, Differential or Mirror)

f. Backup Status

g. Offsite storage information

h. Comments

12.2. 12 A register should also be maintained to track the recovery testing process. The register should detail the following.

- Serial Number of backup media
- Application name
- System Official name
- Date of testing
- Recovery Status
- Comments

12. 2. 13 The responsible officer should maintain the backup/recovery registers .

12.3 Security of data on backup media

12. 3. 1 Data on backup media should be secured against unauthorized access.

12. 3. 2 Multiple copies of backup should be maintained to deal with media failure based on the criticality and risk level of information backed-up. Data backup can be taken on different media including tape drives, CD-ROMs, hard disks, network storage etc.

12. 3. 3 Backup media should be secured against environmental and physical threats.

12. 3. 4 For critical applications, a copy of the backup should be stored offsite in a secure manner to protect against unauthorized activity. Distance between primary and offsite location should be decided as per recovery time constraints. Backup media should be properly packaged to prevent damage and tampering while transferring to offsite location.

12. 3. 5 Backup media should be disposed under the following conditions.

12.3.5.1 Media life has expired

12.3.5.2 Media is damaged and data is not accessible

12. 3. 6 Adequate security measures should be taken before disposing the media. Media Handling Policy should be followed for disposal of media.

12.4 Recovery Testing

12. 4. 1 Testing should be done periodically to ensure that data can be recovered fromthe backup media when required.

12.5 Documentation

12.5. 1 ITSD should be responsible for creating, maintaining and distributing the documents for backup and recovery procedures

12.5.1.1 Backup procedure documents should specify the following including standards and procedures defined in this document

- Which files need to be backed up?
- Frequency and type of backup
- How to verify that backup has been taken properly
- Time frame for retention of backup media
- Instructions about maintaining backup registers

12.5.1.2 Recovery procedure documents should specify the following including standards and procedures defined in this document

- The recovery steps
- How to verify if recovery is successful
- Frequency of recovery
- Instructions about maintaining recovery testing registers

13 Disaster Recovery

13.1 Policy Statement

13.1.1 Information systems that are critical to the Bank's business should be planned for continuity of operations in the event of disasters. Disaster Recovery Plan (DRP) which is part of Business Continuity plan should be formulated, maintained, tested and updated for such systems. The Disaster Recovery Plan and recovery strategies should be derived from Business Continuity plan of respective units. The plan should provide for appropriate safeguards to minimize the risk, cost, and duration of disruption to business processes caused by disasters.

Standards and Procedures

13.2 Need for Disaster Recovery

13. 2. 1 All applications which are critical to Bank's business, and any downtime of such application could result in considerable loss of business for the Bank, should have a Disaster Recovery (DR) plan. All these applications should have necessary provisions for timely recovery in the event of a disaster. A disaster is defined as a sudden, unplanned calamitous event that creates an inability on the part of an organization to provide the critical business functions for some predetermined period of time and which results in great damage or loss.

13. 2. 2 For the purpose of DR planning, the application should be considered as a single entity which has the following components - application software, supporting network links and devices and all associated infrastructure including servers and clients required for accessing the application data

13. 2. 3 ITSD and ASP will be responsible for developing disaster recovery strategy and plan for their respective domain applications.

13.3 Business Impact Analysis

13. 3. 1 The ITSD team should conduct a business impact analysis (BIA) taking into account the predetermined period of disruption/disaster as approved in Business Continuity plan of the application. The objectives of BIA are

13.3.1.1 Determine Banking functions supported by the application

13.3.1.2 Determine interdependencies between these Banking functions and dependencies on any other applications/processes.

13.3.1.3 Manpower and infrastructure requirements and assessent

13.3.1.4 Identify disaster scenarios and assess impact of outage

13.3.1.5 Determine acceptable downtime for Banking functions

13. 3. 2 BIA will consider the following aspects.

13.3.2.1 Loss to the Bank if the application fails e.g. financial loss, reputational loss

13.3.2.2 Legal and regulatory requirements.

13.3.2.3 Identify various possible disaster scenarios including physical damage/ destruction of servers, of Data Centre, of communication links or major power outages.

13.3.2.4 Resources required for running the application

13.3.2.5 Both the qualitative and quantitative impact of failure should be considered. Quantitative impact should estimate the monetary loss either in absolute value or percentage scale. Qualitative impact should detail out intangible losses that can impact operationally but that cannot be quantified in monetary terms.

13. 3. 3 ITSD and ASP should arrive at the Recovery Time Objective (RTO) and Recovery Point Objective (RPO) based on the results of BIA. Recovery Time Objective (RTO) is the time within which business functions or application systems must be restored to acceptable levels of operational capability to minimize the impact of a disaster.

13. 3. 4 RPO is defined as the point in time to which data should be recovered by DR plan. RPO will be a trade-off between the cost of lost data/cost of updating data from other sources versus cost of recovering to the most current data.

13.4 Disaster Recovery (DR) Strategy

13. 4. 1 The DRP team and ASP should evaluate different recovery strategies based onthe RTO for the application. This various DR strategies include the following:

13.4.1.1 On-site backup only

13.4.1.2 Alternate warm site with periodic data updation with primary site - Warm site will have all the necessary IT equipment including severs, desktops and

network links. Latest data has to be restored before personnel can move in and operations can start. Typical recovery time will be more than a day.

13.4.1.3 Hot site → Hot site will have all the necessary IT equipment and data replication will be enabled with primary site to ensure that site is always current in terms of operational readiness. The only delay involved in starting operations is for the personnel to move in. Typical recovery time will be within a day.

13. 4. 2 DRP team should select one/multiple recovery strategy based on the RTO. Cost/benefit analysis should be done for the selected strategy/s. DRP team should also identify the requirements for executing the strategies.

13. 4. 3 DRP team should determine the recovery point objective (RPO) within the chosen strategy to achieve the set RPO as decided under BIA process.

13. 4. 4 Based on the inputs received from DRP team, Application Owner should take a decision on the DR strategy.

13.5 Disaster Recovery (DR) Plan

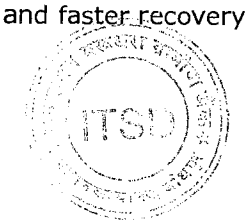
13. 5. 1 Disaster recovery plan should be developed based on the strategy. DR plan should contain emergency response plan, recovery plan and restoration plan. DR plan will contain details on what steps will be taken in the event of a disaster and should be developed by DRP team with participation from select users.

13. 5. 2 DR plan should identify an emergency response team and clearly identify the steps to be taken in the event of disaster.

13. 5. 3 DR plan document should be stored securely with easy accessibility to recovery team and associated team members. Approved copies of the plan should also be stored in offsite locations. Copies of DR plans for branches / offices should be available with Controllers.

13.6 Testing of DR Plan

13. 6. 1 Test exercise should be conducted at least yearly by DR testing team to verify the appropriateness of the DR plan. There should not be a gap of more than 6 mix between two consecutive DR testing exercise. This will create familiarity with the procedures before disaster, which will result in less confusions and faster recovery times.



13.7 Review of DR Plan

13. 7. 1 ITSD should be responsible for reviewing and updating the DR strategy and DR plan at least yearly.

13.8 Documentation of DR Plan

- DR Plan must be documented, approved by ITSD.
- All branches /ROs are instructed to comply with the following instructions relating to DR Plan.

14 Physical Security

14.1 Policy Statement

14. 1. 1 All sites, which house Bank's IT infrastructure and critical IT assets, should be protected from unauthorized physical access and environmental threats. All physical access and movement of IT assets should be monitored and reviewed.

Standards and Procedures

14.2 Physical Access Control

14. 2. 1 Areas identified as sensitive for IT operations should have a clearly defined perimeter that restricts access only to authorized users. This will include critical information processing facilities and Servers in branches and critical server areas in administrative offices. These secure areas should have adequate protection against unauthorized physical access to avoid theft or damage. Security guards

14.2.2.1 All employees should have photo-identity card with a serial number (for example employee number, PF Index number etc.)

14. 2. 2 Access to critical information processing facilities should be provided only after necessary approval from appropriate authority.

14. 2. 3 External people should be accompanied by Bank staff when entering/working in critical information processing facilities.

14.3 Security of Communication links and Power Cables flowing from outside through the premises

14. 3. 1 Communication links and Power Cables should be protected underground, where possible, or with adequate alternative protections.

14. 3. 2 Power cables should be segregated from communications links to prevent Electro-magnetic interference and should run in a way that a gap of at least one-foot is maintained between them.

14. 3. 3 Cables should be clearly labeled and documented to minimize handling errors such as accidental patching of wrong network cables.

14.4 Security of Servers at the Branches/Offices

14. 4. 1 The server area at the branches should be protected from risks arising due to Electromagnetism like UPS.

14. 4. 2 Access to Servers/Computers during leave/holidays should be restricted and controlled to authorized users only. Records should be maintained for such access.

14. 4. 3 It should be ensured that all branches/offices housing computer equipments should have preferably dedicated Earthing. Same should be checked for normalcy at regular intervals.

14.5 Environmental Protection

14. 5. 1 All IT equipment should have UPS (uninterrupted power supply) facility. UPS should have enough capacity to carry load of critical servers for sufficient time period. Arrangements should also be made for supply of power from a back-up generator.

14. 5. 2 Emergency power off switches should be provided in accessible locations

14. 5. 3 There should be adequate provision for fire detection and control including the following.

14.5.3.1 Fire/Smoke detectors and alarms should be installed

14.5.3.2 Fire extinguishers (water sprinklers and FM-200 / Carbon Dioxide) based) should be installed at easily accessible places.

14.5.3.3 Emergency telephone numbers for fire support personnel should be displayed.

14.5.3.4 Emergency evacuation procedures should be displayed.

14.5.3.5 Combustible materials like computer stationery should not be stored near the servers.

14. 5. 4 All personnel should be trained in use of fire extinguishers.

14. 5. 5 Eatables should be restricted to the dining area only. Smoking is prohibited in the branches/ offices.

14. 5. 6 System rooms should be kept clean and free from dust and dirt.

14.5.7 The severs and computer equipments should be secured from water leakage due to supporting facilities, heavy rain fall, and flood.

14. 5. 8 Continuous monitoring systems including Close circuit TV (CCTV) should be installed to monitor critical areas in branches/offices.

14.6 Record Maintenance for Monitoring

14. 6. 1 Records should be maintained for logs of CCTV camera, Accesscards, Biometric Access. Procedure should be devised for secure maintenance of recorded data as per record retention policy of the Bank.

14.7 Testing/Drill Exercise

14. 7. 1 Testing of fire alarms smoke detectors, cctv camera etc. should be conducted at least once in a year.

14.7. 2 List of emergency contact numbers should be displayed at identified locations.

14.8 Insurance

14.8. 1 All IT assets should be insured comprehensively covering the relevant risks.

14.9 Implementation of Physical Security

14. 9. 1 ASP/Branch Manager/ITSD should draw up detailed physical security plan and monitoring procedure specific to their systems based on the above guidelines. they are also responsible for implementing these plans and procedures.

15 Acceptable Usage

15.1 Policy Statement

15.1.1 IT assets of the Bank are provided for business purposes and authorized users should adhere to safe and acceptable usage practices that do not disrupt business or bring disrepute to the Bank. Standards should be defined for safe and acceptable usage of assigned IT resources and privileges including desktops, computer accounts, business applications, computer networks and for protection of information in physical or logical form and maintenance of Intellectual Property Rights by the users of information systems.

Standards and Procedures

15.2 Desktop Usage

15.2.1 Users are responsible for the security of their desktops and should take adequate measures to restrict physical and logical access to their desktops.

15.2.1.1 Desktop includes personal computers, and servers provided by Bank for official purpose.

Configuration & Installation

15.2.2 All desktops will be configured by Database Channel Manager (DBCM) as per the secure configuration standards provided by ITSD. Users should not change any hardware configuration, settings in operating system or any applications installed on their desktops. If users require any change in hardware like increase in system memory or software settings they should contact respective System Officials. No CD-ROM or PEN drive or any other external device should be attached to the desktop & all the USB ports should also be disabled as per the policy.

15.2.3 Users should not install any software or applications on their desktop that is not authorized for Bank's business. If the users require additional software, they should contact the System Official/Dept. Head/Branch Manager. Users should get their desktops formatted/repaired by designated AMC vendors preferably supervised by System / Bank Officials. Successful backup of critical

applications or data must be ensured before formatting of desktops.

15. 2. 4 Users should not connect modems to their machines unless and otherwise approved by the appropriate authority. Accessing external networks including Internet, using modems exposes the entire network to several risks. Users who require access to external networks through modem dialup, should get the approval from ITSD.

Protection Measures

15. 2. 5 To prevent the risk of unauthorized access, users should adopt the following measures-

15.2.5.1 Log out of all applications or turn off the desktop if they are leaving their desktop unattended for extended period of time

It is recommended to Use Boot level password/ power on password for all desktops.

Where systems (like branch servers) are required to be kept powered on for business purposes, then the system should be physically locked

15.2.5.2 To prevent unauthorized access while desktop is unattended for short duration, lock the workstation eg. using Windows Logo Key+ L and enable the screen saver with password protection

15.2.5.3 Do not enable sharing of folders in your Desktop with other users over the network except where specifically authorized.

Anti-virus

15. 2. 6 Users should not disable the installed anti-virus agent or change its settings defined during installation. This includes settings for daily virus scan, exception for drives for scanning, anti-virus server address and signature update schedules.

15. 2. 7 Users should not disrupt the auto virus scan scheduled on their desktop. If the scan is affecting system performance, users should contact System Official for resolution.

15. 2. 8 All files and emails received from external sources should be scanned for virus before opening. This includes files in removable media like CDs, Pen drives,

ITSD

DVDs, any other storage devices, Internet downloads, Email attachments or files etc. shared through network.

15. 2. 9 User should report to DBCM on any virus detected in the system and not cleaned by the anti-virus.

15.3 Mobile and Portable Devices (MPDs) like Laptop / Notepad/ Tablets etc.

15. 3. 1 MPD users should take additional responsibility for the security of their laptop/notepad type devices and the information it contains. Users should adopt the following measures and consult ITSD for any clarification

15.3.1.1 Ensure that MPD is configured as per the secure configuration documents provided by ITSD. Do not install unlicensed or doubtful software/ applications.

15.3.1.2 Enable boot level password/ power on password for additional protection. This will prevent any unauthorized person from even booting up your MPD.

15.3.1.3 All sensitive data on MPDs should be secured through password protection with encryption. This will reduce the risk of unauthorized access to confidential data in the event of loss of MPDs.

15.3.1.4 Whenever connecting to the LAN, ensure that anti-virus agent is installed with latest signatures on the MPD. User should ask DBCM to install anti-virus agent and update the signatures over LAN before accessing any application.

15.3.1.5 Take adequate measures for physical protection of laptop including not leaving MPDs unattended in public places or while traveling

15. 3. 2 If the MPD has modem/ dial up facility for Internet, users should disconnect Internet connection before connecting to LAN. Users having dialup facility are recommended to have personal firewall installed to prevent unauthorized access to their MPD while connected to Internet.

15. 3. 3 Loss of MPD should be reported immediately to the local police and to the controller and ITSD

15.4 Password Security

15.4.1 Users are responsible for all activities originating from their computer accounts. Users should protect the confidentiality of their accounts through good password management and should not allow anyone else to operate their accounts.

Password construction

15. 4. 2 Users should choose passwords that are easy to remember but difficult to guess. Some of the guidelines for password constructions are-

15.4.2.1 Do not use own name, short form of own name, own initials, names of family, friends, co-workers, company or popular characters

15.4.2.2 Do not use personal information like date-of-birth, address, telephone numbers etc

15.4.2.3 Do not use common words found in English dictionary.

15.4.2.4 Do not use word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc

15.4.2.5 Do not use any of the above preceded or followed by a digit (e.g., secret1, 1secret)

15.4.2.6 Strong passwords would have a minimum length of 8 characters and can be constructed through a mix of numerals (1,2,3 etc), special characters (!,@,#,$ etc) and Uppercase and Lowercase alphabets (A,B,C, a, b, c etc).

15.4.2.7 One way to create complex but easy to remember passwords is to take a known word or phrase and convert it using numerals, special characters and capital letters. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation. Similarly the word might be "complex" and password could be: "cOmp1@x)".

Password Protection

15. 4. 3 Users should not share their passwords with anyone including colleagues. Users should also not ask others (including customers and colleagues) for their passwords. All passwords are to be treated as sensitive, confidential information.

15. 4. 4 Users should ensure that nobody is watching when theyare entering

password into the system. Users should also not watch when others are entering passwords in their system.

15. 4. 5 User should not keep a written copy (in paper or electronic form) of password in easily locatable places.

15. 4. 6 Users should change their password regularly. Users must change their passwords under any of the following circumstances-

15.4.6.1 At least once in 90 days.

15.4.6.2 As enforced by system (applications and operating system)

15.4.6.3 If password has been shared with someone else

15.4.6.4 As soon as possible, after a password has been compromised or after you suspect that a password has been compromised.

15. 4. 7 User should report to the DBCM if account is locked out before 3 invalid attempts. All operating systems and applications should be configured to lock out the accounts after 3 invalid attempts. If the account gets locked out before 3 attempts, this could be because someone else was trying to guess the password.

15.5 Internet Usage

15. 5. 1 Internet access is provided to users for the performance and fulfillment of job responsibilities. Users should access Internet for business purposes and restrict non-business activities over Internet. It is important that all connections be secure, controlled, and monitored.

15. 5. 2 Users should not use Internet facilities to

15.5.2.1 Download or distribute malicious software or tools or to deliberately propagate any virus.

15.5.2.2 Violate any copyright or license agreement by downloading or distributing protected material

15.5.2.3 Upload files, software or data belonging to Bank to any Internet site/social media like Facebook, Whatsapp etc. without authorization of the competent authority.

15.5.2.4 Share any confidential or sensitive information of the Bank with any Internet site/social media like Facebook, Whatsapp etc. without authorization of the competent authority.

15.5.2.5 Post views or opinion on behalf of the Bank with any internet site /social media like Facebook, Whatsapp etc. without authorization of the competent authority.

15.5.2.6 Post remarks that are defamatory, obscene or not in line with Bank's policy on any subject.

15.5.2.7 Conduct illegal or unethical activities including gambling, accessing obscene material or misrepresenting the Bank. In case such misuse of the Internet access is detected, Bank can terminate the user Internet account and initiate disciplinary action against the user.

15. 5. 3 Users are responsible for protecting their Internet account and password. Users will be held responsible for any misuse of Internet access originating from their account.

15. 5. 4 Users should ensure that security is enabled on the Internet browser as per guidelines given below-

15.5.4.1 Configure browser not to remember web application passwords. (On Internet Explorer browser. Click Tools > Internet Options > Content > Auto Complete. Uncheck all options.

15.5.4.2 Set browser security setting to medium. (On Internet Explorer browser Click Tools > Internet Options > Security > Default Level. Set this to Medium)

15. 5. 5 Users should ensure that they do not access websites by clicking on links provide in emails or in other websites. When accessing a website where sensitive information is being accessed or financial transactions are done, it is advisable to access the website by typing the URL address manually rather than clicking on a link.

15. 5. 6 Bank reserves the right to monitor and review Internet usage of users to ensure compliance to this policy.

15.6 Email Usage

Email Service

15.6.1 Bank provides electronic mail resources to support Bank's business communication. Use of Bank's official mail account for personal purposes is

discouraged.

15. 6. 2 Users will be provided with a fixed amount of storage space in their mailboxes at the Email server. Mailbox size and e-mail attachment size for sending will be decided by CET based on business needs. Users are advised to periodically delete or download older mails from their mailbox into their machines.

15. 6. 3 Users are advised to retain important mails for record purposes in their machine or other media.

Types of messages

15. 6. 4 Confidential or sensitive information should not be transmitted over email unless it is encrypted or password protected. User should mark the email as confidential in the subject line in respect of email containing sensitive information.

15. 6. 5 Users owning the email account should be fully responsible for the content of email originated, replied or forwarded from their account to other users within or outside the Bank. The Bank is in no way responsible for the content of the email, be it body of mail or the attachment.

15. 6. 6 In case of inappropriate use of the email system the email account can be terminated and the Bank could take appropriate action.

15.6.6.1 Using email system to copy and/or transmit any document, software or other information protected by copyright or any other law.

15.6.6.2 Emails for personal gain or profit or job search.

Account protection

15. 6. 7 Users should protect their email account on the server through strong password and should not share their password or account with anyone else. Similarly, all Emails stored locally on the user's machine should also be protected by password.

Monitoring & Reporting

15. 6. 8 Bank reserves the right to monitor email messages and may intercept or disclose or assist in intercepting or disclosing Email communications to ensure that email usage is as per this policy. User communications are not considered private and by using Bank's email resources, users are deemed to have consented to having their communications monitored by authorized

personnel at Bank's discretion.

15. 6. 9 Users should promptly report all suspected security vulnerabilities or incidents that they notice with the Email system to IT Department.

15.7 Document and Storage Security

15. 7. 1 All documents containing sensitive information should be marked as "confidential" both in electronic and print format. Care should be taken to ensure confidentiality while these documents are transmitted over email, fax or other communication media or during printing and photocopying of documents.

15. 7. 2 All removable media including CD, DAT tape must be labeled as "confidential" if it is used to store "confidential" documents.

Security of information

15. 7. 3 Sensitive information should not be discussed in the presence of external personnel or other Bank employees who do not 'need to know' that information.

15. 7. 4 Sensitive information may get revealed unintentionally due to unsafe practices. Care should be exercised in the following scenarios to protect sensitive information-

15.7.4.1 Reading confidential documents in public places

15.7.4.2 Discussing confidential information in public places

15.7.4.3 Working on laptops in public places

15.7.4.4 Answering to queries over phone to unverified persons

15.7.4.5 Providing information to vendors/ suppliers

15. 7. 5 Posting information to various websites like social networking websites, marketing websites etc.

15.8 Incident Reporting

15. 8. 1 Users of IT systems should report any breach of security incidents identified on their IT systems to the branch manager at branches / Dept. Head or controller in Administrative Offices. They will escalate it to ITSD. Incidents may result in un-authorized access, disclosure of information, corruption of information or denial of service. Users can follow these guidelines in identifying an incident:

15.8.1.1 Abnormal system resource usage → If the CPU, memory utilization on a system is very high compared to normal usage in past, the system could have been compromised. Attackers use compromised systems for spreading viruses or attacking other machines leading to high resource utilization.

15.8.1.2 Abnormal, slow response for application → Users could experience extremely slow response times if the application servers or the network has been compromised and is being used for malicious purposes. Virus or worm outbreak could lead to network congestion that would in-turn cause application responses to be slow and unstable. Report instances where the response is extremely slow as compared to past usage.

15.8.1.3 Data corruption → If the user finds that data or files stored on the desktop has been either deleted or modified without their knowledge this could be sign of a compromised system.

15.8.1.4 Change in desktops → If your desktop configuration looks different from normal days in terms of applications installed, screen savers or icons on the screen or the desktop is misbehaving in terms of opening up new screen/ applications without your command and these changes have been done without your knowledge, it could be an indication of someone else using your desktop.

15.8.1.5 Changes in passwords → Users should report if they find their passwords do not work or their account has been locked without their knowledge. Any changes in user passwords could be indications of system compromise. Also report if you have suspicion of someone else using your account like emails sent from your mail id, or application accessed from your account or data posted from your account without your knowledge.

15.8.1.6 Virus infection → Users should report any virus or worm that infected one or more hosts at their site. However viruses or worms that are detected and cleaned by anti-virus software need not be reported, only those which are not getting cleaned and infecting the system needs to be reported.

15.8.1.7 Changes in applications → If the applications accessed by you look different from their normal appearances or your level of access in the application appears to have been modified (either increased access or

decreased access), the application may have been compromised.

15.8.1.8 Security weakness detected → If any weakness has been detected by you in the applications accessed by you that can cause unauthorized access or modification or lead of any kind of compromise, report such weaknesses to prevent any loss to Bank in future.

15.8.1.9 Violation by others → If you come across any instance of security violations committed by others like running of malicious tools, trying to break into system or committing IT frauds or thefts, copyright or license agreement violations, you should report such instances. Care should be taken not to report minor or unsubstantiated activities.

15.9 Security Violations

16.9.1 Certain categories of activities, which have the potential to harm, or actually harm information assets of the Bank are defined as security violations and are strictly prohibited. All security violations will entail disciplinary/financial/legal action. A security violation is any attempt to breach the security of IT resources, whether or not it results in actual damage or financial loss. The following are examples of security violations

15.9.1.1 Connecting modems to machines without approval

15.9.1.2 Introducing virus

15.9.1.3 Sniffing on the network

15.9.1.4 Password guessing

15.9.1.5 Computer impersonation

15.9.1.6 Erasing or modifying data on central systems without authority

15.9.1.7 Downloading or transmitting objectionable content (through Email or Internet)

15.9.1.8 Running scans or attack tools

15.9.1.9 Bypassing access control mechanisms

15.9.1.10 Exploiting any system vulnerability

15.9.1.11 Installing or distributing unlicensed software

15.9.1.12 Vandalism

15.9.1.13 Computer fraud or theft

16 Personnel Security

16.1 Policy Statement

16.1. 1 All authorized users including employees, vendors, contractors, third-party users etc. with access to information systems of the Bank should be made aware of their responsibilities in protecting information systems of the Bank, Authorized users should ensure adherence to information security responsibilities and any failure in this regard will entail appropriate actions by the Bank. Access to information systems will be provided based on job responsibilities and revoked or modified with changes in such responsibilities.

Standards and Procedures

16.2 Recruitment and Service Conditions

16.2. 1 Prior to recruitment of employees or engagement of staff on contract basis for computer-related positions of trust, like System Officials appropriate verification checks need to be carried out by the appropriate authority designated by the Bank or vendor management as acceptable to the Bank. This may include the following:

a. Verification of identity by Government issued Identity Card
b. Verification of references
c. Verification of employment history including any instance of misuse of information assets during employment
d. Verification of academic qualifications and/or certifications
e. Police verification check
f. Credit check

16.2. 2 For postings of existing employees in the Bank in computer related positions of trust, like System Officials, network administrators, database administrators and facilities management personnel for sensitive applications (refer glossary), Bank will lay down the criteria for screening employees, by considering, among other things, the following:

a. Qualification and experience required for the role
b. Previous instance of misuse of information assets

16.2. 3 It should be ensured by Application Owner that all authorized users of the Bank and vendor employees undertake to protect the information assets as part of their job responsibilities. Specifically, authorized users should undertake to observe the following conditions:

a. Keep all relevant data of the Bank as confidential

b. Access only the relevant data which is required for the job

c. Follow the acceptable usage policy of the Bank

16.2.4 A specimen of the Undertaking to be provided by the employees and authorized users is annexed. However, those employees who have already submitted the form for Fidelity and Secrecy in terms of BANK(RRB) General Regulations at the time of their appointment need not submit afresh.

16. 2. 5 Job rotation should be enforced for employees in computer-related positions of trust.

16. 2. 6 Reliance/dependency on single person on key areas should be avoided. Succession plans should be developed for Technical personnel deployed at critical locations. Adequate second line should be ensured for development/maintenance activities.

16. 2. 7 All external entities like contract staff or vendors, contractors, third-party users, consultants, having access to information assets of the Bank should sign information security undertaking and non-disclosure agreement. ITSD will develop and maintain standard non-disclosure agreement as approved by law dept. and security undertaking for external parties. Departments responsible for employing external parties should ensure signing of these documents by external parties.

16.3 Training and Awareness

16. 3. 1 All employees of the Bank should be provided with a basic awareness on their security responsibilities as per the policies and procedures of the Bank to enable them to protect Bank's information assets.

16. 3. 2 ITSD should arrange and coordinate periodical security training and awareness programs through the training systems of the Bank.

16.3.2.1 Regular and updated security awareness among employees can be provided through e-communication of information on policy and practice i.e. Tip of the Day, Precautions in routine working etc on Bank's portal.

16. 3. 3 Personnel staffing to conduct the IS Audit should have appropriate information security qualification like CISA/ISA/CISM/CISSP/ISO:27001(ISMS:2005) certifications.

16. 3. 4 Respective Application Owners / Heads of Departments should ensure that vendors, contractors, third party users are properly briefed on their information security roles and responsibilities prior to being granted access to sensitive information or information systems.

16.4 Compliance

16. 4. 1 Every employee of the Bank and employees of engaged external entities must agree to perform his security responsibilities and comply with the requirements specified in the security policies. Non-compliance with security policies should be dealt with appropriate action which may include disciplinary action/legal/financial actions as applicable.

16.5 Security Violations

16. 5. 1 Certain categories of activities, which have potential to harm, or actually harm information assets of the Bank are defined as security violations and are strictly prohibited. All security violations will entail disciplinary action. A security violation is any attempt to breach the security of applications, network and IT devices, whether or not it results in actual damage or financial loss. The following are examples of security violations-

16.5.1.1 Impersonation (also called as spoofing) - Impersonation involves any attempt to disguise identity while interacting with systems, which includes using other user's accounts or making transaction look coming from different IP address, constructing an electronic mail so that it appears to be from someone else, manipulating electronic packets, electronic directories or other electronic data to impersonate someone else or to mask own identity. Any authorized masking of IP addresses and computer accounts at security devices like firewall is not a violation.

16.5.1.2 Sniffing- Sniffing involves capturing communication in the network meant for other users either through use of tools from desktop or by introducing any device in the network for the purpose of interception or capturing packets. Sniffing conducted by authorized personnel for network diagnosis or for security monitoring purposes is not a violation.

16.5.1.3 Unauthorized connectivity- This involves any connectivity between the Bank's systems/ networks to other systems/ networks including connectivity to Internet or partner/ customer networks that is not authorized by ITSD.

16.5.1.4 Introducing virus- Any attempt to introduce or deliberately propagate viruses, worms, Trojans or other malevolent programs that can result in disabling of network or systems or loss of data.

16.5.1.5 Exploiting any system vulnerability- Involves taking advantage of security weakness in the systems or any administrative shortcomings to obtain unauthorized access or make unauthorized modification/ deletion or to steal information or to cause failure of the systems.

16.5.1.6 Unauthorized access- Involves access into systems where user doesn't have authorized account or attempts to bypass any mechanism on the network and systems that is used for controlling access and rights of users including bypassing firewalls or authentication scheme in applications & operating system or manipulating directories of systems to increase access levels

16.5.1.7 Installing or distributing unlicensed software- Involves installing, copying or distributing any copyright protected material on systems of the Bank in contradiction to license agreements

16.5.1.8 Denial of system or service- Involves attempt to obstruct legitimate users from accessing system/ network through disabling multi-user systems or clogging network or running denial-of-service tools

16.5.1.9 Password guessing- Involves attempt to guess passwords of other users or accounts either manually or through any password guessing tools

16.5.1.10 Unauthorized modification- Involves any unauthorized and deliberate deletion or change or tampering of the data, system files and applications residing on the multi-user systems of the Bank

16.5.1.11 Downloading or transmitting objectionable content- Involves downloading obscene and illegal data/ software from Internet or other systems/ networks into the systems/ network of the Bank or transmitting objectionable content to others using Bank's systems/ network

16.5.1.12 Vandalism- causing deliberate/ malafide damage to computer hardware of the Bank or sabotage the functioning of Bank's system

16.5.1.13 Fraud- fraudulently obtaining a financial or other advantage, or causing detriment to another by the use or manipulation of data

16.5.1.14 Theft- theft of any hardware device or software or data that is the property or in the custody of the Bank

16.5.1.15 Disabling security features- Involves disabling any installed security mechanism of the systems without authority of Application Owner/ ISD including audit trails, encryption protocols

16.5.2 Transmitting unsolicited/bulk emails and files to multiple users without approved business requirements.

16. 5. 3 Security Violations can be brought into notice by

16.5.3.1 Any employee of Bank or engaged external entities when security violations are observed

16.5.3.2 Bank's internal audit reports or

16.5.3.3 Compliance reports during external audit or review

16.5.3.4 Branch Heads/dept. Heads during routine supervision

16. 5. 4 Security violations should be investigated and appropriate action including disciplinary action may be initiated by the Controllers after careful study on technical aspects.

16. 5. 5 Controllers can take any of the following actions based on the analysis of the security violations-

16.5.5.1 Suspension of access privileges

16.5.5.2 Change of job responsibilities

16.5.5.3 Disciplinary action under service rules

16.5.5.4 Civil and criminal proceedings, under legal provisions including IT Act 2000

16.6 Responding/Reporting Security Incidents

16. 6. 1 All employees or employees of external entities have the responsibility to report suspected information security incidents and vulnerabilities as soon as possible to their controllers, designated Bank's official System Official/ITSD.

16.7 Transfer/Termination / Retirement procedures

16. 7. 1 In the event that employees including contract employees of the Bank or employees of vendors and external entities like auditors etc., are being transferred/terminating their employment/ engagement with the Bank or being terminated by the Bank, employees retiring from the Bank, the Branch Manager/dept. Head is responsible for-

16.7.1.1 Ensuring IT assets, such as access cards, Pen Drives, Laptops/Notepads given by the Bank, in the custody of the person are returned unless and otherwise permitted.

16.7.1.2 Ensuring that Bank related information is not retained or carried with him/her after the contractual relationship with the Bank ceases. A declaration/certificate to that effect should be obtained from the leaving employee.

16.7.1.3 Notifying all System Officials to terminate user accounts

16. 7. 2 In case of user, who is posted at sensitive area, has given notice to resign or being transferred or leaving the services for the Bank, should preferably be moved to non-sensitive work areas immediately by ensuring readiness of second line.

16.7. 3 Before services are discontinued access rights on sensitive IT systems or areas should be reduced or removed immediately depending on the risk involved in allowing the employee/user to continue in the same position. For example:

16.7.3.1 If termination of services is initiated by the employee or by management and the reason of termination;

16.7.3.2 The current access provided to employee/users.

16.7.3.3 The value of the assets currently accessible etc.

16.8 Information Security – User Undertaking

I agree to abide by the Bank's Information System Security policy. I undertake to

- Keep all relevant data of the Bank as confidential
- Access only the relevant data that is required for the job
- Follow the acceptable usage policy of the Bank

- Perform the security responsibilities and comply with the requirements specified in the security policies

I understand the importance of information security and agree to take all reasonable precautions, to protect the information assets of the Bank. I also understand that non-compliance with security policies can lead to disciplinary action [for Bank's employees] or financial/legal actions as per the agreement [for vendor, contractors, and third-party personnel].

In the event of my resignation, retirement or termination of services with Bank, I undertake as under:

- I shall continue to abide by the declaration of fidelity and secrecy/ non-disclosure agreement executed by me at the time of my employment/services with Bank.
- I shall not share any information regarding internal workings of Bank's IT Systems.
- I shall not share any information regarding internal operations, systems and procedures of Bank.
- I shall not utilize my knowledge of Bank's systems and procedures to carry out, overtly or covertly, any activities, which may lead to financial loss to Bank.
- I shall not use my knowledge of Bank's customers and business information acquired during my tenure to the detriment of Bank's interests.

If any loss is caused to Bank on account of any breach of the above, Bank shall be at liberty to take such action, as would deem fit, which would include legal action.

Date:

User Name

User ID

Signature of User

PF Number / Name of Organization

17 Segregation of Duties

17.1 Policy Statement

- Duties and areas of responsibilities shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the Bank's information system assets.

  This policy applies to SBI officials as well as all authorized users including vendors and third party service providers.
- As the bank has totally outsourced development, customization, processing, administration or management of bank's application software and management of CDC with M/S C-Edge Technologies Pvt Ltd., ASP this area should be taken care of by them as per industry practice.

18 IT Compliance

18.1 Policy Statement

18.1.1 Bank should identify and assess the applicable legal requirements and regulatory directives issued from time to time, with respect to their IT operations supporting business initiatives. Bank should define specific procedures to comply with these requirements.

Standards and Procedures

18.2 Identification of applicable legislation

18.2.1 ITSD should regularly scan the current legislation and identify applicable legal requirements.

18.2.2 ITSD should then send these identified legal requirements to legal Dept for their feedback and confirmation as to their applicability.

18.2.3 Few applicable legal requirements, but not limited to, are as follows:

18.2.3.1 IT Act 2000 & its Amendment 2008

18.2.3.2 Intellectual property rights (Patent Act 1961, Copyright Act 1985)

18.2.3.3 Intellectual property rights include trademarks, patents, source code licenses, software copy rights, document copy rights. Compliance with legislative, regulatory, and contractual requirements on the use of material that has intellectual property rights and use of proprietary software will be ensured by defining and implementing appropriate procedures. Necessary steps are to be taken to protect Bank's Intellectual Property rights like patents / copyrights, trademarks, source code licenses etc.

18.2.3.4 Protection of Organizational records (e-records maintenance) (Banker's Books Evidence Act 1891)

18.2.3.5 Important records should be protected from loss, destruction, and falsification, in accordance with statutory, regulatory, contractual and business requirements. Preservation of records is a fundamental responsibility through which the Banks ensure the continuing availability and reliability of the archived

records that it holds in trust for present and future needs. Preservation of record is also governed by Right to Information Act, 2005 (RTI) and Prevention of Money Laundering Act, 2002 (PMLA) etc. Application Owner should also refer Record Retention Policy and Backup Policy of the Bank.

18.2.3.6 Data protection and privacy of personal information

18.2.3.7 Protection and privacy of organizational data should be ensured as required in legislation, regulations, and contracts. The legislations placing controls on the collection, processing, and transmission of personal data should be strictly followed. Application Owner should also refer to Data Protection Policy of the Bank for identifying different levels of protection.

18.3 Identification of applicable regulatory requirements

18. 3. 1 ITSD should ensure that all latest applicable IT regulatory directives laid down by the regulatory bodies eg RBI, SEBI etc. are identified.

18.4 Application of identified requirements

18. 4. 1 After the identification of legal and regulatory requirements, ITSD in consultation with other HODs and GMs should formulate the procedures for implementation of specific controls to comply these requirements.

18. 4. 2 ITSD should ensure the implementation of identified legal and regulatory requirements in their respective applications and its related IT infrastructure.

18. 4. 3 ITSD should submit the identified legal requirements and its applicable controls & procedures to CISO.

18. 4. 4ITSD should ensure the compliance to these identified requirements when deploying or arranging for deployment of new IT systems.

18.4.5 ITSD shall ensure that the IS Security Policies are in line with the regulatory requirements from time to time.

18.5 Sharing of IT related information or e-records with Legal Agencies or GOI Authorized bodies

18. 5. 1 Any IT related information or e-records can be shared with Legal agencies or GOI Authorized bodies only after receiving a formal written request.

18. 5. 2 After the receipt of formal request, the concerned department should consult the ITSD for respective e-records or information related to the request.

18. 5. 3 The HOD of the concerned department should then analyze these e-records or information for ascertaining the impact of sharing this information, on Bank.

18. 5. 4 The HOD of the concerned department should also consult the Legal Dept before any sharing of information.

18. 5. 5 The HOD of the concerned department should maintain a record of all information shared with Legal agencies or GOI authorized bodies.

18.5. 6 If any e-records are shared with Legal Agencies or GOI authorized bodies, then those e-records should be encrypted or digitally signed by the business owner before sharing. A copy of those digitally signed e-records should be maintained for future reference.

19 User Access and Password Management

19.1 Policy Statement

19.1. 1 Access to information and Information Systems including applications, operating systems, database, should be provided to users only after proper identification and authentication. The allocation and use of privileges should be restricted and controlled. User access to information assets should be reviewed at regular intervals, to ensure that they are maintained in line with business requirements, and accounts which are no longer required should be disabled.

Standards and Procedures

Information Systems should enforce unique user IDs and strong passwords for user authentication. User credentials should be communicated to authorized users through a secure process. Users should be directed to change the passwords at first logon and subsequently at periodic intervals to prevent any unauthorized event. Appropriate compensating controls should be ensured where strong password cannot be enforced by the system.

19.2 User Access Management

Access to users on Information Systems including applications, operating systems, databases, etc should be provided by ensuring following controls:

19. 2. 1 User and business requirements for him/her to access an Information Systems should be identified and approved before providing an access.

19. 2. 2 Access rights to a user should be allocated on principle of least privilege and need to know or need to do/have basis.

19. 2. 3 There should be provision for multiple privilege levels within the Information System. The privilege levels required for a user should be based on roles and responsibilities. Privilege levels should be clearly documented and approved by the Application Owner before being implemented.

19. 2. 4 Wherever the business rules stipulate different financial powers for different categories of staff, the same should be implemented through appropriate privilege levels.

19. 2. 5 All transactions with financial implication should have a separate requestor

and approver. If there are any transactions that can be initiated and completed by the same person, these should be identified, documented and approved by the Application Owner. Logging of user activities and review of the same should be ensured.

19. 2. 6 User access to information should be controlled so as to allow only the required combination of rights like queries, modification, update and delete. For example, the Inspecting/Auditing Officials should have read only privilege, normally confined to auditee's unit and scope of audit.

19. 2. 7 It is possible to have access to the systems at various levels i.e. Operating Systems, Network, Database and Application. Access should be granted at the required level with only minimum privilege as required for the role after analyzing operational requirement of the user and it should be properly documented.

19. 2. 8 ITSD should ensure that access rights of all users should be documented, monitored, reviewed and updated.

19.3 User IDs

19. 3. 1 User IDs should be created or assigned for individual users to distinguish the user's identity uniquely. There should not be generic User ID or more than one user ID for a user on single system with same/ different privilege(s).

19. 3. 2 There should be no sharing of user accounts.

19.3.2.1 In critical cases, where user accounts of administrative privilege or super-user accounts need to be shared, ITSD should identify such cases and implement appropriate compensatory controls on approval of General Manager.

19.3. 3 Temporary user accounts should be disabled immediately after use. Authorizing officials are responsible for disabling of same.

19. 3. 4 Temporary account should be configured for maximum a week. If same is required for more than a week, same should be reviewed and approved by respective controller.

19.3.4.1 I&A Dept need to have an account to be used for periodical system audit. This is a temporary account and should be deleted soon after the audit is completed.

19. 3. 5 User IDs should not give any indication of the user's privilege level.

19.3.6 If user is idle for a pre-specified period of time, the application should automatically log-out his User-ID and user should re-authenticate his/her User ID again with the application.

19.4 New User Approval and Creation

19.4.1 All information systems should have officials identified for

- Approval of user access
- Creation of User IDs and
- Assignment of access privileges.

Approval of user access

19.4.2 When a new user has to be created in the system, the Branch Manager/ Dept Head should approve the request and determine the privilege levels that the user needs. User creation request should be filled completely and should mention all required information of requested user.

Creation of User IDs

19.4.3 All IT systems including application, operating system, database and network/security devices should have officials identified for new user creation (User Control Officer-UCO) and assignment of privileges separately.

19.4.4 UCO should have an account on the Information System for creation of user ID with no transactional privileges assigned to it.

19.4.5 No User ID should be created by UCO without required approval.

19.4.6 The operating procedure for user creation for each application should be defined and implemented after approval from the Application Owner. Same procedures should also be followed for Change in Privilege level to ensure Separation of Duties.

19.4.7 Deletion/Removal of User ID should follow the similar standards and procedures as above. Personnel Security Policy in regard to retirement/ resignation/termination should be followed meticulously.

Assignment of Access Privileges

19.4.8 Application Owner should identify, document various access privileges required to enforce the business rules. Applicable requirements like Financial Powers of officials, Job assignments etc should be taken into account. The following controls should be implemented, while designing and administering

the privilege levels:

19.4.8.1 Access privilege to users should be allocated based on the principle of least privilege. User privileges should be based on a need to have and need to do basis.

19.4.8.2 Privileges granted to the user should not be in conflict with the principles of segregation of duties.

19.4.8.3 For any change in the privileges, the request should be approved by the official designated, before submitting the same to the authorized official to carry out the changes.

19.4.8.4 Access privilege should be assigned with assigning expiry date more than a year or date of retirement or ceasing the engagement with the Bank whichever is earlier. Same should be reviewed accordingly.

19.4.9 A record should be maintained as and when User IDs are created/modified/deleted by UCO and the same should be acknowledged by respective users.

19.5 Password Management

The following standards should be enforced for password management:

19. 5. 1 Users should be verified for his/her identity before providing a new, replacement or temporary password.

19. 5. 2 User ID and Password should be uniquely associated. Generic passwords should not be used for new/reset passwords.

19. 5. 3 Passwords shall have a minimum length of 8 characters.

19. 5.4 Strong passwords having a combination of uppercase andlowercase alphabets, numerals and special characters should be used.

19. 5. 5 The system should force a new user to change the password at first logon and on reset of password.

19. 5. 6 Receipt of passwords should be acknowledged, if feasible.

19. 5. 7 Passwords should be masked while keying-in.

19.5.8 Passwords should be set to expire after a maximum period of 90 days. Wherever feasible, the Information System should provide a mechanism to enforce the change of password periodically and password should not be part of the application source code (i.e. not hard coded into the application).

19. 5. 9 Seven days prior to expiry, a message should be displayed to change the password, after every login, if supported by information system.

19. 5. 10 Password history should be maintained. The last 5 passwords should not be reusable.

19. 5. 11 For applications, users should be allowed to login with old password even after password expiry, but the application should force the user to change the password immediately.

19. 5. 12 For critical systems, users should not be allowed to access information system after a maximum of three invalid input attempts, and user account should be locked out automatically after three invalid attempts.

19. 5. 13 Procedure for unlocking and password reset should be documented. The authorized official only can unlock the user-id or reset the password after due investigation for the cause of account lock. The authorized official should record the unlocking in a register.

19.5.14 Identified Application(s) can also unlock the user-ids after 24 hours automatically.

19.5.15 Passwords display / printing should be masked preventing unauthorized parties from observing them.

19. 5. 16 On change of password, it should be entered twice to confirm the correctness of password and to prevent from being locked out of the system.

19. 5. 17 Password complexity or Password expiry controls need not be implemented for applications being accessed by customers, initially when the application is launched. However, these rules for customer access should be reviewed periodically and appropriate controls can be implemented. User feedback, should be obtained, if felt necessary.

19. 5. 18 Acceptable Usage Policy should be followed for secure password usage by users.

19.6 Security of User credentials

19. 6. 1 User passwords should be stored in encrypted format. Password should not be stored in readable form / hard coded into software/log-in scripts/batch files etc.

19. 6. 2 Information System including operating system, application and database should support encryption mechanism for storing credentials so that it cannot be retrieved by other users

19. 6. 3 Password should be encrypted when transmitted over networks to prevent unauthorized access

19. 6. 4 All super administrative or root password should be kept secured in double lock keys for use in case of emergency situations. Any usage of these passwords should be recorded and changed with new password immediately once need is over and on next logon.

19.7 User Access Review

19. 7. 1 User access reviews should be carried out periodically, at-least once in six months, to ensure that only users who currently require access have access rights and the privileges allocated to the users are in conformity with their current role.

19. 7. 2 User IDs that have not been used for a period of 2 weeks can be considered stale. Stale User IDs should be disabled. ITSD should ensure disabling of stale user IDs regularly.

19. 7. 3 Records of user creation/deletion, password reset, old or previous profiles of the user, access violations, and failed login attempts should be retained in the archives in accordance legal/regulatory/policy requirements.

19.8 Logging

19. 8. 1 Logging should be enabled to track system misuse. Audit enables system administrators to monitor critical events and it is an early warning towards attempts at malicious access. Logs provide the audit trail and play an important role in tracking malicious users in the event of a fraud.

19. 8. 2 The Information Systems should be able to log all security related eventsincluding the following:

19.8.2.1 User access management

19.8.2.2 User Privilege changes

19.8.2.3 User login/logout time

19.8.2.4 Changes in Information System configuration

19.8.2.5 Authentication failures

19.8.2.6 Access to audit trail

19.8. 3 ITSD should determine the retention period for log files. ITSD should consult P&D dept. to ensure that retention periods are compliant with the legal/regulatory requirements and Bank's policy for record retention.

20 Web Presence (Intranet & Internet) and Communications

20.1 Policy Statement

Bank should have its web presence through its own websites and Social Networking Sites. Single domain name policy for own websites should be adopted and implemented. Bank should have a website content management processes to ensure that the information published on websites is accurate, consistent, and current. Employees having social networking sites user accounts should adhere to web browsing practices that do not bring Bank into disrepute. Bank should manage its IT resources to protect against incidents including Website defacement, Web Identity theft, Denial of Service; also Bank's reputation is protected in all manners.

20.2 Standards and Procedures

20.3 Single Domain for Web Presence (Intranet & Internet Websites)

20.3.1 "Single domain name policy" should be adopted and applied across all web facing Banking applications and informational web sites of Bank. The transactional sites should be registered as sub domains of "www.onlinermgb.in" and the
informational sites should be registered as sub domains of "www.rmgb.in".

20.3.1.1 All transactional websites and other websites handling sensitive information should be secured with SSL certificate of adequate strength min. 128 bits.

20. 4 Website Content Management

20. 4. 1 All activities on website should be approved and monitored by General Manager which are as follows:

20.4.1.1 Uploading, editing or display of any information or files on the website should be authenticated and checked.

20.4.1.2 Records for all information or files displayed, uploaded, edited or any other related information of the website should be maintained.

20.4.1.3 ITSD should formulate procedures for website content management activities.

20.4.1.4 P&D should regularly monitor website for validity of contents or displaying of any misleading information on Website.

20.4.1.5 Email Accounts displayed in website for contacting the bank should have a designated official responsible for regular checking and sending appropriate reply to these emails.

20.4.1.6 Compliance with legal, regulatory and government directives eg. violation of copyright, intellectual property rights, data privacy etc.

20. 4. 2 If the Website maintenance is outsourced, then the Application Owner should ensure that the vendor shall not upload, edit, and display any information in the website without prior approval from Bank.

20.5 Social Networking Sites (SNS)

20. 5. 1 Management of Company Profile and User Account in the name of Bank.

20.5.2 Social Networking Sites shall be identified by P&D Dept. P&D Dept shall submit the proposal detailing Social Networking Sites, business requirement for presence on same and nature of presence and scope. Same shall be approved by Chairman for Bank's presence on required Social Networking Sites. Bank shall have only one official profile for the Bank on identified Social Networking Sites (SNS). Bank's presence on Social Networking Sites shall be permitted only for promoting Bank's products and services.

20.5.3 There should be a centralized team for creating, maintaining, monitoring and deleting these official profiles on SNSs.

20. 5. 4 There should be a team for day-to-day posting/reply to messages received on such SNS, from respective requesting group. Such activities including reply messages should be overseen by senior level official

20.5.5 While managing Bank's Profile by centralized team, no confidential information of Bank should be posted or shared. Data Protection Policy of Bank should be adhered to.

20.5.6 A message should be displayed on the Bank's profile on SNS for Bank's customers for not sharing of personal and confidential information within Social Networking site.

20. 5. 7 No profile in the name of Bank should be created without approval.

20. 5. 8 A centralized database of all profiles created in the name of Bank should be maintained by centralized team.

20. 5. 9 Personal User account

20.5.9.1 The employees having personal SNS user accounts should not use them to communicate directly or indirectly on behalf of Bank.

20.6 Web Presence related Incident response

20. 6. 1 Response to incidents on Bank's website should be dealt in accordance with Standards and Procedures on Incident Management.

21 Vulnerability Assessment and Penetration Testing (VAPT) Policy

21.1 Purpose

The purpose of this policy is to ensure that the bank's systems and networks are regularly assessed for vulnerabilities and that any identified vulnerabilities are promptly remediated.

21.2 Definitions

Vulnerability assessment: A process of identifying and classifying security vulnerabilities in a system or network.

Penetration testing: A simulated attack on a system or network to assess its security posture.

Risk: The likelihood and impact of a security vulnerability being exploited.

21.3 Scope

This policy applies to all systems and networks within the bank, including:

- Operating systems
- Applications
- Databases
- Network devices
- Web servers

21.4 Frequency

Vulnerability assessments and penetration tests will be conducted on a regular basis annually. The frequency of assessments and tests may be increased based on the risk profile of the system or network.

21.5 Responsibility

The IT department is responsible for the implementation and enforcement of this policy.

21.6 Methodology

Vulnerability assessments and penetration tests will be conducted using industry-standard methodologies. The specific methodology used will be determined based on the risk profile of the system or network.

21.7 Remediation

Any vulnerabilities identified during a vulnerability assessment or penetration test will be promptly remediated. The remediation process will be documented and tracked.

21.8 Reporting

The results of all vulnerability assessments and penetration tests will be reported to the GM, IT.

22. Cloud Services

22.1 Policy Statement

22.1.1 Owing to the dynamic and changing nature of data processing. The bank may avail cloud services ensuring protection of data, operational integrity, and regularity compliance. The services can be used to deploy bank applications tools and data backup, to facilitate the banking operational aspects.

22.2 Definitions

Cloud computing is a method of delivering Information and Communication Technology (ICT) services where the customer pays to use, rather than necessarily own, the resources. These services are typically provided by third parties using Internet technologies.

At present there are four widely accepted service delivery models:

- Infrastructure as a Service (IaaS);
- Software as a Service (SaaS);
- Platform as a Service (PaaS);
- Network as a Service (NaaS)

Cloud services are provided via four deployment models:

- Private cloud – where services are provided by an internal provider, i.e. IS Services;
- Public cloud – where services are provided by third parties, i.e. external companies or entities, over the public Internet;
- Community cloud – where services are provided by external company(s) or entity(s) for a specific community of users with common interests;
- Hybrid cloud -- where services are provided partly by an internal provider in a private cloud and partly provided by an external company(s) or entity(s) in the public or community cloud.

Cloud services can provide a significant range of benefits to individuals and organisations including increased solution choice and flexibility, faster time to solution, and reduced total cost of ownership. However, the cloud also presents new challenges.

22.3 Selection of Cloud Services Providers

22.3.1 IT Department may use cloud services from reputed and well established companies such as Microsoft, Google, Amazon as per the need. Private cloud service from the ASP also may be availed.

22.3.2 The chosen cloud service providers must align with the bank's data protection and security standards.

22.4 Service Level Agreement

22.4.1 A service level agreement (SLA) describes the service that the third party will provide, the performance targets (e.g. service availability, problem resolution, security, etc) and mechanisms for compensating the bank if the SLA targets are not met. You must ensure that the contract for cloud services includes an SLA that meets business needs.

22.5 Access Control and Data Security

22.5.1 Access to cloud services should be restricted based on job roles and responsibilities. Access should be granted on a need-to-how basis.

22.5.2 All data uploaded to or accessed from cloud services must be classified based on sensitivity.

22.5.3 Cloud storage to be used as secondary data storage solution, Local storage to be primary storage.

23 Staff Accountability Examination for Technology/IT Related Matters

Technology also involves frequent resetting of parameters due to changes in interest rates, service charges and other business needs etc. In such cases, the persons are expected to carry out such work with utmost care and ensure that there are no mistakes in the changes and such changes are properly validated by the supervisors. This is one of the key areas, as the parameter changes are made at the global level and will affect the entire Bank. The income leakages in such cases will be huge. Since, it affects the income of the Bank and also its reputation and may lead to customer complaints, the officials both at the Branch/ User level as well as at IT Department handling such matters have to carry out such work with due diligence and utmost care and have to be made responsible for such parameter changes.

However, sometimes in spite of effecting the changes as required, the system behaves erratically and may not give the expected output resulting in loss/gain of income to the Bank and no apparent negligence on the part of the concerned official is visible. For such systemic failures, the concerned officials generally shall not be made accountable provided, in such cases the Official ensures reporting of the same as per Incidence Reporting procedure of the Bank.

The following lapses/ deficiencies/ irregularities may invite disciplinary action. However, the following list is indicative only and not exhaustive:

23.1 IT Incidents / Cyber Incidents:

- Any act of non-performance or omission resulting in IT/ Cyber Incident including outage of services especially due to negligence or malafide intention of the official.
- Non-reporting of all IT/ IS Incidents within prescribed timelines, as per IT System Incident Reporting Procedure issued by IT Department or Cyber Crisis Management Plan as modified from time to time. For Cyber Incidents, non- follow up of the procedure laid down by IT Department in the relevant SOPs.
- Non-reporting of Cyber Incidents within the timelines prescribed in Cyber Security Policy for reporting to appropriate authorities including RBI, Cert In, NCIIPC etc.
- Non-reporting/ delayed reporting/ non-escalation of any known Security Incident to the appropriate authority.
- Non-follow up of closure of IT Incidents/ Cyber Incidents by initiating corrective/ preventive actions.

- Lapses on the part of official(s) in carrying out Root Cause Analysis (RCA) and closure of Incident. Non- analyzing the reason/ RCA of such Incident and initiating further necessary corrective or preventive action whether it is system related/ human error/ non-follow up of laid down procedures.
- Non-reporting of any financial loss resulted out of the Incident to the Controller(s) as well as to IT Department.
- Necessary follow up of procedure for accounting and recovery of the loss not carried out.
- De-integration of any System from Security Solutions or monitoring system with intention to hide the action.
- Unauthorized Deletion/ Modification of data with ulterior motives in order to dilute audit trail or hide any action.

23.2 Non-compliance of System, Procedures, Policies, Regulatory Instructions:

- Non-follow up/ non-adherence to Bank's laid down policies and procedures/ instructions including Security guidelines resulting in loss/ reputational loss
- Non-rectification/ delayed rectification of any error or bug known or detected resulting in loss to the Bank/ non-functioning of the application/ cyber-attack
- Non-compliance/ delayed compliance of any Regulatory instructions/ Advisories by the concerned official either by negligence or intentional resulting in adverse comments from RBI and other regulators, show cause notice, Penalty(s) from the Regulator etc.
- Submission of any false compliance of any regulatory guidelines/ Policies/ Advisories resulting in loss/ reputational loss/ show cause notice/ penalty etc. to the Bank or otherwise.
- Submission of any false compliance/ delayed compliance to the audit, security review findings etc. to the Bank or otherwise

23.3 Data Leakage:

- Any act resulting in leakage of Bank's data especially sensitive & confidential information to unauthorized persons.
- Sharing of any sensitive/ confidential information to those outside the Bank without approval of appropriate authority.

24 Glossary

24.1 Abbreviations

CAT	:	Central Anti-Virus Team
CCC	:	Change Control Committee
CCIT	:	Corporate Center IT
CERT	:	Computer Emergency Response Team
CET	:	Central Email Team
CFT	:	Central Firewall Team
CMT	:	Central Monitoring Team
CVC	:	Central Vigilance Commission
DCM	:	Data Centre Manager
CIO	:	Chief Information Officer
CISO	:	Chief Information Security Officer
DMZ	:	De-Militarized Zone
DR	:	Disaster Recovery
GUI	:	Graphical User Interface
HTTP	:	Hyper Text Transfer Protocol
IPR	:	Intellectual Property Rights
IS	:	Information Systems
ITSD	:	Information Technology Department
ISSSC	:	Information Systems Security Standards Committee (succeeded 2012byISC)
ISC	:	Information Security Committee
IT	:	Information Technology
LAN	:	Local Area Network
NDA	:	Non-Disclosure Agreement
PKI		Public Key Infrastructure
SCD	:	Secure Configuration Document
SLA	:	Service Level Agreement
SQA	:	Software Quality Assurance
SRS	:	Software Requirement Specifications
UAT	:	User Acceptance Test
UCO	:	User Control Officer
URL	:	Universal Resource Locator
URS	:	User Requirement Specifications
WAN	:	Wide Area Network
P&D	:	Planning and Development

24.2 Definition of Terms

Acceptance Testing	:	Formal testing conducted to determine whether or not a system meets the requirements specified in the contract or by the user. This testing enables the user to determine whether or not to accept the system.
Access Control	:	The process of limiting access to the resources of an IT asset only to authorized users, programs, processes, systems or network.
Accuracy	:	A qualitative assessment of correctness, or freedom from error in data processing

Alert	:	Alerts are often derived from critical audit events. They provide notice of specific attacks directed at IT assets.
Anonymous Login	:	Services may be made available without any kind of authentication. This is commonly done, for instance, with the FTP protocol to allow anonymous access.
Application	:	A software package designed to perform a specific set of functions that is relevant to business, such as accounting, transaction processing or communications.
Application Owner	:	Person having overall responsibility for application security in all activities related to design, development, deployment and support
Audit Trails	:	In computer security systems, a chronological record of system resource usage. This includes user login, file access, other various activities, and whether any actual or attempted security violations occurred, legitimate and unauthorized.
Authentication	:	To verify the identity of a user, device, or other entity in a system, often as a prerequisite to allowing access to resources in a system
Authorization	:	The granting of access rights to a user, program, or process. Usually, authorization is in the context of authentication. Once you have authenticated a user, the user may be authorized different type of access.
Authorized User	:	A user that has been granted permission, with clear limitations, to access information and systems.
Availability	:	The ability to use or access IT resources by authorized users as required. The property relates to the concern that information systems are accessible when needed and without undue delay.
Backdoor	:	Hidden software or hardware mechanism used to circumvent security controls or provide a way to access a computer other than through a normal login.
Banner	:	Display that appears on an information system to notify the user of conditions and restrictions governing system or data use.
Biometrics	:	Automated methods of authenticating or verifying a user based on physical or behavioral characteristics.
Black Box Testing	:	A method of verifying that software functions perform correctly without examining the internal program logic.
Branch Manager	:	Denotes heads of branches irrespective of designation in Bank
Branches	:	Also includes IT processing centers like SOC, MICR, GLS, CMP
Breaches/ Compromise	:	Bypassing of security controls which could result in disclosure or damage of information systems. A violation of controls of a particular information system such that information assets or system components are unduly exposed.
Buffer Overflow	:	This happens when more data is put into a buffer or holding area than the buffer can handle. This is due to a mismatch in processing rates between the producing and consuming processes. This can result in system crashes

		or the creation of a back door leading to system access.
Bugs	:	Any defect in the software that affects its functionality or security
Computer Fraud	:	Computer-related crimes involving deliberate misrepresentation or alteration of data in order to obtain something of value.
Computer related positions of trust	:	Includes system administrators, network administrators, database administrator, facilities management personnel for critical applications like Core Banking, , SBI Connect, etc and persons having rights to create/ modify users on such applications.
Confidentiality	:	The assurance that information is not disclosed to inappropriate entities or processes. Confidentiality is defined as ensuring that information is accessible only to those authorized to have access.
Configuration	:	In configuration management, the functional and physical characteristics of hardware or software as set forth in technical documentation by election of one of the sets of possible combinations of features of a system.
Cookies	:	Data exchanged between an HTTP server and a browser (a client of the server) to store state information on the client side and retrieve it later for server use.
Corporate Center IT	:	Refers to all IT departments reporting to DMD & CIO.
Credit check	:	Verification of pecuniary liability of the person being recruited/engaged by way of declaration by the person himself and by reference to former employer.
Critical Information Asset	:	All information assets whose unavailability, modification/degradation/damage and / or unauthorized disclosure can lead to a significant loss of business and the business cannot continue to perform its primary function in normal manner eg. Core Banking, ATM, Internet Banking, Payment Systems, Mobile Banking, Data Centre, Treasury.
Cryptography	:	Science that provides the means, methods, and apparatus for converting plain text messages into secret messages and vice versa.
Data Integrity	:	The property that data has not been altered or destroyed or lost in an unauthorized or accidental manner.
Default Account	:	A system login account (usually accessed with a user name and password) that has been predefined in a manufactured system to permit initial access when the system is first put into service.
Denial Of Service	:	Any action or series of actions that prevents any part of a system from functioning in accordance with its intended purpose. This includes any action that causes unauthorized destruction, modification, or delay of service.
Dial-Up	:	The service whereby a computer terminal can use the telephone to initiate and effect communication with another computer.
Digital Certificate	:	The electronic equivalent of an ID card that authenticates the originator of a digital signature.

e-Records		Information recorded in a form that requires a computer or other machine to process it.
Effectiveness	:	In security evaluations, an assurance of how well the applied security functions and mechanisms working together will actually satisfy the security requirements.
Employee	:	Refers to supervising, award and subordinate staff employed in the Bank.
End-User/ User	:	Person using application or computer networks for business purposes as opposed to system management purposes. Could be employee of the Bank, customers or partners of Bank.
Environmental Threats	:	Threats caused by environment including fire, humidity, dust or air borne particles, power fluctuations, temperature, flood, earthquake etc.
Exploit	:	To take advantage of a vulnerability in a system to gain access to system or to compromise the system
Fallback Arrangements	:	In the event of failure of transactions or the system, it is the ability to fall back to the original or alternate method for continuation of processing.
Firewall	:	A security software or hardware that sits between two networks and restricts data communication between the networks and thus protects one network against threats from the other network
Functionality	:	Describes features of the IT asset that support the business processes.
Gateway	:	Interface between networks that facilitate compatibility by adapting transmission speeds, protocols, codes, or security measures.
Hoax	:	In virus terms, an Email that warns of an invalid viral infection or risk, causing unnecessary concern to Email users.
Impersonation	:	An attempt to gain access to a computer system by posing as an authorized user.
Information Security	:	Measures that protect information systems by ensuring their availability, integrity, and confidentiality.
Information System	:	The entire IT asset, organization, personnel, and components for the collection, processing, storage, transmission, display, dissemination, and disposition of information.
Interoperability	:	It is the capability of systems to communicate with one another and to exchange and use information including content, format, and semantics.
Intrusion	:	A deliberate or accidental set of events that potentially causes unauthorized access to an information technology (IT) system.
Intrusion Detection System	:	A security system that monitors and analyzes system events for the purpose of finding, and providing real-time or near real-time warning of attempts to access system resources in an unauthorized manner.
IT Assets	:	IT Asset equates to any computerized system or component thereof and thus includes software, hardware, media, data, databases and associated communications

		networks.
IT Service	:	The services provided by information systems to business users including the maintenance and provisioning of applications, network and data processing.
IT Solution	:	Refers to any hardware, software or service or any combination of these related to information technology
Least Privilege	:	Feature of a system in which users are granted the fewest permissions possible in order to perform their tasks.
Lockout	:	The action of temporarily revoking network or application access, normally due to repeated unsuccessful logon attempts.
Login	:	The act of gaining access to a system; usually accomplished by providing a user name and password to an access control system that authenticates the user.
Malicious Code	:	Software that is intentionally included or inserted in a system for a harmful purpose e.g. A virus, worm, Trojan
Material Outsourcing	:	horse, or other code-based entity that infects a host.. Material outsourcing arrangements are those, which if disrupted, have the potential to significantly impact the business operations, reputation or profitability.
Media	:	Short for storage media: physical objects on which data can be stored, such as hard disks, CD-ROMs and tape.
Mobile Code	:	Mobile code is software transferred between systems, e.g. transferred across a network or via a USB flash drive, and executed on a local system without explicit installation or execution by the recipient. Examples of mobile code include scripts (JavaScript, VBScript), Java applets, ActiveX controls, Flash animations, Shockwave movies (and Xtras), and macros embedded within Microsoft Office documents.
Modem	:	A device or application that permits a computer to transmit/receive data over telephone lines
Network Device	:	A device that is part of and can send or receive electronic transmissions across a communications network. Network devices include: end-system devices such as computers, terminals, or printers; intermediary devices such as bridges and routers that connect different parts of the communications network; and link devices or transmission media.
Non-Repudiation	:	A cryptographic service that legally prevents the originator of a message from denying authorship at a later date. A security service by which evidence is maintained so that the sender of data and recipient of data cannot deny having participated in the communication.
Operational Controls	:	Refers to control measures for checking the accuracy and reliability of information processing and means to prevent and correct errors in processes.
Outage	:	The period of time for which a communication service or an operation is unavailable.
Outsourcing	:	Provision of services by third party under contract which

		is of longer duration including maintenance, development, implementation, management or data processing services under the supervision of the Bank.
Patches	:	Small updates to software to address the bugs
Penetration Testing	:	A form of security testing in which evaluators attempt to circumvent the security features of an information system, based on an understanding of system design. Used to develop system controls against intrusion or hacking.
Performance	:	Relates to how well a product or service meets the stated needs including the functionality, capacity, quantity and quality of output.
Policy	:	The set of rules and management intent that prescribe how information systems are managed, protected and distributed within the Bank.
Port Scan	:	An attack that sends client requests to a range of server port addresses on a host, with the goal of finding an active port and exploiting a known vulnerability of that service.
Privilege	:	An authorization or set of authorizations provided on applications or network and governs the level of access of the user
Procedures	:	Procedures are detailed guidelines of how to implement the security controls and who should be responsible for the implementation.
Project Head	:	Person in charge of development/implementation of major IT solutions.
Proxy	:	A software agent that acts on behalf of a user, typical proxies accept a connection from a user, make a decision as to whether or not the user or client IP address is permitted to use the proxy and then completes a connection on behalf of the user to a remote destination.
Quality Assurance	:	A planned and systematic pattern of all actions necessary to provide confidence that products and services conform to established technical requirements, and that satisfactory performance is achieved.
Redundancy	:	Duplication of system components (such as hard drives, power sources, or processors), information (such as backup copies of software or archived files), or personnel intended to increase the reliability or availability of service and/or decrease the risk of information loss
Regulatory Requirement	:	Requirements prescribed by regulators of the Bank - RBI, Ministry of Finance, SEBI etc.
Reliability	:	The extent to which a system can be expected to perform its intended function with required precision.
Remote Access	:	Dial-up access by users through a modem for access to the computer network.
Residual Risk	:	Residual Risk is the risk that remains even after risk treatment. This may be due to cost of implementation is higher than the potential loss.
Risk	:	Risk is a situation with probability of exploitation of vulnerability by threat(s) resulting in negative impact

		once occurred. .
	:	.
Risk Management	:	The total process of identifying, controlling, and mitigating IT system-related risks. It includes risk assessment; cost benefit analysis; and the selection, implementation, test and security evaluation of security controls.
Safeguards/ Security Controls	:	Management, operational, and technical measures prescribed for an IT system which, taken together, satisfy the specified security requirements.
Sanitized data	:	Data taken from production environment and then confidential information like customer information or revenue information is masked or changed before using in test environment.
Security Policy	:	Includes IT Policy, IS Security Policy, Standards, Procedures and Guidelines
Security Weakness	:	Security Weakness is the vulnerability in the system which may be harmful to the system or its operations, especially when this weakness is exploited by a hostile agent or when it is present in conjunction with particular events or circumstances.
Scalability	:	The ability to move application software source code and data into systems and environments that have higher performance requirements without significant modification.
Sniffing	:	The unauthorized interception of information through tapping of wire or network over which the information is flowing.
Social Engineering	:	Attacking or penetrating a system by employing confidence tricks on users, rather than by means of a technical attack.
Software Escrow	:	Keeping the source code of software with a neutral third party with joint rights of vendor & Bank. In the event of vendor going out of business or not supporting the software, the code can be released to Bank.
Spam	:	To indiscriminately send unsolicited or inappropriate messages, especially commercial advertising in mass quantities.
Spoofing	:	A type of attack in which the attacker steals a legitimate network (e.g. IP) address of a system and uses it to impersonate the system that owns the address.
SSH	:	A protocol for secure remote login and other secure network services over an insecure network.
Standards	:	Standards define the specific requirements for meeting the policy objectives and include both technical and non-technical measures
Statutory requirement	:	Requirements mandated under legislative acts or law of the land.
Stealth Rule	:	A stealth rule is a rule which disallows any communication to the firewall itself from unauthorized networks/hosts. It is a rule to protect the firewall itself

		from attacks.
System official	:	Refers to IT personnel responsible for administration of routine system activities of servers, desktops, network and applications.
System Operations	:	Systems Operations refers to a team, or possibly even a group within the IT department/ wing, which is responsible for the running of the centralized systems and networks.
System Room	:	All areas which host servers or network equipment like system rooms in branches, CAP etc
Third Party	:	Visitors, on-site and off-site contractors, hardware and software vendors, repair personnel, technical support staff, ex-employees, temporary workers, cleaning and facilities maintenance personnel etc.
Threat	:	Any circumstance or event with the potential to cause harm to a system in the form of destruction, disclosure, modification of data, or denial of service.
Transition	:	Refers to the period in outsourcing where the process or set of activities is being taken over from one party by other party
Trojan horse	:	A malicious program, such as a virus or a worm, hidden in an innocent-looking piece of software, usually for the purpose of unauthorized collection, alteration, or destruction of information.
Upgrade	:	The process of replacing a version of software or hardware with a newer product release designed to meet new requirements, or generally improve performance.
User department	:	Refers to the Dept that is the user of IT application and IT services.
User ID	:	Unique symbol or character string used by a system to recognize a specific user.
Vulnerability	:	A weakness in system security procedures, system design, implementation, internal controls, etc, that could be exploited to violate system security policy.
White Box Testing	:	Testing of software for security features by evaluating its internals including design/ architecture and code.
Worm	:	An independent program that replicates complete copies of itself from machine to machine across network connections, often clogging networks and information systems as it spreads.

**********End of Document**********