Global IME Bank
ग्लोबल आइएमई बैंक लि.
सबैका लागि बैंक

Information Technology Policy

Revised: January 2024

Preamble

In exercise to the power conferred by Section 22 of Bank and Financial Institution Act 2073 and the Article of Association of Global IME Bank Limited, the Board of Directors of Global IME Bank Ltd has approved this policy vide its…….... Board Meeting dated ……for implementation. This policy has been prepared in accordance with Information Technology Guidelines 2012, Nepal Rastra Bank (Central Bank) Directive/Circulars and amendments thereof issued time to time.

Version Control

Version Control No.	Date	Remarks
Version 1	March 2013	Revised
Version 2	November 2017	Revised
Version 3	August 2020	Revised
Version 4	March 2022	Revised
Version 5	January 2024	Revised

Approval Sheet

Prepared By :	Shikhar Subedi Information Security Officer	

Reviewed By :	Manindra Raj Joshi Head of Digital Banking	
	Anil Joshi Chief Information Technology Officer	
	Buddhi Akela Chief Risk Officer	

Supported By :	Suman Pokharel Deputy Chief Executive Officer	
	Surendra Raj Regmi Senior Chief Executive Officer	
	Ratna Raj Bajracharya Chief Executive Officer	

Approved By:	Board of Directors	

Table of Contents

CHAPTER 1 Introduction

1.1 Overview

As the role of Information Technology (IT) in Banks has changed from a support factor to a part of business itself, formulation of Information Technology Policy has become necessary. IT Policy needs to address various IT services being used at the Bank on a daily basis. In addition, IT Policy must focus several IT areas such as computer hardware, computer software, computer networking, network security devices, etc. IT Policy should be able to address all IT related tasks at the Bank and at the same time should be practicable to be implemented. In addition, the IT Policy should be able to comply with regulatory requirements. Having taken into consideration the above factors, IT/DB Department at Global IME Bank has formulated the IT Policy accordingly. If there are other specific IT related policies required such as Information Security Policy, Business Continuity Policy, these policies will be formulated separately.

1.2 Strategic IT plans

Information Technology strategic processes are integral components within the organizations governance structure to provide reasonable assurance that both existing and emerging business goals and objectives will be attained as a critical facilitator for enhancement of competitive advantages. Hence, Bank shall develop a board approved IT related strategy. IT strategy shall be long-term and short-term and long-term strategy shall be mapped to short term strategy periodically.

1.3 Strategic Planning

Strategic Planning from an Information Technology relates to the long-term direction Bank wants to take in leveraging IT for improving its business processes. Information Technology Department is responsible for developing and implementing a strategic plan that fulfils the Bank's mission and goals.

The strategic IT plan will cover Bank's at least 5 years of investment in technology. The long-term plan will also be broken down into short-term plan to cover the year-to-year operations.

1.4 IT Steering Committee

A high-level steering committee shall be formed to authorize and oversee implementation of IT initiatives, projects, acquisition of new system and other related activities.

The duties and responsibilities of IT Steering Committee are as follows:

- Review the long- and short-range plans of the IT Department to ensure that they are in accordance with the cooperate objectives.
- Review and approve major acquisitions of hardware and software within the limits approved by the board of directors.

- Approve, recommend and monitor major projects and the status of IS plans and budgets, establish priorities, approve standards and procedures and monitor overall Information System performance.
- Review and approve sourcing strategies for selection or all IS activities, including insourcing or outsourcing, and the globalization or offshoring of functions.
- Review adequacy of resources and allocation of resources in terms of time, personnel and equipment.
- Make decisions regarding centralization versus decentralization and assignment of responsibility.
- Support development and implementation of an enterprise wide information security management program.
- Report to the board of directors on Information system activities.

CHAPTER 2 Information Security Education

2.1 Overview

Information Technology (IT) and Digital Banking (DB) Department at Global IME Bank is always aware of Information Security and always educates employees, vendors, customers, and other concerned stakeholders about the Information Security issues.

2.2 Information Security Awareness Programs

Information Security awareness programs are required for employees, vendors, customers, and other concerned stakeholders because all concerned need to be up-to-date with latest information security issues. With ever emerging new and sophisticated information security issues, all concerned parties should be able to understand these issues and deal effectively with such issues.

The Policy to adhere are:

- The Bank shall be transparent regarding information security related matters and address such matters to all the concerned parties. By this process, the concerned parties should be able to understand information security issues and shall also be able to effectively deal with such issues. In addition, a mechanism to track effectiveness of training programs should be developed as per the requirement.
- The Bank shall conduct information security awareness programs to all the concerned parties such as employees, customers, and other stake holders. The Bank shall ensure that adequate awareness of information security issues are informed to the customers via notice and other media such as publication of guidelines/manuals and periodic circulation of important security related information. For employees, information security awareness programs are to be conducted on time to time basis. Further, information security guidelines should be circulated periodically and published internally. For any information security issue raised by employees, it should be promptly addressed by IT Department. For any product purchase, a comprehensive risk assessment should be done in coordination with the concerned vendor or the concerned stakeholder.

2.3 Adequate Education to Customers

Customers engaging in electronic banking activities can expose their electronic identity (card number, personal identification number, usernames, and passwords), devices, and computer systems to various information security risks. Therefore, the Bank shall ensure that customers are adequately educated so that the customers take appropriate security measures when they engage in electronic banking activities, ln addition, the Bank shall have proper procedure to promptly respond to customer's queries on electronic banking.

The Policy to adhere are:

- The Bank shall publish necessary guidelines related to proper use of electronic banking channels such as ATMs, Internet banking, Mobile banking, etc. These guidelines are to clearly list the information security

risks associated with concerned electronic banking channels. In addition, these guidelines are also to list the security measures that the customers must take in order to safeguard their electronic identity, devices, and computer system while using electronic banking. Furthermore, the Bank shall form a support unit that to promptly address any customer issues related to electronic banking, include the information security related issues.

2.4 Safety and Soundness of Electronic Banking System

It is very important that the Bank uses appropriate customer authentication system in electronic banking channels because customers do not necessarily need to be present "in-person" at the Bank's premises to conduct electronic banking activities. As a result, there is risk of unauthorized access to electronic banking channels. Therefore, the Bank shall ensure that the electronic banking system is safe from unauthorized access. In addition, the customers shall be adequately educated about securing their credentials in electronic banking channels.

The Policy to adhere are:

- The Bank shall always attempt using strong customer authentication system in electronic banking channels with latest security measures available in the market. This is to ensure that the risk of unauthorized access to electronic banking channel is minimized. However, presence of strong customer authentication system in electronic banking channels does not automatically minimize the risk of unauthorized access. Therefore, the Bank is to also ensure that the customers are adequately educated about securing their credentials in electronic banking channels. For this purpose, the Bank shall publish necessary guidelines and circulate information security issues to the customers on periodic basis.

CHAPTER 3 Information Disclosure and Grievance Handling

3.1 Overview

The Bank shall make proper disclosure of information that is related to electronic banking channels such as risks/benefits of electronic banking channels, costs associated with electronic banking channels, terms and conditions of electronic banking channels, etc. The disclosure of such information to customers helps them to make an informed decision in regards to selection of electronic banking channel(s). In addition, there is risk associated with electronic banking channels through unauthorized access and/or fraudulent use of electronic banking channel(s) that cause disputes. Henceforth, the bank is to formulate appropriate dispute resolution process to effectively resolve disputes and in proper time frame. Moreover, the bank is also to properly address customer's queries and/or grievance in any aspects of electronic banking channels so that efficiency of customer service is exhibited.

3.2 Publication of Clear Information about Dispute and/or Problem Resolution Process

The Bank shall publish clear information about dispute and/or problem resolution process in case of fraudulent access to customer's electronic banking account so that in case a problem arises, it can be properly dealt with.

The Policy to adhere are:

- The Bank shall carefully conduct risk analysis and then formulate appropriate risk bearing terms and conditions for electronic banking delivery channels and publication of this is to be done accordingly. In addition, the Bank should have a unit to promptly response to customer's grievances regarding various aspects of e-banking channels. Whatever problems are reported in regards to electronic banking channels, the concerned unit is to ensure that such problems are resolved properly and at the earliest.

3.3 Publication of Privacy/Security Policy and Cost of Electronic Banking Channels

The Bank shall publish customer privacy/security policy, cost of subscription/transaction, etc. for all electronic delivery channels so as to provide customers the information on cost and privacy/security aspects. This is to ensure that the customers are given transparent information on electronic banking channel with the purpose to help them make informed decision regarding whether to subscribe to these electronic delivery channels.

The Policy to adhere are:

- The bank shall be transparent regarding subscription cost, transaction cost, and privacy/security policy of e-banking channels to its customers. In addition, the Bank is to clearly publish cost of e-banking channels in the website and other applicable locations, documentation for this is to be properly maintained. Furthermore, the Bank is to clearly inform e-banking customers about benefits and risks of electronic banking channels through the front office at the time of customer’s subscription to e-banking channels.

3.4 Information of ATM Cost to Customers

The Bank shall clearly inform the customers about cost involved with ATM transactions so that the customers themselves become aware of cost factor before proceeding with ATM transactions.

The Policy to adhere are:

- The Bank shall be transparent regarding cost of ATM channel to its customers. For this purpose, the Bank is to clearly publish cost of ATM at appropriate channels so that the customers themselves become aware of ATM cost factor before proceeding with ATM transactions.

3.5 Development of Dispute Handling Mechanism

The Bank shall develop proper dispute handling mechanism with expected timing of response from the Bank. This shall ensure that in event a dispute arises it will be handled with proper procedure and will be settled in proper time frame.

The Policy to adhere are:

- The Bank shall carefully conduct risk analysis and then formulate appropriate dispute handling mechanism with expected time of the Bank's response. The Bank shall have a unit to promptly response to disputed transactions in electronic banking channels. Whenever disputes occur, the concerned unit is to ensure that such disputes are handled properly and resolved at the earliest.

3.6 Responsibility of Grievance Handling

The Bank shall develop a proper grievance handling procedure with expected timing of the Bank's response so that all types of grievance related to electronic banking channels are properly addressed.

The Policy to adhere are:

- The Bank shall formulate appropriate grievance handling procedure with expected time of the Bank's response. The Bank shall have a unit to promptly response to customer's grievance on all types of electronic banking channels. Whenever customers raise grievances, the concerned unit is to ensure that such grievances are properly addressed.

3.7 Providing Clear Information about Risk / Benefits of using Electronic Banking Channels

The Bank shall provide clear information about risk and benefits of using electronic banking channels so as to facilitate customer's decision regarding using electronic banking channels.

The Policy to adhere are:

- The Bank shall be transparent regarding risks and benefits associated with use of electronic banking channels. The Bank shall publish such information accordingly through appropriate channel(s). In addition, the Bank shall clearly mention the protection mechanisms being implemented in electronic banking channels.

CHAPTER 4 Outsourcing Management

4.1 Overview

Outsourcing can be defined as a process contracting an internal business function to an outside organization. Outsourcing is usually done to save time, cost, or resources. Outsourcing, if implemented properly, can bring several advantages such as focus on core activities, minimization of cost, staffing flexibility, implementation of new technologies, reduced reliance on internal staff, etc. However, Outsourcing can also bring loss of control, hidden costs, and issues with security/confidentiality etc.

The Bank should carefully analyze both advantages and disadvantages before proceeding with outsourcing IT service(s). Furthermore, the Bank shall ensure that the concerned service provider(s) are capable of providing required level of service. Moreover, the Bank shall also ensure that all outsourced service(s) are able to comply with legal/regulatory requirements.

Depending on the type of services, outsourced services can be hosted in the Bank's premises itself or they can be hosted in the service provider's premises. Depending on where the service is hosted at, the service provider can either take full responsibility of managing the service hosting or providing technical support only. In addition, an outsourced service shall have an agreement between the Bank and the service provider covering various aspects of the service and for a predefined time period. Upon expiration of the predefined time period, the agreement can be extended for another time period and so on.

4.2 Evaluation of Risk before Entering Outsourcing Agreement

Due to the risk of outsourced service impacting business operation, it is important that the Bank shall evaluate risk before entering outsourcing agreement so that all possible risks are identified and mitigated.

The Policy to adhere are:

- The Bank shall make proper risk evaluation before outsourcing an IT service. The risk evaluation process is to include identification of all types of risks associated with outsourcing. The process is also to include preventive measure and/or contingency plans that are to be taken to minimize the risks. In addition, the Bank shall evaluate risks of outsourced service(s) annually, by visiting outsourced vendor office premises. Moreover, appropriate service provider is to be selected based on several criteria such as capability, credibility, reliability, etc.
- Vendor risk assessment/visit report must be maintained by the respective department and submitted for review to the Information Security unit, Internal Audit, etc.

4.3 Compliance with Bank's Security / Privacy Terms and Conditions

Due to the fact that the service provider can access an outsourced service. Appropriate measures shall be taken to ensure that the service provider complies with the Bank's security / privacy terms and conditions.

The Policy to adhere are:

- For each outsourced service, there is to be an appropriate service level agreement between the Bank and the concerned service provider. The agreement shall be properly documented and made readily available

when required, In the agreement, necessary terms and conditions regarding compliance with the Bank's security/privacy matters are to be clearly mentioned. The Bank shall make sure that the concerned service provider understands all such terms and conditions.

4.4 Adequate Control for Outsourced Services

Since the service provider can logically / physically access an outsourced service. Appropriate logical access control and physical access control shall be implemented.

The Policy to adhere are:

- The Bank shall take suitable measures to implement appropriate control for logical access and physical access for an outsourced service. For logical access such as remote access to a service, the Bank shall ensure that the service provider has secure access only. Furthermore, the service provider is to be provided access only on demand and for genuine purpose only. In addition, Service provider's logical access is to be constantly monitored. Upon completion of work, the logical access is to be removed. For physical access also, the Bank shall allow access only on demand and for genuine reasons. Moreover, the Bank shall ensure that the identity of service provider is established before allowing physical access. Like logical access. Physical access is to be closely monitored, supervised, and access removed after completion of work.
- However, if the Data Center (production Site, Disaster Recover Site, etc.) hosting is outsourced, physical access must be controlled through appropriate safety measures of the service provider. These safety measures must meet the minimum required safety norms of the Bank and must be applicable for both Bank's authorized IT resources and authorized outsiders equally. In addition, activities of outsiders must be supervised by authorized IT resources. Further, access of service provider's onsite resources to the Bank's property at Data Center must be restricted through appropriate level of physical and logical controls as well as necessary clause(s) in the service level agreement itself.

4.5 Compliance with Regulatory Requirements

For an outsourced service, there is a risk of non-compliance with regulatory requirements because the concerned service provider may not take all the necessary measures of compliance.

The Policy to adhere are:

- The Bank shall evaluate all aspects of regulatory compliance before outsourcing a service. Further, the Bank shall ensure that the concerned service provider is capable of complying with regulatory requirement(s). The clauses of regulatory compliance are to be included in the agreement with the service provider. During inspections / supervisions from concerned regulatory authority, the Bank shall coordinate with the service provider and provide required access to the regulatory authority.

4.6 Process for Monitoring, Control, and Evaluation of Outsourced Services

Even though the Bank may outsource a service, still the Bank will be responsible for maintaining integrity of the outsourced service provided that the Bank maintains licensing/contract of the service or the Bank owns the data of the service or the Bank maintains total ownership of the service. Therefore, the Bank shall take appropriate measures to monitor, control, and also periodically evaluate the outsourced service.

The Policy to adhere are:

- The Bank shall take appropriate measures to monitor and control outsourced services with focus on nature, scope, complexity and risks associated with such services. Proper monitoring is to be done to determine how efficiently the service is operating. Proper control mechanisms are to be in place to ensure that the service provider does not have unrestricted access to the service. Further, the outsourced service is to be periodically evaluated to judge its overall performance and help the Bank to make an informed decision regarding continuation of service provider for that particular service.

4.7 Uncompromised Service Quality and Availability

Even though the Bank may outsource a service, still the Bank will be responsible for maintaining quality and availability of the outsourced service even if the Bank has just subscribed to the service. It should not be acceptable that the Bank compromises on quality and availability of service simply because the service has been outsourced.

The Policy to adhere are:

- During the selection process of an outsourced service provider, the Bank shall take into factor how well the service provider will be able to provide the service. The factors to be considered here are whether the service provider can provide the service with acceptable level of quality and with reasonable downtime tolerance. The Bank shall further constantly monitor the service to determine how well it is functioning and to make necessary follow-up with the service provider if there has been any compromise in the service quality and availability. Furthermore, in the agreement with service provider, necessary terms and conditions are to be included to have provision of cancelling agreement if the service is not up to a satisfactory level. In addition, the agreement can also include clauses of penalty in terms of financial aspects as well.

4.8 Ensuring Continuity of Critical Services

There is always a probability that the service provider of an outsourced service goes out of business. In such case, the continuity of an outsourced service can be impacted. Therefore, the Bank shall have a contingency plan in place so that continuity of outsourced service is maintained. This is especially important for a service that is deemed critical in nature.

The Policy to adhere are:

- The Bank shall have suitable strategy in place to deal with the scenario of service provider going out of business. For services where switching to another service provider is a solution, then the same is to be done accordingly.
- However, for certain services, switching to another service provider may not be the proper solution such as for software services. For these types of services, best effort is to be made to include the "software source code acquisition" clause in the agreement's terms and conditions. This is to ensure that the Bank will possess software source code if the service provider goes out of business. This will help the Bank to continue providing the service either by in-house administration/development of the software or the same through another service provider.
- If acquiring software source code is not possible, the reason(s) for the same is to be documented properly. Moreover, in all outsourced service agreements, appropriate terms and conditions are to be included so as to prevent the service provider from terminating the contract without proving the Bank guilty of an act or

the service provider itself going out of business. This is to ensure that the service provider does not have the right to terminate agreement at will.

4.9 Outsourced Hosting of Services

There are emerging technologies like data center hosting, disaster recovery site hosting, cloud computing, virtualization, etc. Since such services can be hosted outside the Bank's premises, issue of security, availability, integrity, compliance, etc., may arise.

The Policy to adhere are:

- The Bank shall carefully evaluate advantages and disadvantages of outsourced service hosting and then decide on use of emerging technologies like data center hosting, disaster recovery site hosting, etc. accordingly. There are various matters to be considered for such types of services such as risk factors, security factors, service availability factors, compliance factors. Additional factors such as geographical location of the site, physical facilities in the site, security measures applied in the site, etc. are also to be considered before deciding on outsourced hosting of services. Further, the Bank is to have appropriate level of service level agreement, which also must address all risks associated with outsourced hosting of service.

4.10 Provisions in Outsourcing Management

Outsourcing function not to be outsourced in case of core functions, function that requires specific knowledge, processes and critical staffs and in case of contractual or regulatory restrictions preventing outsourcing.

Service Level Agreement should serve as instrument for control. It shall contain at least below mentioned clauses:

- Service level Agreement to contain measurable performance requirements.
- Confidentiality agreements protecting both the parties
- "Right to Audit" clause.
- Business Continuity and Disaster Recovery Procedures.
- Protecting Intellectual Property Rights.
- Requirements for Confidentiality, Integrity & Availability (CIA) of resources/systems/data.
- Penalties clause

4.11 Globalization of IT function/services

Globalization requires setting up IT function at remote or offshore location. Globalization may or may not be outsourced.

Following issues need to be addressed for smooth functioning of IT function/services from offshore location:

- Legal and Regulatory Issues
- Continuity of Operations
- Telecommunication issues
- Cross -border and cross-cultural issues.

CHAPTER 5 IT Operations

5.1 Overview

The services of the Bank are technology based and availability of these services is of utmost importance to the daily work in the Bank. Information Technology (IT) Department administers technology based services in the Bank. Therefore, it is absolutely necessary that IT Department has a stable infrastructure and efficient operations system so as to continue providing uninterrupted technology based services in the Bank.

5.2 Segregation of Work

Due to the importance of IT operations in smooth functioning of daily work in the Bank, it is necessary that the daily IT work be segregated into different units and responsibilities of each unit be clearly defined.

The Policy to adhere are:

- Daily work at IT Department shall be segregated into different units and each unit shall be responsible for managing the work assigned to it. Several units shall be formed depending on the requirement of daily work. Considering work load of each unit, sufficient resources shall be assigned to the respective units.

5.3 Dual Control in IT Operations

IT Department shall make sure that all systems have dual control mechanism, where applicable. However, this may not be possible as some systems may not implement dual control mechanism in their core functionality.

The Policy to adhere are:

- Dual control mechanism shall be adhered to in all IT systems and as far as practically applicable. For systems that do not facilitate dual control mechanism, only authorized IT resource(s) are to make modifications to the system and proper documentation of the same should be maintained. Further, the documentation shall be reviewed regularly by a higher level resource(s) from IT or by resource(s) from another department as appropriate. This must be done to maintain necessary check and balance in systems where dual control is not possible at the system level itself.

5.4 Dual Administrative Access in IT Operations

IT Department shall ensure that an alternate resource has also administrative access credentials of IT services apart from a prime resource. This is to ensure that in absence of prime resource, IT operations will continue smoothly.

The Policy to adhere are:

- Dual administrative access / PAM (Privilege Access management) shall be implemented in all IT services / applications. One resource alone shall not possess administrative access credentials of a particular service or multiple services. Having administrative access credentials assigned to one specific resource increases reliance on that particular resource. In absence of that particular resource, it becomes difficult to administer services. Therefore, administrative access credentials for any service are to be given to at least two resources. The selection of resources is to be determined by whether or not the resources are capable of administering concerned service(s). The dual administrative access and PAM shall be implemented in all applications, hardware systems, communication system, and security systems. Likewise, the administrative

passwords shall be lodged in a sealed envelope by each administrator and store in a vault room or fireproof safe having dual custody. Such password shall be extracted in the case of emergency with the approval of Chief IT under intimation to the holder. Once the password is extracted, the concerned administrator should change the Password and re-lodge accordingly.

5.5 Implementation of Change Management Procedure

The Bank shall implement a process to assess, authorize, plan, test, implement, and document changes to critical systems. This will ensure that detailed record of each and every change is maintained, which is required for documentation purpose for legal/regulatory requirements and/or as per the Bank's own record keeping requirements.

The Policy to adhere are:

- Technology does not remain the same forever as technology will change over the course of time. A proper "Change Management" process shall be implemented when changes are required to be applied to critical systems. There needs to be a process to assess the need for change, authorize, plan, test, and finally implement the change. The process is to be documented properly. Hence, "Change Management" procedure is to be implemented for critical systems as per legal/regulatory requirement and/or for the Bank's own record keeping requirements.

5.6 Close Supervision of Access to Systems

All the systems implemented in the Bank are developed and/or distributed by vendors and/or suppliers and/or developed in-house. Sometimes, the vendors/suppliers/in-house developers need to access these systems in order to troubleshoot problems. Apply patches/enhancements, etc. ln addition, sometimes consultants need to access systems in order to analyze / evaluate performance of the system, etc.

The Policy to adhere are:

- The Bank shall provide system access to authorized vendor, supplier, consultant, or in-house developer only if there is a valid reason for access with due approval from competent authority. This is to be done for all systems and/or services where such access is required. Whatever the type of access sought by the outsider, the same shall be provided only after approval from Chief Information Technology Officer and notification of ISU. The access, once provided, shall be constantly monitored and supervised. Once the task is completed, the access shall be immediately removed. If system access is to be provided at sensitive premises like the Data Center, the same shall be constantly monitored and also supervised by concerned IT resources. If system access at branches is to be provided, then the same shall be monitored and supervised by the concerned branch resources. For system access required by in-house developer. it must be authorized and supervised by respective IT resources as per reporting hierarchy or from Chief Information Technology Officer and the activity must be documented appropriately'.

5.7 High Degree of Availability of Services

The Bank shall ensure that there is high degree of availability of all services, with focus on services whose downtime tolerance is low. Bank shall also ensure that there are adequate system and human resources to constantly reliable services.

The Policy to adhere are:

- The Bank shall analyze services based on downtime tolerance. Priority should be given to services where downtime tolerance is nil or minimal. Depending on a service's priority level, appropriate hardware and software backup are to be in place.
- To ensure availability of all services, the Bank shall have proper backup in terms of IT human resources also. This is to ensure that qualified and capable IT resources are always available to respond to any technical problem.

5.8 Risk Assessment as part of IT Operations

The Bank shall conduct risk assessment for all IT services on as part of daily IT operations so that probable events affecting service delivery can be identified and suitable steps can be taken to resolve them.

The Policy to adhere are:

- All services of the Bank shall be monitored as part of routine of IT operations and appropriate checklist shall be maintained for the same. In event of any problem is identified, it shall be immediately reported to the concerned resources so that the problem can be promptly addressed. In addition, as part of daily End-of-Day (EOD) operation in core banking system, a checklist shall be maintained. One of the purposes of the EOD checklist is to help in identifying problem in EOD operations. In event of any problem in EOD operation, it shall be reported to the concerned resources so that the problem can be promptly addressed.

CHAPTER 6 Information System Acquisition, Development and Implementation

6.1 Overview

Software system integrity and performance stability cannot be undermined due to the fact that day-to-day operations of the Bank depend on various software systems that are implemented at the Bank. Hence, failure of a software system in terms of poor performance, inconsistent data integrity, or security loopholes can have negative impact on daily operations at the Bank. Therefore, a software system should maintain satisfactory level of performance, consistent data integrity, high level of security, and above all fulfilling business requirements as well as user friendliness. For that reason, an appropriate software package should be acquired and/or developed in a systematic manner, the software properly tested, and then the software finally deployed in live environment.

6.2 Systematic Process for Selection of Software System

A systematic process needs to be in place for selection of a software system in order to evaluate the technical and financial aspects of various proposals and then select the appropriate software package.

The Policy to adhere are:

- The Bank shall make proper evaluation for requirement of a new software system. Concerned business units/departments are to justify need for new system and to list down all functional requirements and document the same accordingly. Information Technology / Digital Banking Department is to list down security / performance requirements as well as technical specifications and document the same accordingly
- If the software is to be developed/delivered by an outside organization. A Request for Proposal (RFP) to be prepared & forward same to the organizations that are capable of developing the software. The RFP is to outline all the requirements of the software and is to facilitate concerned organizations to submit proposals. The Bank shall review all proposals as per technical and financial terms. Then the Bank shall select a proposal that is technically sound and also financially feasible.
- If the software is to be developed internally, then the Bank shall ensure that there are internal resources capable of developing the software and then proceed with internal development of software. Even though the software system may be internally developed, it is still to meet all the functional requirements as well as security/performance requirements.

6.3 Budgetary Provision for Procurement of Hardware/ Software

The General Service Department (GSD) of the Bank is responsible for procurement and timely delivery of all hardware and software as required by Information Technology / Digital Banking Department as per the budget provision made.

The Policy to adhere are:

- Information Technology / Digital Banking Department shall make yearly budgetary provision for procurement of hardware and software and upgradation of infrastructure under their respective area of responsibility i.e. Local Area Networks, Wide Area Networks, Core Banking System and Alternate Delivery Channels based on their business plans. Chief Information Technology Officer / Chief Digital &

Transaction Banking Officer has ultimate responsibility for getting the budgetary approvals for requested items and for any excess over budget relating to a particular Team.

6.4 Systematic Process for Software Development

A systematic software development process shall be undertaken to design, build, test, and implement software. The systematic process must be followed to ensure that the software encompasses all requirements and is free of faults and loopholes when it is implemented in live.

The Policy to adhere are:

- A systematic process is to be undertaken for software development. Generally, a software development process includes several successive steps such as requirements gathering, creation of software prototype, testing of the prototype, further revisions of the prototype and additional testing until the requirements are fulfilled, and finally implementation of the software. The concerned authority at the Bank is to supervise the development process and to make coordination with different stakeholders throughout the development process. Further, the concerned authority at the Bank shall authorize deployment of software in live environment upon completion of the development process. Systematic software development process does help identification of issues during the development phase so that the same get resolved.

6.5 Incorporation of Security Requirements during Development Process

Software development process may focus primarily on functionality and may not pay much attention to the security requirements. As a result, when the software is implemented in live, the functionality aspect could be satisfactory but the security aspect may have several loopholes. Therefore, a software development process must incorporate implementation of security requirements so that when software is implemented in live all the security requirements are satisfied accordingly.

The Policy to adhere are:

- In addition to functional requirements, security requirements such as access control. Authentication, authorization, system activity logging, data integrity, audit trail, etc. Are to be incorporated during the design phase and as per the requirements. This is to ensure that the security requirements are implemented in software and the same get properly tested before the software system is implemented in live environment.

6.6 User Acceptance Testing before Implementation of Software System

Comprehensive software testing must be done in order to identify all software loopholes and performance related issues so that these issues are resolved before the software goes live.

The Policy to adhere are:

- The Bank shall ensure all functional, security, and performance requirements of a software system are fulfilled before the software system is implemented in live. A comprehensive User Acceptance Testing (UAT) is to be done for any software system that is to be implemented at the Bank. Depending on the importance of the software, a UAT team is to be formed by including members from respective units of the Bank. The UAT process is to test every aspect of software including the functionality, security, and performance aspect. If any issues/vulnerabilities are identified, they are to be promptly reported to the

concerned authority. Then the concerned authority is to coordinate with the software development team to resolve the reported issues/vulnerabilities. Once the UAT results are satisfactory, then the software is to be ready' for deployment in live environment.

6.7 Implementation of Audit Trail in Software Systems

Depending on the requirement of maintaining audit trial, a software system should be able to maintain detail records of various activities, which will be helpful for audit and/or investigative purpose.

The Policy to adhere are:

- As per the requirements, software systems are to implement audit trial detailed enough to facilitate obtaining forensic evidence. A comprehensive audit trail is to be implemented in critical applications and the same also implemented in other applications as per the requirements. That is, the software is to maintain record of each and every important event such as detailed record of each and every transaction. This is to be done to ensure that in event of an investigation, necessary details related to the investigated subject matter are retrieved. In addition, appropriate level of audit trial is to be maintained so as to comply with legal/regulatory requirements.

CHAPTER 7 Information System Audit

7.1 Overview

Information System Audit also known as System Audit is an independent process of evaluating information system in an organization. System Audit shall consist of evaluating various aspects of a system such as functionality, access control, security, data integrity, etc. Further, System Audit shall also include evaluation of outsourced services and also inspections of contracts for such outsourced services. In addition, System Audit shall also incorporate evaluation of Information System processes such as governance, operations, management, documentation, etc. information System Audit is important for an organization because it is able to effectively evaluate overall performance as well as able to find out lapses and loopholes in the Information System.

7.2 System Audit through Internal Resources

The Bank shall make necessary provisions to conduct system Audit through internal Audit Department at least once a year. This shall be done to ensure that the information system at the Bank gets evaluated regularly and independently of Information Technology resources.

The Policy to adhere are:

- The concerned department at the Bank shall take initiative to conduct System Audit. Further, the concerned department is to ensure that there are internal resources capable of doing the System Audit. Moreover, the Bank is to ensure that System Audit is done at least once a year. Periodic system Audit is important because the audit process can find out security lapses / loopholes in the Information System so that the same can be corrected promptly. Hence, it is necessary that the Information System of the bank gets evaluated on a periodic basis through a System Audit.

7.3 System Audit through External Resources

As per the requirements, the Bank should be able to conduct system Audit through External Resources, which will provide additional insight into the Bank's Information System through expert external resources. Further. System Audit through external resources can be done if the Bank does not have capable internal resources to perform System Audit.

The Policy to adhere are:

- As per the requirements, the Bank shall conduct System Audit through external resources. The Bank is to appoint a qualified external organization to do System Audit. The external organization is to be appointed based on capability of doing System Audit and within a predefined time period. Even though the System Audit is done through external organization, the bank is to be responsible for audit planning and implementation.
- Vulnerability Assessment and Penetration Testing (VAPT) of all IT applications/system shall be conducted Semi-annually.
- The Bank shall collect and review VAPT of all the application procured from Vendors before Go live.

7.4 Review of System Audit Report

System Audit report is the final report prepared by internal or external auditor after the end of audit process and is given to the concerned stakeholder. The report must be reviewed to eliminate loopholes/security lapses and also to implement modifications/improvements as recommended by the report.

The Policy to adhere are:

- The Bank shall carefully review the System Audit Report and give priority to loopholes/security lapses as mentioned in the report. Upon consideration of various factors such as existing Information System infrastructure / resources, the Bank is to take necessary steps to remove loopholes/ security lapses as pointed by the report. Further, the Bank is also to review suggestions for modifications/improvements mentioned in report and consider the same for implementation as per the requirements.

CHAPTER 8 Fraud Management

8.1 Overview

With the introduction of various types of electronic delivery channels and rapid adaptation of these channels by banks, the occurrence of electronic frauds is also increasing. An electronic fraud is a fraudulent activity done through electronic channels with the aim to acquire electronic identify of public and to use the same electronic identity for one's own benefit at the expense of the public. As a result, the Bank needs to spread necessary awareness to the customers regarding safeguarding their electronic identifies. The Bank shall also identify and document all types of electronic attacks and report the same to the concerned regulatory authorities as appropriate.

8.2 Identification and documentation of electronic attacks

The Bank shall be able to identify and document occurrences of electronic attacks and report the same to the concerned regulatory authorities are required.

The Policy to adhere are:

- The Bank shall incorporate necessary mechanisms in electronic delivery channels to track down events that are related to attempts of acquiring electronic identity of others. The Bank shall periodically review such events. Further, the Bank needs to promptly address any complaint of electronic identity theft and immediately respond to the complaint. In addition, as required by the regulatory authorities, the Bank shall make reporting of electronic attacks whenever there are incidents of such attacks.
- If any kind of unauthorized suspect is identified, Bank's Incident Response Plan and Procedure must be invoked and appropriate steps taken to deal with possible consequences.
- In case of any cyber-attacks in the Bank’s IT infrastructure, report has to be documented and submitted to Senior Management.
- Customers shall be made aware of frauds along with fraud identification, avoidance and protection measures. Different mediums such as websites, social media pages, SMS/email and mobile/Internet banking application can be used to aware the customers.

8.3 Customer Awareness Regarding Frauds in Electronic Banking Channels

The Bank shall ensure that the customers get adequate information regarding various electronic banking channels. Further, the Bank shall also ensure that the customers are made aware regarding protecting their electronic identity while using electronic banking channels.

The Policy to adhere are:

- The Bank shall take necessary steps to ensure that the customers get adequate information regarding various electronic banking channels. Further, the bank needs to increase customer awareness regarding frauds in such electronic banking channels. As applicable, customers are to be informed regarding electronic fraud identification techniques, electronic fraud avoidance techniques, and protection measures against electronic frauds so that they can avoid being target of electronic fraudsters while using electronic banking channels.

CHAPTER 9 Purchases and Installing Hardware

9.1 Specifying Information Security Requirements for New Hardware

The purchase of new computers and peripherals requires careful consideration of our business needs because it is usually expensive to make subsequent changes.

The Policy to adhere are:

- All purchases of new systems hardware or new components for existing system shall be made in accordance with information security and other policies of the Bank as well as technical standards. Such requests to purchase must be based upon user requirements and take account of long term organizational business needs.

9.2 Specifying Detailed Functional Needs for New Hardware

It is necessary to specify, in detail, the specific functional performance and capacity requirements as part of the hardware purchasing process. The document specifying these detailed requirements is usually called "Request for Proposal (RFP)". The system must have adequate capacity or else it may not be able to function properly. There shall have adequate arrangements for proper maintenance of the system. However, the service of vendors is of utmost importance for smooth operation of the business. This policy specifies guidelines to be followed by the bank for procuring and hiring different service to be rendered by each and every service provider. This also covers the basic principles applicable to all service providers to ensure spontaneous services so that the Bank's operations are not hampered.

The Policy to adhere are:

- Hardware must be purchased through a structured evaluation process, where necessary. The detail Hardware specification shall be mentioned clearly before doing the Hardware evaluation process.
- All purchase of new systems, computer hardware and software or new component for existing systems must be done on the basis of the business needs and requirements after due approval.
- All purchase must be made in accordance with the Bank's Financial Bylaws.
- All new hardware and software installation are to be planned formally and notified to all concerned units ahead of the proposed installation date.
- There shall be proper fall back plan before deploying any new hardware and software in the Bank's IT infrastructure.
- All hardware and software must be tested fully and comprehensively and formally accepted by user before being transferred to the live operations.
- All hardware and software under procurement shall have comprehensive warranty to cover operational risk
- The period of warranty coverage shall be determined by the procuring entity depending on the nature of the components but the period shall not be less than twelve (12) months.
- The description of warranty must clearly mention warranty coverage (parts, labor and service), type of warranty (comprehensive), duration and any provision for penalty when the said warranty is not complied with an acceptable level.

9.3 Installing New Hardware

Installation of new equipment must be properly considered and planned to avoid unnecessary disruption and to ensure that the Information Security issues are adequately covered.

The Policy to adhere are:

There are two types of computer hardware:

Category	Hardware Names
Type 'A'	Server and their accessories, cloud server /services
Type 'B'	Workstation, printers, scanner, and related computer accessories

- **For hardware Type 'A'**: All new hardware installations are to be planned formally and notified to all interested and related parties ahead of the proposed installation date. Information Security requirements for new installation are to be circulated for comment to all interested and related parties, well in advance of installation.
- **For hardware Type 'B'**: The computer hardware and/or its accessories are to be tested properly and then dispatched to the concerned branch/department for installation. If required, a technician from IT to visit the concerned branch/department and do the installation.

9.4 Testing System and Equipment

New hardware shall be tested to ensure it is working correctly, and then shall be tested periodically to ensure continued effective functioning.

The Policy to adhere are:

- All server hardware equipment shall be fully and comprehensively tested and formally accepted by all concern before being transferred to production environment. For the hardware used by end users at branch/department level, concerned IT resource(s) are to test overall functionality of hardware and then dispatch it to the concerned branch/department.

CHAPTER 10 UPS (Uninterruptible Power Supply) and Cabling

10.1 Supplying Continuous Power to Critical Equipment

An Uninterruptible Power Supply (UPS) is a critical hardware component which enables continuity of function in event of a power failure.

The Policy to adhere are:

- An Uninterruptible Power Supply shall be installed to ensure the continuity of services during power outages.

10.2 Managing and Maintaining Backup Power

Issues may arise when standby generators are not used as a safeguard against main electricity failure. Such generators are usually employed with UninterruptiblePower Supply.

The Policy to adhere are:

- Secondary and backup power generators shall be installed where necessary to ensure the continuity of services during power shedding/failures. In Data Center, the UPS power backup time must be minimum of two hours and provision of generator as secondary backup system is a must. In branches, the UPS power backup time must be minimum of 10 to 15 minutes and there must also be provision of generator. For ATM power backup, there must be at least 4 hour's battery backup system.
- The concerned department/branch is responsible for installation, management and monitoring of generators.

10.3 Installing and Maintaining Network Cabling

Network cabling remains a vulnerable target as in many organizations it is exposed and unprotected.

The Policy to adhere are:

- Network cabling shall be installed and maintained by qualified technicians to ensure the integrity of both the cabling and wall mounted sockets. The departments / branches are responsible to protect used / unused network sockets from use by external resources such as third parties.

CHAPTER 11 Consumables

11.1 Controlling IT Consumables

IT consumables are printer forms, stationery, printer papers, toner and ribbons being used for its day to day operations.

The Policy to adhere are:

- IT consumables shall be purchased in accordance with the organization's approved budget and procedures as mentioned in the Bank's Financial Administration Bylaws. Uses of such consumables shall be checked/monitored to control and discourage theft and misuse.

11.2 Using Removable Storage Media including USB Drives /CDs / DVDs

When using removable storage media, there is additional information security risks associated with the portability of the media.

The Policy to adhere are:

- Only personnel who are authorized to install or modify software shall use removable media. Any other persons shall not have access to use removable media such as writable CDs/DVDs, USB drives (pen drives), external hard disks, etc. There shall be provision in system level to block use of external drives to end users except for those who have approval from the concerned authority for using such devices.

CHAPTER 12 Working Off-Premises or Using Outsourced Processing

12.1 Contracting or Using Outsourced Processing

Inadequate performance can affect our Bank's information processing and business operations and poor reliability can affect the performance of our business.

The Policy to adhere are:

- Persons responsible for commissioning outsourced computer processing must ensure that the services used are from reputable and qualified organizations and/or authorized distributor/partner of the concerned service that operate in accordance with quality standards, which shall include a suitable Service Level Agreement (SLA) duly meeting the Bank's requirements.

12.2 Moving Computer Related Hardware from One Location to Another

This is regarding the physical removal and relocation of computer related hardware from one location to other.

The Policy to adhere are:

- As per the organizations internal policies and practices, any movement of hardware between the organization's locations shall be strictly controlled by authorized personnel and subsequent update of hardware inventory registry to be done by respective department accordingly.

12.3 Issuing Laptop / Portable Computers to Personnel

Laptops / Tablets - even electronic organizers, which connect to and store organization's data - are included within this policy. Collectively, they are referred to as portables computers.

The Policy to adhere are:

- If there is requirement of a portable computer, it must be approved by the concerned authority. Portable computers must be used for official purpose only and shall not be used to store personal information. In addition, when portable computers are provided to the concerned staff, they must sign-off a document to verify that they have received and taken custody of the device. At the time of handover, the device must be in proper condition. Further, appropriate documentation during assigning custody and handover of portable computer must be maintained.

12.4 Using Laptop / Portable Computer

Laptops and portables have unique security issues, primarily because of their size and mobility.

The Policy to adhere are:

- Persons who are provided with portable computers and who intend to travel for official purposes must be aware of the information security issues relating to portables computing facility and implement the appropriate safeguard to minimize the risk. In addition, users must take responsibility for the security of information held on such devices including the physical security of the device itself.

CHAPTER 13 Documenting Hardware and Other Hardware Issues

13.1 Managing and Using Hardware Documentation

Documentation refers to both operating manual and technical documentation that should be provided by the supplier / vendors.

The Policy to adhere are:

- The hardware documentation must be made available when needed.

13.2 Maintaining a Hardware Register or Inventory

A register / database of all computer equipment used within the organization are to be established and maintained.

The Policy to adhere are:

- A formal Hardware Inventory of all computer equipment is to be maintained and kept up-to-date.

13.3 Disposing of Obsolete and Non-repairable Equipment

This policy deals with the issues that should be addressed when disposing of computer equipment, either for use by others or scrap/ re-cycle.

The Policy to adhere are:

- Authorized personnel who have ensured that the relevant security risks have been mitigated may only dispose equipment owned by the Bank. Furthermore, computer equipment that is obsolete and non-repairable must be disposed. The disposal must be done as per the Bank's internal policies and guidelines.

13.4 Recording and Reporting Hardware Fault in Servers

Hardware faults in servers are to be recorded and reported to the appropriate authority or maintenance contractor for corrective action.

The Policy to adhere are:

- All information system hardware faults in server shall be reported promptly and recorded in a hardware fault register or recorded digitally.

13.5 Insuring Hardware

All the Hardware should be covered with adequate insurance.

The Policy to adhere are:

- Computing equipment and other associated hardware belonging to the organization must carry appropriate insurance coverage against hardware theft, damage or loss where applicable. The concern department at the Bank should be responsible for insurance of all computer hardware.

13.6 Taking Equipment off the Premises

When taking the Bank equipment off site. Proper authorization should be obtained and next to ensure the physical security of the equipment. A further critical consideration is the security of any information contained on it. Often, the data is far more valuable than the equipment itself.

The Policy to adhere are:

- Only authorized personnel are permitted to take equipment belonging to the Bank out of the premises to the authorized hardware service center. In addition, the concerned department must maintain record of such equipment movement.

13.7 Maintaining Hardware (On-site or Off-site support)

The arrangement made for maintaining computer equipment, whether through on- site support or off-site support.

The Policy to adhere are:

- All equipment owned, leased or licensed by this organization must be supported by appropriate maintenance facilities from qualified technicians. Hardware maintenance either on-site or off-site through external resources must be done in compliance with Information Security aspects.

13.8 Damage to Equipment

Damage to equipment must be reported as soon as it is noticed.

The Policy to adhere are:

- Deliberate or accidental damage to organization property must be reported to the concerned staff as soon as it is noticed.

CHAPTER 14 Processing Information and Documents

14.1 Networks

- Configuring Networks

Configurations of network impacts directly on its performance and affects its stability and Information security.

The Policy to adhere are:

- The network must be designed and configured to deliver high performance, reliability, and security to meet the needs of the Bank

- Data Center Network

The core of the Bank's network is the Data Center itself. All branches. Off-branch ATMs, and other locations have direct connectivity with the Data Center and Disaster Recovery (DR) site directly connects to the Data Center. In the event there of network problem at Data Center, it will impact the Bank's entire computer network and service delivery.

The Policy to adhere are:

- The Data Center is to be connected to all branches, off-branch ATMs. and Disaster Recovery (DR) site by a secured network. The Data Center itself must be protected from public network via a security device such as network firewall. Due to the critical role of Data Center in the Bank's computer network, the Data Center is to have at least dual link, In addition, the Data Center is to have provision of dual network security device in failover mode so that if one device fails another device can continue to provide network service without causing any interruption in the service.

- Branch Network

Since all branches connect to the Data Center to get IT services such as core Banking system, it is very important that the network downtime in branches is very minimal.

The Policy to adhere are:

- All branches are to have direct connectivity to the Data Center and also to have dual links where possible. When branches have dual-link provision, one of them is to be assigned as primary link and the other is to be assigned as secondary link. The assignment of primary or secondary link must take into account the following factors such as link type, bandwidth, and uptime reliability. In addition, the branch must connect to the Data Center through a secured network.

- Off-Branch Network

All off-branch networks such as ATMs, counters, etc., connect to the Data Center. Since off-branch locations are outside a branch premise. a separate connectivity is required to connect to the Data Center. This can either be local connectivity, which is connectivity to the nearest branch, or this can be direct connectivity to the Data Center.

The Policy to adhere are:

- Off-Branch locations are to have direct connectivity to the Data Center where possible. Otherwise, local connectivity to the nearest branch network can be obtained. In addition, an off-branch location must connect to the nearest branch or Data Center through a secured network.

- Disaster Recovery Site Network

The Disaster Recovery (DR) Site needs to have continuous connection to the Data Center so that the vital IT services and data are synchronized at all times.

The Policy to adhere are:

- There must be dual link provision between the Data Center and DR site so that in event there is problem with one link, another link can continue to maintain connectivity. In addition, the DR site must connect to the Data Center through a secured network.

- Managing the Networks

All networks require ongoing management.

The Policy to adhere are:

- Suitably qualified staffs are to manage the network and preserve its integrity in collaboration with outsourced parties when required. In addition, amendments to network configuration must be authorized and documented accordingly.

- Defending Network Information from Malicious Attack.

This is regarding the measures taken by an organization to defend computer system against unauthorized access.

The Policy to adhere are:

- Operating and application software, database, the networks and computer communication systems must all be adequately' configured and safeguarded at all times against unauthorized network intrusion.

14.2 System Operations and Administration

- Appointing System Administrators for Servers

The system administrator is responsible for overseeing the day-to-day running of servers. This usually entails ensuring that the computer system is available and appropriately configured to perform required tasks. System Administration necessarily involves a substantial amount of administrative and security-related work.

The Policy to adhere are:

- The servers are to be managed by a suitably qualified system administrator who is responsible for overseeing the day-to-day running and security of the systems.

- Administering System

A system administrator is often in a powerful position because they normally set the user access criteria for all systems. This raises a range of Information Security issues. The Administrator must have an adequate level of skill on the system within their area of responsibility.

The Policy to adhere are:

- System Administrators must have adequate experience in the wide range of systems and platforms used. In addition, they must provide user access on the basis of requirement and documentation of user access must be maintained.

- Controlling Data Distribution

This is to ensure that the Bank's data and information are neither divulged nor accessible to unauthorized persons.

The Policy to adhere are:

- For authorized personnel, the appropriate data and information must be made available as and when required; for all other persons, access to such data and information must be prohibited with appropriate technical control mechanisms.

- Managing System Operations and System Administration

This is regarding the procedures by which IT systems are run and maintained on a day-to-day basis.

The Policy to adhere are:

- The systems must be operated and administered using standard procedures in a manner. which is both efficient but also effective.

- Managing system Documentation

It is the management of the documents provided for the operation and maintenance of the system.

The Policy to adhere are:

- System documentation is a basic requirement to the organization. Such documents must be kept up-to-date and be made available when required.

- Monitoring Error Logs in Servers

Error logs are the reports produced by system relating to errors or inconsistencies in the system.

The Policy to adhere are:

- Error logs must be properly reviewed and managed by the authorized and qualified staff.

- Scheduling System Operations

Certain systems need to run on proper schedule such as End-of-Day operations in core banking system

The Policy to adhere are:

- System Operations schedules are to be formally planned, authorized and documented.

- Synchronizing System Clocks

System clocks of all computer systems at the Bank shall be set to correct time. time zone settings and correct date.

The Policy to adhere are:

- Server clocks must be synchronized regularly specially between the various processing platforms. In addition, personal computer and laptop clocks must be set to the correct time and date through systematic process. Further, end users shall not be allowed to change system clock of their computers.

- Responding to System Faults

Hardware and/or software faults may impact our system making accurate and timely processing difficult.

The Policy to adhere are:

- Only qualified authorized staff or approved third party technicians may repair information systems hardware and/or software faults.

14.3 E-mail and World Wide Web

- Setting up Internet Access

The Internet is a worldwide web based information service that can be made available to required users in the Bank.

The Policy to adhere are:

- For Internet access in an organization, there must be a mechanism to get the internet access, when provided shall be used only for official purpose. In addition, contents that are offensive in the organization and for the jurisdiction of law shall not be viewed.

- Downloading Files and Information from the internet.

There are significant Information Security risks when any files (including graphic files of any format), programs, scripts etc. are downloaded from Internet.

The Policy to adhere are:

- Internet access must not be given to all staffs and only to those users who are authorized. Further, these authorized users should be allowed to download files from the internet for official purpose only. There must be restrictions in internet access based on various technical parameters and based on various levels of user groups.

- Filtering Inappropriate Material from the Internet

Many organizations with in-house IT capabilities are now placing restrictive filters, which prevent access by employees through the Internet to sites displaying inappropriate materials.

The Policy to adhere are:

- The Bank shall use software filters and other techniques whenever possible to restrict access to inappropriate information on the Internet by the staff.

- Hosting a Website

There are many potential Information Security threats that we should be aware of when we host an Internet Web Site.

The Policy to adhere are:

- The Bank can host the website with all required security measures in place to prevent potential Information Security threats. Otherwise. The Bank can assign a reliable and/or authorized third parry to host the website with proper Service Level Agreement.

- Maintaining Web Site

Information on the Website, whether being hosted by an ISP or in-house, must be kept updated and secured, even during periods of Web site maintenance.

The Policy to adhere are:

- The Website is an important marketing and information resource for us and its safety from unauthorized intrusion is a top priority. Only qualified authorized persons may amend the website and maintain documents of such amendments.

- Sending Email

The use of email has escalated to the point where it is obligatory for all companies to be accessible through this medium.

The Policy to adhere are:

- Email ID creation process must be standard. Email shall only be used for business purposes using terms, which are consistent with other form of business communication. ln addition, email attachments shall be auto scanned for viruses and malwares.

- Receiving Email

The use of email has escalated to the point where it is obligatory for all companies to be accessible through this medium. The content of emails received without authentication may be considered unreliable.

The Policy to adhere are:

- Incoming email must be treated with utmost care due to its inherent information security risk. The opening of email with file attachment is not permitted unless such attachments have already been scanned for possible virus or other malicious code.

- Setting up Intranet Access

An intranet is a web based information service that is available within the Bank and its internal networks

The Policy to adhere are:

- Person responsible for setting up Intranet access must ensure that proper access control mechanisms are in place and Intranet itself should be accessible within the Bank's network only. The Intranet users must be aware that the Intranet contains confidential information of the Bank. In addition, contents of Intranet should not be disclosed to any unauthorized resources within and outside the Bank. If the access is required to outsider within the organization, it must follow for due approval process.

- Receiving Misdirected information by E-mail

We should never bother to respond to unsolicited emails.

The Policy to adhere are:

- Unsolicited emails are to be treated with caution, not be responded to, and shall be immediately deleted. ln addition, the event must be immediately reported to concerned IT staff / ISO.

- Forwarding Email

When we forward an email to someone, we are also adding our name and other details to it. Ensure we are comfortable with the information contained in the original. Any security risk associated with the original rnail to us will also apply to the forwarded email.

The Policy to adhere are:

- Ensure that information we are forwarding by email, especially attachments, is correctly addressed and only being sent to appropriate persons.

- Addressing a Group Mail

The use of group mail is now becoming a necessity as many organizations have group mails for branches/departments so that it is easier for one person to address a group.

The Policy to adhere are:

- Group mails are to be created as per the requirement with proper procedure and appropriate approval. All users should send emails to a group only after knowing who the recipients are. Users are not to address group mail if all recipients of the group do not need that email.

14.4 Data Management

- Transferring and Exchanging Data

This is regarding the way in which data is distributed across networks both public and private and by other means e.g. exchange of tapes, disks, and optical disks.

The Policy to adhere are:

- The data travelling between the Data Center and branches should be in encrypted form F transferred through other means, it should be done only by authorized personnel.

- Managing Data Storage

The storage of information and data is a day-to-day function for all organizations. lt requires careful management to ensure that Information Security issues are dealt with adequately.

The Policy to adhere are:

- Day to day data storage must be ensured that the current data is readily available to authorized users and that data backups are both created and accessible in case of need.

- Archiving Documents

We may wish to archive documents for various reasons, such as lack of space in the live system, removal of old data that has been processed at the end of re-defined period or legal requirement to retain the information for future reference.

The Policy to adhere are:

- The archiving of documents must take place with due consideration for legal regulatory and business issues with liaison between technical and business staff. The policy for archiving should be set by the department that is responsible for determining the policy. In addition, individual departments / divisions may have their own document archiving policy.
- Information Retention Policy

This section is related to retaining information other than document of files

The Policy to adhere are:

- The information created and stored in Information Systems must be retained for a minimum period that meets both legal and business requirements.

- Setting up New Databases

Databases are set-up so that specific data can be stored, retrieved and reorganized. This makes the maintenance of security and integrity of the data particularly very important.

The Policy to adhere are:

- Database must be fully tested for both business logic and processing capabilities prior operational usage. Whereas such databases are to contain information of a personal nature procedures and access controls must ensure compliance with necessary guidelines.

- Saving Data I Information by Individual Users

Saving of data in a structured and timely manner is good practice for users of workstations and terminals.

The policy to adhere are:

- All users of information systems whose job function requires them to create or amend data files, must save their work in the system regularly in accordance with best practices, to prevent corruption or loss through system or power malfunction. Users need to back up their data either in different logical hard drive in the same disk or in different hard disk whatever is applicable.

14.5 Backup Recovery and Archiving

- Restarting or Recovering System

The facilities employed to ensure that servers re-starts successfully after a voluntary or enforced closed down.

The Policy to adhere are:

- Adequate back up and system recovery procedures must be in place for all services.

- Managing System Backup and Recovery Procedures

The need for, and creation of, end of day backup files cannot be over emphasized as they allow us to restore either the whole system or perhaps selected data files. To a specified end of day position. However, the procedures used to initiate such a recovery must be clearly documented and tested.

The Policy to adhere are:

- In this context, the data backup and restoration process refers to the data stored in hard drive at server level or at storage level for various applications as opposed to user's data stored in hard drive of individual workstations.
- Data backup is an important step in the process of data management in an organization. This process is to create a replica of data which preserves data's state as of the particular time, i.e. when the backup was

created. The purpose is not just to keep archive of data for future retrieval but also to support Disaster Recovery (DR) process.

- Data restoration means reloading the backed-up data directly into the system in exactly the same state as when it was backed-up. In case of disaster, which can range from either small hardware or software failure in server level or full-fledged failure at data center, the role of data backup and restoration is vital in bringing back systems to normal working condition and within quick period
- Therefore, the process of data backup for each system is dependent on how critical the data of that system is for the organization. Depending on criticalness of the data, the backup frequency is determined accordingly with more critical systems having more frequent backups. For example, mission critical applications like Core Banking System needs to have real-time or to say at least near real-time data backup process. This is to ensure that in case of disaster, the backup can be restored so that the data restoration is 100% or say at least 99%

- Recovery and Restoring of Data Files

Saving of data on a backup tape or disc for critical system applications is a core process in the security of our information. On the other hand, appropriate restoration procedure must be adhered to ensure the validity of data backup and as a drill for disaster recovery process.

The Policy to adhere are:

- Data must be restored in a separate standby or test system on regular basis primarily for the purpose of additional verification regarding accuracy of data backup process. Data backup can be taken when required, but if it is not restored regularly then there is no concrete way of knowing whether the backup process is accurate or not. Given that all systems if not all mission critical systems such as CBS do have a separate test or standby system, it is inoperative that data is restored periodically so that it acts as extra level of validation for data backup process being carried out in the organization.
- The frequency of data restoration must be dictated by criticalness of the system with more mission critical systems requiring more frequent data restoration. For Core Banking System, restoration must be done at least once a week. For other systems, restoration frequency can be determined as per the need. Data restoration in respective system can be more frequent than defined in the policy. This is especially true for Core Banking System as restoration may be required as when needed sometimes daily or even multiple times a day. Nevertheless, the restoration document must be maintained properly for Core Banking System compulsorily and for other systems optionally as required
- It is to be noted that all systems may not have a separate standby or test system in place where data restoration can be done. In such cases, the validity of data backup can be done by checking validity of backup process and checking various attributes of backup file such as file size.

14.6 Securing Data

- Sharing Information

Sharing information between different divisions, groups or sections of our Bank are often necessary for the business to function. This raises information security issues.

The Policy to adhere are:

- Concerned departments shall ensure that all employees are fully aware of their legal and corporate duties and responsibilities concerning the inappropriate sharing and releasing information, both internally within the Bank and to external parties.

- Sending information to Third Party

When sending information to external parties the principal consideration should be the integrity and confidentiality of the data.

The Policy to adhere are:

- Prior to sending information to third parties, the intended recipient must be authorized to receive such information and non-disclosure agreement to be signed where applicable. In addition, the third party also must adopt appropriate procedures and information Security measures to assure the confidentiality and integrity of the information remain intact while maintaining appropriate documentation.
- Fire Risk to Critical System Information

Fire is one of the worst non-technology risks we may face. It can cause significant structural damage to our systems.

The Policy to adhere are:

- All critical system data and information must be protected against the risk of fire damage at all times. The level of such protection must always reflect the risk of fire and appropriate numbers of fire extinguishers should be in place.

- Dealing with Sensitive Financial Information

Financial information is usually sensitive, especially in the current contest competitive market.

The Policy to adhere are:

- Financial information is sensitive so it must be properly managed and stored. ln addition, authorized users who have access of sensitive financial information are not to disclose it to unauthorized resources both within the Bank and outside the Bank.

14.7 Purchasing, Installing and Maintaining Application Software

- Specifying User Requirement for Software

Before deciding on the purchase of new software, it is essential to specify the business and technical requirement that need to be met. This is usually accomplished by means of a User Requirement Specification (URS).

The Policy to adhere are:

- All requests for new application systems or software enhancements must be presented to the concerned authority with the business case with the business requirements presented in a User Requirement

Specification document. The User Requirement Specification document must be made by the concerned department.

- Selecting Business Software Packages

Selecting the right package is critical. Because it is expensive to correct mistakes and will have consequences for years to come.

The Policy to adhere are:

- The software should fulfill the User Requirement Specification (URS). In addition, the software should be technically sound and shall be cost effective. Moreover, the concerned department that had made URS should be satisfied with the software. Then onwards the proposal to select the business software package should be placed before the concerned authority.

- Using Licensed Software

We must be licensed to use software and adhere to the terms and condition of the End User License Agreement. It is necessary to comply with legal requirements and to retain our eligibility for ongoing vendor support.

The Policy to adhere are:

- The Bank must maintain appropriate licenses for software for which license must be maintained as per the standard practice and/or required by the regulatory authority.

- Using Freely Available Software

There are several types of software which are available for free. Still it is necessary to comply with legal requirements and to retain our eligibility for use of freely available software. ln addition, it is still necessary to comply with the terms and norms of free software

The Policy to adhere are:

- As per the Bank's requirements, if freely available software is useful for the Bank, then it can be considered for use. However, such software should be used only after full testing and full assurance that it is technically acceptable to use.

- Implementing New / Upgraded Software

All software including operating system needs to be updated periodically as per need basis and as per technical feasibility. Whether this is a simple upgrade or a complete re-write of main system, it involves a series of steps, whose length depends on the size and complexity of the system.

The Policy to adhere are:

- The implementation of new or upgraded software must be carefully planned and managed, ensuring that the increased information security risks associated with such projects are mitigated using a combination of

procedural and technical control techniques. For implementation of new software and/or for software upgrade, a task force could be formed.

14.8 Software Maintenance and Upgrade

- Applying Patches to Software

Patches are software bugs fixes, that is, they resolve problems reported by users.

The Policy to adhere are:

- Patches to resolve software bugs in system applications may only be applied where verified as necessary and with authorization from concerned authority where applicable. They must be from a reputable source and are to be thoroughly tested before use. Proper documentation must be maintained as well.

- Upgrading Software

The status of the software is rarely static. Software companies are either releasing bugs fixes or introducing new versions with enhanced functionality.

The Policy to adhere are:

- Qualified personnel must properly test upgrades to software before they are used in a production environment. If this process cannot be done solely by Bank's personnel, then this process can be outsourced.
- The process of software upgrade must be documented. The upgrade must be tested thoroughly with reference to an appropriate checklist. If the test results are as per the business requirements, the software upgrade must be implemented in live environment upon due approval from the concerned authority, In addition, appropriate technical procedure must be followed during upgrade process with provision of rollback to existing version as the contingency plan.

- Responding to Vendor Recommended Upgrades to Software

Although software may be operating satisfactorily, vendors will pronate the latest releases to make additional sales and in order to migrate all customers into a common version. This reduces their support costs improves service levels. However, upgrades usually entail risks.

The Policy to adhere are:

- The decision of software upgrade must be supported by strong case of functional & technical requirements with the benefits of upgrade outweighing associated technical risks and financial costs, if any. Further it must be strongly supported by necessity for such changes and should not be upgraded if it is not necessarily at all in present context. The decision of not doing software upgrade must be supported by strong case against the upgrade due to technical risks, financial cost, and whether the upgrade is genuine necessity in day-to-day task at the organization. Further, software upgrade task can be postponed to future date and reevaluation of upgrade done at that future date.

- Interfacing Applications Software / Systems

Many software packages can exchange data and link with a variety of systems. Such interfaces often need to be specially customized for legacy systems. Interfacing will be complex process requiring data first to be exported from one system, then refined in proper format, and finally imported to into the target system.

The Policy to adhere are:

- Developing interfacing software systems is highly technical task and should only be undertaken in a planned and controlled manner by properly qualified personnel. If there is a justifiable need to develop the interface, then only should it be developed. Further, the development process must follow common software development process and require approval from concerned authority before it is implemented in Live.

- Supporting Application Software

The adequacy of routine applications support (Help Desk) can greatly influence frequency and severity of the problems we experience. Where such support is not readily available, technical staff and users may try to fix problems themselves following various ideas.

The Policy to adhere are:

- All application software must be provided with the appropriate level of technical support to ensure that any software problems are handled efficiently with their resolution in an acceptable time. If further technical support is required, then it can be obtained from the vendor or authorized distributor/reseller of the software. Service Level Agreement is mandatory for all application software that have been procured and/or developed through outsourcing. This only includes applications that have been developed or procured specifically for the Bank's need and excludes any common Operating System or utility related application(s). lf the application software has been developed in-house, then it must be supported through qualified internal resources that have the capability of providing technical support for such application software.

- Operating System Software Upgrade

Like any other systems the operating system (OS) of a computer uses software, which from time to time requires patches and upgrades. However, unlike individual applications software upgrades, problems with OS can impact on all applications running on the computer.

The Policy need to adhere are:

- Necessary upgrade to the Operating Systems of any of the Bank's computer systems must have the associated risk identified and be carefully planned, incorporating tested fallback procedures, and all applications should be able to run smoothly.

- Support for Operating Systems

The operating systems of desktop systems will generally run without much of substantial interference. However, for servers, day-to-day housekeeping is normally required.

The Policy need to adhere are:

- Operating systems in servers must be regularly monitored and all required housekeeping routines must be adhered to. This process must be documented.

- Recording and Reporting Software Faults in Servers

A software fault in server stops the proper and reliable use of an application or features of applications.

The Policy to adhere are:

- Software faults in servers are to be formally recorded and reported to those responsible for software support and maintenance. The issue has to be solved at the earliest with all necessary technical support from outside parties/partners/vendors as applicable.

14.9 Other Software Issues

- Disposing of Software

Software is often licensed indefinitely. However, a change of organization circumstances may result in a decision to stop using a certain systems or to move to another. The removal and disposal of the software needs be considered

The Policy to adhere are:

- The disposal of the software should only take place when it is formerly agreed that the system is no longer required and that its associated data files, which may be archived, will not require restoration at a point in time. Appropriate procedure has to be followed during disposal, which includes raising genuine requirement for disposal of software with strong case against its use in the future, approval of disposal from appropriate authority within the organization, approval of disposal from appropriate regulatory authority if in case disposal requires approval from regulatory authority, and proper plan of action for disposal.

14.10 Developing and Maintaining and In-House Software

- Software Development

14.10.1.1 Software Development Process

Over the course of time, there is a need to customize existing software or to develop new software at the Bank

The Policy to adhere are:

- Software development for or by the Bank must always follow a formalized development process which itself is managed under the project in question. The software requirements and specifications must be finalized. Priority must be given to in-house development. If in-house development is not possible due to excessive time consumption or inadequate resources, then the software development project should be outsourced. Further, it may not be possible to develop all kinds of software within the organization given that complex software applications are developed at software firms that deploy numerous developers. Nevertheless, irrespective of whether the development is in-house or outsourced, a proper plan of action is required. This usually includes requirements gathering, requirements finalization, analysis of whether this

can be done in-house or outsourced, selection of appropriate resources or vendor for development, the development process itself, the user acceptance testing process, and the go-live process. The last process i.e. go-live process, must always be done after due approval from concerned authority and with appropriate plan of action. Further, cost approval must be obtained from appropriate authority if the development process requires cost either in-house or through outsourcing.

14.10.1.2 Making Emergency Amendments to Software

The emergency measures that we should adopt if it becomes necessary to amend the live software environment immediately.

The Policy to adhere are:

- Emergency amendments to software are to be discouraged, except in circumstances previously designated by concerned authority as critical. Any such amendments must strictly get approval from the concerned authority and follow a proper plan with appropriate documentation.

14.10.1.3 Establishing Owner for System Enhancement

Ensuring that users recognize and accept their responsibilities for enhancements, this should always be driven by the needs of business.

The Policy to adhere are:

- All proposed system enhancements must be business driven and supported by an agreed business case. Functional ownership and responsibility for any such enhancements must be taken by the concerned department. Technical ownership and responsibility for any such enhancements must be taken by Information Technology department.

14.10.1.4 Justifying New System Development

Developing a system from scratch as opposed to enhancing a present system represents a major decision. The business case for a customized development must be very strong indeed to reject the selection of a suitable packages solution.

The Policy to adhere are:

- The concerned department must finalize the requirements of new system. Study of whether required system is available in the market should be done. If the new system is not readily available in the market, then suitable vendor must be selected to develop the new system. In addition, the selection criteria should include capability of the vendor to develop the new system.

14.10.1.5 Managing Change Control Procedure

Change control ensures that all changes are analyzed and authorized. The management of the process is used to enforce the requirement.

The Policy to adhere are:

- All changes to programs must be properly authorized and tested in a test environment before moving to the production environment and proper documentation must be maintained. Further, approval from concerned authority is a must when changes are implemented in live environment.

14.10.1.6 Separating System Development and Operations

Organizations are likely to have separate systems operations and system development department and networks. It is nevertheless vital to separate these functions.

The Policy to adhere are:

- The organization must ensure that proper segregation of duties applies to all areas dealing with systems developments, system operations or system administrations.

- Testing and training

14.10.1.7 Managing Test Environment

This is the process to keep system testing separate from live operational work.

The Policy to adhere are:

- There must be a separate test environment for all systems as applicable. Before implementation, proper testing should be done in test environment. Only after achieving required output and verification, the same should be applied to live environment and proper documentation should be maintained.

14.10.1.8 Using Live Data for Testing

Ideally, all testing would utilize only realistic test data, expressly created for the purpose. However, in practice that may not be feasible, but it may be necessary to use a copy of current data files.

The Policy to adhere are:

- Only the concerned authority is given rights to copy live data to test environment. Appropriate documentation must be maintained when live data is copied to the test environment. The use of live data for testing new system or system changes may only be permitted to staffs who are involved in testing. Furthermore, test users can be given additional roles or upgraded roles in the test environment.

14.10.1.9 Capacity Planning and Testing of New and Amended Systems

The system testing process should also verify that new or amended systems are able to handle the expected transaction volumes, delivering both acceptable performance and resilience.

The Policy to adhere are:

- The concerned department must also be involved in functionality testing. These systems must be tested for capacity, peak loading and hardware sizing. They must demonstrate a level of performance and resilience that meets the technical and business requirements of the Bank.

14.10.1.10 Training in New System

This is to ensure that all users both business and technical are adequately trained in the use of all new systems and enhanced systems.

The Policy to adhere are:

- Training is to be provided to users and technical staff in the functionalities and operations of all new systems. Training should be given to develop trainers. These trainers should provide the same training to other staffs in their branches and departments. If the training in new systems is not possible internally, then the training can be outsourced.

- Documentation

14.10.1.11 Documenting New and Enhanced System

New and enhanced systems are to be adequately documented. All too often. Due to budget and other resources limitations, documentation can be limited or even totally ignored. The information security threats become substantial especially where changes or amendments are required, possibly at short notice for regulatory or other reasons.

The Policy to adhere are:

- All new enhanced system must be fully supported at all times by comprehensive and up to date documentation. Documentation can be developed in-house or can be obtained from the concerned vendors.

- Other Software Development

14.10.1.12 Acquiring Software developed by Vendor

This is in regards to acquiring software that is provided by outside suppliers, either as a package or as customized development to meet the specific needs of our Bank.

The Policy to adhere are:

- The software developed by vendor must meet the User Requirements Specification and offer appropriate product support. In addition, a Service Level Agreement is mandatory for vendor developed software.

14.11 HR Management

- Creation and Deletion of User IDs

All the new recruited staffs are to be provided with new User IDs as applicable e.g. System ID, Email ID, Finacle access ID, etc. Likewise, upon resignation/termination if any staff, his/her all user IDs and accesses in system must be deleted.

The Policy to adhere are:

- When recruiting and deploying any staff in the Bank (Department/branch), HR department and the concerned department head/ branch manager must inform to IT/DB department to create User IDs of such

staff as appropriate to him/her in writing/email with required application/standard form and upon receipt of such request, IT/DB Department shall create User IDs of such staff as requested to provide access in the system, CBS and other system to perform day to day task. Likewise, if any staff resigned or terminated from the Bank, HR department shall inform in writing/email to IT/DB and other department and IT/DB and other department shall delete all user IDs pertaining to such staff in the system with effect from the end of last working day (effective date of resignation).

- **IT /DB Training**
  Bank should assess the requirement of expertise to successfully complete required IT/DB Functions. A periodic IT/DB training requirement for IT/DB personnel, according to the IT/DB functions of the Bank should be assessed

The Policy to adhere are:

- Human Resource Department in coordination with Information Technology and Digital banking department send their staffs for IT/DB training to acquire skills, depending on their job responsibilities. The training requirement should be as per the Human Resource Policy.

CHAPTER 15 Migration Policy

A data conversion (also known as data porting) is required if the source and target systems utilize different field formats or sizes, file/database structures, or coding schemes.

The objective of data conversion is to convert existing data into the new required format, coding and structure while preserving the meaning and integrity of the data. The data conversion process must provide some means, such as audit trails and logs, which allow for the verification of the accuracy and completeness of the converted data. This verification of accuracy and completeness may perform through a combination of manual processes, system utilities, vendor tools and one-time-use special applications.

The Policy to adhere are:

- Bank should have a migration standard procedure with details of migration process to ensure principle of information security. After each stage of migration and after completion of migration, explicit sign offs from application owner should be taken to ensure data integrity, completeness and consistency of data.

CHAPTER 16 Capacity Management

Capacity management is the term describing a variety of IT monitoring, administration and planning actions that ensure that a computing infrastructure has adequate resources to handle current data processing requirements across the entire service lifecycle, as well as the capacity to accommodate future loads.

The capacity management procedure concerns performance, memory, and physical space, and shall cover both the operational and development environment, including hardware, human resources, networking equipment, peripherals, and software.

The Policy to adhere are:

- Bank shall practice to optimally utilize the existing capacity before adding new IT resources.
- Bank shall monitor its IT resources quarterly to determine the shortage or excess of resources.
- The use of resources must be monitored, tuned and projections to be made of future capacity requirements to ensure the required system performance to meet the business objectives.
- Different parameters such as data storage capacity (in database systems, file storage areas, etc.); processing power capacity (e.g. adequate computational power to ensure timely processing operations.); and communications capacity (often referred to as “bandwidth” to ensure communications are made in timely manner) shall be monitored proactively by the Bank on quarterly basis.
- Resource utilization report shall be submitted to Senior Management on quarterly basis for review.
- All the corrective actions shall be applied before the capacity usage reaches to critical point.
- There shall be formal SOPs for handling, monitoring and managing the capacity/utilization for the IT systems/network infrastructure resources within the Bank.

CHAPTER 17 Service Level Agreement (SLA) and Non-Disclosure Agreement (NDA)

A service-level agreement (SLA) is a document that outlines a commitment between a service provider and a client, including details of the service, the standards the provider must adhere to, and the metrics to measure the performance. An NDA or non-disclosure agreement is a binding contract between two or more parties that prevents sensitive information from being shared with others.

The Policy to adhere are:

- There shall be maintenance service arrangement for all hardware and software for post warranty period
- The Bank may have service level agreement with the vendor for critical hardware and software. In that case, the bank shall exercise utmost care in having a contract without an interruption due to delay in renewal of contract.
- All the agreements with the vendors shall be reviewed by the Bank's Legal Department compulsorily.
- The Bank shall ensure that the equipment does not contain sensitive live data when hardware is taken by the vendors for servicing/repair.
- Service Contracts with all service providers including third-party vendors shall include:
    - Parties to the contract with address.
    - Definitions of terms, if necessary.
    - Measurable services/deliverables.
    - Background check on all the employees of the third-party, who will be providing services to the Bank as support personnel.
    - Timing/schedules, i.e. service levels,
    - Roles and responsibilities of contracting parties, including an escalation matrix clearly mentioning response time and resolution time.
    - Pricing of the contract
    - Penalty Clause, Confidentiality clause, Termination clause,
    - Contact person names (on daily operations and relationship levels),
    - Renewal period
    - Modification clause
    - Frequency of service reporting,
    - Warranties, including service suppliers' employee liabilities, 3rd party liabilities and the related remedies
    - Geographical locations covered
    - Ownership of hardware and software,
    - Documentation to be maintained (e.g. logs of changes, records of reviewing, event logs),
    - Audit right of access (internal audit, external audit, other audit as may be appropriate),
    - Any other clause considered fit for the contract.
- Bank must obtain non-disclosure agreement (NDA) with all the vendor that provides support to the Bank.

CHAPTER 18 Disaster Recovery

Disaster Recovery policy is considered as the Technology Aspect of Business Continuity Plan. There are many applications and services in banking system that are highly mission, critical in nature and therefore requires high availability, and fault tolerance to be considered while designing and implementing Disaster Recovery.

The Policy to adhere are:

- Disaster Recovery (DR) Site must be in place replicating the DC (Data Centre) of the Bank.
- DR site must be locally mirroring to the DC site, replicating all resources.
- DR architecture has to be designed with high-availability and without single point of failure. Accordingly, with respect to performance and availability aspects following architectures have to be designed and documented to ensure high level of up time:
    - DC architecture
    - DR architecture
    - Network and security architecture
    - Branch or delivery channel architecture
- Configurations of servers, network devices and other products at the DC and DR have to be identical at all times. This includes patches that are applied at DC periodically and changes made to software from time to time by customization and parameterization to account for the regulatory requirements, system changes etc.
- Periodic checks with reference to ensuring data and transaction integrity between DC and DR are mandatory.
- Disaster Recovery Architectures have to have a defined RTO (Recovery Time Objective) and RPO (Recovery Point Objective) parameter. These two parameters have a very clear bearing on technology aspects as well as the process defined for cut over to DR and competency levels required to change over in specified timeframe.
- The DR (Disaster Recovery) drill must be conducted at least once in every six months and will have to ensure that the above parameters of RTO and RPO are strictly complied with.
- A disaster recovery plan shall be in place and must dictate every facet of recovery process, include the followings:
    - What events denote possible disasters;
    - What people in the bank have the authority to declare a disaster and thereby put the plan into effect;
    - The sequence of events necessary to prepare the backup site once a disaster has been declared;
    - The roles and responsibilities of all key personnel with respect to carrying out the plan;
    - An inventory of the necessary hardware and software required to restore production;
- A disaster recovery plan must be a living document; as the data center changes, the plan must be updated to reflect those changes.

CHAPTER 19 Virus Protection

Antivirus software is essential to protect computer from viruses and other types of malware, such as ransomware, adware and spyware. It works by scanning files for known viruses and malicious code and then blocking or removing them from the system.

The Policy to adhere are:

- Antivirus software must be installed in each server, ATMs and end-user computer.
- Virus auto-protection mode and auto scan must be enabled.
- Anti-virus software shall always be updated with the latest virus definition file automatically.
- All computers in the network must get updated signature software automatically from the server.

CHAPTER 20 Asset Disposal

Asset disposal is the elimination of an asset from a Bank records, typically by selling or scrapping of unwanted or end of life IT assets in a safe and environmentally responsible way.

The Policy to adhere are:

- When IT assets have reached the end of their useful life for any reason, they shall be disposed properly. Disposal refers to physical destruction or selling of the assets.
- After mitigating the relevant security risks, GSD to dispose the equipment owned by the Bank. Furthermore, computer equipment that is obsolete and non-repairable must be disposed. The disposal must be done as per the Bank's internal policies and guidelines.
- Disposal of media requires authorization by the data owner of record. In addition, the owner of the physical media must also authorize disposal.
- The IT Department shall properly remove all data prior to fine disposal and document all the details including date, staff performing and verifying disks wipe.
- The IT Department must securely erase all storage mediums in accordance with current industry best practices.
- Upon disposal, assets shall be removed from Fixed Assets Record.
- No IT assets shall be disposed of via skips, dumps, landfill, etc. All electronic drives must be degaussed or overwritten with a commercially available disk cleaning program. Hard drives may also be removed and rendered unreadable (drilling, crushing or other demolition methods). During physical disposal, along with IT Department, GSD shall also be present.

CHAPTER 21 Remote Access

Remote access refers to the technology that allows authorized person to access a bank computer or network from a remote location. Remote access is built to help connect and gain access to internal network resources, such as IT/DB services, data, and applications, from any location.

The Policy to adhere are:

- The Bank may sometimes provide employees, vendors, and others with access to the institution's network and computing resources through external connections. Those connections are typically established through modems, the internet, or private communication lines. The access may be necessary to remotely support the institution's systems or to support institution operations at remote locations. In some cases, remote access may be required periodically by vendors to make emergency program fixes or to support a system.
- Bank shall carefully consider the security of any remote access solutions that involve running a remote access server on the same host as other services and applications.
- While using Internet-based remote access, Bank needs to establish a virtual private network (with IPsec or SSL) over the Internet to securely communicate data packets over public infrastructure. Two factor authentication process shall be enabled (e.g. PIN based token card with a one-time random password generator, or token based PKI).
- Remote access privilege shall be granted for specific purpose of the Bank after due approval from Senior Management.
- There shall be regular review of remote access approval from ISO.
- Remote access privileges to the Bank's network if required shall be given the same consideration as the user's onsite connection to the Bank.
- Bank shall consider the balance between the benefits of providing remote access to additional resources and the potential impact of a compromise of those resources. Bank shall ensure that any internal resources it chooses to make available through remote access are hardened appropriately against external threats and that access to the resources is limited to the minimum necessary through firewalling and other access control mechanisms.
- All the vendor support report onsite and offsite shall be maintained by respective Department in coordination with Vendor. Report shall be reviewed by Information Security unit on periodic basis.
- Remote Access should only be obtained as per the Remote Access guidelines of the Bank
- Notify ISU for every remote access that has been granted along with purpose to vendor/ After/before office hours.

CHAPTER 22 IT/DB Governance

IT governance is an element of corporate governance, aimed at improving the overall management of IT. The framework enables to manage IT risks effectively and ensure that activities associated with information and technology are aligned with their overall business objectives of the Bank. Since IT/DB is very critical in supporting and enabling business goals and is strategic for business growth, due diligence on its governance is essential. IT /DB governance is a continuous process where IT/DB strategy drives the process using necessary resources.

The Policy to adhere are:

- Bank shall assess the requirement of expertise to successfully complete required IT/DB functions.
- A periodic IT/DB training requirement for IT/DB personnel of the bank shall be assessed.
- Bank shall have performance monitoring and measuring system of IT/DB functions and it shall be reported to appropriate level of management.
- Banks shall implement international IT/DB control framework such as COBIT as applicable.
- Bank shall be adequately aware of the IT/DB resources of the bank and ensure that it is sufficient to meet the business requirements
- Information Security Officer (ISO) shall be responsible for coordinating and communicating security related issues within the organization or with relevant external organization.
- Enhanced IT/DB performance through the implementation of effective IT/DB Risk Management, efficient IT/DB process and maintaining availability of IT/DB services.
- Bank shall increase stakeholder confidence regarding IT/DB Risk Management.
- Bank shall carryout detail risk analysis before adopting new technology/system since it can potentially introduce new risk exposure.
- Bank shall have process in place to identify and adequately address the legal risk arising from cyber law and electronic transaction related laws and acts of Nepal.
- Bank shall increase the awareness to safeguard valuable IT/DB assets throughout the organization.

CHAPTER 23 Check and Reviews

The functions of IT/DB department are to be monitored/reviewed on periodic basis to ensure all the procedures detailed here in and duly complied with.

The Policy to adhere are:

In order to maintain proper control and system in the IT/DB departments following checks and review shall be carried out on periodic basis.

a. **Quarterly**: Information Security Officer or the person as designated by him/her must ensure that the procedures detailed herein have been duly complied with.
b. **Annually**: Information Security Officer must ensure that this IT policy is reviewed once in a year and any amendment, deletion and addition as required due to the new development have been done vide amendment. If no change required, notification of the same is recorded and continued the same.
c. **Annually**: Chief Internal Audit Department shall carry out internal audit of IT/DB department at least once in a year to ensure that all the provisions detailed herein have been duly complied with.