Internship Report

On

"IT Policy of Shahjalal Islami Bank Ltd."

(A study on Head Office)

Prepared For

Md. Noman Hossain Chowdhury

Senior Lecturer

BRAC Business School

BRAC University

Prepared By

Shiab Khan

ID# 13164039

MBA

BRAC University

BRAC University
Date of submission: 17/08/2015

Letter of Transmittal

Date: August 17, 2015

Mr. Md. Noman Hossain Chowdhury

Senior Lecturer

BRAC University

Subject: Submission of Internship Report on **"IT Policy of Shahjalal Islami Bank Limited".**

Dear Sir,

In connection of my practical orientation in Shahjalal Islami Bank Ltd., I would like to submit my report to you for your perusal. I have prepared this report on the basis of my practical exposure at IT Division of Shahjalal Islami Bank Ltd.

I enjoy preparing this report, which enriched my partial knowledge of the theoretical concept. I tried to reflect the operational aspects of the Bank, which is complementary to the theoretical and practical knowledge.

I will be very glad if the report can serve its actual purpose and I am ready to explain anything to you if you feel necessary.

Yours Sincerely,

……

Shiab Khan

MBA Program

ID NO: 13164039

Major in Finance

BRAC University

Declaration

I, Shiab Khan, hereby declare that the report of internship Program titled "IT Policy of Shahjalal Islami Bank Limited" is uniquely prepared by me.

I confirm that, the report is only prepared for my academic requirement not for other purpose. It might be with the interest of opposite party of the corporation. I also assure that this report is not submitted anywhere of Bangladesh before me.

……..

Shiab Khan

ID NO: 13164039

Major in Finance

MBA Program

BRAC University

Acknowledgement

At first I want to express my gratitude to Almighty Allah for giving me the strength and the composure to finish the task within the scheduled time. Then I am very grateful to the Shahjalal Islami Bank Ltd. for providing me the opportunity to complete my internship program.

I received cordial cooperation from the officers and members of staffs of Shahjalal Islami Bank Ltd., IT Division. I want to express my cordial gratitude to them for their cooperation without which it would not be possible to complete the report.

I would like to express my deep sense of gratitude & sincere appreciation to my internship supervisor Mr. Md. Noman Hossain Chowdhury, Senior Lecturer, BRAC Business School, BRAC University for his continuous support & guidance during the practical orientation period. His suggestions and comments were really a great source of spirit to make the report a good one.

Finally I am really thankful to Mr. Md. Rafiqul Islam, Executive Vice President & Head of IT, Mr. Md. Rezaul Karim, Executive officer of the Shahjalal Islami Bank Ltd IT Division for giving me the excellent opportunity to do my practical orientation in their branch.

.

Thanks all from core of my heart.

Contents

Executive Summary

IT Policy is a systematic approach to policies required to formulate for ensuring manageability, confidentiality, integrity, availability and security of information and information systems. This Policy also covers all information that electronically generated, received, stored, printed, scanned, and typed. The provisions of this Policy are applicable for Shahjalal Islami Bank Limited. All activities and operations required to ensure data security including infrastructure, facility design, physical security, surveillance system, network security, disaster recovery and business continuity planning, use of hardware and software, data disposal, and protection of copyrights and other intellectual property rights.

Information Technology (IT) is the bedrock for the Bank's survival and development in a rapidly changing global environment, and challenges us to devise bold and courageous initiatives to address a host of vital skilled human resources. In addition, an Information Technology Policy built on reliable human resources and infrastructure constitutes the fundamental tool and means of assessing, planning, managing development change and for achieving sustainable growth.

Every progressive Bank has its own IT Policy and an implementation strategy to respond to the emerging global reality and thus avert becoming a victim of the digital divide.

Information Technology Security (ITS) achieved by implementing a suitable set of controls, including policies, procedures and standards. Specific Security Policy is required to establish for all information/computer users of the Bank. This approved IT Policy has been updated to reflect the rapidly changing Technologies within the Bank, to assist users of these facilities to ensure that the facilities are properly protected and those specific IT security objectives are met. Following the IT Policy, information system services of the Bank in accordance with Information Technology standards, guidelines and best practices of the Bank can ensuring that its information technology and business systems may be protected and controlled.

Chapter One

Introduction

1.1 Introduction

This document describes Information Technology (IT) Policy of Shahjalal Islami Bank Limited (SJIBL). IT policy, like other organization policy, is generally focused on what should be done and on what parties are responsible for different activities. However, policy generally steers clear of describing how these activities should be performed. That, instead, is the role of procedures and standards, discussed in this Policy. All concerned both in the Branches or in the Head Office of the Bank shall observe and follow the guidelines provided in this document.

The policy statements developed for all levels of users acting in different roles in the IT system of the Bank including general users of different software used in the Bank, all officials of SJIBL is responsible for maintaining the system, and the members of the top management of the Bank.

1.2 Definitions

Information System - An electronic information system that processes data electronically through the use of information technology - including but not limited to computer systems, servers, workstations, terminals, storage media, communication devices, network resources, and any other input/output devices.

Confidentiality - The principle of confidentiality means keeping information given by or about an individual in the course of a professional relationship secure and secret from others. Only authorized persons are allowed to know or gain access to the information stored or processed by Information Systems in any aspects.

Integrity - Only authorized persons are allowed to make changes to the information stored or processed by Information Systems in any aspects.

Availability - Information Systems should be available to users at any given or specified period depending on business need.

IT Policy - A documented list of management instructions that describe in detail the proper use and management of resources relating to IT with the objective to protect these resources as well as the information stored or processed by Information Systems from any unauthorized disclosure, modifications or destruction.

Official - Persons employed by the Bank irrespective of the employment period and terms.

Data Center (DC) - A centralized data processing facility that houses Information Systems and related equipment. A data center (or data centre or datacentre or datacenter) is a facility used to house computer systems and associated components, such as telecommunications and storage systems. It generally includes redundant or backup power supplies, redundant data communications connections, environmental controls (e.g., air conditioning, fire suppression) and security devices.

Computer Room/Server Room - A dedicated room for housing computer Server(s) and other necessary equipment either in the Branch or in the Head Office for processing business

data.

Malicious Codes - Programs that cause undesirable effect to the Information Systems. Examples of malicious codes include computer viruses, network worms, Trojan horses, logic bombs, and spy ware etc.

Information Technology (IT) - The term 'information technology' means computers, ancillary equipment, software and firmware (Hardware) and similar procedures, services (including support services) and related resources. This also includes any equipment or interconnected system or subsystem of equipment, which used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.

Sensitive data - Sensitive data encompasses a wide range of information and can include: ethnic or racial origin; political opinion; religious or other similar beliefs; memberships; physical or mental health details; personal life; or criminal or civil offences. These examples of information are protected by civil rights. Sensitive data can also include information that relates to as a consumer, client, employee, patient or student; and it can be identifying information as well: like national ID or voter ID number, Tax Identification number, Passport number, contact information (address, e-mail account, phone number), KYC, Client Account information (A/C balance and other info, if any), identification cards and numbers, birth date, and parents' names. All of this data belongs to the bank's employee/customer of the bank. We should have full rights to access and use this information and also have rights to know how others are doing the same. Just like other belongings we should be protective of this information too.

1.3 Scope of the Policy

This document addresses uses and security considerations of information systems of the Bank in the following areas:

a) IT Security Management;
b) IT Operation Management;
c) Physical Security;
d) Information Security Standard
e) Access Control Security;
f) Data Security;
g) Application Security;
h) Network & Communication Security;
i) Software Development and Acquisition;
j) System Support Management
k) Business Continuity and Disaster Recovery Plan;
l) Security Risk Assessment & Management;
m) Procurement and Service Provider Management

1.4 Objectives of the Policy

This Policy defines the requirements of the Bank, which must adhere. The objectives of the policy are:

a) To establish a standard IT Policy & IT Security management;
b) To Identify the Information System Risk and their management;
c) To communicate the responsibilities of the IS users for the protection of the system;
d) To prioritize information and information systems those require protect;

e) To aware and training, the users associated with managing the IT infrastructure;
f) To establish a technology based electronic paperless Bank;
g) To explain procedure for periodic review of the policy and system security measures;
h) To improve the overall smooth operation and business of the Bank;

Chapter Two

IT Security Management Policy

IT Security Management ensures that the IT functions and operations of the Bank efficiently and effectively managed. IT Division ensures maintenance of appropriate systems documentations, particularly for systems, which support financial reporting. They have to participate in IT security planning to ensure that resources allocated consistent with business objectives. Also ensure sufficient and qualified technical officials are employed in the Bank; so, that continuance of the IT operation area is unlikely to be seriously at risk all times.

IT Security Management deals with IT Security Policy, Documentation, Internal Information System Audit, Training, and Insurance. IT security planner and/or management shall be responsible for overall IT security management.

2.1 IT Security Policy

This document provides the Policy for Information System and its secured usage for the Banks. It establishes general requirements and responsibilities for protecting Information and Information System. The policy covers common technologies such as computers & peripherals, data and network, web system, and other specialized IT resources. The Bank's delivery of services depends on availability, reliability, and integrity of its information system. Therefore, Bank must adopt appropriate methods to protect its information system. The senior management of the Bank must express commitment to IT security by continuously increasing awareness and ensuring training of the Bank's official.

The policy will require regular update to cope with the evolving changes in the IT environment in the Bank.

2.1.01 Policy Statement

a) Security means protection of Data & Equipments from Internal and External threats.
b) Data, the priceless assets of the Bank should be protected from any level of hackers.
c) To avoid fraud and forgery data & equipments should be maintained in a secured manner.
d) Priority should be given at the highest level for the security aspects of data and equipment.
e) There should be 02 (two) types of Security like Physical & Logical.
f) Security Policy includes data, data handling, user, & access control of users, external attack, hardware, and location & position of hardware.

2.1.02 Detail Policy:

2.1.02.01 Physical Security

a) Entrance should be controlled & monitored in the Branches during banking hour/ peak hour

and after banking hour/off peak hour in due course.

b) Entrance should be controlled in the Data Center and Server/Computer Room.
c) Modern CCTV system to be implemented with proper application.
d) Log Book is to be maintained for entrance Data Center in Head office and Server/Computer Room in Branches.

- Data Security Storage Device i.e. Data Safe should be procured for the preservation of Data Cartridges, CD/DVDs, License Copies, Agreements etc.
- Security Devices to be used in the following manner:
  1. Router, Firewall etc. Security Devices should be used in the LAN and WAN.
  2. World-renowned Branded Security Devices should require for the Bank.
  3. There should be separate Servers for Database, Application, Exchange, Mails, & others
  4. and the Servers should be located in different places.
  5. Redundant Hardware storage e.g. PC Server, Workstations, Monitor, Scanner, &Printers
  6. should be procured for instant support.

2.1.02.02 Logical Security

a) Access into the application system
   a) Access into the Server should strictly control using Administrative Password.
   b) Access into the Server through Workstations to be controlled, and monitored by the System and Database Administrator.
   c) Access into the Workstations to be properly monitored and controlled.
b) Usage and operations of Hardware & Application systems
   1. Usage of the Server & Workstations to be controlled by the System Administrator.
   2. Usage of Network Devices to be maintained sophisticatedly.
   3. Usage of Printers, Movable devices & other computer components are to be used, and maintained very carefully.
   4. Usage of any movable device as if Floppy or flashes are strictly prohibited.
   5. Usage of Banking Software should strictly be controlled by the system Administrator. The Application Software only to be used as on when required.
   6. Access into the database system should strictly be controlled. Only authorized personnel may have access into the database as a very special case. Database password should be kept in lock and key.
   7. On-line transactions among the branches should be checked and verified frequently in a day by the system administrator very carefully.
   8. On-line transactions with Head Office should be taken in a shadow file and having final checking & confirmation those may be integrated into central systems.
c) Sharing resources
   1. Sharing of resources to be setup to avoid repetition of works and to quicker functionalities.
   2. Unlimited access to be prohibited always in sharing all sorts of resources.
   3. Sharing of resources should be controlled through maintaining passwords.
d) Users
   1. The branch incumbent should select executives and Officers as ‘User’, who used to work in the Information System with Banking Software. Everyone should have a user ID(name/number (employee id)). Every individual should maintain a password to work into the system.
   2. Competent authority may permit every individual ‘User’ against their assigned official works/jobs and responsibilities. Branch incumbents are advised not togive extra limit and maintenance permission for the officials, who are in probation period.

3. Individual 'User' should be liable for each and every transaction entered by them as marked in the application log file and transaction file against their user ID.
4. Competent authority should maintain a 'User' list with given permissions to the individuals with duly signed and date.

e) Log Reports
1. Log Reports to be maintained for access into the system and uses of different applications accordingly in detail.
2. Log Reports for all exceptions of the system should also be maintained properly.

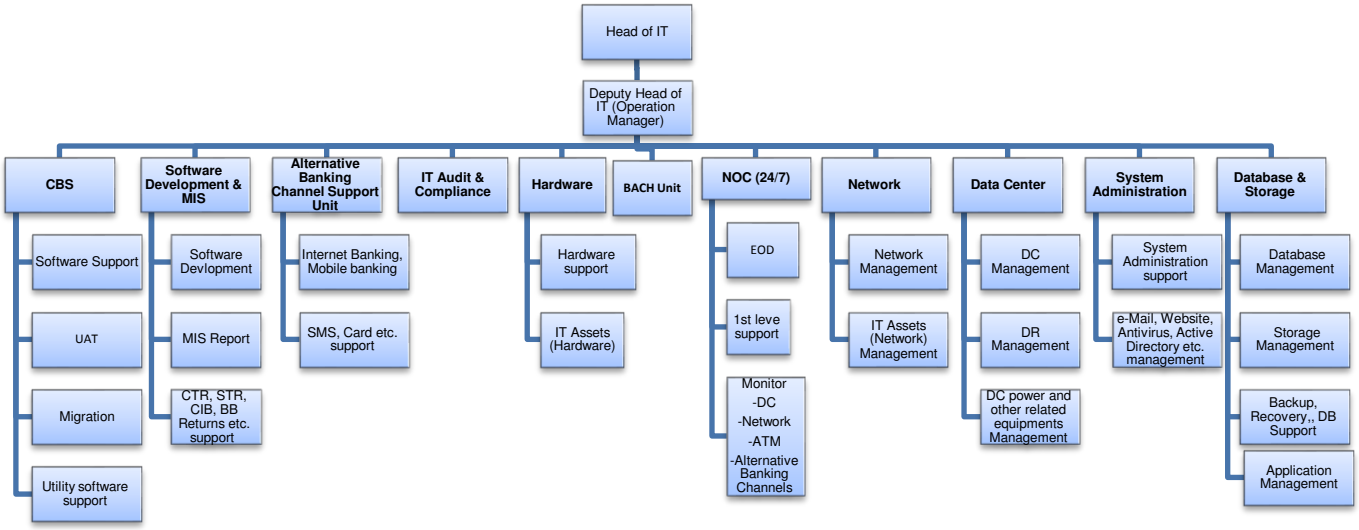
f) Software Security
1. Data should be transferred using cryptography technology through WAN.
2. Sensitive Data should be preserved in the Database in encrypted format.
3. Security Software to be installed in the LAN & WAN bridges and in the Servers.
4. Anti-Virus, Anti-spam and Anti-warm tools should be install, and update in the system on a regular basis.

2.2 Documentation Policy

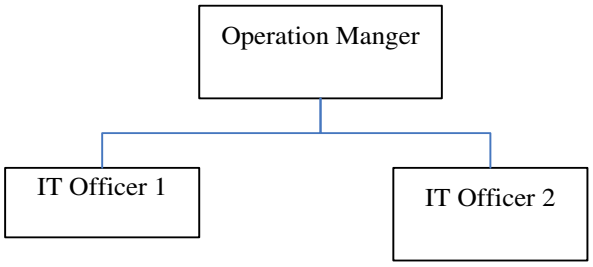
IT division shall establish, document and maintain a security incident handling/ reporting procedure for their Information Systems.

a) Documents are to be included with Notes, Memos, Minutes, Resolutions, Decisions, Circulars, Office Orders, Instructions, Letters, Applications, Mails, Agreements, Contracts, Bills and any other documents used in the Banking operations.
b) Documents are to be preserved in two ways: Scanning physical documents into electronic format and documents to be prepared in electronic format.
c) Manual documents are to be converted into electronic formats.
d) Internal Memo/Circular should be generated through Intranet mail after completion of full automation.
e) Board/EC/Audit/Shariah Memo are also to be submitted in electronic format.
f) Documents are to be prepared manually in physical format until necessary rules and regulations are not modified for digital documentations and digital signature.
g) All electronic/digital documents should be tagged with digital signature.

2.2.01 Organogram chart of IT Division.


Head of IT
Deputy Head of IT (Operation Manager)
CBS
Software Development & MIS
Alternative Banking Channel Support Unit
IT Audit & Compliance
Hardware
BACH Unit
NOC (24/7)
Network
Data Center
System Administration
Database & Storage
Software Support
UAT
Migration
Utility software support
Software Devlopment
MIS Report
CTR, STR, CIB, BB Returns etc. support
Internet Banking, Mobile banking
SMS, Card etc. support
Hardware support
IT Assets (Hardware)
EOD
1st leve support
Monitor
-DC
-Network
-ATM
-Alternative Banking Channels
Network Management
IT Assets (Network) Management
DC Management
DR Management
DC power and other related equipments Management
System Administration support
e-Mail, Website, Antivirus, Active Directory etc. management
Database Management
Storage Management
Backup, Recovery,, DB Support
Application Management

2.2.02 Branch Organogram with IT support Personnel.



Job Responsibility:

- Maintain physical security of IT room
- Maintain Log Register for the personnel who visit the IT room
- Maintain proper communication with IT for different purpose.
- Check the branch e-mail and communicate it to the Operation Manager for necessary compliance
- Maintain antivirus operation as per guideline provided by IT as and when required
- Coordinate the auditors during IT Audit
- Arrange IT Operation training within branch in association with IT as and when required.
- Preserve and distribute Operation Manual, IT policy and other IT related documents, IT circulars and guideline circulated by Head Office among the branch users for their use.
- Help the branch to carry out the other instructions of IT Division conveyed time to time.

2.2.03 Segregation of duties for IT tasks.

Segregation of duties is a key concept of internal controls of an organization. Increased protection from fraud and errors the Bank must balanced with the increased of cost and effort required. Segregation of duties should be exists for IT tasks of all IT personnel.

2.2.04 Job description (JD) for each Team.

Job Description (or better known in short as JD) is a document that used to indicate scope of work for the employee. It is often used in hiring process as well as job design. This piece of document gives an employee a good picture of what his/her responsibility is, and a manager good picture of who does what in the team. Shahjalal Islami Bank Limited creates a flexible employee centric JD instead of a static organization structure centric one. The Bank looks very fundamental and simple following issues in Job Description:

Identify Goals, Share Goals with Team, Team to Build JDs, Analyze undesired task, Assign undesired task, Hiring Process, Keeping them high-level, Encourage employees to share and Goal Focused, not JD Focused.

Job description (JD) for each individual of IT department/division and Branch IT support unit with fallback support personnel should be documented.

2.2.05 Scheduled roster for shifting duties.

In the roster for shifting duties, the employer operates 24 hours in a day, seven days in a week, all year round. Scheduled roster for the personnel doing shifting duties should be documented. Payment will be made for duty on holydays.

2.2.06 Fallback plans for system support personnel.

Fallback plans for various levels of system support personnel should be documented.

2.3 Internal Information System Audit Policy

Internal Control and Compliance Division shall carry out internal Information System Audit.

Internal Information System Audit Team should have sufficient IT Audit Expertise/ Resources and should be capable of conducting Information System Audit.

Information Systems shall periodically evaluated by IT auditors to determine the minimum set of controls required to reducing risk to an acceptable level. An annual system audit plan shall be developed. Bank shall also ensure that audit issues are properly tracked out and in particular, completely recorded, adequately followed up and satisfactorily rectified.

Auditing of compliance of computer and network security policies shall be performed periodically.

Use of software and programs for security audit analysis shall be restricted and controlled.

The Branch/Department/Division of Head Office shall respond appropriately to address the recommendations made in the last Audit Report. This must be documented and kept along with the Audit Report.

2.4 Training Policy

All officials should get proper training, education, updates, and awareness of the IT Security activities as relevant with their job function.

All IT Personnel should get the minimum level of Business Foundation Training.

IT has to provide necessary training when New system: IT through HR/ training branch/concerned users provide training.

Branch has to send request for required IT related training.

As a substitute of arrangement of training at ITD, Training material may be supplied in a central location as pdf and video CD with live training demo may be sent to branch end for necessary training.

2.5 Insurance or Risk Coverage Fund Policy

All IT assets should be under Insurance coverage to be maintained by Financial Administrative Division.

Adequate insurance coverage or risk coverage fund shall be maintained so that costs of loss and/or damage of the IT assets can be mitigated.

2.6 Problem Management Policy

Bank shall establish a process to log the information system related problems and incidents. IT division shall establish incident detection and monitoring mechanism to detect contain and ultimately prevent security incidents.

Process shall have the workflow to assign the issue to a concerned person to get a quick, effective, and orderly response., As for example,

1. Workflow for Hardware team,
2. Workflow for Network Team,
4. Workflow for Database & Storage Team,
5. Workflow for CBS Team,
6. Workflow for software Team and
7. Workflow for NOC/DC/DR
8. Workflow for system administration.

Process shall be established to perform necessary corrective action within the period according to the problem's severity.

Problem findings and action steps taken during the problem resolution process shall be documented.

Process shall be established to review and monitor the incidents.

IT division shall ensure that system logs and other supporting information are retained for the proof and tracing of security incidents.

2.7 Risk Management Policy

Information Systems security risk assessments for information systems and production applications shall be performed at least twice in every year. A security risk assessment shall also be performed prior to major enhancements and changes associated with these systems or applications. Effective risk management system shall be in place for any new processes and systems as well as a post-launch review.

Use of software and programs for security risk assessment analysis shall be restricted and controlled.

The risk management function shall ensure awareness of, and compliance with, the IT and IT Security Policy, and to provide support for investigation of any IT related frauds and incidents.

The risk management process shall include:

a) A description and assessment of the risk being considered and accepted for acknowledgement by the owner of the risk;
b) Identification of mitigation controls;
c) Formulation of a remedial plan to reduce the risk;
d) Approval of the risk acknowledgement from the owner of the risk and senior management.
e) A Risk Management Team should be formed which can work jointly with RMU division of the Bank for compliance of Basel Accord.

2.8 Personnel Development & Security Policy

2.8.01 Manpower Recruitment Policy

a) Educational Qualification of fresh recruitment for IT division must be minimum ICT related Graduate but in case experience personnel the qualification may be consider or relaxed.
b) For the recruitment of IT Personnel a comprehensive test to be taken by the expertise.
c) Internet media may be used for the total recruitment management operations.

2.8.02 Personnel Development Policy

a) All the employees of the Bank should have sufficient IT knowledge in connection with banking operations with Information System.
b) IT advancement, up gradation and the new released technology along with Bank's own IT policies, functions, and planning to be informed/provided at all level of management and employees.
c) IT personnel should strengthen their skill and knowledge on latest technology to guide and drive the Bank with the newer facilities and opportunities.
d) Bank will arrange/provide advance training of the IT personnel in local and abroad.
e) IT personnel to be attend in the Seminars/Workshops/Special Training Program on IT in local and abroad on importance and requirement basis.

2.8.03 Personnel Security Policy

Job definition/job assignment and resource allocation should be considered, which might reduce the risk of human error, theft, fraud, or misuse of facilities. Security should be addressed at the recruitment stage. Managers should ensure that job descriptions are addressed with all relevant security responsibilities and in confidentiality agreement.

To ensure the awareness of information security threats and concerns are equipped to support organizational security policy in course of their work. User should be trained about security procedures and the correct use of information processing facilities.

Chapter Three

IT Operation Management Policy

IT Operation Management covers the dynamics of technology operation management including change management, asset management, operating procedures and request management. The objective is to achieve the highest levels of technology service quality by minimum operational risk.

3.1 Change Management Policy

Changes to information processing facilities and systems shall be controlled.

A formal documented process followed for change details, which must governed for all changes of business application implemented in the production environment. Audit logs of changes shall be maintained.

User Acceptance Test (UAT) for changes and upgrades in application shall be carried out before deployment.

As the business practices have been changing day-by-day, it is required quite often to change parameterization of existing products or to introduce new product. The Business Unit of the Bank will decide about such changes or will introduce such product. Before changing any parameterization or before launching any product, the business group must have confirmation from IT Division, whether the system supports the changes or incorporation. Banking Product Development of IT Policy of the Shahjalal Islami Bank Limited covers the procedures before launching any new product.

The activities will be as follows:

a) Business Unit will ask the IT Division for parameterization of the changes or introduction of new product as per Change Request. All the detail information of the request, duly signed by the respective requester, must be attached in separate sheet along with the Change Request Form.
b) IT Officers will check and test the required changes in the Test Server. The activities in the Test Server will be documented as Audit Log for future ready reference. The results or output in the Test Server will be formally referred back to Business Unit.
c) Considering the output of the IT Division, the Business Group will finalize the product or changes and the final request will be placed to IT Division as per the same Change Request Form along with all the detail information of the products or request, duly signed by the respective Requested.
d) IT Division will do the same changes in the Test Server, following the documents prepared earlier. If the desired output is derived, immediately will be put forward to the Business Unit for their acceptance. All of these activities will be documented, as a part of User Acceptance Testing.
e) If success, the same changes or parameterization will be done in the Production Server after having the Approval from Head of IT.

f) All the steps or activities done in the Production Server Should documented as Audit Log for future ready reference.
g) After the completion, it will be referred to the Business Unit, who will then circulate to all the respective Branches, informing about the changes or parameterization done in the Production Server.

3.2 IT Asset Management Policy

IT Assets shall be clearly identified and an Inventory with significant details must be maintained.

All assets associated with the information facilities must be labeled with tag and name. Asset inventory must be reviewed at least once a year.

All data on equipment and associated storage media must be destroyed or overwritten before sale, disposal, or reissue.

Bank must comply with the terms of all software licenses and must not use any software that has not been legally purchased or otherwise legitimately obtained.

Software used in production environment must be subjected to a support agreement.

Software used in any computer must be approved by the authority. Use of unauthorized or pirated software must be strictly prohibited throughout the Bank. Random checks shall be carried out to ensure compliance.

3.2.01 Hardware Inventory Management and Tracking Policy

Prior to distribution to the Division/department/Branch, IT Division shall require to entry data into hardware Inventory Management software.

A non-removable tracking sticker on a visible place of the hardware shall be stamped for tracking.

After payment is made, FAD should update the Inventory through an application client provided by IT division to the person delegated by FAD.

3.2.02 Hardware Repairing & Troubleshooting Policy

Each member of Hardware and System Support Team of IT Division is individually responsible for Hardware repairing, maintaining, troubleshooting, and sending to respective Branch/Department/ Divisions. They are also responsible for Operating System, Application software, Antivirus, Banking Software (BankUltimus) etc. installation, maintenance, and troubleshooting.

If end user encounters any malfunction or dysfunction with desktop computer, s/he should immediately contact system support Team of IT Division over ticket management software, telephone, e-mail or through a forwarding letter. System Support Team members try to give solution over telephone. If it is not possible to solve the problem by IT Division over telephone then depending on nature of problem, one of the following two decisions could be taken:

a) Sending one hardware engineer at Branch end or

b) Sending PC to IT Division of Head Office for repairing of damaged component.

The former one is usually follows for branch LAN renovation, virus cleaning from the branch, providing training to the mass users and the latter one for Desktop, PC/Printer, UPS, network or other equipments.

Employees needing computer hardware other than what is stated above must request such hardware from the IT Division. Each request will be considered on a case-by-case basis in conjunction with the purchase committee of the Bank.

3.3 Disposal of IT Assets

3.3.1 Purpose

The purpose of this procedure is to establish and define standards and restrictions for the disposal of non-leased IT equipment in a legal, cost-effective manner. Shahjalal Islami Bank Limited (SJIBL) surplus or obsolete IT assets and resources (i.e. desktop computers, servers, databases, etc.) must be discarded according to legal requirements and environmental regulations through the appropriate personnel/unit and the SJIBL upgrade guidelines. Therefore, all disposal procedures for retired IT assets must adhere to SJIBL-approved methods.

3.3.2 Scope

This procedure applies to the proper disposal of all non-leased SJIBL IT hardware, including PCs, printers, handheld devices, servers, databases, hubs, switches, bridges, routers, and so on. SJIBL-owned surplus hardware, obsolete machines, and any equipment beyond reasonable repair or reuse are covered by this procedure. Where applicable, it is desirable to achieve some residual value of the IT asset in question through reselling, auctioning, donation, or reassignment to a less-critical function.

3.3.3 Definitions

1. “Non-leased” refers to any and all IT assets that are the sole property of the SJIBL; that is, equipment that is not rented, leased, or borrowed from a third-party supplier or Banks partner.
2. “Disposal” refers to the reselling, reassignment, recycling, donating, or throwing out of IT equipment through responsible, ethical, and environmentally sound means.
3. “Obsolete” refers to any and all equipment which no longer meets requisite functionality.
4. “Surplus” refers to hardware that has been replaced by upgraded equipment or is superfluous to existing requirements.
5. “Beyond reasonable repair” refers to any and all equipment whose condition requires fixing or refurbishing that will likely cost equal to or more than total replacement.

3.3.4 IT Asset Types

This section categorized the types of assets subject to disposal.

1. Desktop workstations (CPU, Monitor, Key Board, Mouse)
2. Laptop
3. Printers, Multifunction machines, Projectors
4. UPS

5. Scanners
6. Servers
7. Storage
8. Tape Library
9. Firewalls
10. Routers
11. Switches
12. Racks
13. DC and DRS IT supporting equipment
14. Memory devices

3.3.5 Guidelines

Disposal procedures of all IT assets and equipment will be centrally managed and coordinated by the Hardware Team of IT Division. The Hardware Team is also responsible for backing up and then wiping clean of SJIBL data all IT assets slated for disposal, as well as the removal of SJIBL tags and/or identifying labels. The Hardware Team is responsible for selecting and approving external agents through proper channel for recycling hardware and/or sanitizing hardware of harmful toxins before shipment to landfills.

3.3.6 Practices

Acceptable methods for the disposal of IT assets are as follows:

a) Sold in a public forum.
b) Auctioned online.
c) Sold as scrap to a licensed dealer.
d) Used as a trade-in against cost of replacement item.
e) Reassigned to a less-critical business operation function.
f) Donated to schools, charities, and other non-profit organizations.
g) Recycled and/or refurbished to leverage further use (within limits of reasonable repair).
h) Discarded as rubbish in a landfill after sanitization of toxic materials by an approved service provider as required by local regulations.

3.4 Operating Procedure Policy

Operating procedures shall be documented, maintained, and available for the users related to their job function.

Changes to operating procedures must be approved by management and documented.

Operating procedures shall cover the followings where appropriate:

a) Documentation on handling of different processes;
b) Documentation on scheduling processes, system start-up, close-down, End of Day, restart and recovery (centralized/decentralized);
c) Documentation on handling of exception conditions;
d) Schedule system maintenance;

3.5 Active Directory Policy

3.5.01 Active Directory:

- Focal point for network & user management.
- Central authority for network & application security.
- Integration point for bringing systems together.

3.5.02 Benefits of Active Directory

Active Directory helps small and medium size organizations with a reliable working environment for the end-users, which offers the highest levels of reliability and performance. So, users can perform their work as efficiently as possible, as well as providing a more secure and manageable environment to make the lives of the domain easy to track any miss utilization & disoperation and bring under control.

The following sections will review the advantages of Active Directory in these areas:

3.5.02.01 Increasing the Productivity of Users

(a) The Power of Group Policy

- Creating Standardized Configurations, Settings, and Options.
- Automatic Access to Local Resources.
- Enabling Features and Functions on the Fly.
- User Profiles and Redirected Folders.
- Offline Folders.

(b) Windows Update Services
(c) Remote Assistance
(d) System Quarantine

3.5.02.02 Reducing the Burden of IT Administration

a) Server Performance and Reliability
b) Administrative Benefits of Group Policy
   1. Account Password Policies :
      i. The password definition parameters ensure that minimum password length is specified at least 6 characters, combination of uppercase, lowercase, numbers & may include special characters.
      ii. Password history maintenance ensures same passwords to be used again after at least 4 times.
      iii. The maximum validity period of password shall not be beyond the number of 30 to90 days cycle.
   2. Account lockout Policies:
      i. Account shall be locked up after 3 unsuccessful login attempts.
c) Software Installation Restriction Policies
d) Remote Installation Services
e) Remote Administration
f) Improving Fault Tolerance to Minimize Downtime
g) The Distributed File System

h) Volume Shadow Copy Service
i) Advanced Server Recovery
j) Enhanced Security.
k) File-Level Encryption
l) IP Security
m) Improved Management Tools
n) Configure Secure Servers

3.6 Change Management Policy of in-house software:

Live in-house software may require some changes (major/minor) in the following cases:

1. Expected result is not found:
   When new variety or exception is applied, expected result may not be found. Then software team modifies and executes required changes in the software.
2. Requirement of additional reports:
   When additional reports or scope is required, the user sends a request to Head of IT with the details. Software team does and executes required changes in the software as instructed by Head of IT. The new requirement details are documented. Such as new user interface of report format.
3. Up gradation of software tools and data bases:
   Change of technology may be required. In-house software requirement is approved from competent authority. Software is developed as per In-house software development policy.

Chapter Four

Physical Security Policy

Shahjalal Islami Bank requires sound business and management practices to implement in the workplace to ensure that IT resources are properly protected. The responsibility of each department is to protect technology resources from unauthorized access in terms of both physical hardware and data perspectives. In fact, the effective security measure for assets in the workplace is a responsibility held jointly by both management and employees.

4.1 Access Control Policy

A list of persons who authorized to gain access to data center, server rooms, computer rooms or other areas supporting critical activities, where computer equipment and data are located or stored, shall be kept up-to-date and be reviewed periodically.

Access keys, cards, passwords, etc. for entry to any of the Information systems and networks shall be physically secured or subject to well-defined and strictly enforced security procedures.

Automatic protection features (e.g. password protected screen saver, keyboard lock) in servers, computer terminals, workstations should be activated if there has been no activity for a predefined period to prevent illegal system access attempt. Alternatively, the logon session and connection should be terminated. In addition, user workstation should be switched off, if appropriate, before leaving work for the day or before a prolonged period of inactivity.

Physical security involves providing environmental safeguards as well as controlling physical access to equipment and data. The following safeguard methods are believed to be practical, reasonable, and reflective of sound business practices.

4.1.01 Data Center Access Policy

a) Physical security shall be applied to the information processing area or Data Center. Data Centre is the restricted area and unauthorized access prohibited.
b) Number of entrance into the Data Centre will be limited, locked, and secured.
c) Access Authorization procedures will exist and apply to all persons (e.g. employees and vendors). Unauthorized individuals and cleaning crews will be escorted during their stay in the Data Centre.
d) Bank will maintain access authorization list, documenting individuals who authorized to access the data centre and that will reviewed and updated periodically.
e) Access log with date and time, will be maintained documenting individuals who have accessed the data centre.
f) Visitor Log will exist and need to be maintained.
g) Security guard will be available for 24 hours.
h) There will be Emergency exit door available.

4.1.02 Server Room Access Policy

a) Server room has a glass enclosure with lock and key with a responsible person of the branch.
b) Physical access shall be restricted, visitors log will be exist and maintained for server room.
c) Access authorization list will be maintained and reviewed on regular basis.

4.2 Environmental Security Policy

Careful site selection and accommodation planning of a purpose-built computer installation shall be conducted.

Data centers and computer rooms shall have good physical security and strong protection from disaster and security threats, whether natural or caused by other reasons, in order to minimize the extent of loss and disruption.

Backup media containing business essential and/or mission critical information shall be sited at a safe distance from the main site in order to avoid damage arising from a disaster at the main site.

4.2.01 Data Center Environmental Safety Policy

a) Protection of Data Center from the risk of damage due to fire, flood, explosion and other forms of disaster shall be designed and applied.
b) Sufficient documentation is essential regarding the physical layout of the data centre.
c) Documentation regarding the layout of power supplies of the data centers and network connectivity should be prepared.
d) Floors to be raised with removable square blocks or channel alongside the wall to be prepared, which allow all the data and power cabling to be in neat and safe position.
e) Water detection devices should be below the raised floor, if it is raised.
f) Any accessories, not related to Data Center should not be allowed to store in the Data Centre.
g) Existence of Closed Circuit Television (CCTVs) camera is must for DC and it should be monitor regularly.
h) Data Centre must show the sign of "No eating, drinking or smoking".
i) Dedicated Office Vehicles for any emergency purpose should always be available on site. Availing of public transport should be avoided while carrying critical equipments outside the bank's premises to avoid the risk of any causality.
j) Address and telephone or mobile numbers of require emergency contact persons (e.g. Fire service, police station, service providers, vendor, and all IT personal) should be available to cope with any emergency.
k) Proper attention must be given with regard to overloading of electrical outlets with too many devices. Proper and practical usage of extension cords should be reviewed annually in the office environment.
l) Power supply system and other support units must be separated from production site and placed in secure area to reduce the risks from environmental threats.
m) Power supply from source (Main Distribution Board or Generator) to Data Center must be dedicated. Electrical outlets from these power sources for any other devices must be restricted and monitored to avoid the risk of overloading.
n) Development and test environment shall be separated from production.

o) Data Center shall have dedicated fulltime supported telephone communication.

4.2.02 Data Center Security Maintenance

a) Level 1: Physical Entrance
b) Level 2: Operating System
c) Level 3: Database

4.3 Fire Prevention Policy

a) Wall, ceiling, Floor, and door of Data Center should be fire-resistant.
b) Fire suppression equipments should be installed.
c) Automatic fire alarming system shall be installed and tested periodically.
d) There shall be fire detector below the raised floor, if it is raised.
e) Electric and data cables in the Data Center must maintain industry standard quality and to be concealed.
f) Any flammable items shall not be kept in the Data Center.

4.4 Physical Security for IT Assets

a) All Information Systems shall be placed in a secure environment or attended by the officials to prevent unauthorized access.
b) Users in possession of laptop, portable computer, personal digital assistant, or mobile computing devices for business purposes shall safeguard the equipment in his/her possession, and shall not leave the equipment unattended without proper security measures.
c) IT equipment shall not be taken away from sites without proper control.

Chapter Five

Password Policy

5.1 Overview:

All employees and personnel that have access to organizational computer systems must adhere to the password policies defined below in order to protect the security of the network, protect data integrity, and protect computer systems.

5.2 Purpose:

This policy & order is designed to protect the organizational resources on the network by requiring strong passwords along with protection of these passwords, and establishing a minimum time between changes to passwords.

5.3 Scope:

This policy & order applies to any and all personnel who have any form of computer account requiring a password on the organizational network including but not limited to a domain account and e-mail account.

5.4 Password Requirements (subject to change):

Those setting password requirements must remember that making the password rules too difficult may actually decrease security if users decide the rules are impossible or too difficult to meet. If passwords are changed too often, users may tend to write them down or make their password a variant of an old password, which an attacker with the old password could guess. The following password requirements are given below:

1. Minimum Length - 6 characters recommended for singly usage and 8 characters for dual usage
2. Maximum Length - 14 characters
3. Minimum complexity - No dictionary words to be included. Passwords should use three of four of the following four types of characters:
    1. Lowercase
    2. Uppercase
    3. Numbers
    4. Special characters such as!@#$ %^&*(){}[]
4. Passwords are case sensitive and the user name or login ID is not case sensitive.
5. Password history - Require a number of unique passwords before an old password may be reused. This number should be no less than 03.
6. Maximum password age - 90 days
7. Minimum password age - 2 days
8. Store passwords using reversible encryption or sealed & signed by authorized officials into a secured vault. This should not be done without special authorization by

the IT Division since it would reduce the security of the user's password.

9. Account lockout threshold - 3 failed login attempts
10. Account lockout duration - the account lockout should be between 30 minutes and 2 hours.
11. Password protected screen savers should be enabled and should protect the computer within 5-10 minutes of user inactivity. Computers should not be unattended with the user logged on and no password protected screen saver active. Users should be in the habit of not leaving their computers unlocked. User can press the CTRL-ALT-DEL keys and select "Lock Computer".

Chapter Six

Network Policy

The Shahjalal Islami Bank Limited has the responsibility for securing its networking systems against unauthorized access, while making the systems accessible for legitimate and administrative usages. This responsibility includes informing persons who use the network systems of expected standards of conduct and encouraging their application. It is important for the user to practice ethical behavior in computing activities because the user has access to many valuable and sensitive resources and the user is computing practices can adversely affect the work of others. Improper use and abuse of networks will not be permitted. Presently SJIBL has two-fiber optic WAN connectivity into data center as well as Branches. Near future the Bank will be established another WAN connectivity through radio/VSAT.

6.1 Network Policy

Prior approval from the Head of IT and Manager, IT Security is required to connect one Information System with another Information System. The security level of the Information System being connected shall not be downgraded.

a) Maintenance arrangement/agreement to be made with the supplier/vendor or any other third party at least one calendar month prior to the expiry of free service and warranty period.
b) Preference to be given for the maintenance arrangement/agreement with the suppliers/ vendors
c) Internal setup and arrangement to be ready for support, services, and maintenance.
d) Sufficient Expertise/Professionals to be recruited/trained for the above.
e) Necessary equipments/machineries to be procured/purchased for the above.
f) Regional Offices/Branches may be allowed to complete/solve minor problems of Network by any third party having permission from Head Office
g) Electronic and manual Log book to be maintained by Head office, Regional Office and Branches for support service and maintenance record.
h) Regional Offices/Branches should send all the equipments/machineries to Head Office, which are non-repairable/out of order
i) Necessary support devices/items to be stocked/procured/purchased for immediate support of Head Office, Regional Office and Branches.
j) Network installation configuration as per requirements and maintain documentation and standards

6.1.01 Scope:

a) Network equipments (Router, Switch shall be configured) in a secure environment.
b) Groups of information services, users, and information systems shall be segregated in networks, e.g. VLAN.
c) Unauthorized access and electronic tampering shall be controlled strictly.
d) Firewall shall be in place on the network for any external connectivity.

e) Redundant communication links shall be used for WAN.
f) There shall be a system to detect unauthorized intruder in the network.
g) Connection of personal laptop to office LAN or any personal wireless modem with the office laptop/desktop must be secured.

6.1.02 Networking Hardware Procurement/Purchase Policy

a) Requisitions/Requirements to be generated through proper channel.
b) Requirement analysis to be carried by Information Technology Division and recommendation to be placed before the Procurement Committee/Competent authority.
c) As per latest Procurement Regulation maintained by Procurement Committee of SJIBL and that will be proceed for publishing Tender Notice in the Daily Newspaper/collecting spot quotations as per approval of the Competent Authority.
d) Purchase and Procurement Committee will evaluate the Tender Documents/Quotations submitted by vendors.
e) Evaluation and Comparative statement with specific proposal to be placed before the appropriate level of management as per financial discretionary power for approval.
f) Work Orders to be issued having approval of the competent authority.
g) Items/components are to be received along with Challan/Delivery Memo.
h) Data/information is to be entered in details into the Computerized Inventory Management System/Registers and transfer/locate the items/components accordingly.
i) Certification/comments of the item/component's status are to be collected before allowing payments of bills.
j) Warranty coverage and follow-up for maintenance arrangement should be maintained.
k) Service agreement where applicable to be arranged.

6.1.03 Network Systems Policy

a) Systems are to be included with Network Equipments, Network, Firewall, Cryptography, Operating Systems, Utility software etc.
b) For the standard setup of the network systems in the Bank, Cisco Switches, Cisco Routers, Radio Base Station etc. should be installed.
c) Industry standard architecture should be installed in setting LAN and WAN.
d) All systems should be open-standard.

6.1.04 Design, Planning, Approval, Implementation & Maintenance of LAN & WAN

a) Designing the WAN setup in a ISO certification standard manner.
b) Creating and Maintaining the design documentation in a secured manner.
c) Core devices capabilities analysis and deployment planning.
d) Branch devices capabilities analysis and deployment planning.
e) Implementation planning.

6.1.05 Network Security Policy

a) The Network Design and its security are implemented under a documented plan.
b) Creating and maintaining the design documentation of the security area.
c) Branch security area analysis and deployment of planning.
d) Physical security for the network equipment should be ensured. Specifically:

i. Access (Physical & Logical) should be restricted and controlled.
ii. These should be housed in a secure environment.

e) The sensitive information should be kept in restricted area in the networking environment.
f) Unauthorized access and Electronic tampering is to be controlled strictly.
g) Security of the network should be under dual administrative control.
h) Core Firewalls devices are in place on the network for any external connectivity.
i) Redundant communication links are used for WAN.

6.1.05.01 Network Design

Following a structured set of steps when developing and implementing network, security will help to address the varied concerns that play a part in security design. Many security strategies have been developed in a haphazard way and have failed to actually secure assets and to meet a customer's primary goals for security. Breaking down the process of security design into the following steps will help effectively plan and execute a security strategy:

a) Identify network assets.
b) Analyze security risks.
c) Analyze security requirements and tradeoffs.
d) Design a security plan.
e) Define a security policy.
f) Develop procedures for applying security policies.
g) Develop a technical implementation strategy.
h) Achieve buy-in from users, managers, and technical staff.
i) Train users, managers, and technical staff.
j) Implement the technical strategy and security plan.
k) Test the security and update if any problems are found.
l) Maintain security.

6.1.05.02 Modularizing Security Design

Security experts promote the security defense in depth principle. This principle states that network security should be multilayered, with many different techniques used to protect the network and each mechanism should have a backup mechanism. This is sometimes called the belt-and-suspenders approach. Both a belt and suspenders ensure that trousers stay up. A networking example is to use a dedicated firewall to limit access to resources and a packetfiltering router that adds another line of defense.

In general, using a modular approach to security design is a good way to gain an understanding of the types of solutions that must be selected to implement security defense in depth. The next few sections cover security for the following modules or components of an enterprise network:

a) Internet connections
b) Remote-access and virtual private networks (VPN)
c) Network services and management
d) Server farms
e) User services
f) Wireless networks

6.1.06 Physical Security

Security Devices to be used in the following manner:

a) Router, Firewall etc. Security Devices should be used in the LAN and WAN.
b) World-renowned Branded Security Devices should be setup for the Bank.
c) There should be separate room for implementation of security devices, router, and other network devices.
d) Redundant Hardware e.g. Router, Switch, Firewall, optical-converters etc. should be setup for instant support.

Bank requires that sound business and management practices must be implemented in the workplace to ensure that information and technology resources are properly protected. It is the responsibility of each department to protect technology resources from unauthorized access in terms of both physical hardware and data perspectives. In fact, the effective security measure of assets in the workplace is a responsibility held jointly by both management and employees. Physical security involves providing environmental safeguards as well as controlling physical access to equipment and data. The safeguards methods are believed to be practical, reasonable, and reflective of sound business practices.

6.1.07 Supervision, Control, & Monitoring of Network Securities

a) Controlling the Securities through Intrusion Prevention System (IPS) or Intrusion Detection System (IDS).
b) The network team should properly monitor network. Monitoring software may be used for proper monitoring.
c) Supervision and monitoring of Securities area at all level of HO and Branches.
d) Internet threats protection.
e) Integrations with system admin securities.

6.1.08 Password Control

a) Access into the Network Equipments should strictly be controlled using Administrative Password.
b) Access into the Network Equipment through Workstations to be controlled, and monitored by the Administrator.
c) Access into the Network Equipment to be properly controlled.
d) Password to be maintained as strictly confidential. System Administrative Password should be preserved in safe custody.
e) Users should be liable to maintain his/her own password and the Password should not be maintained by a name or any likings.
f) Password may be chosen with mixed characters (e.g. 32bQt_N) and to be of at least eight characters, which detail mention on password policy chapter 5.
g) The maximum validity period of password should be 60 days.
h) The maximum number of invalid logon attempts should be 03 (Three) consecutive times.
i) Password history maintenance is enabled in the system to allow same passwords can be used again after at least 4 times.
j) Password entries must be masked.
k) The terminal inactive time allowable for users should be set where necessary.
l) Sensitive passwords have to be preserved in a sealed envelope with movement records for usage in case of emergency.

m) Audit trail should be available to review the user profile for maintenance purpose.

6.1.09 Policy Statement

a) Network to be setup within the Head Office, Back Office, Disaster Recovery Center, Central Bank, Local & Foreign Banks, Branches, Remote sites, Valued Clients and other regulatory bodies to share the resources and to provide better services.
b) Security measures should strictly be maintained before adding any node within the network.
c) Security Policies of the Bank to be implemented for network.
d) Network setup should be in international standard architecture and structured format.
e) Network equipments/devices and accessories should be international standard.
f) Network Management Software to be used for Network Monitoring and management.

6.1.10 Firewall Policy

a) There should be a system to detect the unauthorized intruder for network.
b) All ports except usable ones shall be blocked.
c) Data rate per port per channel has to be limited.
d) Ingress/Egress packets must be logged and stored.
e) NAT shall be used as much as possible. Network Security Policy
f) Security means protection of Data & Equipments from Internal and External threats.
g) Data, the priceless assets of the Bank should be protected from any level of hackers.
h) To avoid fraud and forgery data & equipments should be maintained in a secured manner.
i) Priority should be given at the highest level for the security aspects of data and equipments.
j) There should be 02 (two) types of Security like: Physical Security & Information Security.
k) Security Policy includes data, data handling, user, & access control of users, externalattack, hardware, and location & position of hardware.
l) There should be a team of 'Network Administrator' assigned by the competent authority for the Head Office to follow-up and maintain security of all networks.

6.1.11 Control & Monitoring of LAN & WAN functionalities

a) Bandwidth consumption analysis.
b) Bandwidth management
c) Load Balancing management.
d) NOC member functionalities formation.
e) Network management software to be used for Network Management protocol (SNMP).

6.1.12 Local Area Networks (LAN) Policy

a) Cabling should be structured. Fiber optic cable to be preferred for LAN cabling; initially Cat5/Cat6 cable may be used.
b) Rack, Patch Panel, Cable Management Unit, Patch Cord, Drop Cable, Face Plate, RJ45 etc. are to be used in connection with LAN setup.
c) Separate Domain (VLAN) for each Department/Division is to be setup in the Switch.
d) IP based network to be setup for nodes and all IPs are to be maintained confidentially.

e) Network policies to be determined in the server for each domain.

6.1.13 Wide Area Networks (WAN) Policy

a) Physical Fiber optic cable connectivity should be preferred for WAN setup within HO and Branch LANs.
b) Wireless connectivity may be set before having physical connectivity for WAN.
c) For the full setup of on-line Banking primary connectivity should be physical and redundant may be wireless.
d) Virtual Private Network should be setup in connection with WAN through Service Providers Bridge/Tunnel.
e) Data should be transmitted through WAN using cryptography technology.
f) Security measures should be taken into consideration in WAN connectivity and usage at a highest level of priority as per security policies of the Bank.

6.1.14 Upgrade design, setup, and security levels of LAN & WAN

a) Upgrade of the WAN setup in an ISO certification standard manner.
b) Upgrade of Core devices and deployment planning.
c) Upgrade Branch devices and deployment planning.
d) Security measures should strictly be analysis before adding any new node within the Network.

6.1.15 Maintain log records of LAN & WAN status.

a) Design and approval of network monitoring software with log/report option
b) Supervision and monitoring of network monitoring software with log/report option
c) Archive planning of logs/reports

6.1.16 Router -Switch Data Backup & Restoration Policy

a) Data means all sorts of information kept in printed or electronic format in The Shahjalal Islami Bank Limited.
b) Data should be preserved in a secured manner in our designated FTP server (Hard Disk), PC for Network Administrator's & removable disks (e.g. CD/DVD).
c) Removable disks should be preserved under lock and key in safe custody outside Location (geographically Separate) of the related office (Head Office or Branchoffice).
d) There should be at least one backup copy kept on-site for time critical delivery.
e) Branches and Head Office should preserve Network related data such as router images & configurations in our FTP server as well as Network Administrator's PC on weekly basis.
f) The backup log sheet is maintained, checked, & signed by Team Leader.
g) The backup inventory is maintained, checked, & signed by Team Leader.
h) The ability to restore from backup media is tested at least quarterly.
i) Backup Media must be labeled properly indicating contents, date etc.
j) Backup CD/DVDs should be preserved at Head Office in a Fungus & Dust Free, Fireproof Data Safe/Vault.

6.1.17 Redundant Access Policy from Branch to Head Office

The Branch will consider a disaster branch if both of the link goes down & unable to restore more than 6 hours. Hence, in that situation the steps will be followed as guided by System Support Team.

6.2 VPN Policy

8.2.01. Purpose

The purpose of this policy is to provide guidelines for Remote Access Virtual Private Network (VPN) connections to SJIBL banking network

6.2.02. Scope

This policy applies to all SJIBL employees, Link Vendors, and others including all personnel affiliated with third parties utilizing VPNs to access the SJIBL network. This policy applies to implementations of VPN that allow direct access to SJIBL network from outside the SJIBL network.

6.2.03. VPN approval

a) Approved SJIBL employees and authorized third parties (vendor support, etc.) may utilize the benefits of a VPN, which is a "user managed" service
b) VPN profiles will be created only at the request of a user's by submitting the appropriate VPN Access Request form. Additionally, the user must have read, understood, and acknowledged this policy before using the VPN service.

6.2.04 General Conditions for VPN

a) It is the responsibility of employees with VPN privileges to ensure that unauthorized users are not allowed access to SJIBL internal networks.
b) VPN use is to be controlled using either a one-time password authentication such as a token device or a public/private key system with a strong passphrase.
c) When actively connected to the corporate network, VPNs will force all traffic to and from the PC over the VPN tunnel: all other traffic will be dropped.
d) Dual (split) tunneling is NOT permitted; only one network connection is allowed.
e) VPN gateways will be set up and managed by SJIBL network operational groups.
f) All computers connected to SJIBL internal networks via VPN or any other technology must use the most up-to-date anti-virus software that is the corporate standard (provide URL to this software); this includes personal computer/Laptop.
g) VPN users will be automatically disconnected from SJIBL's network after thirty minutes of inactivity. The user must then logon again to reconnect to the network. Pings or other artificial network processes are not to be used to keep the connection open.
h) The VPN concentrator is limited to an absolute connection time of 24 hours.

6.3 General Network Protections

Internal network addresses, configurations and related system or network information shall not be publicly disclosed.

All internal networks with connections to other networks or publicly accessible computer networks shall be properly protected.

Security measures shall be in place to prevent unauthorized remote access to the systems and data.

Computer users are prohibited from connecting workstations to external network by means of communication device, such as dial-up modem, wireless interface, or broadband link, if the

workstations are simultaneously connected to a local area network (LAN) or another internal communication network, unless with the approval of the Head of IT.

Computer users shall not connect any unauthorized Information System device to Bank's Information System without prior approval of manager, IT security.

Proper configuration and administration of information / communication systems is required and shall be reviewed regularly.

Connections and links made to outside network shall not compromise the security of information system of the Bank.

Connecting privately owned computer resources to Bank's internal network requires approval from Manager, IT security.

CONFIDENTIAL/RESTRICTED information shall be encrypted when transmitted over an un-trusted communication network.

All network or systems software malfunctions, information security alerts, warnings, suspected vulnerabilities, and the like, and suspected network security problems, shall be reported immediately only to the responsible party according to the incident handling procedure.

Chapter Seven

Internet and Web Surfing Policy

7.1 Introduction

This policy will explain how to introduce a policy that clearly states what acceptable internet is and e-mail usage.

The internet is an essential tool for many businesses. E-mail and the web offer a variety of ways to improve communications with employee, customers, and suppliers.

However, allowing employees access to the internet carries risks. If they accidentally or deliberately access illegal web content, e.g. anything related to indecent material, business could be open to prosecution. There is a security risk - employees could download and install software that may infected by a virus. In addition, any abuse of e-mail facilities could cause internal and external problems. For example, sending bulk e-mail could result in system overload and network congestion.

7.2 Requirement of internet and e-mail policy

There are three major reasons to introduce policy for internet and e-mail use within business:

- To protect the business from possible legal action resulting from personnel actions - employee are legally responsible for personnel actions when they are using the internet or e-mail at work.
- To ensure that communications resources are not wasted and productivity does not suffer.
- To help protect the business from potentially damaging viruses which could be received or downloaded via the internet or e-mail.

In general, providing internet access and e-mail facilities to our employee has tremendous benefits. It can increase efficiency, aid communication and help employees increase their basic IT skills.

Allowing employee to access the internet and e-mail facilities outside working hours can be seen as a perk of the job. However, controlling and policing such access may be difficult.

Trivial abuses of the system include transferring large file attachments, or wasting work time on internet surfing, personal e-mail or online chat. More risks that are serious include:

- Downloading files that contain viruses.
- Obtaining copyrighted material such as music or films.
- Transmitting valuable or sensitive business information without encryption.
- Distributing or relaying offensive or abusive material via e-mail.
- Generating junk e-mail, or spam, via mass mailings.
- Accepting files from people in online chat rooms which could bypass firewalls or e-mail filters.

More misconduct that is serious may result in disciplinary or even legal proceedings. This includes:

- Accessing or downloading pornography or other offensive material.
- Libeling or defaming colleagues or even external business contacts, via e-mail.
- Using the internet to commit fraud or other illegal acts.

Introducing internet and e-mail usage policy should help avoid these risks. It should also ensure that business and employee get the best possible use out of the information system.

Policy should state clearly what is and is not permitted by the employee using the internet or e-mail. It should ensure that employees are aware of the policy and the consequences of breaching them.

7.3 Internet usage policy for officers and executives:

All Internet connections shall be routed through a DMZ firewall and Proxy Server for computers connected to SJIBL network while browsing, downloading, or an attachment of any incoming mail. . In case of any acceptation, Divisional Heads/Branch Managers may send formal requisition to IT Division with proper justification. Head of IT decides to allow his or her internet access from their work place. However, to grant permission, Bank has been declared an internet restricted use policy (IRUP) by IP based.

The IRUP should have some classified policies via Proxy Server:

Classification of Internet policy

a) **All Permission (AP):** Those have all permission including social and security exchange web portal.
b) **Maximum Permission(FP):**Those have full internet access except social web portal(e.g. facebook.com) and some unnecessary web portal which are hampered official environment of the bank (e.g. dsebd.org etc.) from their workplace. Some limited essential newspapers are allowed the office hour.
c) **Partial Permission (PP):**Those have government, educational of Bangladesh, all financial and e-mail web portal.
d) **Only Permission (OP):**Those have Bangladesh bank, SJIBL official site, Google mail and Foreign Remittance related web portal (Western Union, MoneyGram and Xpress Money etc.)
e) **Limited Permission (LP):** Only Bangladesh Bank and its e-services (Online CIB services**,** LC Monitoring System, Web Upload and Online Foreign Exchange Transaction Monitoring System)
f) **Restricted Permission (RP):** Some social, Security exchange web portal and essential newspapers are allowed behind the office hour (before 10.00 am and after 6.00 pm). On the basis of requirement of division and approved by the Head of IT security exchange web portal (e.g. dscbd.org) may be allowed in the officer hour.

7.4 E-mail usage policy for officers and executives:

E-mail has become an essential tool of modern business communications. It is fast and efficient, but can also potentially be a source of embarrassment or even litigation.

1. The mails will be considered as an evidence of any pursuance. i.e. requisition procedure to Divisional Heads/Branch Managers.

2. Leave application will not be processed through this mail.
3. Investment proposal DFA/Acknowledgement can be sent to Investment Division actual proposal to be sent having necessary correction physically.
4. IT Support request form can be sent through proper channel.
5. Scanned Image of Circulars can be sent to the Divisions/Branches.
6. Transmission of any confidential mater to any third party having proper approval.
7. It is not the replacement of earlier Divisional/Branch e-mail addresses. These e-mail addresses will be created by "employees' Name' and the earlier e-mail addresses will be used on behalf of Divisions/Branches.
8. All employees will be eligible to get the e-mail address by their Title/first name/short name followed by employee ID.
9. HRD, HO shall send to IT division of the Name, Designation and posting details of the employees.
10. Email may be used personal purpose.

Official procedure of maintaining e-mail by officers and executives:

(a) Usage of e-mail for executives and officers:

1. e-mail address will be created for all employees including cash in charge. Cash officers will not get e-mail ID. Shahjalalislmaibank.com has been defined as the domain name of SJIBL.
2. Using a part of employee name with his/her employee ID, e-mail ID will be created by Head Office. As an example, employee name Md. Aby Syeed Alamgir having his employee ID (1234) will have the e-mail ID alamgir1234@shahjalalislamibank.com which will be determined by Head Office. Please mention that name title and short form of name are not allowed as email ID except MD and AMD
3. There exist group e-mail ID for e-mail communication under restricted use. The groups are namely All Employees, All Branches, All Branch Managers, All Branch Operations Manager, All AD Branches, All Non AD Branches, All ATM Associated Branches, All Departments/Divisions & Branches, All Departments/Divisions, All individual Dept./Divisions Head, BACH, IT Division, CARD Division etc.

4. Usually no individual users are allowed for sending e-mails to all ID all@shahjalalislamibank.com. Important e-mail to all ID can only be sent, after approval of the contents/documents from the approving authority through proper channel. For approval, the content should be sent to Head of operation/AMD while a CC to be sent to the Head of IT and concerned head of the department/division or branch manager. If the approving authority approves the contents/documents and sends a reply of the e-mail to the sender, Head of IT will be acknowledged about the approval through the reply of e-mail. The Head of IT will take necessary steps by which the initiator will be able to send the contents to all@shahjalalislamibank.com through e-mail.
5. HRD will send a request for e-mail ID for new employees to IT Division. IT Division will create an e-mail ID for new employee and duly acknowledge HRD and the concerned employee after creating the ID. Subsequent updates of the list will be published accordingly.
6. Regard all types of official documents received from valid e-mail ID through proper channel as valid and take necessary action accordingly. Official documents are allowed to send to superiors/Divisional or Departmental Heads/Branch Managers by e-mail for taking necessary action.
7. Distribution of scanned Image of signed copy of Circulars to the Departments/Divisions/Branches through e-mail are strongly encouraged for compliance.

8. From now on, e-mails will be considered as an evidence of any pursuance. i.e. requisition procedure to Divisional or Departmental Heads/Branch Managers and as a receipt of circular sent thereby.
9. No image or big file more than the size 10MB is allowed to send through e-mail. To send more than 10 MB, prior permission has to be taken from the Head of IT through proper channel (Branch Manager/Head of the Division).

(b) Internet usage policy for executives and officers:

To use branch e-mail, internet facility is no more required. To use internet for other official requirement, users are requested to send a formal requisition to Head of IT through proper channel (Divisional or Departmental Heads/Branch Managers) with justification. IT Division will arrange access as per approval of Head of Operations. Please mention that as per approval of the Management, IP based Internet Use Policy (IUP) for grant permission for the internet users has already been deployed by the Bank.

Chapter Eight

Infrastructure Policy

- Power System
- Cooling System
- Access Control System
- Surveillance System (CCTV)
- EMS (Environment Monitoring System)
- Auto Fire Suppression System
- DRS Information

8.1 Power System

1. To ensure uninterrupted Power Supply, 02 (Two) Generators are running with Auto Switching System.
2. Among of Two GENSET 330kva will run in Primary/Initial stage. From this 330kva load, 150kva load has dedicatedly assigned for Data Center.
3. Rest 150kva GENSET will be active whenever the Primary 330kva will not trigger.
4. Full Process will be switched automatic through ATS (Automatic Transfer Switch)
5. Two (02) individual ATS is connected & changeover is activated through one Timer.
6. Primary GENSET (330kva) will be trigger within 60 seconds after PDB power failure.
7. Secondary GENSET (150kva) will be trigger within 120 seconds if Primary GENSET (330kva) will not trigger.
8. GENSET system will take care and maintain by the Bank's Electrical Engineer (CSD Division) .
9. Two (02) 30kva APC UPS are simultaneously running over the 24/7 by segregating the total load.
10. Both UPS are giving backup/connected to the device through individual PDU (Power Distribution Unit).
11. AVR (Automatic Voltage Regulator) is maintaining the Voltage Up gradation & Degradation.
12. MCO (Manual Change Over) will be active whenever any emergency maintenance task performed.
13. 04 (Four) individual Main Distribution Board (MDB) has been defined separately for Cooling System of DC, Cooling System of Power Room along with others Utility, Rest of the area from DC & Power Room utility and so on.

8.2 Cooling System

AT DC: To maintain perfect Cooling System in DC there are two Precession ACs run out through the 24/7 basis by turns (12 Hours at a stretch) where each Precession AC belongs 39.5 KW (equivalent to 13.16 Ton).

AT Power Room: To maintain perfect Cooling System in Power Room there are two ACs run out through the 24/7 basis (6 Hours at a stretch) by turns where each AC belongs 3 Ton.

8.2.01 Operational Activities:

a) A Temperature (18 to 26 ^{0} C) has been set up at each PAC for Data Center whenever the temperature goes over (18 to 26 ^{0} C) both the PAC (Precession AC) becomes active & will run till the room temperature goes down below 20^0 C and then one PAC becomes shut down.
b) Humidity is being auto maintained by PAC.
c) Both the PAC is being auto Switch over by turns according to schedule (Time duration: 24 hours).
d) Built in auto notification system appears in its display.

8.3 Access Control System

a) For Data Center, the Access Control System is operating Card or Finger Punching.
b) Access in Data Center along with its surrounded restricted area is being controlled & maintained by Access Control System.
c) Attendance record of all IT officials also maintained from this Access Control System.
d) One manual access log is being maintained for Vendors & others for DC.

8.4 Surveillance System (CCTV)

Entire Data Center is being cover & monitor under the CCTV System which is equipped by 10 Cameras. All of these cameras are controlled & maintained by one DVR which is contained with one 500 GB (38-40 Days video backup) Hard Disk.

a) Resolution 640X512 mp
b) DVR HDD Capacity: 500 GB
c) Recorded Mode: When any motion will be active (Frame Rate: 4.1)
d) Working Period (After 10:00 A.M.): 2.5 Frame Rate
e) Non Working Period (After 06:00 P.M.): 1.6 Frame Rate
f) Video Backup time : 38-40 Days .

8.5 EMS (Environment Monitoring System)

Cooling system, Temperature, Humidity, Water Fire detection, Smoke system all are monitored & reported properly over the network i.e. web based interface.

8.6 Fire Suppression System

Auto Fire Suppression System is being live & operational with very renowned GAS called NAFS125 along with HIT & Smoke Sensor. Two individual Cylinders for DC & Power

Room dedicatedly are assigned to protect any unexpected fire incident.

8.7 Co Location of DRS

a) A Disaster Recovery Site (DRS) is replaced to Disaster Recovery Site service center provided by Square, Gazipur, Kashimpur replicating the Data Center (Production Site) from the previous collocation site CoLoCity (ICOM Bangladesh Limited). It is more than 10 km distance from our DC.
b) Co-Located DRS is equipped with a set of hardware like Application server, Database Server, Storage Device and communication devices like router, switch, firewall is equipment to support the live systems in the event of a disaster.
c) All logistics support & services including security at the DR site is satisfactory.
d) Real times data replication performs on routine basis, which is effectively monitor & reported by DBA Team.

Chapter Nine

Software Development and Acquisition

For any new application or function for the Bank requires analysis before acquisition or creation to ensure that business requirements are met in an effective and efficient manner. This process covers the definition of needs, consideration of alternative sources, review of Technological and economic feasibility, execution of risk analysis and cost-benefit analysis and conclusion of a final decision to 'make' or 'buy'.

Computers and networks shall only run software that comes from trustworthy sources.

No software shall be loaded onto a Bank's computer without prior approval from competent authority.

IT division shall protect their Information Systems from known vulnerabilities by applying the latest security patches recommended by the product vendors or implementing other compensating security measures.

Before security patches are applied, proper risk evaluation and testing should be conducted to minimize the undesirable effects to the Information Systems.

9.1 Software Development Policy

a) The Bank should have written operation manuals for each and every department to be followed for the development/purchase of software as the guideline.
b) The Bank should have Core Banking Solution/Software.
c) The Bank should have the target/detail plan to be a paperless Bank and to incorporate all electronic services/facilities using the latest technology.
d) Software system to be ISO standard and if possible those to be Capacity Maturity Model (CMM) level 4 or 5.
e) Software system should be in 3-tier architecture, whatsoever purchase or develop.
f) The Bank should have a skilled software development team, who are capable to develop open & industry standard systems using the latest tools.
g) Software development to be structured & documented, which should include the followings:
    i. System Survey
    ii. System Analysis
    iii. System Planning & Design
    iv. Pseudo Coding
    v. Interface Design
    vi. Assembly, Module, Object, Procedure, Functions & Library File design and coding
    vii. System testing
    viii. System implementation
    ix. System documentation
h) A skilled Software Team will develop the in-house software as required by Head Office and Branches.
i) User Manuals are to be ready/provided.

9.2 In-house Software Policy

a) Detailed design and technical application requirements shall be prepared.
b) Criteria for acceptance of the requirement shall be defined and approved by the concerned business unit.
c) Application security and availability requirements shall be addressed.
d) Developed functionality in the application shall be in accordance with design specification and documentation.
e) Source code must be available with the concerned department and kept secured.
f) Source code shall contain title area, the author, date of creation, last date of modification, and other relevant information.
g) Software Development Life Cycle (SDLC) with User Acceptance Test (UAT) shall be followed and conducted in the development and implementation stage.
h) System documentation and User Manual shall be prepared and handed over to the concerned department.
i) The Bank must consider necessary 'Regulatory Compliance' requirements.

9.3 Outsourced Software Policy

All the software procured and installed by the Bank shall have legal licenses and record of the same shall be maintained by the respective unit/department of the Bank.

9.3.01 Vendor Selection Policy

a) There must be a core team comprising of personnel from Functional Departments, IT Department, and Internal Audit Department for vendor selection.
b) Vendor selection criteria for application must address the following:
    i. Market presence
    ii. Years in operation
    iii. Technology alliances
    iv. Extent of customization and work around solutions
    v. Performance & Scalability
    vi. Number of installations
    vii. Existing customer reference
    viii. Support arrangement

9.3.02 Software Documentation Policy

a) Documentation of the software shall be available and safely stored.
b) Document shall contain the followings:
    i. Functionality
    ii. Security features
    iii. Interface requirements with other systems
    iv. System Documentation
    v. Installation Manual
    vi. User Manual

9.3.03 Other Requirements

a) There shall have a test environment to ensure the software functionalitiesbefore implementation.
b) User Acceptance Test (UAT) shall be carried out and signed-off before going live.
c) Necessary 'Regulatory Compliance' requirements for banking procedures and practices in the application must be taken into account by the Bank.
d) Any bugs and/or errors found due to design flaws, must be escalated to higher levels in Software Vendors' organization and Bank, and must be addressed in time.
e) Support agreement must be maintained with the provider for the software used in production with the confidentiality agreement.

Chapter Ten

Core Banking Software Policy

Core Banking Software BankUltimus should run smoothly in all the branches. For which a Data Center, a Disaster Recovery Site, Dual Network connectivity and operating policy has been prepared which are currently in operation. To support the users 24 hour support center called NOC (Network Operation Center) is in live. The officers perform their duty in shift, management of which is under Data Center team. Data Center Team circulates roster duty schedule as prepared by them and approved by Head of IT at the end of each month for the next month.

10.1 Operating Policy:

Maker checker request received by IT through proper channel. Initiated by user and approved by Branch Manager. Users are created by Valid admin user of IT Division.

Certain limit is requested by the branch for execution of branch operation.

User permission is sanctioned as per request processed from branch.

Operating time is open as there is no time restriction has yet been instructed by competent authority. The operating time schedule will be implemented as and when instructed by authority.

Operation Calendar for the year is set before start of the year. Other holidays are set as and when required.

Own branch operation, Remote operation, Head office operation all factors are permission based through BankUlitmus system.

New Parameter setting is done by Head Office users. IT users do it as per order circulated by FAD. New GL Account is opened by FAD users as and when required as per proper noting.

Day end operation is done by NOC users of IT division after day close of all the branches.

Dummy Month End operation is performed with the end of day of previous day of end of month before end of month in the UAT environment. During month end A team is formed with Business Team members, Network Team members and software team members for execution of proper support to the branches and head office.

Similarly dummy Year end is also processed in the UAT environment for anticipating the errors or flaws. Due to application of deployment for modification of any function of service charges/government duties, if bugs are found, it is fixed in the UAT. After successful day end and as per service providers recommendation live process is updated.

Ad branches SWIFT operation is done by SWIFT interface of BankUltmus. As per requirement of SWIFT authority at least one SAA user is required to send al the message of AD branches.

Some of the users of a branch must have to have training of BankUltimus. This training provided by IT has a nature TOT so that the trainees may train their other users of the branch. The A list of operation path/User manual soft copy centrally located in the following address path:

IT users are not authorized to make or authorize any financial transaction.

10.2 User Support Policy:

As per working process of IT department. Ticket software, Schedule wise, NOC, Saturday, daily/month end/yearend, support type (by phone, e-mail, ticket, physical on spot). Cards Department for ATM card support.

10.3 Maintenance Policy :

As per agreement service provider provide support. Agreement is duly renewed to ensure proper services. Database maintenance is under Database policy. After migration of all the branches the previous data of PcBANK2000 is preserved in three locations:

- File Server in our DC,
- In the Vault (DVD) of IT Division archive room
- In a portable Hard disk in our DC
- (DVD) In Dhaka Main Branch

We have redundant connectivity for every branches. There must be some risk to become down both the links, although SJIBL considered alternate E1 providers of the connectivity service providers for each branch. When two links become down at a time we seek support from up to top authority of the service providers. Branch may be advised as per the rise of severity level.

Level One. Day close operation time is very near and connectivity is still down:
The branch manager is acknowledged about the details of the matter. Users are requested to wait patiently till next day before start of day at the worst situation.

Level Two: Next day branch operation start time is over still the link is down. Remote transaction and Card transaction status option upon the branch is made to disable. To keep the minimum level of customer service up, the latest customer balance with card transaction details from last day card transaction upon the branch is sent through e-mail. The e-mail is to be received by other source by smart phone/other source of e-mail services. Branch may provide customer services (only deposit and withdrawal) by validating the printed reports received from IT and Card Division.

Chapter Eleven

DATABASE MANAGEENT AND SECURITY

Backup and Storage Policy

11.1 Scope m

a) Data means all sorts of information kept in printed or electronic format of Shahjalal Islami Bank Limited.
b) Data should be preserved in a secured manner in printed format and in fixed (Hard Disk) & removable disks (e.g. DAT/Tape/CD/DVD etc.).
c) Removable disks should be preserved under lock and key in safe custody outside location of the related office (Head Office or Branch office).
d) Branches and Head Office should preserve banking operational data in re-usable data cartridges on daily basis.
e) Banking operations data and other documents data should be preserved permanently in DAT/Tape/CD/DVD media on half yearly basis.
f) Backup data cartridges/CD/DVDs should be preserved at Head Office in a Fungus & Dust Free, Fireproof Data Safe/Vault.
g) Data Mining Center may be setup in a remote location considering number of branches and volume of data.
h) Data may also be preserved in the internationally established and secured 'Data warehouse' on rental basis.

11.2 Backup

Shahjalal Islami Bank Limited (SJIBL) is operating business of both Centralized and Distributed System for banking operation. 93 branches with Head Office are running in Central System. DBA Team follows the following as their Backup and Recovery Plan for Central Core Banking System.

11.3 Backup Plan

Database (DB) backup using various technologies

Shahjalal Islami Bank Limited is taking **full backup** using Data Pump utility and Recovery Manager (RMAN) of production database as core database size is small in present time. We will take incremental backup in future when the backup time of RMAN reaches more than 2 hours.

Backup Recovery Team

IT Division of Shahjalal Islami Bank Limited possesses two teams who are responsible for taking core data backup manually. Teams are:

1. DBA (Database Administration) Team
2. NOC (Network Operation Centre) Team

The responsibility of Backup and Recovery system of SJIBL is belongs to DBA team members. DBA team members will monitor the total backup and recovery system and follow up with NOC member for regular operation. Each working day NOC team takes Before End of Day (EOD) data backup manually after close marking of all Ultimus Branches and After EOD backup is also taken everyday manually.

We used to take RMAN before start of EOD operation as well as fracture the DR-Clone LUNs to ensure for the one-day-back data.

Moreover, DBA team sends important copies of backup data to remote place to Gulshan Branch in two Portable Hard Disk Drive (HDD) alternatively. Portable HDDs are carried in and out by Assigned Officers from IT Division.

Levels of Backup and Recovery system

NOC team takes schedule backups of **Before EOD** (BEOD) and **After EOD** (AEOD) in various levels and managing backup and recovery system which increases the higher level of data protection resolution. These levels have decreased the disaster levels. The levels are:

A. Daily Backup System
B. Month end and large deployment
C. Raid Level protection
D. Advanced Storage Technology (PR and DR site data replication & Cloning)

A. Daily Backup System:

Oracle Database Backup Technology:

DBA team have implemented backups operations of SJIBL Database in three (3) methods:

1. Data Pump/Export Backup
2. RMAN Backup
3. Flash Back Technology

Data Pump Backup:

NOC team takes the Before EOD backup manually. One copy of BEOD data file is saved in Core DB server and a copy has moved out to Core-DB File Ferver (10.101.1.71). After EOD backup is also taken by NOC team and one copy of backup has gone to tape library automatically and also moved out to Core-DB file server (10.101.1.71). Image and Signature data has been also taken backup from a different schema named ‘image_user’ in every Friday.

All scripts are fired from ‘db1’ server by NOC team member by their own individual User ID with limited privileges.

RMAN Backup:

For Production Database:

NOC is taking backup RMAN manually. NOC team member is taking RMAN backup before EOD operation every day.

In every day scheduled backup, we are managing our backup system in below structure:

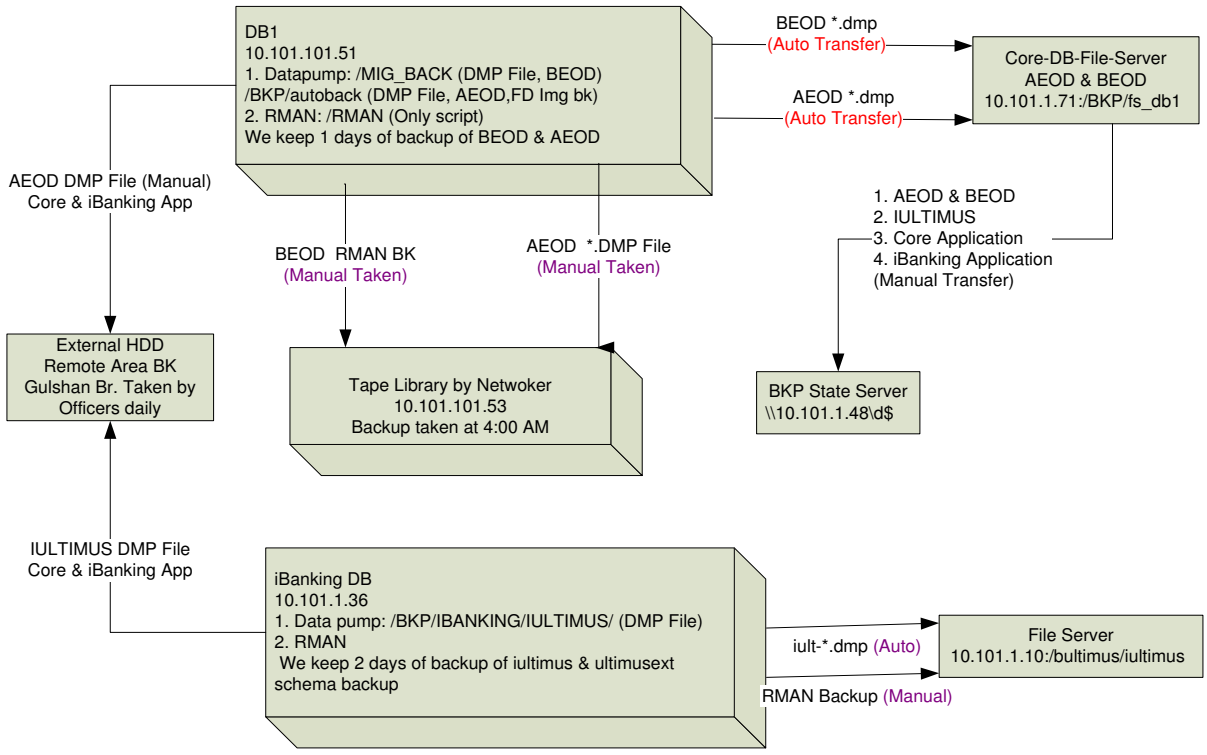
Regular Creation of Flash Back point:

The Production Database is set to flashback mode. And also flashback Recovery area is setup so that in case of recovery the database point in time recovery will be fast and also provides a unified storage location for all recovery related files and activities in an Oracle database.

Before start EOD process EOD user made a flashback point for any kinds of emergency database restore. Every EOD user has own user id and password.

B. Month end and Big deployment Backup System:

In the period of month-end we have taken extra backup, if it is required. Moreover, in case of big deployment RMAN backup has been taken by DBA team. Besides this we have enable the **Flashback** in our system. Before big deployment or Month End, we have to create **restore point** by Flashback technology.



C. Raid Level protection:

This is storage in built technology. RAID levels are implemented by EMC engineer like **Raid 1/0** AND **Raid 5** for the case of Disk Failure. The storage system automatically generates error message while any disk fails or any block corruption in HDD.

We have a replication in PR side internally which is called 'Clone'. Data of Raid 1/0 has been cloned into Raid 5 level LUNs. Now in present scenario, we have mounted Report-DB-Server in PR-cloned LUNs which are fractured and synchronized everyday. Tues cloned consistence data is one day old which also prevents the system from logical corruption or human's unwanted logical errors.

In DR site production data has been replicated from PR RAID 1/0 To DR Raid 1/0 LUNs which is called 'Mirroring'. In DR site data also replicated internally in Raid 5 level LUNs.

In four spaces production data has been replicated. But in DR site in Raid 5 disk groups have been fractured and synch everyday for due to any inconsistence and error for any reason in Database.

11.4 Advanced Storage Technology (PR and DR site data replication & Cloning)

SJIBL is the first bank that uses both Cone-Fracture and Snap-Shot technology for Report DB Server and UAT DB server accordingly in Bangladesh. City Bank and Eastern Bank use partially of these technology but not all.

1. DC-DR Data Synch (Mirroring Technology)
2. Clones Synch-Fracture
3. Snap-Shot Technology

DC-DR Data Synchronization/ Data Replication (Mirroring Technology)

DBA team member monitors the data replication between DC and DR. Data Replication is based on two technologies:

a. Synchronous
b. Asynchronous

a. Synchronous: Data is being mirrored to DR site by dark fibre of 4 Gbps through Fibre Cable (FC) constantly using Synchronous technology **previously**. This data replication was totally depends on dark fibre where data is replicating using light technology. Storage domain is kept normal state while dark fibre connectivity is being consistence state.

Drawbacks:
Sometimes it was observed that production environment went very slow during banking transaction hour. Several calls were generated from branches of Bank. IT Management decided to migrate from Synchronous to Asynchronous technology to rectify the problems. To do so properly DBA team configuring iSCSI port to transfer data to DR Site to through Ethernet post rather than FC port.

b. Asynchronous: Storage system-based asynchronous replication overcomes the typical dis-advantages of synchronous replication, such as the requirement of a high-bandwidth network connection and distance limitations. In addition, when purchased as part of the storage system, asynchronous replication is more economical than add-on replication technologies like continuous data protection.

Moreover, there is no impact on performance of Production environment. Thirty (30) minutes of time interval is exists on data replication. DBA can protect replication of erroneous data to DR site for any kinds of logical disaster, if errors/logical disaster can be identified within 30 minutes.

After successful migration the DR site to Kashimpur, Gazipur proposed bandwidth will be 50 Mbps as decision of IT management.

Storage Clone Synch-Fracture

In our Storage system we have implanted the Clone LUNs Synch-Fracture in both DC and DR site. DBAs make synch-fracture on demand based on DBA's operations tasks. Ultimus Report Server is running using this technology.

NOC member make fracture DR-Clone-LUNs just before EOD operation regularly for protecting any kinds of logical disaster during EOD operation. Any kinds of logical disaster during EOD operation, rollback can be possible in terms of this Storage Technology.

Chapter Twelve

Recommendation and Future Planning Policy

12.1 Cloud Computing

12.1.01 Overview

Cloud Computing is a recent revolution in the world of Information Technologies that enables a convenient way to share resources. It is model providing on-demand network access to configurable IT devices and services (e.g. Servers, Storage, and Applications) gathered as a network of computing resources located anywhere, being shared among its users. Cloud Computing can provide greater flexibility and improved levels of service, while making costs more transparent and increasing institutional efficiency. It is anticipated that the use of Cloud Computing services will grow significantly over the next generation.

This policy is intended to ensure that the use of these services is managed in accordance with existing IT requirements, and to provide a level of Head of IT oversight to address the possibility of a higher level of risk existing because of these new and still-evolving IT service models. The primary reason for this policy is to facilitate a well-managed and successful adoption of Cloud Computing by establishing a process that directs attention to IT related requirements, management processes, and risk factors.

12.1.02 Scope

Cloud Computing is a computing model in which technology resources are delivered over the network. Rather than implementing and maintaining, IT services locally, customers of cloud computing buy IT capabilities from providers that manage the hardware and software that operate those services. Resources including infrastructure, software, processing power, and storage are available from the cloud. However, migrated cloud platforms and services cost benefits as well as performances are neither clear nor summarized. Globalization and the recessionary economic times have not only raised the bar of a better IT delivery models but also have given access to technology-enabled services via internet.

However, in spite of the cost benefits, many IT professional believe that the latest model i.e. "Cloud Computing" has risks and security concerns. The following factors should be considered during cloud computing:

a) Idea behind cloud computing.
b) Monetary cost benefits of using cloud with respect to traditional premise computing.
c) Security issues of cloud computing.

We have tried to find out the cost benefit by comparing the Microsoft Azure cloud cost with the prevalent premise cost.

12.1.03 Policy

Use of Cloud Computing services must be formally authorized in accordance with the IT Division.

Use of Cloud Computing services must comply with all current laws, IT security, management policies, and risk.

Use of Cloud Computing services must comply with all privacy laws and regulations, and appropriate language.

Cloud Computing services will not be avail without any writing approval of IT Division. The Head of IT division will certify that security, privacy, and other IT management requirements that adequately addressed prior to approving use of Cloud Computing services.

The Cloud Computing service may not be put into production use until IT Division has provided written approval.

12.1.04 Guidance

Many issues should be considered carefully before adopting a Cloud Computing solution. The list below features some of the more important issues to consider using Cloud Computing:

a) More efficiency or effectiveness for the IT investment.
b) Need for a specific Cloud Computing characteristic (elasticity, scalability, usage-based model).
c) Be realistic in cost estimates. Consider the total lifecycle costs, not just the cost of implementation.

12.1.05 Security Issues

Weigh the security threats and opportunities that are present for public, private, and community Clouds.
Consider how disaster recovery and continuity of operations planning will be addressed. Identify all systems of records to be hosted in the cloud.

Specify the retention time for all system backups.

Consider how records management and electronic discovery will be managed in the cloud environment.

Consider issues of data ownership and portability. How would it migrate from a given Cloud Computing infrastructure to another one at some point in the future?

12.2 Cryptography and Digital signature

A digital signature is a technique for establishing the origin of a particular message in order to settle later disputes about what message (if any) was sent. The purpose of a digital signature is thus for to bind its identity to a message.

We use the term signer for an entity who creates a digital signature and the term verifier for an entity who receives a signed message and attempts to check whether the digital signature is "correct" or not. Digital signatures have many attractive properties and it is very important to understand exactly what assurances they provide and what their limitations are. While data confidentiality has been the driver behind historical cryptography, digital signatures could be the major application of cryptography in the years to come.

12.2.01 The electronic signature

1. The electronic will be uniquely linked to the signatory
2. It will be capable of identifying the signatory
3. It will be created using means under the sole control of the signatory
4. It will be linked to data to which it relates in such a way that subsequent changes in the data are detectable.

12.2.02 Digital signature on a message:

a) Data origin authentication of the signer: digital signature validates the message in the sense that assurance is provided about the integrity of the message and of the identity of the entity that signed the message.
b) Non-repudiation: digital signature can be stored by anyone who receives the signed message as evidence that the message was sent and of who sent it. This evidence could later be presented to a third party who could use the evidence to resolve any dispute that relates to the contents and/or origin of the message.

12.2.03 Input to a digital signature

a) The message
    i. Digital signature needs data origin authentication (and non-repudiation). The digital signature itself must be a piece of data that depends on the message, and cannot be a completely separate identifier.
    ii. It may be sent as a separate piece of data to the message, but its computation must involve the message.
b) A secret parameter known only by the signer
    i. Digital signature needs non-repudiation; its calculation must involve a secret parameter that is known only by the signer.
    ii. The only possible exception to this rule is if the other entity is totally trusted by all parties involved in the signing and verifying of digital signatures.

12.2.04 Properties of digital signature

a) Easy for the signer to sign message: There is no point in having a digital signature scheme that involves the signer needing to use slow and complex operations to compute a digital signature.
b) Easy for anyone to verify a message: Similarly we would like the verification of a digital signature to be as efficient as possible.
c) Hard for anyone to forge a digital signature: It should be practically impossible for anyone who is not the legitimate signer to compute a digital signature on a message that appears to be valid. By "appears to be valid" we mean that anyone who attempts to verify the digital signature is led to believe that they have just successfully verified a valid digital signature on a message.

12.2.05 Arbitrated digital signatures

1. Arbitrated digital signatures
    a) meet the security requirements and

b) Have the properties that we required for a digital signature.
2. Verify and check the first MAC, computed using KS.
3. Recognize the main (practical) problem with implementing arbitrated signature.

12.2.06 Basis of signature security

1. The basis of digital signature offer data origin authentication.
2. Digital signature offer non-repudiation.
3. The security properties of a MAC and a digital signature.

The vast majority of digital signature techniques do not involve having to communicate through a trusted arbitrator. A true digital signature is one that can be sent directly from the signer to the verifier. For the rest of this unit when we say "digital signature" we mean "true digital signature".

Digital signatures are in some senses a complimentary technology to public key encryption, offering data origin authentication and non-repudiation of digital messages. Digital signatures have different properties and offer different guarantees to hand-written signatures. The security of digital signatures critically relies on the security of the keys that are used to create and verify them.

12.3 Recommendation

1. Two way verification system for internet Banking. After every login user will send a OTP (One Time password) to their email address and mobile number. This OTP will use for final verification.
2. SMS Banking service should be improved.
3. Now a day's Mobile Banking is one of the popular form of banking, but Shahjalal Islami Bank still failed to introduce this service. Mobile Banking service should be introduced as early as possible.
4. Still there are some bugs in Core Banking software which hamper EOD process of Bank, These Bugs should be solved as early as possible.
5. Shahjalal Islami Bank has introduced Ticket Management System for giving quick support to branch user. Same can be introduced for our clients for giving quick support of SMS and Internet Banking.

Chapter Thirteen

Conclusion

The Banking Industry has changed the way they provide services to their customers and process information in recent years. Information Technology has brought about this momentous transformation. Security of Information for the Bank has therefore gained much importance, and it is vital for us to ensure that the risks are properly identified and managed. Moreover, information and information technology systems are essential assets for the Banks as well as for the customers and stakeholders. Information assets are critical to the services provided by the Banks to the customers. Protection and maintenance of these assets are critical to the organizations' sustainability. Shahjalal Islami Bank Limited takes the responsibility of protecting the information from unauthorized access, modification, disclosure, and destruction.

The Bank has prepared the IT Policy as a requirement and as appropriate to the use of Information Technology for their operations. It also sets forth the Code of Professional Ethics to guide the professional and personal conduct of employee's.

Employees of the Bank shall:

1. Support the implementation of, and encourage compliance with, appropriate standards, procedures, and controls set this policy for information systems.
2. Perform their duties with objectivity, due diligence and professional care, in accordance with professional standards and best practices.
3. Serve in the benefit of stakeholders in a lawful and honest manner, while maintaining high standards of conduct and character, and not engage in acts discreditable to the profession.
4. Maintain the privacy and confidentiality of information obtained in the course of their duties unless disclosure is required by legal authority. Such information shall not be used for personal benefit or released to inappropriate parties.
5. Maintain competency in their respective fields and agree to undertake only those activities that they can reasonably expect to complete with professional competence.
6. Inform appropriate parties of the results of work performed, revealing all significant facts known to them.
7. Support the professional education of stakeholders in enhancing their understanding of IS security and control.

Failure to comply with this Code of professional Ethics can result in an investigation into an employee's conduct and ultimately, in disciplinary measures.

All employees may share the Information Technology facilities of the Bank. The facilities provided to the employees for conducting Bank business. The Bank does permit of its employees to use of the facilities, including computers, printers, e-mail and internet access. However, these facilities may used by every employee, since misuse by even a few individuals has the potential to negatively impact productivity, disrupt Bank business and interfere with the work or rights of others. Therefore, all employees expected to exercise

responsible and ethical behavior when using the Bank's Information Technology facilities. Any action that may expose the Bank to risks of unauthorized access to data, disclosure of information legal liability, or potential system failure is prohibited and may result in disciplinary action up to and including termination of employment and/or criminal prosecution.

The use of the Bank's information technology facilities in connection with Bank business and limited personal use is a privilege but not a right, extended to other organizational employees. Users of the Bank's computing facilities are required to comply with all policies referred to in this document.

The policy covers the usage of all of the Bank's Information Technology and communication resources, including, but not limited to:

- All computer-related equipment, including desktop personal computers(PCs), portable PCs, terminals, workstations, PDAs, wireless computing devices, telecomm equipment, networks, databases, printers, servers and shared computers, and all networks and hardware to which this equipment is connected.
- All electronic communications equipment, including radio communicators, voice-mail, e-mail, fax machines, wired or wireless communications devices and services, internet and intranet and other on-line services
- All software including purchased or licensed business software applications, Bank written applications, employee or vendor/supplier-written applications, computer operating systems, firmware, and any other software residing on Bank-owned equipment.
- All intellectual property and other data stored on Bank equipment.
- The policy will also apply to all users, whether on Bank property, connected from remote via any networked connection, or using Bank equipment.
- All of the above are included whether they owned or leased by the Bank or are under the Bank's possession, custody, or control.

The policy also applies to software contractors, and vendors/suppliers providing services to Bank that bring them into contact with SJIBL's Information Technology infrastructure. The Bank employee who contracts for these services is responsible to provide the contractor/vendor/supplier with a copy of only required clause of this policy before any access given to the Bank Information System. It is the responsibility of all operating units to ensure that this policy clearly communicated, understood, and followed.

To protect the integrity of Bank's computing facilities and its users against unauthorized or improper use of those facilities, Bank reserves the right, without notice, to limit or restrict any individual's use, and to inspect, copy, remove, or otherwise alter any data, file, or system resource which may undermine the authorized use of any computing facility or which is used in violation of Banks rule or policy. Shahjalal Islami Bank Limited also reserves the right periodically to examine any system and other usage and authorization history as necessary to protect its computing facilities.