INFORMATION AND COMMUNICATION TECHNOLOGY SECURITY POLICY

BANGLADESH KRISHI BANK

Information and communication Technology Department

Head Office, Dhaka-1000

June 2014

For Official use only

Prepared by:
Information and Communication Technology Department
Bangladesh Krishi Bank
Head Office
83-85,Motijheel Commercial Area
Dhaka-1000.

Published by:
Organization and Method Department
Bangladesh Krishi Bank
Head Office
83-85, Motijheel Commercial Area
Dhaka – 1000.

Information and Communication Technology Security Policy
June 2014

PREFACE

The Information and Communication Technology (ICT) opens the door of globalization and has become the backbone to modern banking operations. It is also a critical component of the infrastructure for a competitive market economy. The survival and success of a business organization mainly depends on the effective use of ICT

In view of the above, Bangladesh Krishi Bank has already set up an Information Technology platform for its branches and offices. The bank has a vision to expand and to modernize the ICT platform and information systems gradually. Not withstanding the level of computerization, the security requirements of information systems are universal and significant to the sustainability of the ICT platforms. Accordingly, the bank requires policies to secure ICT setup as well as information and to set standards for ICT operations.

It is indeed a great pleasure that ICT department of the bank has prepared a book titled "Information and Communication Technology Security Policy" in accordance with the guideline given by Bangladesh Bank, existing rules and regulations. The book contains the policies applicable to ICT Management, ICT Operation Management, Information System Physical Security, Information Security Standard, Business Continuity and Disaster Recovery plan, ATM,Mobile Financial Services,Procurement § Service Management. Different types of ICT Forms (According to Bangladesh Bank's guide line) are also incorporated in the Appendix.

I express my thanks and gratitude to the Board of Directors of the bank for providing their kind approval of the policy.

However, implementation of the Policy is rather more important than its existence. Henceforth all concerned are requested to accomplish their business in accordance with the guidelines contained herein. I belive, our faithful adherence to this policy will speed up sustainable development of Bangladesh Krishi Bank.

Dated : June 2014
Dhaka

(Md. Abdus Salam)
Managing Director

Glossary and Acronyms

2-FA	- Two Factor Authentication
AMC	- Annual Maintenance Contract
AML	- Anti-Money Laundering
BCP	- Business Continuity Plan
BRP	- Backup and Restore Plan
CCTV	- Close Circuit Television
CD ROM	- Compact Disk Read Only Memory
DC	- Data Center
DDoS	- Distributed Denial of Service
DoS	- Denial of Service
DR	- Disaster Recovery
DRP	- Disaster Recovery Plan
DRS	- Disaster Recovery Site
E-mail	- Electronic Mail
FIs	- Financial Institutions
I-banking	- Internet Banking
ICT	- Information and Communication Technology
IDS	- Intrusion Detection System
IPS	- Intrusion Prevention System
IT	- Information Technology
JD	- Job Description
LAN	- Local Area Network
PCI DSS	- Payment Card Industry Data Security Standard
PCs	- Personal Computers
PDA	- Personal Digital Assistant
PIN	- Personal Identification Number
PKI	- Public Key Infrastructure
SDLC	- Software Development Life Cycle
SLA	- Service Level Agreement
SSL	- Secured Socket Layer
UAT	- User Acceptance Test
UPS	- Uninterrupted Power Supply
User ID	- User Identification
VLAN	- Virtual Local Area Network
WAN	- Wide Area Network

INDEX OF CONTENTS

CHAPTER – 1

1.0 Information and Communication Technology

Information and Communication Technology (ICT) plays a vital role in present world. The advancement of Communication and Information Technology is one of the major attributing factors for the emergence of globalization of financial markets. The banking industry has changed the way they provide service to customers and process information in recent years. Information and Communication Technology has brought about this momentous transformation. Security of ICT systems for a financial institution has therefore taken on a greater importance, and it is vital to ensure that such risks are properly identified and managed. Moreover Information and information technology systems are essential assets of the bank and customers as well. Protection and maintenance of these assets are important for sustainability of any organization. Banks must take the responsibility of protecting this information from unauthorized access, modification, disclosure and destruction to safeguard customer's interest.

This document provides the policy for Information and Communication Technology and ensures its secured use for Bangladesh Krishi Bank (BKB). It establishes general requirements and responsibilities for protecting ICT systems. The policy covers common technologies such as computers and peripherals, database and network, web system and other ICT resources. The bank's delivery of services depends on availability, reliability and integrity of its information and Communication technology system.

The policy will require regular updates to cope with the evolving changes in the ICT environment both within the bank and overall industry. The senior management of the bank must express a commitment to ICT security by continuously heightening awareness and ensuring training of the Bank officials. Compliance plans in case of noncompliance issues should also be formulated time to time.

1.1 Information and Communication Technology in Bangladesh Krishi Bank

In spite of all limitations, Bangladesh Krishi Bank has entered into the arena of Information and Communication Technology to meet the demand of time and is making every endeavour to turn traditional banking operations into the most modern banking system. Initially a computer section was started with two Micro Computers under the Loan Recovery Division in 1987. Subsequently the Computer Section turned into Computer Cell in a very limited scale. It began to expand with more microcomputers and necessary system software time to time. In 1993, the span of Computer Cell further extended by procurement of multi-user and multitasking machine i.e. Mini Computer System. As the scope of computer operations expanded more, the Computer Cell of the Bank turned into a full-fledged department with the approval of the Ministry of Finance. The Computer Department of the Bank started its functioning in January, 2004.To cope up with the changing senerio of the banking environment like speedy money transaction, real time banking and use of modern communication technologies for banking services etc. the Bank has changed its **IT** Department's name as **ICT** (Information and Communication Technology) Department in August 2013.

1.2 Automation of Branch Banking Operations

Introduction of the automated modern banking system, instead of traditional manual banking, is the prime need of time. To meet the situation, Bangladesh Krishi Bank prepared a 5-year plan during the financial year 1998-99. The plan was duly approved by the Board of Directors of the Bank and subsequently by the Ministry of Finance of the Government of the People's Republic of Bangladesh. The plan is to be implemented in five phases which are as follows:

1.2.1 First Phase: The implementation of the first phase of the computerization plan started in the year 1999 and it was completed in following manner:

a. **Branches:** One-stop service facilities were introduced under individual local area network system in 28 branches of the bank including four corporate branches in Dhaka, Chittagong, Khulna and Sylhet cities.

b. **Head Office:** The secretariat of the managing director, office of the deputy managing directors and general managers along with most of the departments in head office were brought under computerization through stand alone personal computer or local area network system with necessary equipment.

c. **Divisional Offices:** Personal computers with related accessories were supplied to all Divisional offices at field level to work on the basis of stand alone system.

1.2.2 Second and Third Phase: After accomplishment of the first phase the bank completed the second and third phases as described below:

a. **Branches:** One stop service was introduced in 55 branches located at different cities, district headquarters and in places having business potentialities over the country.

b. **Head Office:** As a part of computerization process, the existing systems based on a stand alone personal computer were upgraded into a local area network and the other departments of the head office were equipped with necessary instrument.

c. **Other Controlling Offices:** The process was completed with the expansion of computerized system in all Chief Regional Offices , Regional Offices and Divisional Audit Offices of the Bank.

1.2.3 Fourth and Fifth Phase: After completion of second&third phases, the fourth and fifth phases have been completed as described below:

a. **Branches:** One Stop Service has been introduced in 44 branches located at different cities, urban areas and in places having business potentialities over the country.

b. **Head Office and Other Controlling Offices:** The Data Center construction is completed in the Head Office and full fledged operation is running. Core Banking Software has also been established. Now CBS is being installed & implemented in various branches.The plan of expansion of computerized system to all Chief Regional Offices , Regional Offices and Divisional Offices of the Bank is included in these phases.

1.3 ICT vision of the Bank

Now, the bank has 177 computerized branches where offline banking software is running. Among them, targeted 40 branch offices are going under the hood of online Core Banking Software (CBS), which is to be completed by June 2014 (39 branches have already been completed). In the next step another 60 branches will be under the CBS by the year 2016. Moreover, The Bank will include all of the 177 computarized branch offices into CBS. The Bank has also the vision to include all of its branch offices into CBS gradually.

Already, Mobile Banking Financial Service with the help of Dutch Bangla Bank and Brac Bank has been introduced in various branches and this service will be available in all the branches of the Bank.

ATM has been established in 5 more branches with out-sourcing and it is a contuning process. The bank is also going to establish DRS at Bangladesh Krishi BankTraining Institute, Mirpur.

In continuation of the modernization program, the bank has an intention to provide modern business facilities at the doorsteps of the valued customers through Internet Banking in all branches. The Bank in the near future will provide better services to the valued clients by implementing modern banking products and services following the market trends and technical changes in the ICT sectors .

CHAPTER – 2

2.0 Information and Communication Technology Security Policy

This chapter describes the Information and Communication Technology Security Policy of Bangladesh Krishi Bank.

This Information and Communication Technology Security Policy complies with the guideline supplied by Bangladesh Bank (Guideline on ICT Security for Scheduled Banks and Financial Institutions, April 2010, Version 2.0). This policy requires approval of the Board of Directors of Bangladesh Krishi Bank . It provides the policy for Information and Communication Technology and ensures secured use for the bank. Information security means protection of the data, applications, networks and computer system from unauthorized access, alteration or destruction.

2.1 Scope

This Policy is a systematic approach required to formulate for ICT and also to ensure security of information and information systems. It covers all information that is electronically generated, received, stored, printed, scanned and typed. However, the provisions of this policy shall be applicable to:

- Bangladesh Krishi Bank for all of its information and communication technology systems.
- All activities and operations required to ensure data security including facility design, physical security, network security, disaster recovery and business continuity planning, use of hardware and software, data disposal and protection of copyrights and other intellectual property rights.
- All users, customers, agents, employees concerned with information and information technology system.

2.2 Objectives

The objectives of the Information and communication technology security policy of Bangladesh Krishi Bank are as follows:

(1) To establish a standard ICT management;

(2) To help the bank for secured and stable setup of its ICT platform;

(3) To establish a secured environment for data processing;

(4) To identify information security risks and their management;

(5) To communicate the responsibilities for the protection of information and provide training regarding information system security;

(6) To prioritize information and information systems for protection;

(7) To review periodically the policy to formulate procedure and security measures ;

(8) To provide automated banking facility to the customer;

(9) To develop human resources with current electronic banking system;

(10) To prescribe mechanisms that help to identify and prevent the compromise of information security and the misuse of Bank data, applications, networks and computer systems.

2.3 Basic Principles

The following are the generally accepted principles based on which ICT policy is formulated**:**

2.3.1 **Accountability:** The responsibility and accountability of information/data custodians, information/data providers, users and other parties concerned with the security of information should be explicit.

2.3.2 **Awareness:** To foster confidence in information systems, custodians, providers and users shall have access to all documentation about information security policies and procedures.

2.3.3 **Ethics:** In the provision of information systems and the establishment of information security, the rights and legitimate interests of the organisation's personnel, its customers and business partners should be honoured.

2.3.4 **Business Perspective:** Security processes shall take account of and address the relevant business considerations and viewpoints; these include commercial, technical, administrative, organisational, operational, behavioral, ethical and legal/ statutory aspects.

2.3.5 **Proportionality:** The level and cost of security processes should be appropriate and proportionate to the value and degree of reliance on information systems and to the severity, probability and extent of potential or actual harm to the organisation.

2.3.6 **Integration:** Security processes should be coordinated and integrated with each other and other measures, procedures and practices of the bank to create a coherent system of information security.

2.3.7 **Timeliness:** Action to respond to an information security breach should be timely and coordinated to prevent and overcome the breach of security.

2.3.8 **Reassessment:** The security of information systems should be reassessed periodically recognising that information systems and the requirements for their security vary over time.

2.3.9 **Freedom of Information:** The freedom of information should be compatible with the legitimate use and flow of data and information like the provisions in the e-governance policy(s) of the government.

2.3.10 **Risk Mitigation:** Risk analysis is to be carried out based on value, need and type of different ICT entities. Accordingly, risk mitigation plan is to be framed for secured use of the ICT entities.

CHAPTER- 3

3 .0 Information and Communication Technology Management

The Management must ensure that the functions relating to the Information and Communication Technology are efficiently and effectively managed. They should be aware of the capabilities of ICT and be able to appreciate and recognize opportunities and the risk of possible abuses. The management of the bank should have a commitment to information technology security by continuously enhancing awareness and ensuring training of the bank staff. ICT Management deals in ICT policy formulation, system documentation and assists in the internal ICT audit, training and insurance activities. ICT security planner and/or steering committee shall be responsible for overall ICT security management.

3.1 ICT Management Area

3.1.1 The ICT Management should ensure maintenance of appropriate system documentations, particularly the systems which support financial reporting.

3.1.2 The ICT Management should participate in planning relating to the Information and Communication Technology to ensure that allocated resources are consistent with business objectives.

3.1.3 The ICT Management should ensure that sufficient properly qualified technical staff is employed so that continuance of the ICT operation area is unlikely to be at risk at all times.

3.2 Implementation of Information and Communication Technology Policy

3.2.1 The ICT Management will ensure the implementation of the Information and Communication Technology policy in the Bank. The policy covers common technologies like computers and peripherals, data and network, web system and other ICT resources.

3.2.2 The senior management of the bank must express a commitment to ICT security by continuously increasing awareness and ensuring training of the bank staff. The policy will require regular updates to cope with the evolving changes in the Information and Communication Technology environment.

3.3 ICT related Documentation

3.3.1 There shall be an Organization chart for ICT Department (centralized/ decentralized). This shall be a part of the bank's overall organization chart duly approved by the Government .

3.3.2 There shall be documented job description for each ICT personnel of different Offices/ Branches.

3.3.3 Job description (JD) for each individual within ICT department/division should be documented

3.3.4 A scheduled roster for ICT activities should be documented properly and be reviewed time to time by the head of the department or office.

3.3.5 Segregation of duties for ICT tasks shall be maintained and reviewed time to time by the head of the department or office.

3.3.6 Fallback plans for various levels of system support personnel shall be formulated, maintained and reviewed time to time by the head of the department or office.

3.4 Internal ICT Audit

3.4.1 Internal Information System Audit shall be carried out by internal Audit or relevant Department (other than ICT Department).

3.4.2 Internal Audit shall have sufficient ICT expertise/resources capable of conducting ICT Audit. At least one ICT expert/resource person shall be included in the audit team while auditing ICT related branches and offices.

3.4.3 Internal ICT audit shall be done on periodical basis according to the bank’s internal audit policy.

3.4.4 The ICT audit report should be treated as confidential and must be preserved for respective Audit and Inspection including Bangladesh Bank officials as and when required.

3.4.5 The bank/branch shall take appropriate measures to implement the recommendations made in the last Audit Report. This must be documented and kept along with the Audit Report as mentioned above.

3.5 Training of ICT Personnel

3.5.1 ICT personnel should be given adequate training on relevant ICT tasks.

3.5.2 The employees should be trained on aspects of importance and awareness of Information and Communication Technology.

3.5.3 Bank shall also ensure the minimum level of Business Foundation Training for ICT personnel.

3.6 Insurance and Depreciation

3.6.1 Due to rapid fall in the market value of computer hardware, the bank generally should consider obtaining insurance coverage only in case of costly and/ or specialized computer hardware and software. This decision will be taken on individual basis based on opinion of the management.

3.6.2 All insurance matter for computer hardware should be conducted by the Department assigned by the management of the Bank.

3.6.3 Depreciation at the rate of **20%** per annum shall be charged on Computer Hardware on straight-line method.

3.7 Problem Management

3.7.1 Bank shall establish a process to log the information system related problems and incidents.

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

3.7.3 Process shall be established to perform necessary corrective action within the time frame according to severity of the problem.

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

3.7.5 Process shall be established to review and monitor the incidents.

3.8 Risk Management

3.8.1 Effective risk management system shall be in place for any new processes and systems as well as a post-launch review.

3.8.2 The risk management function shall ensure awareness of, and compliance with , the ICT security control policies, and to provide support for investigation of any ICT related frauds and incidents.

3.8.3 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.

CHAPTER- 4

4.0 ICT Operation Management

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

4.1 Change Management

4.1.1 All changes implemented in the production environment must be governed/ supported by a formal documented process including forms with necessary change details. A sample document form has been provided in **ICTF- 1.**

4.1.2 Audit Logs of changes should be made available for ready references.

4.1.3 Signed off declaration from the vendor should be obtained before implementation of changes in production.

4.1.4 User Acceptance Test (UAT) should be completed before implementation of the application related change. A sample form for UAT has been given in **ICTF-2.**This document should be preserved for ready reference.

4.2 Asset Management

4.2.1 A register of inventory for hardware and software must be kept with all significant details and will be reviewed on 30th June every year. A sample form has been provided in **ICTF-3**. A record of this review must be maintained.

4.2.2 All assets associated with the information facilities must be labeled with tag and name.

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

4.2.4 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.

4.2.5 Software used in production environments must be subject to a support agreement.

4.2.6 No software shall be used in any computer without approval of the competent authority. Use of unauthorized or pirated software must be strictly prohibited throughout the bank. Random checks should be carried out to ensure compliance.

4.3 Operating Procedure Management

4.3.1 Operating procedures must exist (Documented) for all ICT(Information and Communication Technology) related functions.

4.3.2 Changes in operating procedures must be authorized by the competent authority and documented properly.

4.3.3 Operating procedures cover the following where appropriate:

a. Documentation on handling of different process.

b. Scheduling processes, including target start and finish times.

c. Documentation on handling of error and exception conditions.

d. Documentation for secure disposal of output from failed processing runs.

e. Documentation on system start-up, closedown, re-start and recovery.

f. System maintenance schedule.

4.4 Request Management

4.4.1 ICT Services mean any services relating to installation, maintenance, replacement of computer hardware and peripherals, communication hardware and media, operating and application software including efforts for development of human resources.

4.4.2 Before the delivery of any ICT service a formal request process must be established. A sample Request Form has been provided in **ICTF- 4.**

CHAPTER- 5

5.0 Physical Security

Bangladesh Krishi Bank needs sound business and management policies to cater the Bangladesh Bank's IT security policy, hence, to protect information and communication technology related resources are properly protected. Each department of the bank is responsible to protect their own hardware and data as well. Each department should take proper steps to secure their hardware and data from unauthorized access as well as physical security i,e: hardware . In fact, the effective security measure for 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 acces to equipment and data. The following safeguard methods are believed to be practical, reasonable and reflective of sound business practices.

5.1 Physical Security for Tier-1

5.1.1 Professional and competent technicians should be engaged for installation of equipment and after installation another team of technicians should check and make sure that the equipment is properly installed.

5.1.2 Data Center Access

5.1.2.1 Physical security shall be imposed in the information processing area or Data Center.

5.1.2.2 The data Center must be a restricted area and only authorized people should be allowed access to the center.

5.1.2.3 To enter into the data center one should use digital punch card/ finger print etc.

5.1.2.4 A monitoring authority should provide authorization to some reliable persons. Unauthorized people must be escorted during their stay in the Data Center.

5.1.2.5 The access authorization list shall be maintained and reviewed periodically for the authorized person to access the Data Center(Ref. Access Authorization List **ICTF-5**)

5.1.2.6 Access logs with date, time and purpose shall be maintained for the vendors, service providers and visitors supposed to enter into the Data Center (Ref. Access Log Book **ICTF-6,**Visitors log book-**ICTF7**)

5.1.2.7 Security guard shall be available for 24 hours.

5.1.2.8 The emergency exit door must exist and the pathway shall be clear with proper indication.

5.1.3 Environmental Security

Environmental Security shall be maintained such as water leakage protection, humidity, fire, air pressure, temperature etc.

5.1.3.1 Protection of Data Center from the risk of damage due to fire, flood, explosion and Other forms of disaster shall be designed and applied. To build Data Center and Disaster Recovery Site in the multi-tenant facilitated building is discouraged.

5.1.3.2 Physical layout of Data Center including power supply and network connectivity shall be documented .

5.1.3.3 Development and test environment shall be separated from production.

5.1.3.4 Raised floor with removable blocks or channels alongside the wall shall be prepared to protect data and power cables from interception and any sort of damages.

5.1.3.5 Water detection devices shall be placed below the raised floor, if it is raised.

5.1.3.6 Any accessories not related/associated to Data Center shall not be allowed to store in the Data Center.

5.1.3.7 Closed Circuit Television (CCTV) camera shall be installed for monitoring and the monitoring unit must be placed in a suitable location.

5.1.3.8 The sign of **"No eating, drinking or smoking"** shall be put on display.

5.1.3.9 Dedicated office vehicles for any of the emergencies shall always be available on site. Availing of public transport must be avoided while carrying critical equipment outside the bank’s premises to avoid the risk of any casuality.

5.1.3.10 The data Center shall be supported by full-time telephone communication.

5.1.3.11 Address and telephone / mobile numbers of all contact persons (e.g. fire service, police station, service providers, vendors and all ICT personnel) must be available to cope with any emergency situation and should be on display.

5.1.3.12 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.

5.1.3.13 Power supply from source (Main Distribution Board or Generator) to Data Center must be ensured. Electrical outlets from these power sources for any other devices must be restricted and monitored to avoid the risk of overloading.

5.1.3.14 The following environmental controls shall be installed:

a) Uninterrupted Power Supply (UPS) with backup units

b) Backup Power Supply

c) Temperature and humidity measuring devices

d) Water leakage precautions and water drainage system from Air Conditioner

e) Air conditioners with backup units. The industry standard cooling system may be introduced to avoid the water leakage and faults in the water drainage system with the conventional air conditioning system.

f) Emergency power cut-off switches where applicable

g) Emergency lighting arrangement

h) Dehumidifier for humidity control

The above shall be regularly tested and maintenance service contract shall be made for 24x7 basis.

5.1.4 Fire Prevention

5.1.4.1 Wall, ceiling and door of Data Center shall be fire-resistant.

5.1.4.2 Fire suppression equipment shall be installed.

5.1.4.3 Automatic fire alarming system shall be installed and tested periodically and all the employees should be trained on fire drill.

5.1.4.4 There shall be fire detector below the raised floor, if it is raised.

5.1.4.5 Electric and data cables in the Data Center must maintain a quality and be concealed.

5.1.4.6 Any flammable items shall not be kept in the Data Center.

5.2 Physical Security for Tier-2

5.2.1 Server Room Access

5.2.1.1 Server room must have a glass enclosure with lock and key to be looked after by a responsible person of the Branch.

5.2.1.2 Physical access shall be restricted, visitors log must be maintained in server room (Ref. Visitors Log Book **ICTF-7**).

5.2.1.3 Access authorization list must be maintained and reviewed on regular basis(Ref. Access Authorization **List ICTF-5**)

5.2.2 Environmental Security

5.2.2.1 Server must have password protected screen saver that shall be activated after a period as per bank's policy.

5.2.2.2 There shall be a provision to replace the server within shortest possible time in case of any disaster.

5.2.2.3 Server room shall be air-conditioned.

5.2.2.4 Water leakage precautions and water drainage system from Air Conditioner shall be installed.

5.2.2.5 Power generator shall be in place to continue operations in case of power failure.

5.2.2.6 UPS shall be in place to provide uninterrupted power supply to the server.

5.2.2.7 Proper attention must be given on overloading electrical outlets with too many devices.

5.2.2.8 Channel alongside the wall shall be prepared to allow all the cabling to be in neat and safe position with the layout of power supply and data cables.

5.2.2.9 Proper earthing of electricity shall be ensured.

5.2.2.10 Address and telephone / mobile numbers of all contact persons (e.g. fire service, police station, service providers, vendors and all ICT/ responsible personnel) must be available to cope with any emergency situation.

5.2.3 Fire Protection

5.2.3.1 Power supply must be switched off before leaving the server room.

5.2.3.2 Fire extinguisher shall be placed outdoor of the server room. This must be maintained and checked on an annual basis.

5.3 Physical Security for Tier-3

5.3.1 Computer Room Access

5.3.1.1 The PC running the branch banking software must be placed in a secured area and held by a responsible person in the Branch.

5.3.1.2 The access authorization list must be maintained and reviewed on a regular basis.

5.3.2 Environmental Security

5.3.2.1 PC must have password-protected screensaver which shall be activated after a period as per bank's policy.

5.3.3 Fire Protection

5.3.3.1 Preventive measures shall be taken to protect computer room from short circuits.

5.3.3.2 Power and other connecting cables for PCs must be kept secured from physical damage.

5.3.3.3 Power supply of the PC shall be switched off before leaving the branch.

5.3.3.4 Fire extinguishers with expiry date shall be placed beside the power distribution board. This must be maintained and checked on an annual basis.

5.3.3.5 Proper earthing of electricity shall be ensured.

5.4 Physical Security for Desktop and Laptop Computers

5.4.1 Desktop computer shall be connected to UPS to prevent damage of data and hardware.

5.4.2 Before leaving a desktop or laptop computer unattended, users shall apply the "Lock Workstation" feature.

5.4.3 Password protected screen saver shall be used to protect desktop and laptop from unauthorized access.

5.4.4 Laptop computers that store confidential or sensitive information must have encryption technology.

5.4.5 Desktop and laptop computers and monitors shall be turned off at the end of each workday.

5.4.6 Laptop computers, computer media and any other forms of removable storage (e.g. diskettes, CD ROMs, zip disks, PDAs, flash drives) shall be stored in a secured location or locked cabinet when not in use.

5.4.7 Other information storage media containing confidential data such as paper, files, tapes, etc. shall be stored in a secured location or locked cabinet when not in use.

5.4.8 Individual users must not install or download software applications and/or executable files to any desktop or laptop computer without prior authorization.

5.4.9 Desktop and laptop computer users shall not write, compile, copy, knowingly propagate, execute, or attempt to introduce any computer code designed to self-replicate, damage, or otherwise hinder the performance of any computer system (e.g. virus, worm, Trojan etc).

5.4.10 Any kind of viruses shall be reported immediately.

5.4.11 Viruses shall not be deleted without expert assistance unless otherwise instructed.

5.4.12 User identification (ID) and authentication (password) shall be required to access all desktops and laptops whenever turned on or restarted.

5.4.13 Standard virus detection software must be installed on all desktop and laptop computers and shall be configured to check files and scan routinely the system for viruses.

5.4.14 Desktop and laptop computers shall be configured to log all significant computer security relevant events. (e.g. password guessing, unauthorized access attempts or modifications to applications or systems software.)

5.4.15 All computers shall be placed above the floor level and away from windows.

CHAPTER- 6

6.0 Information Security Standard

The objective of this chapter is to cater the Information Security Policies and Standards to be adopted according to the Bangladesh Bank

6.1 Access Control for Information Systems

6.1.1 User ID Maintenance

6.1.1.1 Each user must have a unique User ID and a valid password.

6.1.1.2 User ID shall be locked up after 3 unsuccessful login attempts.

6.1.1.3 User ID and password shall not be same.

6.1.1.4 User ID Maintenance form (Ref. User Creation Form **ICTF-8**) with access privileges shall be duly approved by the appropriate authority.

6.1.1.5 Access privileges shall be changed/ locked within 24 hours or as per bank's policy when users' status is changed or user leaves the bank.

6.1.2 Password Control

6.1.2.1 The password definition parameters ensure that minimum password length is specified according to the Bank's ICT Security Policy (at least 6 characters, combination of uppercase, lowercase, numbers & may include special characters).

6.1.2.2 Administrative password of Operating System, Database and Banking Application shall be kept in sealed envelope and kept in a safe custody (centralized/decentralized)(Ref. Password Handover Form **ICTF-9**).

6.1.2.3 The maximum validity period of password shall not be beyond the number of days permitted in the Bank's ICT Security Policy (within 30 to 90 days cycle).

6.1.2.4 The parameters control the maximum number of invalid logon attempts shall be specified properly in the system according to the ICT Security Policy of the Bank (maximum 3 consecutive times).

6.1.2.5 Password history maintenance shall be enabled in the system to allow same passwords to be used again after at least 4 times.

6.1.2.6 The session time-out period for users shall be set in accordance with the bank's Policy.

6.1.2.7 The operating time schedule for the users shall be defined where necessary.

6.1.2.8 Audit trail shall be available to review the user profile in the application.

6.1.3 Input Control

6.1.3.1 The software shall not allow the same user to be both maker and checker of the same transaction. Management approval must be in place for delegation of authority.

6.1.3.2 Audit trail must be clearly marked with User Id and date-time stamp.

6.1.3.3 The system shall be restricted from being accessed especially in sensitive data/fields.

6.2 Network Security

6.2.1 The Network Design and its security shall be implemented under a documented plan.

6.2.2 Physical security for the network equipment shall be ensured.

Specifically:

a) Access shall be restricted and controlled.

b) Network equipment shall be housed in a secure environment.

6.2.3 Groups of information services, users, and information systems shall be segregated in networks, e.g. VLAN.

6.2.4 Unauthorized access and electronic tampering shall be controlled strictly.

6.2.5 Firewall shall be in place on the network for any external connectivity.

6.2.6 Redundant communication links shall be used for WAN.

6.2.7 There shall be a system to detect unauthorized intruder in the network.

6.2.8 Connection of personal laptop to office LAN or any personal wireless modem with the office laptop/desktop must be secured.

6.3 Data Encryption

6.3.1 Mechanism shall be in place to encrypt and decrypt sensitive data travelling through WAN or public network.

6.4 Virus Protection

6.4.1 Antivirus software shall be installed in each server and computer whether it is connected to network or not.

6.4.2 Virus auto protection mode shall be enabled.

6.4.3 Anti-virus software shall always be updated with the latest virus definition file.

6.4.4 All computers in the network shall get updated signature of antivirus software automatically from the server.

6.4.5 Bank may arrange awareness program for the users about computer viruses and their prevention mechanism.

6.5 Internet and e-mail

6.5.1 All Internet connections shall be routed through a firewall for computers connected to network and Anti-Virus Gateway like Web shield, Trend Micro etc. to get protection from spam, worm, Trojan etc. that is accessing in bank's network while browsing, downloading, or an attachment of any incoming mail to the PCs connected to bank's network.

6.5.2 Access to e-mail system and internet shall only be obtained through official request.

6.5.3 E-mail system and internet shall be used according to the bank's policy.

6.5.4 Concerned department shall perform regular review and monitoring of e-mail service.

6.5.5 Users shall not use profanities, obscenities, or derogatory remarks in email messages regarding employees, customers, competitors, or others.

6.5.6 All attachments with the incoming e-mail messages shall be monitored especially for viruses.

6.5.7 Mail server must have latest anti-virus signature.

6.6 Transactions through Alternative Channels

6.6.1 Services through Mobile

Controls over mobile transaction are required to manage the risks of working in an unprotected environment. Therefore, banks shall establish following control procedures to ensure confidentiality, integrity, authenticity and non-repudiability:

6.6.1.1 Appropriate risk mitigation measures shall be implemented like transaction limit, transaction frequency limit, fraud checks, AML checks etc. depending on the risk perception, unless otherwise mandated by the regulatory body.

6.6.1.2 Services provided by banks through mobile shall comply with security principles and practices for the authentication of transactions mandated by the regulatory body.

6.6.1.3 Proper level of encryption and security shall be implemented at all stages of the transaction processing. The following measures with respect to network and system security shall be adhered to:

a) Implement application level encryption over network and transport layer encryption wherever possible.

b) Establish proper firewalls, intrusion detection system (IDS), intrusion prevention system (IPS), data file and system integrity checking, surveillance and incident response procedures.

c) conduct periodic risk management analysis, security vulnerability assessment of the application and network at least once a year.

6.6.1.4 Bank shall comply with 'Regulatory Compliance' requirements of the country.

6.6.1.5 Proper documentation of security practices, guidelines, methods and procedures used in such mobile services shall be maintained and updated.

6.6.2 Internet Banking

Information involved in internet banking passing over public networks shall be protected from fraudulent activity, contract dispute, and unauthorized disclosure and modification. Therefore, bank shall establish following control procedures:

6.6.2.1 I-banking standards shall be included in the Bank's ICT Security Policy.

6.6.2.2 Network and Database administrator shall ensure the security issues of I-banking.

6.6.2.3 Bank shall introduce logical access controls to data, systems, application software, utilities, telecommunication lines, libraries, system software, etc. Logical access control techniques may include user-ids, passwords, smart cards, biometric technologies or other industry standards.

6.6.2.4 Bank shall ensure real time security log for unauthorized access.

6.6.2.5 Bank shall define technology security protocols for I-banking solutions like PKI (Public Key Infrastructure), SSL (Secured Socket Layer), 2-FA (Two Factor Authentication), RSA, VASCO etc.

6.6.2.6 All computer accesses, including messages received shall be logged. Security violations (suspected or attempted) shall be reported and followed up. Bank shall acquire tools for monitoring systems and the networks against intrusions and attacks.

6.6.2.7 The information security officer, system auditor or any other concerned shall undertake periodic penetration tests of the system, which may include:

a) Attempting to guess passwords using password-cracking tools.

b) Searching for back door traps in the programs.

c) Attempting to overload the system using DDoS (Distributed Denial of Service) & DoS (Denial of Service) attacks.

d) Checking of commonly known holes in the software, especially the browser and the e-mail software exist.

e) Checking the weaknesses of the infrastructure.

f) Taking control of ports.

g) Cause application crash.

h) Injecting malicious codes to application and database servers.

6.6.2.8 All applications of bank shall have proper record keeping facilities for legal purposes. Bank may keep all received and sent messages in restricted form.

6.6.2.9 Security infrastructure shall properly be tested before using the systems and applications for normal operations. Banks might upgrade the systems by installing patches released by developers to remove bugs and loopholes, and upgrade to newer versions which give better security and control.

6.6.3 Payment Cards

Bank providing the payment card services must comply with the industry security standards, e.g.- Payment Card Industry Data Security Standard (PCI DSS) to ensure the security of cardholder's data. The PCI DSS includes following requirements for security management, policies, procedures, network architecture, software design and other protective measures:

6.6.3.1 PINs used in transactions shall be processed using equipment and methodologies to ensure that they are kept secured.

6.6.3.2 Cryptographic keys used for PIN encryption/decryption and related key management shall be created using processes to ensure that it is not possible to predict any key or determine that certain keys are more probable than other keys.

6.6.3.3 Secret or private Keys shall be conveyed or transmitted in a secured manner.

6.6.3.4 Unencrypted Key loading to hosts and PIN entry devices shall be handled in a secured manner.

6.6.3.5 Randomized Keys shall be used in a manner that prevents or detects their unauthorized usage.

6.6.3.6 Keys shall be administered in a secured manner.

6.6.3.7 Equipment used to process PINs and keys shall be managed in a secured manner.

CHAPTER- 7

7.0 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'.

7.1 In-house Software

7.1.1 Detailed design and technical application requirements shall be prepared.

7.1.2 Criteria for acceptance of the requirement shall be defined and approved by the concerned business unit.

7.1.3 Application security and availability requirements shall be addressed.

7.1.4 Developed functionality in the application shall be managed in accordance with design specification and documentation.

7.1.5 Source code must be available in the concerned department and kept secured.

7.1.6 Source code shall contain title area, the author, date of creation, last date of modification and other relevant information.

7.1.7 Software Development Life Cycle (SDLC) with User Acceptance Test (UAT) shall be followed and conducted in the development and implementation stage.

7.1.8 System documentation and User Manual shall be prepared and handed over to the concerned department.

7.1.9 Necessary ‘Regulatory Compliance’ requirements must be taken into account by the Bank.

7.2 Outsourced Software

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.

7.2.1 Vendor Selection

7.2.1.1 There must be a core team comprising of personnel from Functional Departments, ICT Department and Internal Audit Department for vendor selection.

7.2.1.2 Vendor selection criteria for application must address the following:

a) Market presence

b) Years in operation

c) Technology alliances

d) Extent of customization and work around solutions

e) Performance & Scalability

f) Number of installations

g) Existing customer reference

h) Support arrangement

7.2.2 Software Documentation

7.2.2.1 Documentation of the software shall be available and safely stored.

7.2.2.2 Document shall contain the followings:

a) Functionality

b) Security features

c) Interface requirements with other systems

d) System Documentation

e) Installation Manual

f) User Manual

7.2.3 Other Requirements

7.2.3.1 There shall be a test environment to ensure the software functionalities before implementation.

7.2.3.2 User Acceptance Test shall be carried out and signed-off before going live.

7.2.3.3 Necessary 'Regulatory Compliance' requirements for banking procedures and practices in the application must be taken into account by the Bank.

7.2.3.4 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.

7.2.3.5 Support agreement must be maintained by the provider for the software used in production with the confidentiality agreement.

CHAPTER- 8

8.0 Business Continuity and Disaster Recovery Plan

The Business Continuity Plan(BCP) is required to cover operational risks and should take into account the potential for wide area disasters, data centre disasters and the recovery plan. The BCP should take into account the backup and recovery process. Keeping this into consideration this chapter covers BCP, Disaster Recovery Plan and Backup/ Restore plan.

8.1 Business Continuity Plan (BCP)

8.1.1 There must be a Business Continuity Plan, in line with business, for ICT in place.

8.1.2 All the documents related to business continuity and disaster recovery plan must be kept in a safe and secured location. One copy can be stored in the office for ready reference.

8.1.3 Business Continuity Plan (BCP) must contain the following:

a) Action plan for:

- Disaster during office hours ,
- Disaster outside office hours, and
- Immediate and long term action plan in line with business.

b) Emergency contact addresses and phone numbers including vendors.

c) Grab list of items such as backup tapes, Laptops etc. in case of an immediate evacuation.

d) Disaster recovery site map.

8.1.4 Business Continuity Plan (BCP) must be reviewed at least once a year.

8.2 Disaster Recovery Plan (DRP)

8.2.1 A Disaster Recovery Site (DRS) must be in place replicating the Data Center / Production Site.

8.2.2 Disaster Recovery site should be at a minimum of 20 (twenty) kilometers radial distance from the central data center. Otherwise bank should follow the Central Bank i.e. Bangladesh Bank standard.

8.2.3 Disaster Recovery Site should not be placed under same utility services as the data center.

8.2.4 Disaster Recovery Site should be equipped with compatible hardware and telecommunications equipment to support the live systems in the event of a disaster.

8.2.5 Appropriate physical and environmental security should be provided at the Disaster Recovery Site.

8.2.6 Information security should properly be maintained throughout the fallback and DR recovery process.

8.2.7 An up-to-date and tested copy of the DR plan is to be securely held off-site. DR plans exist for all the critical services where DR requirement is agreed with the business.

8.2.8 DR test is to be successfully carried out at least once a year.

8.2.9 DR Test documentation should include at least:

a)Scope - description of planned tests with expected success criteria.

b)Plan - detailed actions with timetable.

c)Test Results.

8.3 Backup/ Restore Plan (BRP)

8.3.1 Backup means saving of data or information to assure business continuity in case of a loss of resources at the production site.

8.3.2 There should be a documented backup procedure. Information and communicaton technology department/computer department of the bank should formulate backup procedure which will be reviewed annually.

8.3.3 Backup copies of information should be stored off-site at a geographically separate and safe environment.

8.3.4 At least one backup copy should be kept on-site office for the moment of critical delivery.

8.3.5 The backup cycle is based on the following:

Backup for branch-banking operation should be taken daily in appropriate media /device. Provision for both incremental and full backup should be kept to avoid corruption of data as well as save time and money.In other cases, backup should be taken daily/weekly/ monthly/ quarterly and half-yearly basis depending on the nature of the database and/ or operations.

8.3.6 The backup media should be sent off-site immediately after the backup has been taken.

8.3.7 The backup log book in form of **ICTF-10** should be maintained, checked and signed by the Branch Manager/ Head of the Department/Office.

8.3.8 The backup inventory is maintained, checked and signed by supervisor.

8.3.9 The ability to restore from backup media is to be tested at least quarterly.

8.3.10 Backup media must be labeled properly indicating contents, date etc.

CHAPTER- 9

9.0 ATM

ATM security is one of the gravest concerns among all ATM owners and consumers. With growing ATM frauds and thefts it's necessary to follow some important security measures related to ATM usage. The ATM frauds not only cause financial loss to banks but they also undermine customers' confidence in the use of ATMs . It is therefore in the interest of banks to prevent ATM frauds . A coordinated and cooperative action on the part of the bank, customers and the law enforcement machinery is required to prevent ATM burglary attacks.

9.1 ICT persons' awareness and actions

a. Sending Pin and Card through different media. (Separate Courier service).

b. Distributing Pin and Card to customer through different personnel from Branch.

c. Anti Skimming Device installation.

d. Ensuring that the CCTV are working 24/7

e. Monitoring CCTV video regularly.

f. Provide training to Security Guard as well as ATM department Official.

g. Security guard should check identification of the people (Online Vendor, ATM Vendor, CCTV vendor, ATM Department Official) who want to work inside ATM room.

h. Security guard will notice ATM related Department every time any vendor official or ATM official from Bank

i. Try to employ Security guards from banks employees rather than from Security Service Provider.

j. Check carefully any modification of any device in the ATM
booth facility by concerned Bank personnel.

k. Strong SLA with the service provider.

9.2 Lock and Closing Devices

a. Mechanical locks

1. Allow the opening of safe door only through the combination of different keys
2. Each key in the hands of different persons.

b. Electronic Locks

1. Higher level of functionality

2. Allow multiple combinations, each assigned to a different ATM maintenance facilitator
3. Different passwords for operator, supervisor and conveyor
4. Allow opening of safe during specific time periods (pre-programmed)

Report remotely to monitoring system

9.3 Alarms and Sensors

a. Alarms

1 Detect open / closed state of the safe door

2 Monitor different parameters that can be indicative of a robbery attempt

b. Sensors

1 Temperature sensor to detect piercing with torch

2 Tilting sensor to detect detachment of safe (for transportation)

3 Vibration sensor to detect piercing with tool (drilling, cutting)

4 Door sensor to detect if door is tampered with outside of cash handler or servicing

CHAPTER- 10

10.0 Mobile Financial Services (MFS)

Bangladesh Krishi Bank is the largest state owned bank and it is liable to its own customers as well as to the whole nation for providing better banking services. As the banking industry of Bangladesh has grown tremendously in volume and complexity over the recent years Krishi Bank needs financial viability , profitability, innovative ideas to retain the valuable market share and compete in the banking sector. Krishi Bank also needs to serve the rural & underprivileged people through basic banking services. In this circumstance, rapid growth of mobile phone and wide range of the coverage of Mobile Network Operators (MNOs) can be an important tool of the trade for extending banking services to the unbanked/banked population. In order to ensure the access of unbanked people by taking advantage of countrywide mobile network coverage, Bangladesh Krishi Bank has taken some principles from Bangladesh Bank's guideline on **Mobile Financial Services (MFS) for the Banks.**

10.1 Applicable Sectors for Mobile Financial Services

Bangladesh Krishi Bank may apply this Mobile Financial Services in the following sectors (according to Bangladesh Bank's guideline):

1. Disbursement of inward foreign remittances
2. Cash in /out using mobile account through agents/Bank branches/ ATMs/Mobile Operator's outlets.
3. Person to Business Payments [P to B](ex: utility bill payments or merchant payments)
4. Business to Person Payments [B to P] (ex: salary disbursement, dividend and refund warrant payments, vendor payments)
5. Government to Person Payments [G to P] (ex: elderly allowances, freedom-fighter allowances, subsidies)
6. Person to Government Payments [P to G] (ex: taxes, levy payments)
7. Person to Person Payments [PtoP] (ex:One registered mobile account to another registered mobile account)
8. Other Payments (ex: microfinance, overdraft facility, insurance premiums, deposit pension scheme deposits)

10.2 Rules & Regulations

Bangladesh Bank only supports the Bank led Mobile Financial Services (MFS)**.** Bangladesh Krishi

Bank has gotten the nod of that service. It shall offer an alternative to conventional branch-based banking to the unbanked population through Mobile Financial Services. Krishi Bank can also get help from other Banks or employ agents to provide that service.

10.2.1 The Bank shall have to submit the agreement (s) /MOU (s) containing Service Level Agreement (SLA) signed between the bank and its partners/agents before launching the product.

10.2.2 The Cash Points/Agents shall have to be selected by the bank and a list of the Cash Points/ Agents with their names and addresses shall have to be submitted to the Department of Currency Management and Payment System (DCMPS), Bangladesh Bank and will be updated on monthly basis.

10.2.3 At any point of time, the relevant balance in the bank book shall be equal to the virtual balance of all registered mobile accounts shown in the system. The Bank will be the custodian of individual customers' deposits.

10.2.4 The inward foreign remittance (credited to Nostro **Accounts** of Banks) transfer arrangement through designated Cash Points/Agents will be used only for delivery in local currency.

10.2.5 The platform should not be used for cross border **outward remittance** of funds without prior approval from Bangladesh Bank.

10.2.6 Mobile Account will be a non-chequing limited purpose account.

10.3 Transaction Limit

Bangladesh Krishi Bank has the right to fix the transaction limit as well as overall cap (per customer/ per month) for Person to Person Payments as and when needed according to Bangladesh Banks permissible limit.

10.4 Charge for the Services

For these products and services the Banks may fix up charges which will be under Bangladesh Bank oversight.

10.5 Interest/Profit

The Bank shall pay **interest/profit** on the deposits lying with the customers’ mobile accounts.

10.6 Anti-Money Laundering Compliance

10.6.1 The Bank and its partners shall have to comply with the prevailing Anti-Money Laundering (AML)/Combating the Financing of Terrorism (CFT) related laws, regulations and guidelines issued by Bangladesh Bank from time to time.

10.6.2 The Bank shall have to use a new 'Know Your Customer (KYC)' format as given in **MFSF-1**. The Bank will be responsible for authenticity of the KYC of all the customers.

10.6.3 The Bank shall have to follow full KYC format issued by Anti Money Laundering Department (AMLD) of Bangladesh Bank for the cash points/agents/partners.

10.6.4 The Bank shall ensure that suspect transactions can be isolated for subsequent investigation. The Bank shall develop an IT based automated system to identify suspicious activity/transaction report (STR/SAR) before introducing the services.

10.6.5 The Bank shall immediately report to Anti-Money Laundering Department of Bangladesh Bank regarding any suspicious, unusual or doubtful transactions likely to be related to money laundering or terrorist financing activities.

10.7 Record Retention

MFS transaction-records must be retained for six (06) years from the origination date of the entry. The Bank must, if requested by its customer, or other Receiving Bank(s), provide the requester with a printout or reproduction of the information relating to the transaction. The Bank should also be capable of reproducing the MFS transaction-records for later reference, whether by transmission, printing, or otherwise.

10.8 Selection of Partners/Agents

It is the Bangladesh Krishi Bank’s responsibility to identify, contract, educate, equip and monitor activities of the agents on a regular basis. There must be clear, well documented Agent Selection Policy and Procedures. The agreement signed between the bank and the agents will primarily include business hours of the cash points/agents, standard of performance, fees permissible by Bangladesh Bank, customer service and dispute resolution procedure. Those who have country-wide branch network such as NGOs, the MNOs or Govt. Postal Department may act as partner/agent. The Bank should publish list as well as addresses of cash points/agents/partners in the bank’s website.The following issues should be taken into account for selection of partners/agents:

10.8.1 Competence to implement and support the proposed activity ;

10.8.2 Financial soundness;

10.8.3 Ability to meet commitments under adverse conditions;

10.8.4 Business reputation;

10.8.5 Security and internal control, audit coverage, reporting and monitoring environment;

10.9 Security Issues

1. The following properties need to be addressed to offer a secure infrastructure for

financial transactions using mobile technology:

a. **Confidentiality:** Property that ensures transaction information which cannot be viewed by unauthorized persons.

b. **Integrity:** Property indicating transaction information which remains intact during transmission and cannot be altered.

c. **Authorization:** Property indicating the authentic user having proper permission to perform the particular transaction. It ensures how the system decides what the user can do.

d. **Non-repudiation:** Property indicating the particular transaction initiated by a user who cannot be denied by him/her later.

2. All the transactions must be authenticated by the account holders using their respective Personal Identification Number (PIN) or similar other secured mechanism. To facilitate the mobile financial services, the said PIN may be issued and authenticated by the bank maintaining proper protection and security features.

3. The bank should ensure that a proper process is put in place to identify the customer when the service is being enabled.

4. A second factor of authentication should be built-in for additional security as chosen by the bank.

10.10 Interoperability

1. The Bank may link their mobile financial services with those of other banks for the convenience of the users.

2. Mobile account may be linked with customer's bank account (if any).

10.11 Customer/Employee Education and Awareness

The Bank shall take appropriate measures (may issue proper guidelines for dealing with customer service and customer education) to raise awareness and educate their customers and employees for using Mobile Financial Services**.**

10.12 Complaints and Grievance Redressal Procedure

1. The Bank shall be held responsible to protect consumer rights and dispute resolution. The Bank may address dispute resolution with the assistance of selected partners/agents.

2. The Bank shall have to disclose the risks, responsibilities and liabilities of the customers on their websites and/or through printed material. Customers must be made aware of

the risks prior to sign up.

3. Bilateral contracts have to be drawn up between the payee and the bank, the participating banks and service providers should clearly define the rights and obligations of each party.
4. The grievance handling procedure including the compensation policy should be disclosed.
5. Whenever any consumer is dissatisfied by the action of the bank, the consumer can register complaint with Bangladesh Bank to mediate the dispute. In that case decision from Bangladesh Bank will be final.

N.B: Operational circular / circular letters regarding mobile financial service (MFS) of BKB (Including BKB-DBBL & BKB-bKash MFS) are to be treated as the part of this ICT security policy / manual.

CHAPTER- 11

11.0 Procurement and Service Management

The purchase of computer hardware, software and peripherals requires careful consideration of bank's business needs because these are usually expensive to make subsequent changes. The system must have adequate capacity or else it may not be able to function properly. There shall have adequate arrangements for proper maintenance of the system. However, the service of vendors is of utmost importance for smooth operation of the business in modern business organizations. This chapter specifies policies and procedures to be followed by the bank for procuring and hiring different service to be rendered by each and every service provider. This also covers the basic principles applicable to all service providers to ensure spontaneous services so that bank's operations are not hampered.

11.1 Computer Hardware and Software Procurement

11.1.1 All purchase of new systems, computer hardware and software or new component for existing systems must be made in accordance with the applicable Government/Bank procurement policies and procedures as well as technical standards.

11.1.2 Except for minor purchase (as is mandated by the delegation of financial power), hardware and software must be purchased through a structured/formal evaluation process.

11.1.3 Purchase must be done on the basis of the business needs and requirements to be assessed by the competent authority.

11.1.4 All new hardware and software installation are to be planned formally and notified to all interested parties ahead of the proposed installation date**.**

11.1.5 All hardware and software must be tested fully and comprehensively and formally accepted by user before being transferred to the live operations.

11.1.6 All hardware and software under procurement shall have comprehensive warranty to cover operational risk.

11.1.7 The period of warranty coverage should be determined by the procuring entity depending on the nature of the components but the period should not be less than twelve (12) months.

11.1.8 The description of warranty must clearly mention warranty coverage (parts, labor and service), type of warranty (comprehensive), duration and any provision for penalty when the said warranty is not complied with at an acceptable level.

11.2 Service Level Agreement (SLA)

11.2.1 There should be maintenance service arrangement for all hardware and software for post warranty period.

11.2.2 There should be service level agreement between the vendor and bank for all sensitive hardware and software.

11.2.3 The Annual Maintenance Contract (AMC) with the vendor shall exist only for usable hardware and software.

11.2.4 For sensitive hardware and software items, the concerned authority shall exercise utmost care in having a contract without an interruption due to delay in renewal of contract.

11.2.5 The user site should ensure that the equipment does not contain sensitive live data when hardware is taken by the vendors for servicing/repair.

11.2.6 Service Contracts with all service providers including third-party vendors should include:

a) Parties to the contract with address,

b) Definitions of terms, if necessary,

c) Measurable service/deliverables,

d) Timing/schedules, i.e. service levels,

e) Roles and responsibilities of contracting parties, including an escalation matrix clearly mentioning response time and resolution time,

f) Pricing of the contract,

g) Penalty Clause,

h) Confidentiality clause,

i) Contact person names (on daily operations and relationship levels),

j) Renewal period,

k) Modification clause,

l) Frequency of service reporting,

m) Termination clause,

n) Warranties, including service suppliers’ employee liabilities, 3rd party liabilities and the related remedies,

o) Geographical locations covered,

p) Ownership of hardware and software,

q) Documentation to be maintained (e.g. logs of changes, records of reviewing event logs),

r) Audit rights of access (internal audit, external audit, other audit as may be appropriate),

s) Any other clause considered fit for the contract.

11.3 Outsourcing

11.3.1 Outsourcing shall be done for activities not usually performable using normal capacity of man, materials and resources of the Bank.

11.3.2 The economic validity shall be studied before considering any sort of outsourcing.

11.3.3 The risk and security concerned with outsourcing shall be considered carefully.

11.3.4 The legal implication behind outsourcing shall be carefully examined.

11.3.5 The technical aspect of any activities should be examined by the technical committee or by the technical consultant according to the nature of the activities concerned.

11.3.6 Outsourcing proposal or working paper shall be prepared by the user department/office.

11.3.7 Arrangements for possible acquisition of the source code in case of necessary software through an escrow account.

11.3.8 Outsourcing service contract shall include terms and conditions mentioned in chapter 11.2.6

ICT Forms

BANGLADESH KRISHI BANK **ICTF-1**

............................Office

CHANGE REQUEST FORM

Reference No:	**Date:**
Section I : Requester Information	
Branch/Division Name :	
Submitted by :	
Change Description :	
Change Purpose :	
Request Date :	
Signature and Seal (Requester)	Signature and Seal (Head of the Office)
Section II : Approvals	
The undersigned agrees and accepts the change documented on this form.	
Name :	
Designation :	
Comments :	
Date :	
Signature and Seal :	
Section III : Implementer Details	
The undersigned has implemented the requested change on this form.	

Change reference No. :	
Date of change Implementation :	
Change Implementation Details :	
Was change successful?	Yes No
Name :	
Designation :	
Signature and Seal :	
Signature and Seal	
(Head of Branch/Division)	

(Ref: Para-4.1.1)

BANGLADESH KRISHI BANK **ICTF-2**

.............................Office

USER ACCEPTANCE TEST (UAT)

Reference No:	**Date:**
Application/System Name :	
Change Request Reference :	Date :
Test Scope (Detail plan of test) : Hardware / Software Performance Test/ Security Test Black box/ White box	
Expected Result :	
Actual Result :	

User Acceptance Test	Failure / Success
Comments :	
Signature and Seal :	

(Ref: Para-4.1.4)

BANGLADESH KRISHI BANK

ICTF-3

.............................Office

STOCK REGISTER OF HARDWARE AND SOFTWARE

Name of the item:

SL #	Brand & Model	Description with Specification / Version	Quantity	Identification No	Machine Location	Supplier/ Vendor	Date of Supply	Price	Signature	Remarks
1	2	3	4	5	6	7	8	9	10	11

(Ref: Para- 4.2.1)

BANGLADESH KRISHI BANK

ICTF- 4

............................Office

REQUEST FORM

Reference No.:	**Date:**
Section I : Requester Information	
Branch/Division Name :	
Submitted by :	
Contact No. :	
Request Details :	
Justification :	
Request Date :	
Signature and Seal (Requester)	Signature and Seal (Head of the Office)
Section II : Approvals	
The undersigned agrees and accepts the change documented on this form.	
Name :	
Designation :	
Comments :	
Date :	
Signature and Seal :	

Section III : Implementer Details
The undersigned has implemented the requested change on this form.
Request reference No. :
Date of Request Implementation :
Request Implementation Details :
Was Request done successfully? Yes / No (put details below)
Short description in case of failure :
Name :
Designation :
Signature and Seal :

(Ref: Para-4.4.2)

BANGLADESH KRISHI BANK

ICTF- 5

.............................Office

ACCESS AUTHORIZATION LIST

Serial No.	Name and Designation of the authorized persons	Address	Authorization Validity		Authorization Card No.	Authorized by	Remarks
			From	To			
01	02	03	04	05	06	07	08

(Ref: Para-5.1.1.5)

BANGLADESH KRISHI BANK

ICTF- 6

.............................Office

ACCESS LOG BOOK

(for the use in the Data Center, Server Room, Computer Room)

Date of Access	Name and Designation of the Authorized Persons	Address	Authorization Card No.	Time of Access	Signature of the person	Purpose of Access / Work done	Time of Departure	Signature of the person	Remarks
01	02	03	04	05	06	07	08	09	10

(Ref: Para-5.1.1.6)

BANGLADESH KRISHI BANK

ICTF- 7

.............................Office

VISITORS LOG BOOK

(For the use in the Data Center, Server Room, and Computer Room)

Date of Visit	Name of the visitor.	Address	Purpose of Visit	Time of Access	Signature of the visitor	Work done /Activities during stay	Time of Departure	Signature of the visitor	Remarks
01	02	03	04	05	06	07	08	09	10

(Ref: Para-5.1.1.6)

BANGLADESH KRISHI BANK

ICTF- 8

.............................Office

USER CREATION FORM

(For the use of the user section of branch/department)

01. I. Name of the User :

II. Designation :

III. Address :

IV. Date of Joining :

V. Transfer from :

02. Name of the System/Software :

03. User Status : Administrator/Data Controller/Data processor/ Data Operator/ Teller .

04. User Rights Proposed : Module Name(s) :

(Read, Write, Delete, Copy, Change, Print)

Recommended/Proposed by: Approved By :

Users' Signature:

Signature :
Designation:

Signature :
(Manager/Head of Department or Office).

(*For use of computer section of the branch/computer department/system owner department*)

Accepted for implementation for the following rights:

1.

2.

3.

4.

5.

Signature :

Designation:

(*Branch Manager/ Head of Department office-system owner)*

User Created :

a)On: …………………….. .

b)User ID: ………… .

c)User Password Envelop No : ….. .

Signature with seal

(In charge of System Admistrator)

(Ref: Para-6.1.1.4)

BANGLADESH KRISHI BANK **ICTF- 9**

............................Office

PASSWORD HANDOVER FORM

We, the undersigned handing over and receiving respectively today the ....(*date*) at ………am/pm the sealed cover in respect of the followings:

(1)……………………………………………………………………………………….

(2)……………………………………………………………………………………….

(3)……………………………………………………………………………………….

in terms of the order no……………………………………………………......................dated..…………

of …………………………………… *(name of the order issuing office)* …………………………………..in presence of the following witness (officer/staff).

Signature:

(Handing over Officer)

Name :

Designation:

Address :

Signature:

(Receiving Officer)

Name :

Designation:

Address :

Counter Signature:

Name of the counter signing officer:

Designation:

Address :

NB: *After receiving the passwords the receiving officer will open the sealed envelop alone and confirm the passwords applying in the system/database. S/he will change the passwords just after checking and again handed over the same in a sealed envelop to the Head of the Computer Department/branch manager documentarily.*

(Ref: Para-6.1.2.2)

BANGLADESH KRISHI BANK **ICTF- 10**

.............................Office

<u>BACK UP LOG BOOK</u>

Name of the System:.......................................

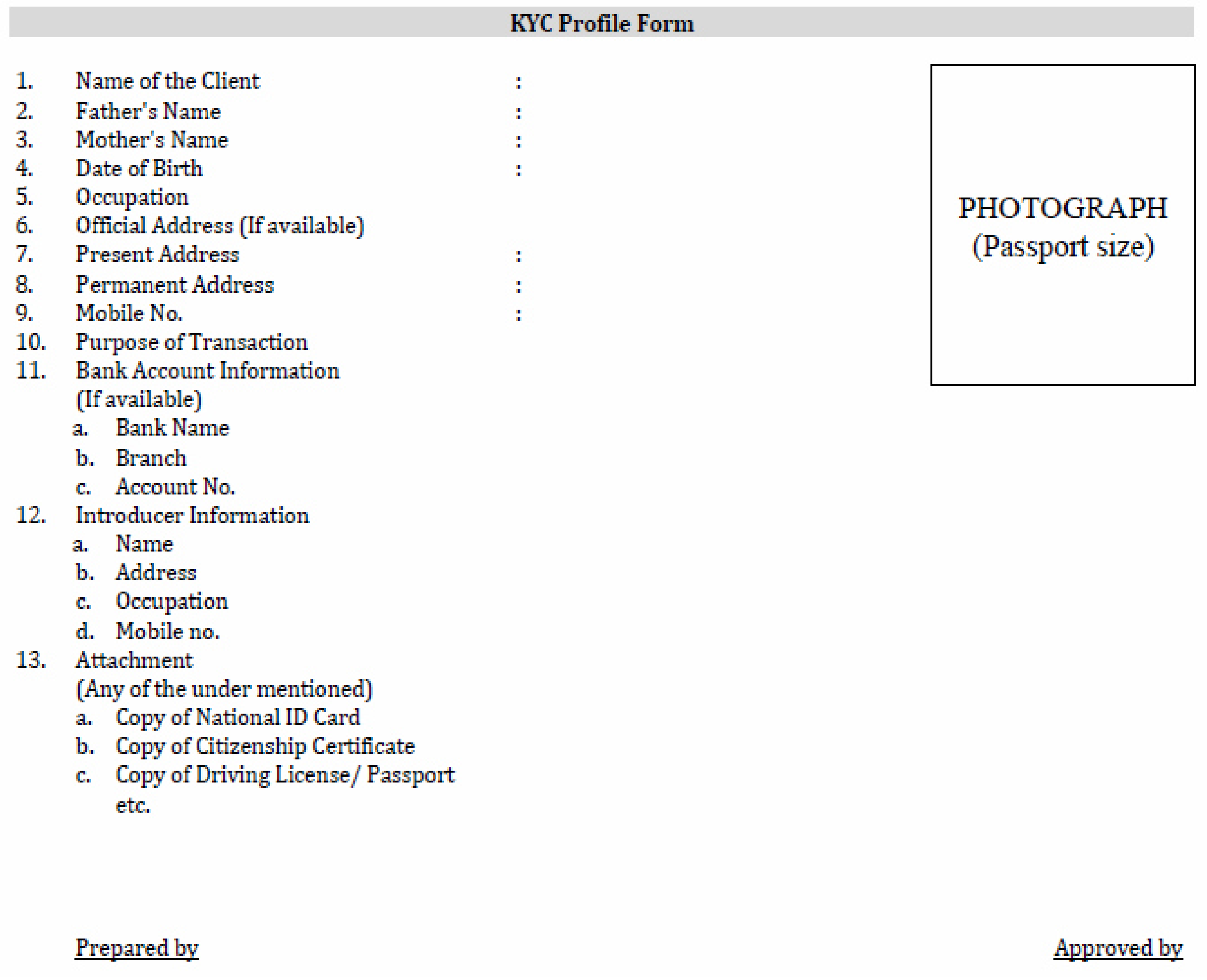
Serial no.	Backup Period / Date	Backup Media	Backup Type (full / incremental)	Backup taken by			Backup sent to	Reference / code no.	Signature of the recipient	Remarks
				Name	Designation	Signature				
01	02	03	04	05	06	07	08	09	10	11

(Ref: Para-8.3.7)

BANGLADESH KRISHI BANK **MFSF-1**

............................Office

Mobile KYC Form



KYC Profile Form

1. Name of the Client :
2. Father's Name :
3. Mother's Name :
4. Date of Birth :
5. Occupation
6. Official Address (If available)
7. Present Address :
8. Permanent Address :
9. Mobile No. :
10. Purpose of Transaction
11. Bank Account Information (If available)
    a. Bank Name
    b. Branch
    c. Account No.
12. Introducer Information
    a. Name
    b. Address
    c. Occupation
    d. Mobile no.
13. Attachment (Any of the under mentioned)
    a. Copy of National ID Card
    b. Copy of Citizenship Certificate
    c. Copy of Driving License/ Passport etc.

PHOTOGRAPH
(Passport size)

Prepared by

Approved by

(Ref: Para-10.6.2)