# INFORMATION AND COMMUNICATION TECHNOLOGY SECURITY POLICY

**Version: 2.0**

# BANGLADESH KRISHI BANK

## Information and Communication Technology Division

**Head Office, Dhaka-1000**

**June 2021**

*For Office use only*

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

**Information and Communication Technology Security Policy**
**June 2021**

## *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 and secure use of ICT services and resources.*

*In view of the above, Bangladesh Krishi Bank has already set up an Information Technology platform for its branches and offices. The bank gradually implementing its vision to expand and modernize the ICT platform and information systems by following the regulatory compliance. With the developments of computerization and fintech in banking operation, 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 Division of the bank has prepared a book titled "Information and Communication Technology Security Policy-2021, Version 2.0" in accordance with the guideline given by Bangladesh Bank, relating the bank's operation. The book contains the policies applicable to ICT Management, ICT Operation Management, Information System Physical Security, Information Security Standard, Business Continuity, Data Center, Disaster Recovery Site, ATM, Digital Banking Apps, Procurement & Service Management etc. Moreover 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 for the **Information and Communication Technology (ICT) Security Policy-2021, Version 2.0** at 783th Board meeting held on 20-01-2021.*

*All the bank personnel specially the Division Heads, Region Heads, Audit office Heads & Branch Managers as well as Head Office personnel must keep themselves well aware and conversant with the contents of this policy and will disseminate all the subordinate employees about the purpose and contents of this policy. Besides that all the BKB personnel must follow the policy meticulously keeping in mind the growing risks and security issues while working in ICT System and Operation.*

*(Md. Ali Hossain Prodhania)*
*Managing Director*

*Dated: June 2021*
*Dhaka*

# Table of Contents

CHAPTER 1

**1. Introduction.......... 7-11**

1.1 Background.......... 8

1.2 Objectives of the policy.......... 9

1.3 Applicability of the Policy.......... 10

1.4 Automation of Branch Banking Operations.......... 10

1.4.1 First Phase.......... 10

1.4.2 Second and Third Phase.......... 10

1.4.3 Fourth and Fifth Phase 11

1.4.4 Six Phase.......... 11

CHAPTER 2

**2. ICT Security Management.......... 12-17**

2.1 Roles and Responsibilities.......... 12

2.1.1 Roles and responsibilities of Board of Directors.......... 12

2.1.2 Formation of ICT Steering Committee.......... 13

2.1.3 Formation of ICT Security Committee & ICT Risk Management Committee.......... 14

2.2 ICT Policy, Standard and Procedure.......... 15

2.3 Documentation.......... 15

2.4 Internal Information System Audit.......... 16

2.5 External Information System Audit.......... 16

2.6 Standard Certification.......... 16

2.7 Security Awareness and Training.......... 17

2.8 Insurance or Risk Coverage Fund and Depreciation.......... 17

CHAPTER 3

**3. ICT Risk Management.......... 18-20**

3.1 ICT Risk Governance.......... 18

3.2 ICT Risk Assessment.......... 19

3.3 ICT Risk Response.......... 20

CHAPTER 4

**4. ICT Service Delivery Management.......... 21-24**

4.1 Change Management.......... 21

4.2 Incident Management.......... 21

4.3 Problem Management.......... 23

4.4 Capacity Management.......... 24

CHAPTER 5

**5. Infrastructure Security Management.......... 25-44**

5.1 Asset Management.......... 25

5.2 Disposal Management.......... 26

5.3 Desktop/Laptop Devices Controls.......... 27

5.4 BYOD Controls.......... 28

5.5 Server Security Controls.......... 29

5.6 Data Center and Disaster Recovery Site Controls.......... 30

5.6.1 Physical Security........................................................................................................ 30
5.6.2 Environmental Security........................................................................................... 31
5.6.3 Fire Prevention........................................................................................................ 32
5.7 Server/Network Room/Rack Controls.................................................................................. 32
5.8 Networks Security Management.......................................................................................... 33
5.9 Cyber Security Management................................................................................................ 34
5.9.1 Prevention of Cyber-attacks..................................................................................... 34
5.10 Cryptography...................................................................................................................... 35
5.11 Malicious Code Protection.................................................................................................. 36
5.12 Internet Access Management............................................................................................... 37
5.13 Email Management............................................................................................................. 37
5.14 CBS Management............................................................................................................... 39
5.15 Vulnerability Assessment and Penetration Testing............................................................. 40
5.16 Patch Management.............................................................................................................. 41
5.17 Security Monitoring............................................................................................................ 41
5.18 Security Controls for Operating System.............................................................................. 41
5.19 Security Controls for Database............................................................................................ 42
5.19.1 Physical Access Control & Personnel Security.................................................... 42
5.19.2 Installation and Configuration Security.................................................................. 42
5.19.3 Networking Security............................................................................................... 43
5.20 Computerized Branch Management..................................................................................... 43
5.21 Sharing Resources............................................................................................................... 44
5.22 Log Reports......................................................................................................................... 44

## CHAPTER 6

**6. Access Control of Information System.................................................................................. 45-47**
6.1 User Access Management..................................................................................................... 45
6.2 Password Management......................................................................................................... 45
6.3 Input Control........................................................................................................................ 46
6.4 Privileged Access Management............................................................................................ 46
6.5 Remote Access..................................................................................................................... 47

## CHAPTER 7

**7. Business Continuity and Disaster Recovery Management.......................................................... 48-52**
7.1 Business Continuity Plan (BCP)............................................................................................ 48
7.2 Developing a Business Continuity Plan................................................................................. 49
7.3 Disaster Recovery Plan (DRP)............................................................................................... 50
7.4 Data Backup and Restore Management................................................................................. 51

## CHAPTER 8

**8. Acquisition and Development of Information Systems.............................................................. 53-55**
8.1 ICT Project Management...................................................................................................... 53
8.2 Vendor Selection for System Acquisition.............................................................................. 53
8.3 In-house Software Development........................................................................................... 54
8.4 Software Documentation....................................................................................................... 54

8.5 Statutory Requirements........................................................................................................ 55

## CHAPTER 9

**9. Alternative Delivery Channels (ADC) Security Management............................................................ 56-62**

9.1 ATM/POS Transactions........................................................................................................ 56

9.2 Internet Banking........................................................................................................ 58

9.3 Payment Cards........................................................................................................ 59

9.4 Mobile Financial Services & Mobile Apps........................................................................................ 60

9.4.1 Mobile Financial Services........................................................................................ 60

9.4.2 Mobile Apps........................................................................................................ 61

## CHAPTER 10

**10. Service Provider Management........................................................................................................ 63-65**

10.1 Outsourcing........................................................................................................ 63

10.2 Service Level Agreement ........................................................................................................ 64

10.3 Selection of Service Provider........................................................................................................ 64

10.4 Cross-border System Support........................................................................................................ 65

## CHAPTER 11

**11. Customer Education........................................................................................................ 66-67**

11.1 Awareness Program........................................................................................................ 66

11.2 Security........................................................................................................ 67

11.3 Penalties........................................................................................................ 67

11.4 User Compliance........................................................................................................ 67

**GLOSSARY AND ACRONYMS........................................................................................ 68-69**

**ICT Forms........................................................................................................ 70-82**

# Chapter 1

## 1. Introduction

Bangladesh Krishi Bank, the largest Specialized Bank of the country, was established under the President Order No. 27 of 1973 to finance the climate-dependent uncertain and risky agriculture sector.

Nowadays Information and Communication Technology (ICT) is a key driver for socio-economic progress and development. Promotion of ICT in various sectors of the economy is, therefore, fundamental to ensuring greater welfare of the society through efficient delivery of services. However, it is extremely important to establish transparency in the service delivery systems to make them open and visible. This is even more important in the Banking sector because Banks deliver services to their clients by creating products designed to suit specific needs. In addition, the significant volume of information that Banking services generate requires speedier processing, storage, retrieval and dissemination for operational efficiency. To cope with these demands and to stay relevant with the pace of changes in the Banking landscape, a migration to systems driven by ICT is inevitable.

Given the level of ICT penetration in the Banking sector, it is essential that the systems developed over time are sustained, properly managed and protected from misuse and unauthorized access. This calls for a consistent policy to guide actions required to develop and upgrade ICT in Banking business environment.

This document formulates the ICT security policy of Bangladesh Krishi Bank (BKB) which covers all computing and communications facilities including all hardware, data, software, networks, facilities and environment associated with information resources. The document also explains the background and constraints within which the current ICT systems were developed and presents the future built upon the experience of the past.

This policy is in line with the ICT guidelines issued by Bangladesh Bank for scheduled Banks and Financial Institutions. It is supplemented by all other Banks policies and by the policies of those networks to which the Bank is interconnected, including applicable government laws regarding information technology.

## 1.1 Background

1.1.1 Bangladesh Krishi Bank has entered into the arena of Information and Communication Technology to meet the demand of time and is making every endeavor 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. 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 with sanction, real time Banking and use of modern communication technologies for Banking up with the changing scenario of the Banking environment like speedy money train services etc. the Bank has changed its **IT** Department's name as **ICT** (Information and Communication Technology) Department in August 2013. Thereafter in 2016 it is turned into ICT Division comprising 3 different departments ICT Operation, ICT Systems and Card & Mobile Banking Department.

1.1.2 Bangladesh Krishi Bank has grown significantly over the years in branch automation Meanwhile BKB has introduced online Banking. Till date 1038 branches are computerized in order to provide various modern Banking facilities. Meanwhile all the branches of the Bank are being operated centralized Core Banking solution (CBS) through own Data Center (DC) and Disaster Recovery Site (DRS).

1.1.3 All branches including Regional offices, Chief Regional offices, Regional Audit Offices, Divisional Offices and Divisional Audit Offices of the Bank have been using computers to perform day-to-day activities and are connected with Internet. Foreign remittance can be disbursed to the beneficiaries instantly through the web based solution of Money gram, Western union, Xpress Money, Ria Money Transfer, Transfast etc. Also all circulars, memo, letters, reports are being transmitted over internet. Besides these, Bangladesh Electronic Fund Transfer Network (BEFTN) is also being used in all branches for transferring foreign remittance as well as local remittance.

1.1.4 Bangladesh Automated Cheque Processing System (BACPS) under Bangladesh Automated Clearing House (BACH) has been implemented successfully in BKB.

1.1.5 A web based software-Integrated MIS has been developed related to Statement of Affairs and Profit & Loss statement from each branch under them where consolidated statements as well as various MIS reports are prepared. SWIFT Service is available in 16 AD (Authorized Dealer) branches of the Bank to facilitate foreign trade operations that include quick disposal of LC's, foreign remittances etc. Moreover Bank has successfully implemented online CIB System in line with Bangladesh Bank's payment system automation program. The Bank has introduced e-GP (Electronic Government procurement) service to facilitate e-tendering introduced by the Government.

1.1.6 Bangladesh Krishi Bank has introduced ATM services for its customers since 2013. ATM card holders can withdraw cash from 08(Eight) own ATM booths (in own premises) located at different places of the country. Furthermore Bank customers can withdraw cash from more than 5000 ATM booths under NPSB (National Payment Switch Bangladesh) powered by Bangladesh Bank.

1.1.7 Bangladesh Krishi Bank has its own website (**www.krishibank.org.bd**) with updated information of the Bank. The Bank also has its own mail solution to provide e-mail facilities to concerned officials of the Bank.

1.1.9 While formulating the policies, applicability as defined in Bangladesh Bank ICT Guidelines for scheduled Banks and Financial Institutions were taken into account.

## 1.2 Objectives of the policy

This policy defines minimum control requirements to which the Bank must adhere. The primary objectives of the guidelines are:

-To ensure a dependable Information Communication System for efficient management;

-To promote and facilitate wide spread use of ICT in all Banking operations;

-To use ICT to ensure enhanced efficiency in service delivery to the clients;

-To develop a large pool of trained ICT manpower to manage and sustain the systems currently in place and to be developed in future;

-To install appropriate safeguards against unauthorized access to the systems;

-To ensure protection of all ICT infrastructures and assets from any misuse and disaster;

-To establish a standard ICT security Policy & ICT security management;

-To help the Bank for secured and stable setup of its ICT platform;

-To establish a secure environment for data processing;

-To identify information security risks and their management;

-To communicate the responsibilities for the protection of information;

-Prioritize information and information systems that are to be protected;

-User awareness and training regarding information security;

-To ensure the best practices (industry standard) of the usage of ICT that is not Limited to this guideline.

## 1.3 Applicability of the Policy

This ICT Security policy is a systematic approach of controls to policies required to be formulated for ensuring security of information and ICT systems. This Guideline covers all information that are electronically generated, received, stored, replicated, printed, scanned and manually prepared. The provisions of this Guideline are applicable for:

**a)** A Bank for all of their Information Systems.

**b)** All activities and operations required to ensure data security including facility design, physical security, application security, network security, ICT risk management, project management, infrastructure security management, service delivery management, disaster recovery and business continuity management, alternative delivery channels management, acquisition and development of information systems, usage of hardware, software and network, disposal policy and protection of copyrights and other intellectual property rights.

## 1.4 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 had 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 six phases which are as follows:

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

- **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.

- **Head Office:** The secretariat of the honorable 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.

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

**1.4.2 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 standalone 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.

**1.4.3 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 fully fledged operation is running. Core Banking Software has also been established. CBS is being implemented in various branches. Up to 31-12-2018 Bangladesh Krishi Bank have run 381 branches under CBS( Core Banking Solution). 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.

1.4.4 **Sixth Phase:** Meanwhile all the 1038 branches of BKB are being operated under Core Banking Solution (CBS). At the moment Bank is working with the vision to integrate various solutions and services like Remittance, BACH, Utility bills Collection etc with Core Banking Solution. ICT Division is working relentlessly to implement the solutions & services. Beside that we are on the verge of launching "BKB APPs"-Digital Banking APP to introduce a new experience.

# Chapter-2

## 2. ICT Security Management

ICT Security Management shall ensure that the ICT functions and operations are efficiently and effectively managed. ICT Security Management deals with Roles and Responsibilities, ICT Security Policy, Documentation, Internal and External Information System Audit, Training and Awareness, Insurance or Risk coverage fund. They have to ensure maintenance of appropriate systems documentations, particularly for systems, which support financial transactions and reporting and will ensure that the following roles and responsibilities are done as per ICT Security Policy:

**a)** Overall Management of the ICT operation.

**b)** To recognize opportunities and risks of possible abuses.

**c)** To be aware of the capabilities of ICT.

**d)** To contribute in ICT security planning to ensure that resources are allocated consistent with business objectives and to ensure that sufficient and qualified technical staffs are employed so that continuance of the ICT operation area is unlikely to be seriously at risk.

**e)** Supervision of software, network communication & hardware operation and their maintenance.

**f)** To provide ICT Security solutions to meet business objectives.

**g)** Contact with 3rd party vendors to finalize the deal of purchase and maintenance/ Service Level Agreement (SLA).

**h)** Monitoring the implementation status of ICT Security Policies.

**i)** Development of the various ICT related policies as per Bangladesh Bank Circular as when required.

**j)** Compliance of issues raised by external and/or internal ICT auditor.

**k)** Testing of Disaster Recovery Site (DRS) & Business Continuity Plan (BCP).

**l)** Strategic planning for development, training and up-gradation of ICT systems in Bank.

### 2.1 Roles and Responsibilities

Well-defined roles and responsibilities of Board and Senior Management are critical while implementing ICT Governance but clearly-defined roles enable effective project control and expectations of organizations. ICT Governance stakeholders include Board of Directors, Managing Director, ICT Steering Committee, ICT Security Committee & Risk Management Committee, Chief Risk Officer and Business Executives.

### 2.1.1 Roles and responsibilities of Board of Directors

**a)** Approving ICT strategy and policy documents.

**b)** Ensuring that the management has placed an effective planning process.

**c)** Ensuring that the ICT strategy is indeed aligned with business strategy.

**d)** Ensuring that the ICT organizational structure complements the business model and its direction.

**e)** Ensuring ICT investments represent a balance of risks and benefits and acceptable budgets.

**f)** Ensure compliance status of ICT Security Policy.

### 2.1.2 Formation of ICT Steering Committee

2.1.2.1 ICT Steering Committee shall be formed with following representatives:

| Sl | Designation | Organization/Department | Position |
|---|---|---|---|
| 1. | Deputy Managing Director | Bangladesh Krishi Bank | Chairperson |
| 2. | General Manager | Planning & Operation Division | Member |
| 3. | General Manager | ICT Division | Member |
| 4. | General Manager | Audit & Inspection Division | |
| 5. | Deputy General Manager | ICT Operations Department | Member |
| 6. | Deputy General Manager | ICT Systems, Card & Mobile Banking Department | Member |
| 7. | Deputy General Manager | Risk Department | Member |
| 8. | Deputy General Manager | ICC Department | Member |
| 9. | Deputy General Manager | Audit Department | Member |
| 10. | Deputy General Manager | Law Department | Member |
| 11. | Deputy General Manager | BCBD Department | Member |

2.1.2.2 This ICT Steering Committee shall have following responsibilities:

**a)** Monitor management methods to determine and achieve strategic goals.

**b)** Aware about exposure towards ICT risks and controls.

**c)** Provide guidance related to risk, funding, or sourcing.

**d)** Ensure project priorities and assessing feasibility for ICT proposals.

**e)** Ensure that all critical projects have a component for “project risk management”.

**f)** Consult and advice on the selection of technology within standards.

**g)** Ensure that vulnerability assessments of new technology is performed.

**h)** Ensure compliance to regulatory and statutory requirements.

**i)** Provide direction to architecture design and ensure that the ICT architecture reflects the need for legislative and regulatory compliance.

### 2.1.3 Formation of ICT Security Committee & ICT Risk Management Committee

2.1.3.1 **ICT Security Committee & ICT Risk Management Committee** should be formed with following form:

| Sl | Designation | Organization/Department | Position |
|---|---|---|---|
| 1. | Deputy Managing Director | Bangladesh Krishi Bank | Chairperson |
| 2. | General Manager | Operation Division | Member |
| 3. | General Manager | ICT Division | Member |
| 4. | Deputy General Manager | ICT Operations Department | Member |
| 5. | Deputy General Manager | ICT Systems, Card & Mobile Banking Department | Member |
| 6. | Assistant General Manager | ICT Systems, Card & Mobile Banking Department | Member |
| 7. | Senior System Analyst | ICT Operations Department | Member |
| 8. | Assistant System Analyst/ Senior Principal Officer/ Programmer/ Principal Officer | ICT Systems, Card & Mobile Banking Department | Member |
| 9. | Programmer | ICT Systems, Card & Mobile Banking Department | Member Secretary |

(The committee can co-opt any other members as per requirement)

2.1.3.2 **This ICT Security Committee & ICT Risk Management Committee** shall have following responsibilities:

**a)** Ensure development and implementation of ICT security objectives, ICT security related policies and procedures.

**b)** To detect ICT related 'Risk' and take initiative to prevent it.

**c)** Giving advice for compliance of ICT Risk Governance, ICT Risk Assessment, ICT Risk Response.

**d)** To advise about the compliance of ICT operation and infrastructure security management.

**e)** Monitoring about the compliance of ICT goods and service related management.

**f)** To advise the compliance of acquisition and development of Information System.

**g)** To suggest the compliance of Business Continuity Plan (BCP) for ICT, Disaster Management Policy (DMP) and Alternate Delivery Channel.

**h)** Provide ongoing management support to the Information security processes.

**i)** Ensure continued compliance with the business objectives, regulatory and legal requirements related to ICT security.

**j)** Support to formulate ICT risk management framework/process and to establish acceptable ICT risk thresholds/ICT risk apatite and assurance requirements.

**k)** Periodic review and provide approval for modification in ICT Security processes.

## 2.2 ICT Policy, Standard and Procedure

2.2.1 This ICT Security Policy will:

**a.** Provide guideline of secure usage of common technologies such as computers and peripherals, data and network, applications and other specialized ICT resources.

**b.** Adopt appropriate controls to protect its information system.

**c.** Continuous awareness and training program for each level of staff and stakeholders about ICT Security shall be ensured by Senior Management.

**d.** Update the policy regular basis to deal with evolving changes in the ICT environment both within the Bank and overall industry as and when required.

**e.** Ensure engaging ICT security professional employed in separate ICT security department/unit/cell for improved and impartial dealing with security incidents, policy documentation, inherent ICT risks, risk treatments and other relevant activities.

**f.** This policy must comply with the 'ICT Security Guidelines' provided by Bangladesh Bank and must be approved by the board.

2.2.2 For noncompliance issues, compliance plan shall be submitted to Bangladesh Bank for taking dispensation as per format provided in **ICTF-11**. Dispensation shall be for a specific period of time.

## 2.3 Documentation

2.3.1 ICT division shall have approved organogram structure.

2.3.2 Branch shall have maintained ICT support unit/section/personnel (Business/ICT) as per organogram.

2.3.3 Each individual within ICT department/division/unit/section/DC/DRS/Branch shall have approved Job Description (JD) with fallback resource person.

2.3.4 The concerned department/controlling office/branch shall be maintained segregation of duties for ICT tasks.

2.3.5 Prescheduled roster for sensitive ICT tasks (e.g. Data Center & DRS maintenance, EOD operation, Network Monitoring, Security Guard for Data Center, ATM Monitoring, etc.) must be ensured.

2.3.6 The concerned department shall maintain detailed design document for all ICT critical systems/services (e.g. Data Center design, Network design, Power Layout for Data Center, etc.).

2.3.7 The concerned department shall be updated "*Operating Procedure"* for all ICT functional activities (e.g. Backup Management, Database Management, Network Management, Scheduling Processes, System Start-up, Shut-down, Restart and Recovery).

2.3.8 Approved relevant requisition/acknowledgement forms shall be used for different ICT request/operation/services.

2.3.9 User Manual of all applications for internal/external users shall be prepared.

## 2.4 Internal Information System Audit

2.4.1 Internal Information System (IS) audit shall be accomplished by Audit Department (Other than ICT Division).

2.4.2 Internal IS audit shall be conducted by adequate IS Audit expertise and skilled personnel. Certified IS auditor along with adequate audit experience in this area of technology should be given preference.

2.4.3 Computer-Assisted-Auditing Tools (CAATs) shall be used to perform IS audit planning, monitoring/auditing, control assessment, data extraction/analysis, fraud detection/prevention and management.

2.4.4 Critical/major technology-based services/processes and ICT infrastructure including operational branches shall be emphasized on annual system audit plan.

2.4.5 Internal Information System audit shall be done periodically at least once a year. The report must be preserved for regulators as and when required.

2.4.6 Audit issues are properly tracked and, in particular, completely recorded, adequately followed up and satisfactorily rectified.

2.4.7 The Bank/branch shall take appropriate measures to address the recommendations made in the last Audit Report (external/internal). This must be documented and kept along with the Audit Report mentioned in above.

## 2.5 External Information System Audit

2.5.1 External auditor(s) shall be engage for their information systems auditing in-line with their regular financial audit.

2.5.2 The audit report shall be preserved for regulators as and when required.

## 2.6 STANDARD CERTIFICATION

**2.6.1** BKB may take initiative for certification process related to Bank’s Information System Security, Quality of ICT Service Delivery, Business Continuity Management, Data Center Management, Payment Card Data Security etc.

## 2.7 SECURITY AWARENESS AND TRAINING

2.7.1 As technology evolves rapidly, the concerned department shall ensure that all relevant personnel are getting proper training, education, updates and awareness of the ICT security activities as relevant with their job function.

2.7.2 The minimum level of Business Foundation Training shall be given to all ICT personnel.

2.7.3 Arrangement of security awareness training/workshop for all staff shall be done time to time.

2.7.4 Adequate training/awareness facilities shall be ensured for IS Audit team considering any new Banking services and technological changes.

2.7.5 To keep updated changing environment, training shall be conducted in the light of ICT Operations, Core Banking System (CBS), Card Operations and other related cells.

2.7.6 Training programs shall be planned for staffs and executives of branches and various controlling offices related to cyber security, importance & awareness of ICT operation and activities.

## 2.8 Insurance or Risk Coverage Fund and Depreciation

2.8.1 Most of the ICT assets of the Bank are purchased with comprehensive warranty. Bank’s ICT equipment is kept in secured location. The Bank enjoys maintenance support under warranty and has maintenance contract with the vendors for mission critical system used by the Bank. Again for hardware insurance, the Bank may look for an insurance company who can provide insurance against data loss.

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

2.8.3 The risk coverage fund shall be maintained properly in the accounting system of Bank.

2.8.4 There shall have a clear policy to use risk coverage fund at necessity if it is maintained.

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

# Chapter 3

## 3. ICT Risk Management

ICT risk is a component of the overall risk universe of an enterprise. Bank faces other risks like Strategic risk, Environmental risk, Market risk, Credit risk, Operational risk, Compliance risk, etc. In many enterprises, ICT related risk is considered to be a component of operational risk. However, even strategic risk can have an ICT component itself, especially where ICT is the key enabler of new business initiatives. The same applies for credit risk, where poor ICT security can lead to lower credit ratings. It is better not to depict ICT risk with a hierarchic dependency on one of the other risk categories.

ICT risk is business risk-specifically, the business risk associated with the use, ownership, operation, involvement, influence and adoption of ICT within Bangladesh Krishi Bank. It consists of ICT related events and conditions that could potentially impact the business. It can occur with both uncertain frequency and magnitude and it creates challenges in meeting strategic goals and objectives.

The Bank should establish risk management system for any new processes and system as well as a post-launch review which shall include description and assessment of identifiable risks and remedial plans approved by appropriate authority.

### 3.1 ICT Risk Governance

3.1.1 BKB shall form an ICT Risk Management Committee to govern overall ICT risks and relevant mitigation measures.

3.1.2 BKB shall define the *Risk Appetite* (amount of risk the Bank is prepared to accept to achieve its' objectives) in terms of combinations of frequency and magnitude of a risk to absorb loss e.g., financial loss, reputation damage.

3.1.3 BKB shall define the *Risk Tolerance* (tolerable deviation from the level set by the risk appetite definition) having approval from the board/Risk Management Committee and clearly communicated to all stakeholders.

3.1.4 BKB shall review and approve risk appetite and tolerance change over time; especially for new technology, new organizational structure, new business strategy and other factors require the enterprise to reassess its risk portfolio at a regular interval.

3.1.5 BKB shall define the risk responsibilities to individuals for ensuring successful completion.

3.1.6 BKB shall define the risk accountability applied to those who owned the required resources and have the authority to approve the execution and/or accept the outcome of an activity within specific ICT Risk processes. Ownership of risk stays with owner or custodian whoever is in better position to mitigate the identified risk for that specific ICT asset.

3.1.7 BKB shall acknowledge all risks by *Risk Awareness* so that those are well understood and known and recognized as the means to manage them.

3.1.8 BKB shall contribute to executive management's understanding of the actual exposure to ICT risk by *Open Communication,* enabling definition of appropriate and informed risk responses.

3.1.9 BKB shall aware amongst all internal stakeholders of the importance of integrating risk and opportunity in their daily duties.

3.1.10 BKB shall be transparent to external stakeholders regarding the actual level of risk and risk management processes in use.

3.1.11 BKB shall begin *Risk-aware Culture* from the top with board and executives, who set direction, communicate risk-aware decision making and reward effective risk management behaviors.

3.1.12 ICT systems, Card & Mobile Banking Department and ICT Operation Department shall report status of identified ICT security risk to the ICT security committee and Risk Management Committee periodically (Half Yearly) or as when required.

## 3.2 ICT Risk Assessment

Meaningful ICT risk assessments and risk-based decisions require ICT risks to be expressed in unambiguous and clear, business-relevant terms. Effective risk management requires mutual understanding between ICT and the business over which risk needs to be managed. All stakeholders must have the ability to understand and express how adverse events may affect business objectives.

**a)** An ICT person shall understand how ICT-related failures or events can impact enterprise objectives and cause direct or indirect loss to the enterprise.

**b)** A business person shall understand how ICT-related failures or events can affect key services and processes.

3.2.1 BKB shall establish business impact analysis needs to understand the effects of adverse events. Bank may practice several techniques and options that can help them to describe ICT risks in business terms.

3.2.2 BKB shall practice the development and use of *Risk Scenarios* technique to identify the important and relevant risks amongst all. The developed risk scenarios can be used during risk analysis where frequency and impact of the scenario are assessed.

3.2.3 BKB shall define *Risk Factors* those influence the frequency and/or business impact of risk scenarios.

3.2.4 BKB shall interpret risk factors as casual factors of the scenario that is materializing, or as vulnerabilities or weaknesses.

3.2.5 ICT systems, Card & Mobile Banking Department and ICT operation Department conduct periodic ICT risk assessment of ICT related assets (process and system) and provide recommendation to risk owners for mitigation.

## 3.3 ICT Risk Response

Risk response is to bring measured risk in line with the defined risk tolerance level for the organization. In other words, a response needs to be defined such that as much future residual risk as possible (usually depending on budgets available) falls within risk tolerance limits. When the analysis shows risks deviating from the defined tolerance levels, a response needs to be defined. This response can be any of the four possible ways such as Risk Avoidance, Risk Reduction/Mitigation, Risk Sharing/Transfer and Risk Acceptance.

3.3.1 BKB shall develop a set of metrics to serve as risk indicators. Indicators for risks with high business impact are most likely to be *Key Risk Indicators (KRIs).*

3.3.2 BKB shall give effort to implement, measure and report different indicators that are equivalent in sensitivity.

3.3.3 Selection of the right set of KRIs, Bank shall carry out:

**a)** Provide an early warning for a high risk to take proactive action.

**b)** Provide a backward-looking view on risk events that have occurred.

**c)** Enable the documentation and analysis of trends.

**d)** Provide an indication of the risk’s appetite and tolerance through metric setting.

**e)** Increase the likelihood of achieving the strategic objectives.

**f)** Assist in continually optimizing the risk governance and management environment.

3.3.4 BKB shall define risk response to bring risk in line with the defined risk appetite for the Bank after risk analysis.

3.3.5 BKB shall strengthen overall ICT risk management practices with sufficient risk management processes.

3.3.6 BKB shall introduce a number of control measures intended to reduce either of an adverse event and/or the business impact of an event.

3.3.7 BKB shall share or reduce risk frequency or impact by transferring or otherwise sharing a portion of the risk, e.g. insurance, outsourcing.

# Chapter 4

## 4. ICT Service Delivery Management

ICT Service Management covers the dynamics of technology operation management that includes capacity management, request management, change management, incident and problem management etc. The objective is to set controls to achieve the highest level of ICT service quality by minimum operational risk.

### 4.1 Change Management

4.1.1 Changes to information processing facilities and systems shall be controlled. A sample document form has been provided in **ICTF- 1.**

4.1.2 Bank shall prepare Business Requirement Document (BRD) which will cover the requirements of system changes and the impact that will have on business processes, security matrix, reporting, interfaces, etc.

4.1.3 All changes of business application implemented in the production environment must be governed by a formal documented process with necessary change details.

4.1.4 Audit trails shall be maintained for business applications.

4.1.5 The Concerned department shall prepare rollback plan for unexpected situation.

4.1.6 User Acceptance Test (UAT) for changes and upgrades in application shall be carried out before deployment. A sample form for UAT has been given in **ICTF-2.** This document should be preserved for ready reference.

4.1.7 User Verification Test (UVT) for post deployment may be carried out.

### 4.2 Incident Management

An incident occurs when there is an unexpected disruption to the standard delivery of ICT services. Bank shall appropriately manage such incidents to avoid a situation of mishandling that result in a prolonged disruption of ICT services.

4.2.1 BKB shall establish an incident management framework with the objective of restoring normal ICT service as quickly as possible following the incident with minimal impact to the business operations. The Bank shall also establish roles and responsibilities of staff involved in the incident management process, which includes recording, analyzing, remediating and monitoring incidents. Before the delivery of any ICT service a formal request process must be established. A sample Request Form has been provided in **ICTF- 4.**

4.2.2 It is important that incidents are accorded with the appropriate severity level. As part of incident analysis, the Bank may delegate the function of determining and assigning incident severity levels to a technical helpdesk function. The Bank shall train helpdesk staff to determine incidents of high severity level. In addition, criteria used for assessing severity levels of incidents shall be established and documented.

4.2.3 BKB shall establish corresponding escalation and resolution procedures where the resolution timeframe is proportionate with the severity level of the incident.

4.2.4 The predetermined escalation and response plan for security incidents shall be tested on a periodic basis.

4.2.5 BKB shall form an ICT Emergency Response Team, comprising staff within the Bank with necessary technical and operational skills to handle major incidents.

4.2.6 In some situations, major incidents may further develop adversely into a crisis. Senior management shall be kept apprised of the development of these incidents so that the decision to activate the disaster recovery plan can be made on a timely basis. Bank shall inform Bangladesh Bank as soon as possible in the event that a critical system has failed over to its disaster recovery system.

4.2.7 BKB shall keep customers informed of any major incident. Being able to maintain customer confidence throughout a crisis or an emergency situation is of great importance to the reputation and soundness of the Bank.

4.2.8 As incidents may trail from numerous factors, Bank shall perform a root-cause and impact analysis for major incidents which result in severe disruption of ICT services. BKB shall take remediation actions to prevent the recurrence of similar incidents.

4.2.9 The root-cause and impact analysis report shall cover following areas:

**a)** Root Cause Analysis

- **i.** When did it happen?
- **ii.** Where did it happen?
- **iii.** Why and how did the incident happen?
- **iv.** How often had a similar incident occurred over last 2 years?
- **v.** What lessons were learnt from this incident?

**b)** Impact Analysis

- **i.** Extent of the incident including information on the systems, resources, customers that were affected;

**ii.** Magnitude of the incident including foregone revenue, losses, costs, investments, number of customers affected, implications, consequences to reputation and confidence;

**iii.** Breach of regulatory requirements and conditions as a result of the incident.

**c)** Corrective and Preventive Measures

**i.** Immediate corrective action to be taken to address consequences of the incident. Priority shall be placed on addressing customers' concerns.

**ii.** Measures to address the root cause of the incident.

**iii.** Measures to prevent similar or related incidents from occurring.

4.2.10 BKB shall adequately address all incidents within corresponding resolution timeframes and monitor all incidents to their resolution.

## 4.3 Problem Management

4.3.1 BKB shall establish a process to log the information system related problems.

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

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

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

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

4.3.6 Ensure necessary corrective action within the time frame bounded by the severity of the problem.

4.3.7 Provide remote systems problems information to specific support units and Regional Help Desks & Support Teams

4.3.8 Provide time-to-time communication support to remote support units.

4.3.9 Ensure Virus detection & eradication at all levels of hardware.

4.3.10 Establish Log-on administration and synchronization across servers and applications.

4.3.11 Ensure efficient administration of user ID's for network applications and tools.

4.3.12 Keep records of all users using the system access created by the vendor/ system administrator.

4.3.13 Ensure safe keeping of Super user passwords in separate locations.

4.3.14 Ensure periodic virus scans for PC / Server to monitor for virus propagation & perform virus detection and eradication.

4.3.15 Provide updated information to all types of users by circular / letter regarding methods to prevent or handle possible virus attack.

4.3.16 Maintain controls to protect printed outputs and portable storage media (tapes & disk packs) from unauthorized access.

## 4.4 Capacity Management

The goal of capacity management is to ensure that ICT capacity meets current and future business requirements in a cost-effective manner.

4.4.1 To ensure that ICT systems and infrastructure are able to support business functions, the Bank shall ensure that indicators such as performance, capacity and utilization are monitored and reviewed.

4.4.2 BKB shall establish monitoring processes and implement appropriate thresholds to plan and determine additional resources to meet operational and business requirements effectively.

# Chapter 5

## 5. Infrastructure Security Management

The ICT landscape is vulnerable to various forms of attacks. The frequency and malignancy of such attacks are increasing. It is imperative that Bank implements security solutions at the data, application, database, operating systems and networks to adequately address related threats. Appropriate measures shall be implemented to protect sensitive or confidential information such as customer personal information, account and transaction data which are stored and processed in systems. Customers shall be properly authenticated before access to online transactions, sensitive personal or account information.

### 5.1 Asset Management

5.1.1 Prior to procuring any new ICT assets, compatibility assessment (with existing system) shall be performed by the Bank.

5.1.2 All ICT assets procurement shall be complied with the government procurement policy as well as the Bank.

5.1.3 Each ICT assets shall be assigned to a custodian (an individual or entity) who will be responsible for the development, maintenance, usage, security and integrity of that asset.

5.1.4 All ICT assets shall be clearly identified and labeled. Labeling shall reflect the established classification of assets.

5.1.5 BKB shall maintain an ICT asset inventory stating significant details (e.g. owner, custodian, purchase date, location, license/serial number, configuration, etc.). A sample form has been provided in **ICTF-3**. A record of this review must be maintained.

5.1.6 BKB shall review and update the ICT asset inventory periodically.

5.1.7 Information system assets shall be adequately protected from unauthorized access, misuse or fraudulent modification, insertion, deletion, substitution, suppression or disclosure.

5.1.8 BKB shall establish a *Disposal Policy* for information system asset protection. All data on equipment and associated storage media must be destroyed or overwritten before sale, disposal or re-issue.

5.1.9 BKB shall provide guidelines for the use of portable devices, especially for the usage at outside premises.

5.1.10 BKB shall provide policy to return back organizational assets from employees/external parties upon termination of their employment, contract or agreement.

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

5.1.12 Outsourced software used in production environment shall be subjected to support agreement with the vendor.

5.1.13 BKB shall approve list of Software which will only be used in any computer.

5.1.14 Use of unauthorized or pirated software must strictly be prohibited throughout the Bank.

5.1.15 All the branches and offices of the Bank have to maintain the stock registers of hardware and software, password change registers, troubleshooting registers of hardware / software, back up protection registers (for offline branch) from the next 5/8/16.

## 5.2 Disposal Management

"Disposal" refers to the reselling, reassignment, recycling, donating or throwing out of IT equipment through responsible, ethical and environmentally sound means.

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.

IT assets and resources (i.e. desktop computers, servers, databases, Network equipments & accessories, all kinds of back-up or storage devices etc.) must be discarded if those are obsolete, spoiled or non repairable (Market value under 1 tk) according to legal requirements/ retention policy and environmental regulations.

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

**a)** Sold in a public forum.

**b)** Auctioned through online/ Paper Advertisement/Notice board.

**c)** Reassigned to a less-critical business operation function.

**d)** Discarded as rubbish in a landfill after sanitization of toxic materials by an approved service provider as required by local or National regulations.

### 5.2.1 PROCEDURE

Approved **Condemnation Committee** of the concerned departments of Head Office or Divisional Offices will, at first, collect the information of the obsolete Hardware and peripherals from different departments of Head office, Divisional Offices, Divisional Audit Offices, Chief Regional Offices, Regional Offices and branches of the Bank. Then the committee will scrutinize the details information of the equipment and identify them identically with their brand name, model, serial number, quantity (location wise), book value, condition etc. The committee then made their recommendation to the management for approval. After getting approval from the management, the goods will be disposed off as per decision.

Concerned department of the Bank will provide guidelines for the use of portable devices, especially for the usage at outside premises.

Bank will provide policy to return back organizational assets from employees/external parties upon termination of their employment, contract or agreement. **In no cases Bank can sell the assets to its employees.**

## 5.3 Desktop/Laptop Devices Controls

5.3.1 Desktop computers shall be connected to UPS to prevent damage of data and hardware.

5.3.2 Before leaving a desktop or laptop computer unattended, users shall apply the "*Lock Workstation*" feature. If not applied then the device will be automatically locked as per policy of Bank.

5.3.3 Confidential or sensitive information that stored in laptops must be encrypted.

5.3.4 Desktop computers, laptops, monitors, etc. shall be turned off at the end of each workday. 5.2.5 Laptops, computer media and any other forms of removable storage containing sensitive

Information (e.g. CD ROMs, Zip disks, PDAs, Flash drives, external hard-drives) shall be

Stored in a secured location or locked cabinet when not in use.

5.3.5 Access to USB port for Desktop/Laptop computers shall be controlled.

5.3.6 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.

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

5.3.8 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).

5.3.9 Any kind of viruses shall be reported immediately.

5.3.10 Viruses shall not be cleaned/ deleted without expert assistance unless otherwise instructed.

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

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

5.3.13 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.)

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

5.3.15 Workstations/Desktop Computers connected to the core network and servers must be located in an area free from physical dangers (e.g., high traffic areas, water leaks, fire hazards, etc.).

5.3.16 Workstations/Desktop Computers connected to the core network and servers must store sensitive information on file server drives and not local drives.

5.3.17 Software to be used on the workstation/Desktop Computers, connected to the core network and servers, must be scanned for viruses.

5.3.18 File Servers should be configured to scan all files on access.

5.3.19 Weekly scans should be undertaken of all file server files.

5.3.20 Computer operation related places should be kept clean. Under no circumstances can any beastly, sparkling and allied objects be placed directly on the floor.

5.3.21 Maintenance of hardware, content, servers, PCs, printers, keyboards, switches etc. need to be regularly cleaned and covered with dust cover after work.

5.3.22 To keep the performance of the UPS up and to prevent the battery from getting damaged, if the power is not available or if the generator is not turned on then the computer should flip the data over and over through the touch / touch button.

5.3.23 In order to avoid unintended electrical accidents at various branches and offices, the server must be properly flown and the associated online / offline UPS should be closed immediately before leaving the electrical connection.

5.3.24 The state holiday, festive holiday, weekly before and at the end of every working day should be flown to the computer by flying off the bus and leaving the office with the switch off and on. However, none of the electrical switches associated with the Uppabong Highlands, Uberpub and Eighth Odyssey can be switched off.

5.3.25 Important data stored on the computer should be used to verify the file size of the office file / folder so that any file can be saved and then used for the purpose. Important information stored on the computer, such as office files / folders should be stored.

## 5.4 BYOD Controls

"Bring Your Own Device" (BYOD) is a relatively new practice adopted by Banks and financial institutions to enable their employees to access corporate email, calendars, applications and data from their personal mobile devices like smart phones, tablet computers, etc. Bank shall be aware of the heightened security risks associated with BYOD due to challenges in securing, monitoring and controlling employees' personal devices.

5.4.1 BKB shall conduct a comprehensive risk assessment on the BYOD implementation to ensure that measures adopted sufficiently to mitigate the security risks associated with BYOD.

5.4.2 BKB shall not proceed with the BYOD implementation if they are unable to adequately manage the associated security risks.

5.4.3 BYOD is associated with a number of information security risks such as:

**a)** Loss, disclosure or corruption of corporate data on Personally Owned Devices (PODs);

**b)** Incidents involving threats to, or compromise of, the ICT infrastructure and other information assets (e.g. malware infection or hacking) of Bank;

**c)** Noncompliance with applicable laws, regulations and obligations (e.g. privacy or piracy);

**d)** Intellectual property rights for information created, stored, processed or communicated on PODs in the course of work for the Bank. Due to information security risks associated with BYOD, employees who wish to opt-in to BYOD must be authorized to do so and must not introduce unacceptable risks onto the Banks' networks by failing to secure their own equipment.

5.4.4 BKB may implement appropriate forms of device authentication for PODs approved by authority, such as digital certificates created for each specific device.

5.4.5 BKB has the right to control its information. This must include the right to backup, retrieve, modify, determine access and/or delete Bank data without reference to the owner or user of the POD.

5.4.6 Any POD used to access, store or process sensitive information must encrypt data transferred over the network (e.g. using SSL or a VPN).

5.4.7 The employee's device shall be remotely wiped if the device is lost, or the employee terminates his/her employment, or ICT detects a data or policy breach, a virus or similar threat to the security of the Bank's data and technology infrastructure.

5.4.8 Any type of mobile phone with private or unauthorized rash, Joy, Chow, averaging rounds, averaging, swept discharges, cannot be connected to the computer or network of Branch / Office/ Datacenter / DRS, or operating a network of ICTs or ICTs.

### 5.5 Server Security Controls

5.5.1 Users shall have specific authorization for accessing servers with defined set of privileges.

5.5.2 Additional authentication mechanism shall be used to control access of remote users.

5.5.3 Inactive session shall be expired after a defined period of inactivity.

5.5.4 Activities of System Administrators shall be logged. Servers containing sensitive and confidential data may export activity logs to a central log host.

5.5.5 The concerned department shall maintain test server(s) to provide a platform for testing of configuration settings, new patches and service packs before applied on the production system.

5.5.6 The concerned department shall ensure the security of file sharing process. File and print shares must be disabled if not required or kept at a minimum where possible.

5.5.7 All unnecessary services running in the production server shall be disabled. Any new services shall not run in production server without prior testing.

5.5.8 All unnecessary programs shall be uninstalled from production servers.

5.5.9 In case of virtualization:

**a)** Bank shall plan of setting limit on the use of resources (e.g., processors, memory, disk space, virtual network interfaces) by each VM (Virtual Machine).

**b)** Host and guest Operating System (OS) must be updated with new/required security patches and other patches if necessary. Patching requirements shall also be applied to the virtualization software.

**c)** Like physical servers, virtual servers need to be backed up regularly.
**d)** Bank shall ensure that host and guests use synchronized time**.**
**e)** File sharing shall not be allowed between host and guest OSs, if not required.

## 5.6 Data Center and Disaster Recovery Site Controls

As critical systems and data of a Bank are concentrated and housed in the Data Center (DC) and Disaster Recovery Site (DRS), it is important that the DC & DRS is resilient and physically secured from internal and external threats.

### 5.6.1 Physical Security

5.6.1.1 Physical security shall be applied to the information processing area or Data Center and Disaster Recovery Site. DC & DRS must be a restricted area and unauthorized access shall be strictly prohibited.

5.6.1.2 The Bank shall limit access to DC & DRS to authorized staff only. The Bank shall only grant access to the DC & DRS on a need to have basis. Physical access of staff to the DC & DRS shall be revoked immediately if it is no longer required.

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

5.6.1.4 Access authorization procedures shall be strictly applied to vendors, service providers, support staff and cleaning crews. The Bank shall ensure that visitors are accompanied at all times by an authorized employee while in the DC & DRS. (Ref. Access Log Book **ICTF-6,**Visitors log book**-ICTF7**)

5.6.1.5 All physical access to sensitive areas must be logged with purpose of access into the Data Center and Disaster Recovery Site.

5.6.1.6 The concerned department shall ensure that the perimeter of the DC & DRS, facility and equipment room are physically secured and monitored. The Bank shall employ physical, human and procedural controls for 24 hours such as the use of security guards, card access system, mantraps and surveillance system where appropriate.

5.6.1.7 Emergency exit door shall be available.

5.6.1.8 Data Center and Disaster Recovery Site must have a designated custodian or manager in charge to provide authorization and to ensure compliance with Policy.

5.6.1.9 An inventory of all computing equipment, associated equipment and consumables housed in DC & DRS must be maintained by the manager or a delegate.

5.6.1.10 Where DC & DRS is operated by an outsourced service supplier, the contract between the Bank and supplier must indicate that all the requirements of Policy regarding physical security must be complied with and that the Bank reserves the right to review physical security status at any time.

5.6.1.11 Where DC & DRS is operated by an outsourced service supplier, the responsibility for physical security lies with the supplier, but access to such facilities dedicated to Bank use must be reviewed and authorized by the Bank.

5.6.1.12 The physical security of Data Center and Disaster Recovery Site premises shall be reviewed at least once each year.

5.6.1.13 No equipments shall be entered or go outside without proper authorization. Proper log must be maintained for the entry & exit of any equipment.

### 5.6.2 Environmental Security

5.6.2.1 Protection of Data Center and Disaster Recovery Site 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 multi-tenant facilitated building is discouraged.

5.6.2.2 Layout design of Data Center and Disaster Recovery Site including power supply and network connectivity shall be properly documented.

5.6.2.3 Development and test environment shall be separated from production.

5.6.2.4 Separate channels for data and power cables to protect from interception or any sort of damages shall be made in the Data Center and Disaster Recovery Site .

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

5.6.2.6 Any accessories or devices not associated with Data Center and Disaster Recovery Site powered off devices shall not be allowed to store in the Data Center and Disaster Recovery Site. Separate store room must be in place to keep all sorts of unused and redundant IT equipments.

5.6.2.7 Closed Circuit Television (CCTV) camera shall be installed at appropriate positions of all sides for proper monitoring.

5.6.2.8 The sign of "No eating, drinking or smoking" shall be in display.

5.6.2.9 Dedicated office vehicles for any of the emergencies shall always be available on-site. Availing of public transport must be avoided while carrying critical equipments outside the Bank’s premises to avoid the risk of any causality.

5.6.2.10 Data Center and Disaster Recovery Site shall have dedicated telephone communication.

5.6.2.11 Address and telephone or mobile numbers of all contact persons (e.g. fire service, police station, service providers, vendors and all ICT personnel) must be available to meet any emergency necessity.

5.6.2.12 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.

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

5.6.2.14 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. Industry standard air conditioning system shall be in place to avoid water leakage from the conventional air conditioning system.

**f)** Emergency power cut-off switches where applicable

**g)** Emergency lighting arrangement

**h)** Dehumidifier for humidity control

5.6.2.15 The above mentioned environmental controls shall be regularly tested and maintenance service contract shall be for 24x7 bases.

### 5.6.3 Fire Prevention

5.6.3.1 Wall, ceiling and door of Data Center and Disaster Recovery Site shall be fire-resistant.

5.6.3.2 Fire suppression equipments shall be installed and tested periodically.

5.6.3.3 Automatic fire/smoke alarming system shall be installed and tested periodically.

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

5.6.3.5 Electric cables and data cables in the Data Center and Disaster Recovery Site must maintain quality and be concealed.

5.6.3.6 Flammable items such as paper, wooden items, plastics, etc. shall not be allowed to store in the Data Center and Disaster Recovery Site.

## 5.7 Server/Network Room/Rack Controls

5.7.1 Server/Network Room/Rack must have a glass enclosure with lock and key under a responsible person.

5.7.2 Physical access shall be restricted, visitors log must exist and to be maintained for the server room(Ref. Visitors Log Book **ICTF-7**).

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

5.7.4 There shall be a provision to replace the server and network devices within shortest possible time in case of any disaster.

5.7.5 Server/ Network Room/Rack shall be air-conditioned. Water leakage precautions and water drainage system from Air Conditioner shall be installed.

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

5.7.7 UPS shall be in place to provide uninterrupted power supply to the server and required devices.

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

5.7.9 Channel alongside the wall shall be prepared to allow all required cabling in neat and safe position as per layout of power supply and data cables.

5.7.10 Address and phone 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.

5.7.11 Power supply shall be switched off before leaving the server room if otherwise not required.

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

## 5.8 Networks Security Management

5.8.1 The concerned department shall establish baseline standards to ensure security for Operating Systems, Databases, Network equipments and portable devices which shall meet organization’s policy.

5.8.2 The concerned department shall conduct regular enforcement checks to ensure that the baseline standards are applied uniformly and non-compliances are detected and raised for investigation.

5.8.3 The Network Design and its security configurations shall be implemented under a documented plan. There shall have different security zones defined in the network design.

5.8.4 All type of cables including UTP, fiber, power shall have proper labeling for further corrective or preventive maintenance works.

5.8.5 The concerned department shall ensure physical security of all network equipments.

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

5.8.7 Unauthorized access and electronic tampering shall be controlled strictly. Mechanism shall be in place to encrypt and decrypt sensitive data travelling through WAN or public network.

5.8.8 The Bank shall install network security devices, such as firewalls as well as intrusion detection and prevention systems, at critical stages of its ICT infrastructure to protect the network perimeters.

5.8.9 The concerned department shall deploy firewalls, or other similar measures, within internal networks to minimize the impact of security exposures originating from third party or overseas systems, as well as from the internal trusted network.

5.8.10 Secure Login feature (i.e. SSH) shall be enabled in network devices for remote administration purposes. Any unencrypted login option (i.e. TELNET) shall be disabled.

5.8.11 The concerned department shall backup and review rules on network security devices on a regular basis to determine that such rules are appropriate and relevant.

5.8.12 The concerned department shall establish redundant communication links for WAN connectivity.

5.8.13 The concerned department deploying Wireless Local Area Networks (WLAN) within the organization shall be aware of risks associated in this environment. Secure communication protocols for transmissions between access points and wireless clients shall be implemented to secure the corporate network from unauthorized access.

5.8.14 SYSLOG Server may be established depending on Network Size to monitor the logs generated by network devices.

5.8.15 Authentication Authorization and Accounting (AAA) Server may be established depending on Network Size to manage the network devices effectively.

5.8.16 Role-based and/or Time-based Access Control Lists (ACLs) shall be implemented in the routers to control network traffic.

5.8.17 Real time health monitoring system for infrastructure management may be implemented for surveillance of all network equipments and servers.

5.8.18 Connection of personal laptop to office network or any personal wireless modem with the office laptop/desktop must be restricted and secured.

5.8.19 The concerned department shall change all default passwords of network devices.

5.8.20 All unused ports of access switch shall be shut-off by default if otherwise not defined.

5.8.21 All communication devices shall be uniquely identifiable with proper authentication.

5.8.22 Role-based administration shall be ensured for the servers.

5.8.23 Any electronic fund transfer instructions / debentures / conferences should go through the Bank's own domain / verified number and the deposit should be collected from the concerned authorities before executing the instruction.

## 5.9 Cyber Security Management

Cyber-attacks against financial services institutions are becoming more frequent, more sophisticated and more widespread. The rise in frequency and breadth of cyber-attacks can be attributed to a number of factors. Activists aim to make political statements through systems disruptions. Organized crime groups, and other criminals breach systems for monetary gain- i.e., to steal funds via account takeovers, ATM heists, and other mechanisms. The fact is that cyber criminals are becoming increasingly advanced with each passing day. They are finding new ways to infiltrate business infrastructures and stealing sensitive data that can cost upwards of billions in losses per year. The Bank should follow ISO 27001/2:2013 standards to protect Bank’s IT infrastructure from potential Cyber threats.

### 5.9.1 Prevention of Cyber-attacks

5.9.1 Keep computer current with the latest patches and updates. By regularly updating computer, block attackers from being able to take advantage of software flaws (vulnerabilities) that they could otherwise use to break into computer system. While keeping computer up-to-date will not protect from all attacks, it makes much more difficult for hackers to gain access to computer system, blocks many basic and automated attacks completely, and might be enough to discourage a less-determined attacker to look for a more vulnerable computer elsewhere.

5.9.2 Make sure computer is configured securely. When install a new computer, pay attention not just to make new system function, but also focus on making it work securely.

5.9.3 Choose strong passwords and keep them safe.

5.9.4 Protect computer with security software. Security software essentials include firewall and antivirus programs. A firewall is usually computer's first line of defense-it controls who and what can communicate with computer online. The next line of defense many times is antivirus software, which monitors all online activities such as mails messages and web browsing and protects and individual from viruses, worms, Trojan horse and other type malicious programs.

5.9.5 Protect personal information. Exercise caution when sharing personal information such as name, home address, phone number, and email address online. Keep an eye out for phony email messages; don't respond to email messages that ask for personal information, pay attention to privacy policies on Web sites and in software.

5.9.6 Guard email address- Spammers and phishes sometimes send millions of messages to email addresses that may or may not exist in hopes of finding a potential victim. Responding to these messages or even downloading images ensures someone will be added to their lists for more of the same messages in the future.

5.9.7 Online offers that look too good to be true usually are.

5.9.8 Review bank and credit card statements regularly.

## 5.10 Cryptography

The primary application of cryptography is to protect the integrity and privacy of sensitive or confidential information. Cryptography is commonly used in Banks to protect sensitive customer information such as PINs relating to critical applications (e.g. ATMs, payment cards and online financial systems).

All encryption algorithms used in a cryptographic solution shall depend only on the secrecy of the key and not on the secrecy of the algorithm. As such, the most important aspect of data encryption is the protection and secrecy of cryptographic keys used, whether they are master keys, key encrypting keys or data encrypting keys.

5.10.1 The concerned department shall establish cryptographic key management policy and procedures covering generation, distribution, installation, renewal, revocation and expiry.

5.10.2 The concerned department shall ensure that cryptographic keys are securely generated. All materials used in the generation process shall be destroyed after usage and ensure that no single individual knows any key in its entirety or has access to all the constituents making up these keys.

5.10.3 Cryptographic keys shall be used for a single purpose to reduce the impact of an exposure of a key.

5.10.4 The effective timeframe that a cryptographic key may be used in a given cryptographic solution is called the cryptoperiod. The Bank shall define the appropriate cryptoperiod for each cryptographic key considering sensitivity of data and operational criticality.

5.10.5 The concerned department shall ensure that hardware security modules and keying materials are physically and logically protected.

5.10.6 When cryptographic keys are being used or transmitted, the Bank shall ensure that these keys are not exposed during usage and transmission.

5.10.7 When cryptographic keys have expired, the Bank shall use a secure key destruction method to ensure keys could not be recovered by any parties.

5.10.8 In the event of changing a cryptographic key, the Bank shall generate the new key independently from the previous key.

5.10.9 The concerned department shall maintain a backup of cryptographic keys. The same level of protection as the original cryptographic keys shall be accorded to backup keys.

5.10.10 If a key is compromised, the Bank shall immediately revoke, destroy and replace the key and all keys encrypted under or derived from the exposed key. The Bank shall inform all parties concerned of the revocation of the compromised keys.

## 5.11 Malicious Code Protection

5.11.1 The environment of Banks including servers and workstations must be protected from malicious code by ensuring that approved anti-virus packages are installed.

5.11.2 Users must be made aware of arrangements to prevent and detect the introduction of malicious software.

5.11.3 Software and data supporting critical business activities must be regularly scanned or searched to identify possible malicious code.

5.11.4 Files received on electronic media of uncertain origin or unknown networks must be checked for malicious code before use.

5.11.5 Attachments to electronic mail must be checked for malicious code before use.

5.11.6 The anti-virus package must be kept up to date with the latest virus definition file using an automated and timely process.

5.11.7 All computers in the network shall get updated signature of anti-virus software automatically from the server.

5.11.8 Virus auto protection mode shall be enabled to screen disks, tapes, CDs or other media for viruses.

5.11.9 A computer virus hoax is a message warning the recipients of a non-existent computer virus. The message is usually a chain e-mail that tells the recipients to forward it to everyone they know. Employees must be made aware of the problem of hoax viruses and must not forward such virus alarms.

5.11.10 A formal process for managing attacks from malicious code must include procedures for reporting attacks and recovering from attacks.

5.11.11 The concerned department may arrange awareness program for the end users about computer viruses and their prevention mechanism.

### 5.12 Internet Access Management

5.12.1 Internet access shall be provided to employees according to the approved Internet Access Management Policy.

5.12.2 Access to and use of the internet from Bank premises must be secure and must not compromise information security of Bank.

5.12.3 Access to the Internet from Bank premises and systems must be routed through secure gateways.

5.12.4 Any local connection directly to the Internet from Bank premises or systems, including standalone PCs and laptops, is prohibited unless approved by Information Security.

5.12.5 Employees shall be prohibited from establishing their own connection to the Internet using Banks' systems or premises.

5.12.6 Use of locally attached modems with Banks' systems in order to establish a connection with the Internet or any third-party or public network via broadband, ISDN or PSTN services is prohibited unless specifically approved.

5.12.7 Internet access provided by the Bank must not be used to transact any commercial business activity that is not done by the Bank. Personal business interests of staff or other personnel must not be conducted.

5.12.8 Internet access provided by the Bank must not be used to engage in any activity that knowingly contravenes any criminal or civil law or act. Any such activity will result in disciplinary action of the personnel involved.

5.12.9 All applications and systems that require connections to the Internet or third-party and public networks must undergo a formal risk analysis during development and before production use and all required security mechanisms must be implemented.

5.12.10 The highest caution and awareness must be exercised when using the Internet. Under no circumstances can you access the web site of the office which is not relevant or not authorized. However, officers / employees of all levels of the Bank can access the official Facebook page of Bangladesh Krishi Bank

5.12.11 No officer / employee shall be able to open any mobile phone or any social media site in the name of Bangladesh Krishi Bank without the permission of the Authority.

### 5.13 Email Management

5.13.1 Email system shall be used according to the Bank's policy.

5.13.2 Access to email system shall only be obtained through official request (Ref. **ICTF-12**).

5.13.3 Email shall not be used to communicate confidential information to external parties unless encrypted using approved encryption facilities.

5.13.4 Employees must consider the confidentiality and sensitivity of all email content, before forwarding email or replying to external parties.

5.13.5 Information transmitted by email must not be defamatory, abusive, involve any form of racial or sexual abuse, damage the reputation of the Bank, or contain any material that is harmful to employees, customers, competitors, or others. The willful transmission of any such material is likely to result in disciplinary action.

5.13.6 BKB email system is principally provided for business purposes. Personal use of the Bank email system is only allowed under management discretion and requires proper permission; such personal use may be withdrawn or restricted at any time.

5.13.7 Corporate email address must not be used for any social networking, blogs, groups, forums, etc. unless having management approval.

5.13.8 Email transmissions from the Bank must have a disclaimer stating about confidentiality of the email content and asking intended recipient.

5.13.9 The Concerned department shall perform regular review and monitoring of email services.

5.13.10 In order to open a new e-mail account or change the defaults, the ICT (Operation) / ICT (Systems, Card and Mobile Banking) department should be requested by e-mail / letter through the appropriate authority.

5.13.11 In any case, the e-mail ID of one office / branch cannot be used by any other office / branch or any office / branch. This creates the possibility of various frauds. If any such fraud is organized, the office / branch of the respective office will be liable.

5.13.12 The Office Head / Branch Manager will either use the e-mail ID itself or will be responsible for checking and sending the e-mail daily to the specified officer through the office order.

5.13.13 For the security of the e-mail, the ID and password will be stored in a secret register by the office / branch manager or the officer nominated by the office / branch manager. The absence of any e-mail while on leave should be maintained in the office / branch of the concerned officer.

5.13.14 Every day since the commencement of the office, the e-mail and website should be checked at least 05 (five) times a day and download the necessary information such as circular, circular letter, instructions issued by head office or other controlling offices.

5.13.15 If anyone retires or leaves from his / her job, ID must be transferred to the Branch Manager/ Office Head. The Branch Manager/ Office Head should inform the ICT Dept for deactivate the ID.

5.13.15 No e-mail can be opened or posted without confirmation of the recipient of the e-mail received in the e-mail account of all BKB offices and branches. Any e-mail from unwanted / unnecessary domain, spam mail should not be opened without prior concentration.

5.13.16 In the event of any operational or financial loss of the Bank for non-disclosure of information due to non-payment of funds, the responsibility of the Controlling Office shall be conferred on the Head / Branch Manager and the concerned Computer Operator or the person responsible.

5.13.17 The e-mail sent from any domain other than "krishiBank.org.bd" domain will not be considered as official e-mail and should be aware about this domain and immediately inform ICT department about such kind of suspicious domain.

5.13.18 Upon receipt of all the e-mail accounts assigned to the BKB's office / branch, the " Default Password " must be changed before adherence to the Principles of Conduct. If you do not change "Default Password" it is likely to be hacked by another user.

5.13.18 Names, phone numbers, organization names, etc., should be used in the e-mail message sent from office / branch to other office / branch, and large file size should be avoided as attachment.

## 5.14 CBS Management

To ensure secured use of CBS, the instructions are stated below:

### 5.14.1 For Branch Office

5.14.1.1 Branch must use prescribed user creation form signed duly to send request to Head Office for a new user;

5.14.1.2 A new user must change the user password immediately after receiving his/her user ID from Head Office. In no way he should continue using Head Office provided password;

5.14.1.3 Every CBS user must keep his/her password secret;

5.14.1.4 CBS user must change user password on a timely basis for example every month;

5.14.1.5 If a user suspects that his/her password is revealed to any other person, he/she must change password immediately;

5.14.1.6 CBS password must be a combination of letters and numbers including minimum a capital letter, a small letter, a special character like !, @, #, $, % etc;

5.14.1.7 No user will use other person’s user ID or no user will allow other person to use his/her user ID;

5.14.1.8 No user will leave his/her desk without logging out from his CBS user;

5.14.1.9 If an employee holding a CBS user ID is transferred to other branch, branch will inform Head Office regarding the transfer immediately;

5.14.1.10 To send any CBS related request through email branch officer must mention his personal detail (at least mail sender’s name, designation, mobile number etc.);

5.14.1.11 Against every transaction including Head Office generated auto transaction branch office must maintain physical voucher singed by due persons;

5.14.1.12 If any suspicious transaction come to the observation, branch must inform Head Office immediately;

### 5.14.2 For Head Office

5.14.2.1 Without receiving request from branch in prescribed user creation form Head Office will create no new CBS ID;

5.14.2.2 In Head Office level, no user will be entitled transaction power in live database;

5.14.2.3 Every CBS user must keep his/her password secret;

5.14.2.4 CBS user must change user password on a timely basis for example every month;

5.14.2.5 If a user suspects that his/her password is revealed to any other person, he/she must change password immediately;

5.14.2.6 CBS password must be a combination of letters and numbers including minimum a capital letter, a small letter, a special character like !, @, #, $, % etc;

5.14.2.7 No user will use other person’s user ID or no user will allow other person to use his/her user ID;

5.14.2.8 No user will leave his/her desk without logging out from his CBS user;

5.14.2.8 To respond to any CBS related request through email, Head Office officer must use his/her professional prudence to be sure about the authenticity of the email.

### 5.15 Vulnerability Assessment and Penetration Testing

Vulnerability Assessment (VA) is the process of identifying, assessing and discovering security vulnerabilities in a system.

5.15.1 The Bank shall conduct VAs regularly to detect security vulnerabilities in the ICT environment.

5.15.2 The Bank shall deploy a combination of automated tools and manual techniques to perform a comprehensive VA. For web-based systems, the scope of VA shall include common web vulnerabilities such as SQL injection, cross-site scripting, etc.

5.15.3 The Bank shall establish a process to remedy issues identified in VAs and perform subsequent validation of the remediation to validate that gaps are fully addressed.

5.15.4 The Bank shall carry out penetration tests in order to conduct an in-depth evaluation of the security posture of the system through simulations of actual attacks on the system.

The Bank shall conduct penetration tests on network infrastructure and internet-based systems periodically or need basis.

## 5.16 Patch Management

5.16.1 BKB shall establish and ensure that the patch management procedures include identification, categorization and prioritization of security patches. To implement security patches in a timely manner, the Bank shall establish the implementation timeframe for each category of security patches.

5.16.2 BKB shall perform rigorous testing of security patches before deployment into the production environment.

## 5.17 Security Monitoring

5.17.1 BKB shall establish appropriate security monitoring systems and processes, to facilitate prompt detection of unauthorized or malicious activities by internal and external parties.

5.17.2 BKB shall implement network surveillance and security monitoring procedures with the use of network security devices, such as intrusion detection and prevention systems, to protect the Bank against network intrusion attacks as well as provide alerts when an intrusion occurs.

5.17.3 BKB may implement security monitoring tools which enable the detection of changes to critical ICT resources such as databases, system or data files and programs, to facilitate the identification of unauthorized changes.

5.17.4 BKB shall regularly review security logs of systems, applications and network devices for anomalies. Logs shall be protected and retained for defined period to facilitate future investigation.

## 5.18 Security Controls for Operating System (OS)

OS security encompasses many different techniques and methods which ensure safety from threats and attacks. OS security allows different applications and programs to perform required tasks and stop unauthorized interference. Without an OS, server/computer would not even start up. The first task of the OS is to manage the starting up the server/computer also known as booting up.

When this happens, the OS makes sure all the various elements of the server/computer are working properly. OS security may be approached in many ways, including adherence to the following:

5.18.1 Performing regular OS patch updates

5.18.2 Installing updated antivirus engines and software

5.18.3 Firewall, network interface should be configured securely. Scrutinizing all incoming and outgoing network traffic through a firewall

5.18.4 Creating secure accounts with required privileges only (i.e., user management). Deactivate the user and other unnecessary users.

5.18.5 Secure access for different applications and programs to perform required tasks and stop unauthorized interference.

5.18.6 Routine maintenance tasks, such as file management, defragmenting disks to optimize hard drive storage, balance the memory; log monitoring and keeping track of power supply should be done.

5.18.7 Limit the number of operating system users.

5.18.8 Limit the privileges of the operating system accounts (administrative, root-privileged, or DBA) for Database host (computer) to the fewest and least powerful privileges required for each user.

5.18.9 Disallow modifying the default permissions for the Database home (installation) directory or its contents.

## 5.19 Security Controls for Database (DB)

Good security for Database requires physical access control, reliable personnel, trustworthy installation and configuration procedures, secure communications, and control of database operations such as selecting, viewing, updating, or deleting database records. Since some of these requirements involve applications or stored procedures as well as human action, security procedures must also account for how these programs are developed and dealt with. Security and monitoring of database should be maintained for minimizing delays and errors and maximizing rapid and thorough accountability. They are discussed in the following sections:

5.19.1 Physical Access Control & Personnel Security
5.19.2 Installation and Configuration Security
5.19.3 Networking Security

### 5.19.1 Physical Access Control & Personnel Security

5.19.1.1 Physical access control stops a variety of potential problems and risks. So Database preparing for accountability and recovery are additional considerations, possibly prompting alarms or video surveillance of entryways.

5.19.1.2 To a very large degree, security depends on individuals. So train personnel not to get careless, resentful, or deliberately undermined or sabotaged.

### 5.19.2 Installation and Configuration Security

Implementing the following recommendations provides the basis for a secure configuration:

5.19.2.1 Should install only what is required. Grant necessary privileges only. Practice the principle of least privilege.

5.19.2.2 Lock and expire default user accounts.

5.19.2.3 Security is most easily broken when a default database server user account still has a default password even after installation. So change default user passwords as per the password policy.

5.19.2.4 Enable data dictionary protection.

5.19.2.5 Restrict operating system access.

5.19.2.6 Keep the database server behind a firewall. Ensure that the firewall is placed outside the network to be protected.

5.19.2.7 Client, Listener, host computer related security should be maintained as per the requirement.

### 5.19.3 Networking Security

Protecting the network and its traffic from inappropriate access or modification is the essence of network security. The following practices improve network security:

5.19.3.1 Network configuration/diagram/structure should be documented and approved.

5.19.3.2 Should use Firewall to encrypt network traffic. Never poke a hole through a firewall.

5.19.3.3 Check network IP addresses.

5.19.3.4 Protect the network access points from unauthorized access. This goal includes protecting the network-related software on the computers, bridges, and routers used in communication.

5.19.3.5Never transfer data over the Internet directly, use encryption through applicable method/devices.

5.19.3.6 Restrict physical access to the network. Make it difficult to attach devices for listening to, interfering with, or creating communications.

5.19.3.7 Configure the firewall to accept only those protocols, applications, or client/server sources that you know are safe.

## 5.20 Computerized Branch Management

5.20.1 Clean Cash, GL Abstract and Interbank Transaction Accounts must be collected from Computer on a daily basis and Balance reports of all types of Deposits and Balance reports of all types of loan accounts on a monthly basis. The date and name of the account should be saved.

5.20.2 All particulars and reports received from the computer regarding the closing of the semi-annual and annual accounts should be prepared in accordance with the circular and enclosed with the signature, clearly mentioning the title above the binding.

5.20.3 Check the computer outputs daily by the officers other than the executing officer / operator (the checker and maker are not the same person) and to be verified with proper seal- signature by two authorized officers.

5.20.4 Forced / Upholsterers, along with litter / straw, should be taken out and stored with proper voucher daily after verification and signed by the 2nd Officer / Authorized Officer.

5.20.5 Every day from the date of the live, soft copy of the Banking data should be stored in different media (multiple / ounce / medicinal discharges) with many different scales and should be kept in a cool and dry place to keep it free from any kind of damage.

5.20.6 Half-yearly / yearly backups must be ensured at least on a quarterly basis which has to be properly stored.

5.20.7 After submitting the check request slips to the computer, the print out (hardcopy) should be stored and verified by an authorized officer in combination with the customer's account and check series.

5.20.8 The actions taken in respect of the application of the stop payment must be printed with such print out upon completion and stored with the account holder's application and recorded in the stop payment register.

5.20.9 The password policy instructions mentioned in Sections 2.0 and 2.2 regarding password should be followed properly. The computer in-charge of the branch, the alternate in-charge and the operators should provide a copy of the office order by providing written instructions for their own work.

5.20.10 If there is no electricity and no generator is turned on then the computer will have to flip the data between 5 to 5 minutes via the Touch Box / Touch Transfer.

### 5.21 Sharing Resources

5.21.1 Sharing of resources to be setup to avoid repetition of works and to quicker functionalities.

5.21.2 Unlimited access to be prohibited always in sharing all sorts of resources.

5.21.3 Sharing of resources should be controlled through maintaining passwords.

### 5.22 Log Reports

5.22.1 Log reports to be maintained for access into the system and uses of different applications accordingly in detail.

5.22.2 Log reports for all exceptions of the system should also be maintained properly.

5.22.3 Hard copies of the above reports to be checked and preserved regularly.

# Chapter 6

## 6. Access Control of Information System

Bangladesh Krishi Bank shall only grant access rights and system privileges based on job responsibility. Bank shall check that no person by virtue of rank or position shall have any intrinsic right to access confidential data, applications, system resources or facilities for legitimate purposes.

### 6.1 User Access Management

6.1.1 BKB shall only grant user access to ICT systems and networks on a need-to-use basis and within the period when the access is required.

6.1.2 BKB shall closely monitor non-employees (contractual, outsourced, or vendor staff) for access restrictions.

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

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

6.1.5 User access shall be locked for unsuccessful login attempts.

6.1.6 User access privileges must be kept updated for job status changes.

6.1.7 BKB shall ensure that records of user access are uniquely identified and logged for audit and review purposes.

6.1.8 BKB shall perform regular reviews of user access privileges to verify that privileges are granted appropriately.

### 6.2 Password Management

6.2.1 The concerned department shall enforce strong password controls over users' access.

6.2.2 Password controls shall include a change of password upon first logon.

6.2.3 Password definition parameters shall ensure that minimum password length is maintained according to Bank's Policy (at least 6 characters).

6.2.4 Password shall be combination of at least three of stated criteria like uppercase, lowercase, special characters and numbers.

6.2.5 Maximum validity period of password shall not be beyond the number of days permitted in the Bank's Policy (maximum 90 days cycle).

6.2.6 Parameter to control maximum number of invalid logon attempts shall be specified properly in the system according to the Bank's Policy (maximum 3 consecutive times).

6.2.7 Password history maintenance shall be enabled in the system to allow same passwords to be used again after at least three (3) times.

6.2.8 Administrative passwords of Operating System, Database and Business Applications shall be kept in a safe custody with sealed envelope(Ref. Password Handover Form **ICTF-9**).

## 6.3 Input Control

6.3.1 Session time-out period for users shall be set in accordance with the Bank's Policy.

6.3.2 Operating time schedule of users' input for Banking applications shall be implemented as per regulatory enforcement unless otherwise permitted from appropriate authority.

6.3.3 Audit trail with User ID and date-time stamp shall be maintained for data insertion, deletion and modification.

6.3.4 Software shall not allow the same user to be both maker and checker of the same transaction unless otherwise permitted from appropriate authority.

6.3.5 Management approval must be in place for delegation of authority.

6.3.6 Sensitive data and fields of Banking applications shall be restricted from being accessed.

## 6.4 Privileged Access Management

Information security ultimately relies on trusting a small group of skilled staff, who shall
be subject to proper checks and balances. Their duties and access to systems resources shall
be placed under close scrutiny.

6.4.1 The concerned department shall apply stringent selection criteria and thorough screening when appointing staff to critical operations and security functions.

6.4.2 Having privileged access, all system administrators, ICT security officers and employees performing critical operations invariably possess the capability to inflict severe damage on critical systems. The Bank shall adopt following controls and security practices for privileged users:

**a)** Implement strong authentication mechanisms;

**b)** Implement strong controls over remote access;

**c)** Restrict the number of privileged users;

**d)** Grant privileged access on a "need-to-have" basis;

**e)** Review privileged users' activities on a timely basis;

**f)** Prohibit sharing of privileged accounts;

**g)** Disallow vendors from gaining privileged access to systems without close supervision and monitoring;

### 6.5 Remote Access

Remote access to systems will have minimized, secure, controlled, authorized and authenticated

6.5.1 The concerned department must authenticate each remote connection and user prior to permitting access to a system.

6.5.2 The concerned department should authenticate both the remote system user and device during the authentication process.

6.5.3 The concerned department should not allow the use of remote privileged access from an un-trusted domain, including logging in as an unprivileged system user and then escalating privileges.

6.5.4 The concerned department should establish VPN connections for all remote access connections Remote access is defined as user access to Bank systems originating outside an Bank network. Remote access by a privileged user to a Bank system via a less trusted security domain (for example, the Internet) may present additional risks. Controls in this section are designed to prevent escalation of user privileges from a compromised remote access account.

# Chapter 7

## 7. Business Continuity and Disaster Recovery Management

### 7.1 Business Continuity Plan

The Business Continuity Plan (BCP) is the predefined mechanism that addresses any kind of disaster which may disrupt/discontinue the business process. This BCP covers the mitigation procedure or immediate and long term action plan to handle the disaster caused by calamities like fire, earthquake, storm/cyclone/flood, bomb blast, terrorist attack, riots, collapse of buildings, theft of equipment's, heavy rainfall or any other natural calamity, Pandemic Flu/Influenza etc or any other pandemic diseases.

This kind of disaster may cause discontinuation of business process due to failure or unavailability of ICT resources, network/WAN down, data loss, DC/DR related disaster like fall down or synchronization error, major virus attack, or any other kinds of disruption to the business process. It puts disaster planning in perspective and makes it more likely that disasters will be handled smoothly and ensures no loss or minimum loss and resume the business process in shortest possible time. Business continuity plans must be reasonable, practical and achievable. This plan may change in response to new business and/or technology. As per ICT Security Policy of Bangladesh Krishi Bank, BKB has designed the departmental Business Continuity and Disaster Recovery Plan.

Business Continuity Plan for Bangladesh Krishi Bank:

7.1.1 BKB must have an approved Business Continuity Plan addressing the recovery from disaster to continue its operation.

7.1.2 Approved BCP shall be circulated to all relevant stakeholders. The recipients would receive a copy of amended plan whenever any amendment or alteration takes place.

7.1.3 Documents related to BCP must be kept in a secured off-site location. One copy shall be stored in the office for ready reference.

7.1.4 The BCP shall be coordinated with and supported by the Business Impact Analysis (BIA) and the Disaster Recovery Plan (DRP) considering system requirements, process and interdependencies.

7.1.5 BCP shall address the followings:

a) Action plan to restore business operations within the specified time frame for: i) office hour disaster ii) outside office hour disaster.

b) Emergency contacts, addresses and phone numbers of employees, venders and agencies.

c) Grab list of items such as backup tapes, laptops, flash drives, etc.

d) Disaster recovery site map

7.1.6 BCP must be tested and reviewed at least once a year to ensure the effectiveness

7.1.7 BCP should explain the Maximum Tolerable Downtime (MTD), Recovery Time Objective (RTO), Recovery Point Objective (RPO) of services and ICT resources.

7.1.8 Plans, measures and arrangements to ensure the continuous delivery of critical services and products, which permits the organization to recover its facility, data and assets.

7.1.9 Identification of necessary resources to support business continuity, including personnel, information, equipment, financial allocations, legal counsel, infrastructure protection and accommodations.

The BCP is able to address the backup, recovery and restore process. Keeping this into consideration, this unit covers Business Continuity Plan (BCP), Disaster Recovery Plan (DRP) for centralized operation and Backup and Restore Plan (BRP) all ICT operations. Creating documents, taking preparation, proper testing, and update plan of BCP which will actually ensure Risk Management Plan and Business Impact Analysis, and create Incident Response and Recovery Plans.

## 7.2 Developing a Business Continuity Plan:

This template incorporates the Prevention, Preparedness, Response and Recovery (PPRR) framework. Each of the four key elements is represented by a part in the Business Continuity Planning Process.

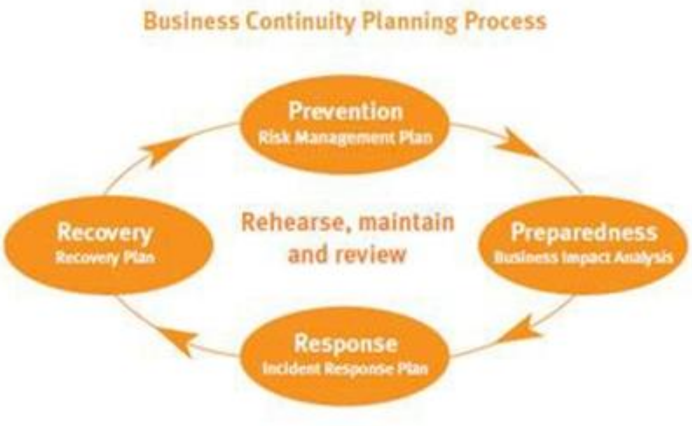

**Figure 7.2: Business Continuity Planning Process**

As

- Prevention - Risk Management planning
- Incorporates the Prevention element that identifies and manages the likelihood and/or effects of risk associated with an incident.
- Preparedness - Business Impact Analysis
- Incorporates the Preparedness element that identifies and prioritizes the key activities of a business that may be adversely affected by any disruptions.
- Response - Incident Response planning
- Incorporates the Response element and outlines immediate actions taken to respond to an incident in terms of containment, control and minimizing impacts.
- Recovery - Recovery planning

  - Incorporates the Recovery element that outlines actions taken to recover from an incident in order to minimize disruption and recovery times.

## 7.3 Disaster Recovery Plan (DRP)

7.3.1 BKB must have an approved Disaster Recovery Plan. In formulating and constructing a rapid recovery plan, the Bank shall include a scenario analysis to identify and address various types of contingency scenarios. The Bank shall consider scenarios such as major system outages which may be caused by system faults, hardware malfunction, operating errors or security incidents as well as a total incapacitation of the primary DC.

7.3.2 BKB shall establish a Disaster Recovery Site(DRS) which is geographically separated from the primary site(minimum 10 kilometers radial distance but choice of different seismic zone will be preferred) to enable the restoration of critical systems and resumption of business operations when a disruption occurs at the primary site.

7.3.3 If Disaster Recovery Site (DRS) is not in different seismic zone, Bank may establish a third site in different seismic zone which will be treated as Disaster Recovery Site(DRS)/Far DC. In such cases the DRS in near location will be treated as Near DC and shall be configured accordingly.

7.3.4 DRS and/or Near DC shall be equipped with compatible hardware and telecommunication equipments to support the critical services of the business operation in the event of a disaster.

7.3.5 Physical and environmental security of the DRS and/or Near DC shall be maintained.

7.3.6 BKB shall define system recovery and business resumption priorities and establish specific recovery objectives including recovery time objective (RTO) and recovery point objective (RPO) for ICT systems and applications. RTO is the duration of time, from the point of disruption, within which a system shall be restored. RPO refers to the acceptable amount of data loss for an ICT system while a disaster occurs.

7.3.7 BKB shall consider inter-dependencies between critical systems in drawing up its recovery plan and conducting contingency tests.

7.3.8 BKB may explore recovery strategies and technologies such as on-site redundancy and real-time data replication to enhance the Bank's recovery capability.

7.3.9 Information security shall be maintained properly throughout the recovery process.

7.3.10 An up-to-date and tested copy of the DR plan shall be securely held off-site. One copy shall be stored in the office for ready reference.

7.3.11 BKB shall test and validate at least annually the effectiveness of recovery requirements and the ability of staff to execute the necessary emergency and recovery procedures.

7.3.12 BKB shall involve its business users in the design and execution of comprehensive test cases to verify that recovered systems function property.

7.3.13 DR test documentation shall include at a minimum of Scope, Plan and Test Result. Test report shall be communicate to management and other stakeholders and preserved for future security.

## 7.4 Data Backup and Restore Management

7.4.1 BKB shall develop a data backup and recovery policy. Each business application must have a planned, scheduled and documented backup strategy, involving the making of both on- and off-line backups and the transfer of backups to secure off-site storage.

7.4.2 Details of the planned backup schedule for each business application must be created in line with the classification of the application and the information it supports and must specify the type of back-up required (full, partial, incremental, differential, real-time monitoring) at each point of the back-up schedule.

7.4.3 The frequency of backups taken for information must be determined in line with the classification of the information and the requirements of the business continuity plans for each application.

7.4.4 The details of the plan backup schedule for each business application must include the retention period for back-up or archived information and the retention period must be consistent with local legal and regulatory requirement.

7.4.5 All media contained back-up information must be leveled with the information content, backup cycle, backup serial identifier, backup date and classification of the information content.

7.4.6 The backup inventory and log sheet shall be maintained, checked and signed by the supervisor (Ref. Backup Log Form **ICTF-10)**.

7.4.7 Bank shall encrypt backup data in tapes or disks, containing sensitive or confidential information, before transported offsite for storage.

7.4.8 At least one copy of backup shall be kept on-site for the time of critical delivery.

7.4.9 The process of restoring information from both on- and off-site backup storage must be documented.

7.4.10 BKB shall carry out periodic testing and validation of the recovery capability of backup media and assess whether it is adequate and sufficiently effective to support the Bank's recovery process.

# Chapter 8

## 8. Acquisition and Development of Information Systems

For developing any new application of business function for the Bank, it requires rigorous analysis before acquisition or development to ensure that business requirements are met in an effective and efficient manner. The 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‘.

Sometimes, many systems fail because of poor system design and implementation, as well as inadequate testing. The Bank shall identify system deficiencies and defects at the system design, development and testing phases. Bangladesh Krishi Bank shall establish a steering committee, consisting of related departments, the development/technical team and other stakeholders to provide oversight and monitoring of the progress of the project, including deliverables to be realized at each phase of the project and milestones to be reached according to the project timetable.

### 8.1 ICT Project Management

8.1.1 In drawing up a project management framework, the Bank shall ensure that tasks and processes for developing or acquiring new systems include project risk assessment and classification, critical success factors for each project phase, definition of project milestones and deliverables. The Bank shall clearly define the project management framework, the roles and responsibilities of staff involved in the project.

8.1.2 Project plan for all ICT projects shall be clearly documented and approved. In the project plan, the Bank shall set out clearly the deliverables to be realized at each phase of the project as well as milestones to be reached.

8.1.3 Bank shall ensure that user functional requirements, business cases, cost-benefit analysis, systems design, technical specifications, test plans and service performance expectation are approved by the relevant business units and ICT management.

8.1.4 BKB shall establish management oversight of the project to ensure that milestones are reached and deliverables are realized in a timely manner.

### 8.2 Vendor Selection for System Acquisition

8.2.1 There must be a core team comprising of personnel from Functional Departments, ICT Systems, Card & Mobile Banking, ICT Operation Department and Internal Control and Compliance Department for vendor selection.

8.2.2 Vendor selection must have conformity with the Procurement Act-2006, PPR-2008 and e-gp system.

8.2.3 Vendor selection criteria for application must address followings:

**a)** Market presence
**b)** Years in operation
**c)** Technology alliances
**d)** Extent of customization and work around solutions
**e)** Financial strength
**f)** Performance and Scalability
**g)** Number of installations
**h)** Existing customer reference
**i)** Support arrangement/ Manpower
**j)** Local support arrangement for foreign vendors
**k)** Weight of financial and technical proposal

## 8.3 In-house Software Development

8.3.1 Detailed business requirements shall be documented and approved by the competent authority.

8.3.2 Detailed technical requirements and design shall be prepared.

8.3.3 Application security and availability requirements shall be addressed.

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

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

8.3.6 User Verification Test (UVT) for post development shall be carried out.

8.3.7 System Documentation and User Manual shall be prepared and handed over to the concerned department.

8.3.8 Source code must be available with the concerned department and kept secured.

8.3.9 Source code shall contain title area with author name, date of creation, last date of modification and other relevant information.

8.3.10 Application shall be in compliance with relevant controls of Bank’s ICT Security Policy.

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

## 8.4 Software Documentation

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

8.4.2 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
**g)** Emergency Administrative procedure

## 8.5 Statutory Requirements

8.5.1 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.

8.5.2 There shall have a separate test environment to perform end-to-end testing of the software functionalities before implementation.

8.5.3 User Acceptance Test shall be carried out and signed-off by the relevant business units/departments before rolling out in LIVE operation.

8.5.4 Necessary Regulatory Compliance requirements for Banking procedures and practices and relevant laws of Government of Bangladesh must be taken into account.

8.5.5 Any bugs and/or defects found due to design flaws must be escalated to higher levels in Software Vendors' organization and Bank in time.

8.5.6 Support agreement must be maintained with the provider for the application software used in production with the confidentiality agreement.

# Chapter 9

## 9. Alternative Delivery Channels (ADC) Security Management

“Channelize through channels” is the new paradigm for Financial related Banking services. Branchless Banking is a distribution channel strategy used for delivering financial services without relying on Bank branches. ATM & POS are Alternate Delivery Channels which provide Banking services directly to the customers. Customers can perform Banking transactions by their card (Debit/Credit) through ATM & POS channel. The channel has enabled Banks to reach a wide consumer-base banking regardless of time and geographic location. ADC ensures higher customer satisfaction at lower operational expenses and transaction costs.

### 9.1 ATM/POS Transactions

The ATMs and Point-of-Sale (POS) devices have facilitated cardholders with the convenience of withdrawing cash as well as making payments to merchants and billing organizations. However, these systems are target where card skimming attacks are organized. ATM security is one of the greatest 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 and customers and the law enforcement machinery is required to prevent ATM burglary attacks. To secure consumer confidence in using these systems, the Bank shall consider putting in place the following measures to counteract fraudsters’ attacks on ATMs and POS devices:

9.1.1 BKB shall install anti-skimming device on ATM devices to detect the presence of unknown devices placed over or near a card entry slot.

9.1.2 BKB shall install detection mechanisms and sends alerts to appropriate channel for follow-up response and action.

9.1.3 BKB shall implement tamper-resistant keypads to ensure that customers’ PINs are encrypted during transmission.

9.1.4 BKB shall implement appropriate measures to prevent shoulder surfing of customers’ PINs.

9.1.5 BKB may implement biometric finger vein sensing technology to resist PIN compromise.

9.1.6 The concerned ATM booth related branch shall conduct video surveillance of activities for 24 hours at these machines and maintain the quality of CCTV footage and preserve for 03(three) months online and at least one year in archive.

9.1.7 BKB shall introduce a centralized online monitoring system for Cash Balance, Loading-Unloading functions, Disorders of machine, etc.

9.1.8 BKB shall deploy security personnel for all ATM devices 24 hour basis.

9.1.9 BKB shall verify that adequate physical security measures are implemented in ATM devices.

9.1.10 BKB shall inspect all ATM/POS devices frequently to ensure standard practice (i.e., environmental security for ATM, anti-skimming devices for ATM, POS device surface tempering, etc.) is in place with necessary compliance. Inspection log sheet shall be maintained in ATM booth premises and centrally.

9.1.11 BKB shall monitor third party cash replenishment vendor’s activities constantly and visit third party cash sorting houses regularly.

9.1.12 The Bank shall train and provide necessary manual to its merchants about security practices (e.g. signature verification, device tampering/ replacement attempt, changing default password verification, etc.) to be followed for POS device handling.

9.1.13 BKB shall educate its customers on security measures that are put in place by the Bank are to maintain by the customers for ATM and POS transactions.

9.1.14 There must be a list inside the booth containing the contact numbers of Bank concerned persons.

9.1.15 All fees/charges related to ATM transaction and the steps showing the proper usages of ATM must be included in a display visible for everyone in ATM booth premises.

9.1.16 Any kind of captured/stole/lost, card holders must inform the related authorities to stop the card for preventing fraud of cards.

9.1.17 Security guard must be trained for proper monitoring and about the fraudulent activities. Time to time they have to monitored. While installing / repairing any new machinery at the AUG booth, the security guard working at the AUG booth will contact the authorized officer of the Bank to confirm the identity of the passenger / persons. If necessary, the concerned Bank officer will be physically present in the booth and confirm the identity of such person / persons.

9.1.18 If the card is trapped at the other Bank during the transaction, the card should be notified to the concerned branch: The customer has to be notified to apply for the duplicate card. The department should notify the department immediately to stop the transaction of the card related to the neighbor.

9.1.19 The ATM's designated officer shall, at least 12 (two) times a month, inspect the ATM booth at the ATM logbook register, notifying the branch manager. In addition, senior executives / executives / officers of the branch including head office, departmental office, main regional / regional office and audit office will regularly visit the ATM booth and inspection feedback should be recorded in the ATM logbook register.

9.1.20 The cardholder should be encouraged to provide the PIN manually in case of a transaction.

9.1.21 Customers need to be informed about the benefits of using the card to encourage card-based transactions and arrange banners, posters for display at the branches and at the visible area of the yard.

9.1.22 In order to discourage customers from cash transactions, automated / digital (pre-operative) procedures such as card (s) will be notified of proper notification and notification of automatic arrangements should be made at the visible location of the branch.

9.1.23 Load money at the ATM booth, inspect the booth, take action to solve any problem in the booth, ensure immediate solution to customers' problems and issue office order to the 02 (two) officers responsible for contacting the head office and ATC-related vendor organization ITCL. Have to inform

9.1.24 In order to ensure immediate resolution of customer problems, arrangements must be made to display the name and contact phone number of the concerned ATM officer at the ATM booth for implementation of the yearly service.

## 9.2 Internet Banking

Information involved in internet Banking facility passing over public networks shall be protected from fraudulent activity, dispute and unauthorized disclosure or modification. Banks' internet systems may be vulnerable as financial services are increasingly being provided via the internet. As a counter-measure, the Bank shall devise a security strategy and put in place measures to ensure the confidentiality, integrity and availability of its data and systems.

9.2.1 BKB shall provide assurance to its customers and users so that online access and transactions performed over the internet are adequately protected and authenticated.

9.2.2 BKB shall properly evaluate security requirements associated with its internet Banking system and adopt mechanisms which are well-established international standards.

9.2.3 BKB shall formulate Internet Banking Security policy considering technology security aspects as well as operational issues.

9.2.4 BKB shall ensure that information processed, stored or transmitted between the Bank and its customers is accurate, reliable and complete. The Bank shall also implement appropriate processing and transmission controls to protect the integrity of systems and data, e.g. SSL, TLS.

9.2.5 BKB shall implement 2FA (two-factor authentication) for all types of online financial transactions. Hardware/Software based tokenization means will be preferred. The primary objectives of two-factor authentication are to secure the customer authentication process and to protect the integrity of customer account data and transaction details as well as to enhance confidence in online systems.

9.2.6 An online session needs to be automatically terminated after a fixed period of time unless the customer is re-authenticated for the existing session to be maintained.

9.2.7 The concerned department shall implement monitoring or surveillance systems to follow-up and address subsequently any abnormal system activities, transmission errors or unusual online transactions.

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

9.2.9 BKB shall maintain high resiliency and availability of online systems and supporting systems (such as interface systems, backend host systems and network equipment). The Bank shall put in place measures to plan and track capacity utilization as well as guard against online attacks. These online attacks may include denial-of-service attacks (DoS attack) and distributed denial of-service attack (DDoS attack).

9.2.10 BKB shall take appropriate measures to minimize exposure to other forms of attacks such as middleman attack which is commonly known as a man-in-the middle attack (MITMA), man-in-the browser attack or man-in-the application attack.

9.2.11 The information security officer or any other assigned person/team 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) and DoS (Denial of Service) attacks

**d)** Checking middleman attacks

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

**f)** Checking the weaknesses of the infrastructure

**g)** Taking control of ports

**h)** Cause application crash

**i)** Injecting malicious codes to application and database servers.

9.2.12 BKB shall educate its customers on security measures to protect them in an online environment.

### 9.3 Payment Cards

Payment cards allow cardholders the flexibility to purchase wherever they want to depend on availability of pos machine. Cardholders may choose to purchase by physically presenting these cards for payments at the merchant pos machine. Payment cards also provide cardholders with the convenience of withdrawing cash at automated teller machines (“ATM”). Payment cards exist in many forms; but magnetic chip cards posing the highest security risks. Sensitive payment card data stored on magnetic stripe cards is vulnerable to card skimming attacks. Card skimming attacks can happen at various points of the payment card processing, including ATMs, payment kiosks and POS terminals.

9.3.1 BKB which provides payment card services shall implement adequate safeguards to protect sensitive payment card data. The concerned department shall ensure that sensitive card data is encrypted to ensure the confidentiality and integrity of these data in storage and transmission.

9.3.2 BKB shall ensure that the processing of sensitive or confidential data is done in a secure environment.

9.3.3 BKB shall deploy secure chips with multiple payment application supported to store sensitive payment card data. For interoperability reasons, where transactions could only be resulted by using information from the magnetic stripe on a card, Bank shall ensure that adequate controls are implemented to manage these transactions.

9.3.4 BKB shall perform (not a third party payment processing service provider) the authentication of customers' sensitive static information, such as PINs or passwords. BKB shall perform regular security reviews of the infrastructure and processes being used by its service providers.

9.3.5 Equipment used to generate payment card PINs and keys shall be managed in a secured manner.

9.3.6 Card personalization, PIN generation, Card distribution, PIN distribution, Card activation groups shall be different from each other.

9.3.7 The Bank shall ensure that security controls are implemented at payment card systems and networks. Bank 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.

9.3.8 BKB shall only activate new payment cards upon obtaining the customer's instruction.

9.3.9 BKB shall implement a dynamic one-time-password ("OTP") as 2FA for CNP (Card Not Present) transactions via internet to reduce fraud risk associated with it.

9.3.10 To enhance card payment security, the Bank shall promptly notify cardholders via transaction alerts including source and amount for any transactions made on the customers' payment cards.

9.3.11 BKB shall set out risk management parameters according to risks posed by cardholders, the nature of transactions or other risk factors to enhance fraud detection capabilities.

9.3.12 BKB shall implement solution to follow up on transactions exhibiting behavior which deviates significantly from a cardholder's usual card usage patterns. The Bank shall investigate these transactions and obtain the cardholder's authorization prior to completing the transaction.

## 9.4 Mobile Financial Services & Mobile Apps

### 9.4.1 Mobile Financial Services

Controls over mobile transactions are required to manage the risks of working in an unprotected environment. The Bank shall formulate security controls, system availability and recovery capabilities, which commensurate with the level of risk exposure, for operations.

9.4.1.1 Security standards shall be followed appropriate to the complexity of services offered.

9.4.1.2 BKB shall clearly identify risks associated with the types of services being offered in the risk management process.

9.4.1.3 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.

9.4.1.4 BKB shall arrange an agreement with Mobile Network Operator (MNOs) to ensure appropriate measures of MFS account for avoiding risk of unwanted transactions.

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

9.4.1.6 BKB shall conduct periodic risk management analysis and security assessment of the MFS operation and take appropriate measures accordingly.

9.4.1.7 BKB shall have conformity with '*Regulatory Compliance'* requirements of the country.

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

### 9.4.2 Mobile Apps

Guidelines apply privacy design principles to applications and their related services designed for mobile devices. Applications and their related services should create good privacy experiences and engender trust based on the principles of transparency, choice and control. Following guidelines seek to articulate the principles in functional terms for mobile application development.

9.4.2.1 Mobile Application should have transparency, easy navigation and mechanisms for users.

9.4.2.2 Developer should use secure and latest development technology to ensure app security.

9.4.2.3 Incorporate more interactive designs, features and user friendly language.

9.4.2.4 To ensure privacy control applications must not access, use and share User-generated data (such as contact lists, videos and photos, messages, emails, notes, and call logs) without prior consent of users unless this is a part of the apps functionality.

9.4.2.5 Ensure appropriate privacy setting for users.

9.4.2.6 Applications must not access, use and share location data without prior consent of users.

9.4.2.7 Do not permit the automatic collection and sharing of User-generated data or location information.

9.4.2.8 Should have retention policy of stored and collected information to the business model and make sure to securely delete it when it’s no longer required.

9.4.2.9 Users should get clear and simple information about privacy options, usage of user generated data and security settings of applications.

9.4.2.10 Do not use any mobile advertising that is not subject to regulatory and self regulatory standards.

9.4.2.11 Avoid any language and style that is not decent, appropriate and suitable.

9.4.2.12 Should have developer responsibility for ensuring end-user privacy is considered and delivered throughout the product lifecycle and through applicable business processes.

9.4.2.13 Should follow the regulatory guidelines and Human-computer interaction (HCI) guidelines.

9.4.2.14 Guidelines of device manufacturers, platforms, and OS companies need to be followed.

# Chapter 10

## 10. Service Provider Management

### 10.1 Outsourcing

10.1.1 The board of directors and senior management shall fully understand risks associated with ICT outsourcing. Before appointing a service provider, due diligence shall be carried out to determine its viability, capability, reliability, track record and financial position.

10.1.2 BKB shall ensure that contractual terms and conditions governing the roles, relationships, obligations and responsibilities of all contracting parties are set out fully in written agreements.

10.1.3 Outsourcing activities shall be evaluated based on the following practices:

**a)** Objective behind outsourcing

**b)** Economic viability

**c)** Risks and security concerns.

10.1.4 ICT outsourcing shall not result in any weakening or degeneration of the Bank's internal controls. The Bank shall require the service provider to employ a high standard of care and diligence in its security policies, procedures and controls to protect the confidentiality and security of its sensitive or confidential information, such as customer data, object programs and source codes.

10.1.5 BKB shall require the service provider to implement security policies, procedure and controls that are at least as stringent as it would expect for its own operations.

10.1.6 BKB shall monitor and review the security policies, procedures and controls of the service provider on regular basis, including periodic expert reports on security adequacy and compliance in respect of the operations and services provided by the service provider.

10.1.7 BKB shall require the service provider to develop and establish a disaster recovery contingency framework which defines its roles and responsibilities for documenting, maintaining and testing its contingency plans and recovery procedures.

10.1.8 BKB shall develop a contingency plan for critical outsourcing technology services to protect them from unavailability of services due to unexpected problems of the technology service provider. This may include termination plan and identification of additional or alternate technology service providers for such support and services.

10.1.9 BKB shall maintain a service catalogue for all third party services received preserving up-to-date information of each service rendered, service provider name, service type, SLA expiry date, service receiving manager, service reporting, emergency contact person at service provider, last SLA review date etc.

## 10.2 Service Level Agreement

10.2.1 There shall be a Service Level Agreement between the vendor and the Bank.

10.2.2 The Annual Maintenance Contract (AMC) with the vendor shall be active and currently in-force.

10.2.3 Dashboard with significant details of SLAs and AMCs shall be prepared and kept updated.

10.3.4 BKB shall ensure that the equipment does not contain sensitive live data when hardware is taken by the service provider for servicing/ repairing.

10.3.5 The requirements and conditions covered in the agreements would usually include performance targets, service levels, availability, reliability, scalability, compliance, audit, security, contingency planning, disaster recovery capability and backup processing facility.

10.3.6 Service contacts with all service providers including third-party vendors shall include:

**a)** Pricing
**b)** Measurable service/deliverables
**c)** Timing/schedules
**d)** Confidentiality clause
**e)** Contact person names (on daily operations and relationships levels)
**f)** Roles and responsibilities of contracting parties including an escalation matrix
**g)** Renewal period
**h)** Modification clause
**i)** Frequency of service reporting
**j)** Termination clause
**k)** Penalty clause
**l)** Warranties, including service suppliers' employee liabilities, 3rd party liabilities and the related remedies
**m)** Geographical locations covered
**n)** Ownership of hardware and software
**o)** Documentation (e.g. logs of changes, records of reviewing event logs)
**p)** Right to have information system audit conducted (internal or external).

## 10.3 Selection of Service provider:

All procurement should be made in a transparent manner through open and competitive bidding. When bulk procurement is possible, piecemeal procurements should be avoided. A specific outfit should be established in the headquarter to guide and manage the procurement process in the divisional and regional levels. Procurement should be made observing the high standard of financial property to maximum economy.

### Hardware:

Hardware procurement should be made consistent with the current business requirements of the Bank duly assessed by a competent committee appointed by the management.

**Software:**

Bank will endeavor to purchase only the most recently upgraded versions of software and/or those in wide use in the industry and are compatible with the hardware in place.
In procuring hardware and software Bank will strike a balance so that too many types are not added which may necessitate keeping too many inventories and making the system vulnerable to incompatibility. Bank will also ensure proper Software License management, service provider management as per industry best practices.

## 10.4 Cross-border System Support

10.4.1 BKB shall provide official authorization/assurance from the group ensuring the data availability and continuation of services for any circumstances e.g. diplomacy changes, natural disaster, relationship breakdown, discontinuity of services, or others.

10.4.2 The Disaster Recovery Site shall be multi-layered in terms of physical location and redundancy in connectivity.

# Chapter 11

## 11. Customer Education

With the advent of electronic Banking, customer's experience of Banking is therefore no longer fully under control of a Bank. In the age of self-service Banking model, a customer also has to be equipped to do safe Banking through self help. It is often said that the best defense against frauds is awareness of customer. With fraudsters constantly creating more diverse and complex fraudulent ruses using advanced technology and social engineering techniques to access their victim's accounts, accelerating awareness among customers became imperative.

It is also important to educate other stakeholders, including Bank employees, who can then act as resource person for customer queries, law enforcement personnel for more understanding response to customer complaints and media for dissemination of accurate and timely information.

### 11.1 Awareness Program

Awareness programs can be successful only if users feel the content is in their interest and is relevant to their Banking needs. For fruitful awareness program to be arranged, the Bank need to identify personnel, awareness material, advertisements and promotions and maintenance of websites.

11.1.1 The needs of the target audience shall be identified, appropriate budgets obtained and priorities established.

11.1.2 The work plan shall clearly mention the main activities with the required resources, timelines and milestones.

11.1.3 BKB shall create and publish proper contents.

11.1.4 The common objectives of the awareness program will be to:

a) Provide general and specific information about fraud risk trends, types or controls to people who need to know.

b) Help customer to identify areas vulnerable to fraud attempts and make them aware of their responsibilities in relation to fraud prevention.

c) Motivate individuals to adopt recommended guidelines or practices.

d) Create a strong culture of security with better understanding and commitment.

e) Help minimize the number and extent of incidents, thus reducing costs directly (fraud losses) and indirectly(reduced need to investigate).

11.1.5 BKB shall deliver the right message contents to the right audiences using the most effective communication channels.

11.1.6 Awareness building collaterals can be created in the form of :

**a)** Leaflets and brochures

**b)** Short Messaging Service (SMS) texts

**c)** Safety tips in account statement and envelopes

**d)** Educational materials in account opening kits

**e)** Receipts dispensed by ATM/POS

**f)** Screensavers

**g)** Electronic newsletters
**h)** DVDs with animated case studies and videos
**i)** Recorded messages played during waiting period of phone Banking calls.

11.1.7 Since the target groups obtain information from a variety of sources, more than one communication channel could be used to engage them successfully.

**a)** Advertising campaigns through print and TV media
**b)** ATM screens, Emails and SMS texts
**c)** Common website developed with content from all stakeholders
**d)** Groups, games and profiles on social media
**e)** Advertisement on online shopping sites
**f)** Billboards
**g)** Online training modules and demos hosted on this site
**h)** Posters in prominent locations such as petrol pumps, popular restaurants, shopping malls, etc.
**i)** Interactive guidance in the form of help lines
**j)** Customer meets and interactive session with specialists
**k)** Talk shows on television/radio.

11.1.8 Continuous improvement cannot occur without knowing how the existing program is working. A well-calibrated feedback strategy must be designed and implemented.

## 11.2 SECURITY

11.2.1 Bank users who identify or perceive an actual or suspected security problem shall immediately contact the IT Cell or ICT Division of BKB.

11.2.2 All sites and downloads may be monitored and/or blocked by BKB if they are deemed to be harmful and/or not productive to business.

11.2.3 To access social media accounts, while conforming the national social media policy.

11.2.4 Users shall not reveal account password or allow another person to use their account (i.e. E-mail, Banking Software, Remittance system) shall not use others credentials.

11.2.5 If any employee is unsure about what constitutes acceptable use he/she should check with their supervisor for further guidance and clarification. Management or supervisory personnel shall consult with the authority of ICT Divission for clarification of these guidelines.

## 11.3 PENALTIES

11.3.1 Any user violating these policies is subject to the loss of ICT resources usage privileges and any other disciplinary actions deemed appropriate by BKB authority.

## 11.4 USER COMPLIANCE

11.4.1 The ICT Division reserves the right to inspect any and all files stored in private areas of BKB network in order to assure compliance with policy.

11.4.2 All terms and conditions as stated in this document are applicable to all our employees, vendors, suppliers and partners who access our network and computers.

# Glossary and Acronyms

| | |
|---|---|
| 2FA | - Two-Factor Authentication |
| ADC | - Alternative Delivery Channel |
| AMC | - Annual Maintenance Contract |
| AML | - Anti-Money Laundering |
| ATM | - Automated Teller Machine |
| BCP | - Business Continuity Plan |
| BIA | - Business Impact Analysis |
| BRD | - Business Requirement Document |
| BYOD | - Bring Your Own Device |
| CAAT | - Computer-Assisted-Auditing Tool |
| CCTV | - Close Circuit Television |
| CD ROM | - Compact Disk Read Only Memory |
| CDs | - Compact Disks |
| CEO | - Chief Executive Officer |
| CIO | - Chief Information Officer |
| CISO | - Chief Information Security Officer |
| CNP | - Card Not Present |
| CTO | - Chief Technology Officer |
| DC | - Data Center |
| DDoS | - Distributed Denial of Service |
| DoS | - Denial of Service |
| DR | - Disaster Recovery |
| DRP | - Disaster Recovery Plan |
| DRS | - Disaster Recovery Site |
| DVD | - Digital Video Disc |
| E-mail | - Electronic Mail |
| EOD | - End of Day |
| ICC | - Internal Control and Compliance |
| ICT | - Information and Communication Technology |
| IDS | - Intrusion Detection System |
| IPS | - Intrusion Prevention System |
| IS | - Information System |
| ISDN | - Integrated Services Digital Network |
| ICT | - Information and Communication Technology |

| | |
|---|---|
| IVR | - Interactive Voice Response |
| JD | - Job Description |
| KRIs | - Key Risk Indicators |
| MITMA | - Man-in-the-Middle Attack |
| NBFI | - Non-Bank Financial Institution |
| OTP | - One Time Password |
| PCI DSS | - Payment Card Industry Data Security Standard |
| PCs | - Personal Computers |
| PDA | - Personal Digital Assistant |
| PIN | - Personal Identification Number |
| PODs | - Personally Owned Devices |
| POS | - Point of Sale |
| PSTN | - Public Switched Telephone Network |
| RPO | - Recovery Point Objective |
| RTO | - Recovery Time Objective |
| SDLC | - Software Development Life Cycle |
| SMS | - Short Messaging Service |
| SQL | - Structured Query Language |
| SSL | - Secured Socket Layer |
| TV | - Television |
| UAT | - User Acceptance Test |
| UPS | - Uninterrupted Power Supply |
| USB | - Universal Serial Bus |
| User ID | - User Identification |
| UTP | - Unshielded Twisted Pair |
| VA | - Vulnerability assessment |
| VLAN | - Virtual Local Area Network |
| VPN | - Virtual Private Network |
| WAN | - Wide Area Network |
| WLAN | - Wireless Local Area Network |

# 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-4.1.6)

BANGLADESH KRISHI
BANK

**ICTF-3**

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

## STOCK REGISTER OF HARDWARE

**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 |

## STOCK REGISTER OF SOFTWARE

| **Srl.** | **Software Title** | **Developed By** | **User** | **Purpose** |
|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 |

BANGLADESH KRISHI BANK

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

**ICTF- 4**

# 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 : | |

BANGLADESH KRISHI BANK

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

## ACCESS AUTHORIZATION LIST

**ICTF- 5**

| 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-5.6.1.3)

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-5.6.1.4)

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-5.6.1.4)

ICTF-8

BANGLADESH KRISHI BANK
………….BRANCH/DEPARTMENT
BRANCH CODE **:** ……………

01. I. Name of the User : P.F Index :

II. Designation (With Mobile No.) :

III. Address : Branch Name : Branch Code :
Branch Phone no. :
Region: Division:

IV. Date of joining :

V. Transfer From : Branch Name: Branch Code:
Previous CBS User Code (If Online) :

VI. Transfer Date :

VII. CBS User Code of this Branch(If Posted Before) :

02. User Status : Entry(Posting)/ Authorizer/ Teller/Clearing /
Trade Finance/ Treasury Management/ Sanchoypatra

03. User Rights Proposed : Module Name(s) :
(Read, Write, Delete, copy, Change, Print)

| | | |
|---|---|---|
| | Recommended/Proposed By: | Approved By : |
| Users' | Signature : | Signature : |
| Signature : | Designation : | (Manager/Head of the Department or Office). |

(*For Use of computer Section of the Branch/computerdepartment/System owner Department*)

| | |
|---|---|
| Accepted for implementation for the | User Created : |
| following Rights: | a) On: …………………….. |
| 1. | b)User ID: …………….. |
| 2. | c)User Password: ………….. |
| 3. | |
| 4. | |
| 5. | |
| | Signature With Seal |
| Signature : | (In charge of system Administrator) |
| (Branch Manager/Head of the Department/office-system owner) | |

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: | Signature: |
| (Handing over Officer) | (Receiving Officer) |
| Name : | Name : |
| Designation: | Designation: |
| Address : | 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-6.2.8)

BANGLADESH KRISHI BANK

**ICTF- 10**

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

## BACK UP LOG BOOK

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-7.6.6)

**ICTF-11**

# Dispensation Form

| | |
|---|---|
| **Reference:______________________________________** | **Date:_________** |

**Section I: Requester Information**

Name of the Office:

Requested by:

Requestor's designation:

Requestor's telephone #:

Request Date:

**Section II: Risk Overview**

Guideline reference (Clause) and description:

Risk Details (Process/Application/System/Product):

Justification:

Plan of mitigation:

Mitigation Date:

**Section III: Approvals**

The undersigned agree and accept the risk documented on this form.

Name:

Designation:

Comments:

Date:

Signature & Seal:

# User Request Form for Domain, E-Mail & Internet Access ICTF-12

| | | |
|---|---|---|
| **User/Access for:** | ☐BKB Executives<br>☐Head Office Employee<br>☐Head of Dept./In-Charge<br>☐Branch Employee | ☐Third-Party/Vendor<br>***Please provide Third-party Declaration also.* |

| | | | | |
|---|---|---|---|---|
| **User Specification:** | ☐Domain ID<br>☐Internet Access<br>☐ Email Address<br>☐Group Email Address | | ☐Domain Administrator<br>☐Local Administrator<br>☐Special Permission | |
| **FOR BKB EMPLOYEE USAGE** | | | | |
| **Requestor Name:** | | **Branch/Department:** | | |
| **Designation:** | | **Email Address:** | | |
| **PF No:** | | **Group Email:**<br>(If required) | | |
| **Employee ID:** | | **Mobile No:** | | |
| **Job Description with justification of access:** | | | | |
| | **(** Do not mention only "official/business purpose". Clarify the specific requirements& Special Permission)** | | | |

| | | | |
|---|---|---|---|
| **FOR THIRD-PARTY/VENDOR USAGE** | | | |
| **Requestor Name:** | | **Designation** | |
| **Company** | | **User Name** | |
| **Access required for (justification of access):** | | **Name & Signature of In-Charge:** | |
| | | | |

**Requester Declaration:**

**For BKB User:**

I agree that I will be held responsible for any breach of confidentiality or actions resulting from misuse of the login names and passwords. I have responsibility to exercise care in the treatment of personal data.

**For Vendor & Third-party user:**

I understand that it is my/my unit head's responsibility to ensure that the access will be revoked after the job completion.
I/ my company shall be liable for any breach on the access granted.

____________________________
**(Requester Signature)**

Approved by:

____________________________________________
**(In-Charge/Manager/Head of Dept.)**

**Serial No: . . . . . . . . .**

## Completion of User Creation for Domain, E-Mail & Internet Access

| | | | |
|---|---|---|---|
| **WILL BE FILLED UP BY ICT DEPARTMENT** | | | |
| **Requestor Name:** | | **Computer Name:** | |
| **Department/Branch** | | **IP Address:** | |
| **User Name:** | | **User Specification:** | |
| **Email Address:** | | | |

| | |
|---|---|
| **JOB DONE BY:** | |
| **Name :** | |
| **Designation:** | |
| **Completion Date:** | |

____________________________

**Approver Signature**

# Bangladesh Krishi Bank

Information & Communication Technology Department

## Confirmation of User Creation for Domain, E-Mail & Internet Access

| | | | |
|---|---|---|---|
| **Confirmation of User Creation** | | | |
| **Serial No:** | | **Email Address:** | |
| **Requestor Name:** | | **User Type:** | |
| **Department/Branch** | | | |
| **Computer Name:** | | | |
| **User Name:** | | | |

____________________________

**Approver Signature**