AGRANI BANK LIMITED

Information & Communication Technology (ICT) Security Policy and Guideline, 2013

1. Preamble

1.1 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.

1.2 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.

1.3 This document formulates the ICT security policy of Agrani Bank Limited (ABL) which covers all computing and communications facilities including all hardware, data, software, networks and facilities 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.

1.4 This policy is inline 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.

2. Background

2.1 Agrani Bank Limited started using computer technology for automation of its various banking operations since pre-liberation, and many important jobs of the bank are currently automated. The Information Technology (IT) & MIS Division of the bank responsible for managing automation of banking operations is well equipped with IBM Midrange (AS400) computers and latest microcomputers and staffed with trained and experienced personnel. The bank uses its in-house software for processing most of the jobs performed in IT Division. The major jobs, handled in IT Division, includes inter-branch reconciliation, foreign bank accounts reconciliation (Nostro Accounts), consolidation of Statements of Affairs / Income & Expenditure Statements, Personnel System, Pay-roll of Head Office employees etc.

2.2 Agrani Bank Limited has grown significantly over the years in branch automation. Till date all 892 branches are computerized with branch banking software. Of which 154 branches are operating under T24 Centralized Online Core banking software (CBS). Rest of the branches will be brought under centralized On-line system in phases.

2.3 All branches including zonal offices, circles offices and divisions 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 using Moneygram, western union, Remit one etc using internet. Also all circulars, memo, letters, reports are being transmitted thru 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.

2.4 Bangladesh Automated Cheque Processing System (BACPS) under Bangladesh Automated Clearing House (BACH) has been implemented successfully in 312 branches.

2.5 A software (Zonal Office Solution) has been developed and installed by IT & MIS Division to all the zonal offices to compile all data related to Statement of Affairs and Profit & Loss statement from each branch under them, and send these to the Head office through internet where consolidated statements as well as various MIS reports are prepared. SWIFT Service is available in 35 AD (Authorized Dealer) branches of the bank to facilitate foreign trade operations that include quick disposal of LC's, foreign remittances etc. The 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 in 86 branches to facilitate e-tendering introduced by the government.

2.6 Agrani Bank Limited has introduced ATM services for its customers since 2002. ATM card holders can withdraw cash from 210 Shared ATM booths (5 in own premises) located at different places of the country. The Bank has planned to introduce its card management system with its own ITM.

2.7 Agrani Bank Limited has its own website (**www.agranibank.org**) with updated information of the Bank. The Bank also has its own mail server to provide e-mail facilities to concerned officials of the bank.

2.8 Currently, Agrani Bank Limited is facing challenges in operating software procured from different vendors due to dissimilarities in operating procedures, platform and consequent incompatibility. However, in developing or purchasing

software bank should be careful about its competitiveness in the market and compatibility with the current and future business environment as well as with other banks.

2.9 While formulating the policies, applicability at all tiers (Tier 1 through Tier 3) as defined in Bangladesh Bank ICT Guidelines for scheduled banks and financial institutions were taken into account.

3. ICT security policies and guideline

Against the backdrop as explained in the preceding section, the following policies have been formulated to realize the ICT vision of the bank.

4. Vision

To harness the potential of ICT as a key contributor to the growth and development of banking business and services of Agrani Bank Limited.

5. Scope

This ICT security Policy is a subset of the Bank's corporate governance policies, providing a systematic framework around which these policies have been formulated, with particular emphasis on the security of information and information systems and also on the Communication System. This covers all aspects of information that are electronically generated, received, stored, printed, scanned, and typed.

This policy is applicable to all of the Bank's ICT systems and all activities and operations required to ensure data security including facility design, physical security, network security, disaster recovery and business continuity planning, use of hardware and software, data disposal, and protection of copyrights and other trade related aspects of intellectual property rights**.**

6. Objectives of the policy and guideline

- To ensure a dependable information system for efficient management and operation of the bank;
- To promote and facilitate widespread 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 installed;
- 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;
- Procedure for periodic review of the policy and security measures;
- To ensure the best practices (industry standard) of the usage of ICT that is not limited to this guideline.

These policies and guidelines are established in order to assure that the investments in ICT generate business value and mitigate all associated risks within a clearly defined structure of roles and responsibilities. These cover all aspects of information that are electronically generated, transmitted, received, stored, printed, scanned, and typed. The provisions of this Guideline apply to:

- *All of the Bank's ICT systems; and*
- *All activities and operations required to ensure data security including facility design, physical security, network security, disaster recovery and business continuity planning, use of hardware and software, data disposal, and protection of copyrights and other intellectual property rights.*

7. Policy Statements

The policy statements along with this guideline have been structured around the objectives of the policy to provide guidance for the action points required for its implementation. It is also established in order to assure that the investments in ICT generate business value and mitigate all associated risks within a clearly defined structure of roles and responsibilities.

8. Categorization of the Bank's ICT Operations

The locations for which the ICT security guidelines are applicable i.e., the Head Office, Zonal Office, Branch and/or Booth of the Bank may be categorized into three tiers as under, depending on their ICT setup and operational environment / procedures :

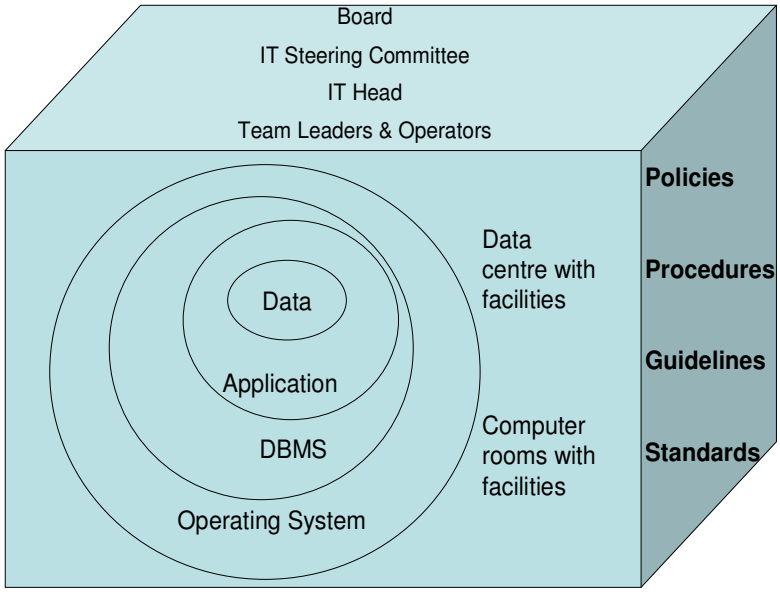
Tier-1: Centralized ICT Operation through Data Center including Disaster Recovery Site (DRS) to which all other offices, branches and booths are connected through WAN. 24x7 hours attended operation.

Tier-2: Head Office, Zonal Office, Branch or booth having Server to which all or a part of the computers of that locations are connected through LAN.

Tier-3: Head Office, Zonal Office, Branch or booth having stand alone computer(s) or ATM(s).

The proposed ICT security guidelines will be applicable for all the three tiers unless otherwise mentioned specifically.

Fig. 1 ICT Universe



9. Terminology

ICT: "Information and communication Technology" (or ICT) refers to computers, accessories, network & communication equipments, software, procedures, information, services and related resources. ICT also include any subsystem of equipment that is used to acquire, store, manipulate, move, control, display, interchange, transmit and receive data or information. It provides support to management, business process and also increases operational skills of the users ,provides tools and facilities which can revitalize the business process and enables better performance with increased reliability, efficiency and security.

Information: "Information" includes data, text, images, sound, voice, codes, computer programs, software and databases.

Computer: "Computer" means any electronic data processing device or system and includes all input, output, processing, storage, computer software, or communication facilities that are connected to it.

Data: "Data" means a representation of information which is used in a computer system or computer network, and may be in any form or stored internally in the memory of the computer.

Database: Traditional "databases" refer to information that is organized by fields, records, and files.

Field: A "field" is a location which is used to store a single piece of information in number, text, symbol, image, audio, video that are being prepared or have been prepared in a formalized manner or have been produced by a computer, computer system or computer

	network and are intended for use in a computer, computer system or computer network.
Record:	A “record” is one complete set of fields.
File:	A “file” is a collection of records
Database Administrator:	A person (or a group of people) who has/have administrative rights to the database and is/are responsible for the maintenance of the performance of the database.
Network Administrator:	The individual who has administrative rights and responsibilities for the installation, management and control of a network.
System Administrator:	A person who has administrative rights and responsibilities for managing an organization's computer and operating system.
DBMS:	A database management system (or “DBMS”) facilitates access to information from a database. It is a collection of programs that enables us to enter, organize, and select data in a database. The term database is used as shorthand for database management system.
Computer resource:	It means computer, computer system, computer network, data, computer database or software.
Computer network:	It means the interconnection of one or more computers whether or not the interconnection is continuously maintained.
Computer Virus:	It means any computer instruction, information, data or program that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a program, data or instruction is executed or some other event takes place in that computer resource.
Computer damage	It means to destroy, alter, delete, add, modify or rearrange any computer resource by any means.
Electronic Form:	In ICT, it means any information generated, sent, received or stored in media, magnetic, optical, computer memory, microfilm, computer generated micro fiche or similar device.
Electronic Record:	It means data, record or data generated, image or sound stored, received or sent in an electronic form or micro film .
Function:	In relation to a computer, includes logic, control arithmetical process, deletion, storage and retrieval and communication or telecommunication from or within a computer.
Access:	It means gaining entry into, instructing or communicating with the logical, arithmetical, or memory function resources of a computer, computer system or computer network.
Encryption:	It is the process of transforming data into an unintelligible form as a means of safeguarding its confidentiality during transmission and while in storage.
Remote Access:	It means gaining entry into, instructing or communicating with the logical, arithmetical, or memory function resources of a computer, computer system or computer network from a remote distance.
Originator:	Refers to a person who sends, generates, stores or transmits any

	electronic message or causes any electronic message to be sent, generated, stored or transmitted to any other person but does not include an intermediary.
Intermediary:	With respect to any particular electronic message "intermediary" means any person who, on behalf of another person, receives/ stores/transmits that message or provides any service with respect to that message.
E-mail:	Electronic mail transmitted through any computer network.
Sensitive Information:	Information that is sensitive to the organization
Unauthorized Disclosure:	To disclose any information through network without any prior permission or proper authorization
ISP:	Internet service provider
Broadband:	Internet connection using cable/wireless media from any ISP .
Modem:	A device which is required to any network link which use telephone or any other network.
Dial up:	When a telephone line is used to connect any network
DSL:	Digital Subscriber's Line.
Server:	A high-configuration computer which is capable of handling large volumes of data and transactions and serves with resources to its clients.
CPU:	"Central Processing Unit" or (CPU) generally means the main body/part of the computer which is a programmable logic device that performs all the instruction, logic, and mathematical processing in a computer.
Clients:	A relatively low configuration computer which shares resources with its server.
SWITCH/HUB:	It is an inter-connector used for connecting computers, printers in a network.
Network connection:	A connection to or with external resources.
Third party:	Any vendor, service provider, party external to the organization.

10. ICT Security Management

ICT security management must ensure that the ICT functions are efficiently and effectively managed. They should be aware of the capabilities of ICT and be able to appreciate and recognize opportunities and the risk of possible abuses. They have to ensure maintenance of appropriate systems documentations, particularly for systems, which support financial reporting. They have to participate in ICT security planning to ensure that resources are allocated consistent with business objectives. They have to ensure that sufficient qualified technical staffs are

employed so that continuance of the ICT operation area is unlikely to be seriously at risk at all times.

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

11. ICT Platform

Data Center, Disaster Recovery and other central servers must be Windows/UNIX / Linux-based and inherently free / protected from virus threats.

- Branch and other local servers may be Windows / Linux based.
- Client Operating System and application software's must be Graphical User Interface based.
- Open standard, client-server Relational Database Management Systems (RDBMS) must be used as Data Repository at the back-end of any software application whenever required.

- Small-scale software applications may be based on file based DBMS like MS Access/ FoxPro / Mysql that allows data manipulation using structured query language. But no flat file (text or binary format) shall be used as data repository.

12. Documentation

The systems already in place and to be developed further to meet future requirements should be documented according to standards set by the management. Any changes in the systems should also be appropriately reflected in the documents to facilitate further improvements in the systems design. Complete technical and user documentation must be provided for the systems together with regular updates in hard and soft copy form.

The following should be documented properly:

- An organogram chart for IT & MIS Department/Zonal office's/Divisions.
- Branch organogram chart with ICT support unit / section/ personnel (business/ICT)
- All records of IT Personnel mentioning skill in special field.
- A mandatory Service Level Agreement (SLA) vetted by skilled lawyer should be accomplished if any services/goods are taken from vendors & this document/agreement must be kept in safe vault.
- Job Descriptions (JD) for each ICT personnel should be prepared.
- A scheduled roster should be maintained for IT Operation.
- Segregation of duties should be maintained for IT tasks.
- Fallback plans for various levels of system support personnel.
- There should be clear instruction/guidelines relating to transfer, placement, promotion etc for IT personnel incorporated in Bank's personnel policies.

13. Internal Information System Audit

- Internal Information System Audit Team shall have sufficient IT Expertise/resources capable of conducting Information system Audit and who will be from relevant departments other than IT & MIS Department.
- IT experts should have training on software packages/ hardware and the team accompanied by the General Audit team of Audit Division will conduct audit in the branches to check fraud and forgery.
- Internal ICT System Audit should be done periodically at least once a year and the report must be preserved for inspection by Bangladesh Bank officials or Bank management or persons selected from the IT & MIS Division as and when required. An Annual System Audit plan shall be developed. Bank shall also ensure that audit issues are properly tracked and, in particular, completely recorded, adequately followed up and satisfactorily rectified.
- Previous reports pertaining to Audit compliance (issues raised/resolved) should be preserved and appropriate measures should be taken to address the recommendations made in the last report.

14. Training and Awareness

- A detailed training needs assessment must be undertaken to identify and document training needs
- Training should be coordinated with the implementation of any proposed systems so that no significant delays occur between commissioning and user training
- Before their deployment in ICT jobs, employees should be given adequate training on the aspects of importance and awareness of IT security.
- All network users and controlling officers on database maintenance, hardware maintenance, network operation, application software maintenance, should be trained on operation and security procedures and should be aware of their importance before assuming their responsibilities.
- A training database should be maintained to use for making decision relating to training and development of IT personnel.
- Minimum level of business foundation training should be arranged for ICT personnel.

15. Insurance or Risk Coverage fund

- Adequate Insurance coverage / or risk coverage fund shall be maintained so that costs of loss and/or damage to hardware/software asset related to ICT can be mitigated.

16. Problem Management

- Maintain a register for reported problems on daily/weekly basis.
- Assign a team to act on problem resolution responsibility.
- Process shall have the workflow to assign the issues to a concerned person to get quick, effective and orderly response.
- Ensure necessary corrective action within the time frame bounded by the severity of the problem.

- Maintain proper documents/registers relating to problem finding and resolution process.
- Provide remote systems problems information to specific support units and Regional Help Desks & Support Teams.
- Provide time-to-time communication support to remote support units.
- Ensure Virus detection & eradication at all levels of hardware.
- Establish Log-on administration and synchronization across servers and applications.
- Ensure efficient administration of user ID's for network applications and tools.
- Keep records of all users using the system access created by the vendor/ system administrator.
- Ensure safe keeping of Super user passwords in separate locations.
- Ensure periodic virus scans for PC / Server to monitor for virus propagation & perform virus detection and eradication.
- Provide updated information to all types of users by circular / letter regarding methods to prevent or handle possible virus attack.
- Maintain controls to protect printed outputs and portable storage media (tapes & disk packs) from unauthorized access.
- Process shall be established to review and monitor the incidents.

17. Appraisal Procedure Guideline

- Manual Appraisal procedure should be replaced by Electronic Appraisal Procedure.
- Electronic documents/proposals to be generated or forwarded to the superior authority through e-mail / file transfer for approval according to level of authority.
- Approval authority at different levels to be approved / rejected, adding comments / proposals / instructions to the next level of approval authority.
- Electronic documentation for appraisal procedures should be supported / backed by physical documentations until digital signature systems and e-documentations are implemented
- Necessary software for Investment Appraisal Procedure, Investment Risk Management, Investment Recovery Management, Human Resources Management, Assets & Liability Management, Management Information Systems (MIS) etc. should be procured / developed for the full functional implementation of Appraisal Procedure Policy.

18. Procurement / Purchase Policy

18.1 Vendor Selection

- Core team should be formed comprising of personnel from Functional Departments, IT Department and Internal Audit Department for vendor selection

- Vendor selection criteria for application should address the following:
  a) Market presence
  b) Years in operation
  c) Technology alliances
  d) Extent of customization and work around solutions
  e) Performance & Scalability
  f) Number of installations
  g) Existing customer reference
  h) Support arrangement

18.2 Hardware Procurement / Purchase :

- Requisitions / Requirements should be made through authorized proper channels.
- Requirement analysis are to be carried out by the IT & MIS Division.
- Recommendations are to be placed before the Procurement Committee and other competent authorities as per latest PPR/PPA. Procurement Committee/Procurement Cell will proceed for publishing tender Notice in the daily News Paper/ Collecting spot quotation as per approval of the competent authority .
- Tender Evaluation Committee will evaluate all the Tender Documents/Quotations
- Evaluation and Comparative Analysis with specific proposals should be placed before the appropriate level of management/ Board as per financial discretionary power for approval.
- Work Orders are to be issued, having approval of the competent authority.
- Items / components are to be received along with Invoices/Challan.
- Data / information relating to hardware and components are to be entered in detail into the Computerized Inventory Management System/Registers, to track transfers, re-locations of all items/components accordingly.
- Certification / comments of the item's / component's status are to be collected before allowing payments of bills.
- Warranty coverage and follow-up for maintenance arrangement should be maintained.
- Service Agreement where applicable are to be secured.

18.3 Software Procurement / Purchase :

- Bank will endeavor to purchase only the most recently upgraded versions of Banking software and/or those in wide use in the industry
- International vendors must offer their software through local business partners who have control over the source codes of the software and any service agreement shall be made with the local counter part of any international vendor.
- Software vendors must conform to internationally-recognized and industry-recognized quality management system standards like ISO or particularly BS7799.
- The Bank should take all steps and, detailed plans for, the reduction in the use of paper / hardcopy documents, and to incorporate all electronic services / facilities using the latest technology to support this objective.
- Software systems should preferably be in 3-tier architecture, regardless of whether they are purchased or developed in-house.
- Only Licensed Software should be purchased for the Bank's usage.
- Base License of all application software should be documented and preserved properly.

- Bank must never purchase/use pirated software.
- Service agreement against purchased software where applicable to be arranged.
- All the software procured and installed by the bank must have legal licenses and record of the same should be maintained by the respective unit/department of the Bank.

18.4 Software Development and Acquisition Policy

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

All in-house software development activities shall be guided and monitored by the Information Technology & MIS Division, Agrani Bank Head Office. Security should be included at the requirement analysis stage of each development or acquisition project. Statement of business requirements for new systems or enhancements to existing systems should specify the necessary controls. All kinds of storage devices or hardcopy containing program source codes shall be kept exclusively in the Information Technology & MIS Division at the Head Office.

18.5 In-house Software *Development Policy*

All in-house software development activities shall be guided and monitored by the ICT Division, Agrani Bank Limited, Head Office. Security should be included at the requirement analysis stage of each development or acquisition project.

- Detailed System Analysis and Design should be carried out under the IT & MIS Division prior to the development of any medium to large scale in-house software application. Small-scale applications may be designed and developed by a single application development team to facilitate rapid implementation requirement.
- The System Analysis and Design document must be jointly reviewed by at least one senior level System Analyst and one senior level Programmer in the IT & MIS Division.
- The System Analysis and Design document must be approved by a Senior System Analyst or equivalent / higher executives and placed for management authorization whenever necessary.
- Information Technology & MIS Division will set up an extensive test environment simulating a real production environment for the purpose of testing in-house developed and externally purchased software.
- The in-house developed software application must be tested by an independent test team comprised of one or more Assistant Programmers and the target user representative in the IT & MIS Division test environment.

- The application development team will prepare user manuals, technical documentation detailing the data structures, algorithms, class diagram etc.
- The archive must be labeled appropriately and handed over to appropriate Security Administration personnel.
- All software development PCs must be connected to a domain under a single Local Area Network to facilitate client server application development activities. There should be a domain server and optionally separate database and application server(s).
- The domain server must host broadband Internet connectivity to provide faster Internet access to the developers for Research and Development activities.
- A rich library should be setup in Information Technology & MIS Division to provide technical books to the IT Personnel to keep their knowledge up-to date.

- Criteria for acceptance of the requirement should be defined and approved by the concerned business unit
- Application security and availability requirements should be addressed
- Source code must be available with the concerned department and kept secured
- Source code should contain title area, the author, date of creation, last date of modification and other relevant information
- Software Development Life Cycle (SDLC) with User Acceptance Test (UAT) should be followed and conducted in the development and implementation stage
- Necessary 'Regulatory Compliance' requirements should be taken into account by the Bank.

18.6 Outsourced Software

Certain areas of business related to ICT to bring in enhanced efficiency may be outsourced.

All the software for the bank must be procured and installed through IT & MIS Division.

18.7 Software Documentation

- Documentation of the software should be available and safely stored
- Document should contain the followings :

a) Functionality
b) Security features
c) Interface requirements with other systems
d) System documentation
e) Installation manual
f) User manual

18.8 Other Requirements :

- A test environment to ensure the software functionalities before implementation should be available
- User Acceptance Test carried out and signed off before going live
- Necessary 'Regulatory Compliance' requirements for banking procedures and practices in the application should be taken into account by the Bank
- Bugs and/or errors to be checked due to design flaws, escalated to higher levels in Software Vendors' organization and bank, and be addressed in time
- Support agreement should be maintained with the provider for the software used in production with the confidentiality agreement

19. Risk management

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.

- Effective Risk management systems shall be in place for any new process and systems with post-launch review.
- Risk management function will ensure awareness of, and compliance with, the ICT security control policies, and to provide support for investigation of any ICT related frauds & incidents.
- The risk management process shall include
  - A description and assessment of the risks being considered and accepted for acknowledgement and approved by the owner of the risk.
  - identification of mitigation controls with remedial plan.
  - Formulation of remedial plan to reduce the risk
  - Approval of the risk acknowledge from the owner of the risk & senior management

20. ICT Operational Management Policy

20.1 Change Management

The objective of ICT change management is to achieve the highest levels of technology service quality by minimum operational risk.

- Changes to information processing facilities and systems shall be controlled.
- All changes of business application implemented in the production environment must be governed by a formal documented process with necessary change details. A sample form has been provided in **Annexure A.**
- Audit Logs of changes has to be maintained available for ready references.
- Signed off from the vendor should be obtained before implementation of changes of production.
- 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 **Annexure B.**

20.2 Asset Management

- An inventory should be kept with all significant details for hardware and software and must be reviewed at least once a year.
- All assets associated with information facilities labeled with tag and name.
- Assets shall be clearly identified and an inventory with significant details must be maintained.
- Bank must comply with the terms of all software licenses and must not use any software that has not been legally purchased or otherwise legitimately obtained.
- All data on equipment & associated storage media should be preserved before destroying or overwritten before sales, disposal or re-issue.
- Software used in any Computer must be approved by the authority. Use of unauthorized or pirated software must be strictly prohibited throughout the bank. Random checks shall be carried out to ensure compliance.
- Software used in production environment must be subjected to a support agreement.

20.3 Operating Procedure

- Operating Procedures shall be documented, maintained & available for the users related to their job function.
- Any changes to operating procedures must be approved by management and documented.
- The followings should be covered by the operating procedures where appropriate:

  a) Documentation on handling of different process;
  b) Documentation on scheduling processes, system start-up, close-down restart and recovery (including target time for start and finish);
  c) Documentation on handling of exception conditions;
  d) Schedule system maintenance.

20.4 Request Management

- To avail any service related to ICT, a formal request process must be established. A sample form has been provided in **Annexure C.**

21. ICT Security Policy

Data & Equipments should be protected from internal and external threats. Data, the most valuable asset for the Bank's operations, should be protected from any level of intruder. To avoid fraud and forgery, data & equipments should be maintained in a secure environment. There should be 2 types of Security, i. e : Physical Security & Information Security. The security policy covers data, data handling, authorized users & access control of users, external attack, hardware and location & position of hardware. There should be a 'IT personnel' for each location of IT operations. Following are the detail policies:

21.1 Physical Security

The objective is to prevent unauthorized access and damage of information assets and protection and it can be achieved by creating several physical barriers around business premises. The physical security can be breached in the form of-unauthorized entry, damage or theft to equipment or document, copying or viewing of sensitive information, alteration of sensitive equipment and information etc. A secured Data Library should be established to preserve Data Cartridges, CDs, License Copies of software, Agreements etc.

Physical security denotes providing environmental safeguards as well as controlling physical access to equipment and data. Adequate physical securities are to be ensured for all ICT assets to prevent any loss or damage from external sources. Data and equipment should be protected from internal and external threats. Data, the most valuable asset for Bank's operations, should be protected from any level of intruder. To avoid fraud and forgery and to prevent unauthorized access, data and equipment should be maintained in a secured environment.

Security devices are to be used in the following manner:

21.1.1.1 In the LAN and WAN environment, security measures should be ensured with Router, Firewall etc.

21.1.1.2 Other Security Devices should be procured and used for each location of IT operation.

21.1.1.3 There should be separate Servers for Database, Application, Exchange, Mails & others and the Servers should be located in different places.

21.1.1.4 Redundant Hardware, storage e.g. PC Server, Workstations, Monitor, Scanner *&* Printers should be procured and kept ready for instant support.

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

21.2 Physical Security Guideline for Tier-1

21.2.1 Data Centre Access

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

21.2.2 Environmental Security

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

- Sufficient documentation is required regarding the physical layout of the data centre including power supply & network connectivity documented.
- Documentation regarding the layout of power supplies of the data centers and network connectivity to be prepared.
- Floors to be raised with removable square blocks or channel alongside the wall to be prepared, which allow all the data and power cabling to be in neat and safe position with a view to protect from the risk of damage due to flood explosion.
- Water detection devices should be below the raised floor, if it is raised. Any accessories, not related to data center should not be allowed to be stored in the Data Centre.
- Existence of Closed Circuit Television **(CCTVs)** camera is required and to be monitored.
- Data Centre must show the **sign of "No eating, drinking or smoking."**

- 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.

- 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.

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

- Address and telephone or mobile numbers of all contact persons (e.g. Fire service, police station, service providers, vendor and all IT personal) should be available to cope with any emergency situation.
- Proper attention must be given with regard to overloading of electrical outlets with too many devices. Proper and practical usage of extension cords should be reviewed annually in the office environment.

- Development & test environment should be separated from production.
- Any accessories not related to / associated to data center will not be allowed to store in the data center.
- The following computer environmental controls to be installed:
    - Uninterruptible power supply (UPS) with backup units.
    - Backup Power Supply.
    - Temperature and humidity measuring devices.
    - Air conditioners with backup units.
    - Water leakage precautions and water drainage system from Air conditioner.
    - Emergency power cut-off switches.
    - Emergency lighting arrangement.
    - Dehumidifier to be installed.
- Determine if the above are regularly tested and that maintenance of service contracts exists on 24x7x365 basis.

21.2.3 Fire Prevention

- The Data Centre wall/ceiling/door should be fire resistant.
- Fire suppression equipment should be installed.
- Procedures must exist for giving the immediate alarm of a fire, and reporting the fire services and to be periodically tested.
- There should be Fire detector below the raised floor, if it is raised.
- Electric cables in the Data Centre must maintain a quality and concealed.
- Any flammable items should not be kept in the Data Centre.

22. Physical Security Guideline for Tier-2

22.1 Server room Access

- Server room must have a glass enclosure with lock and key with a responsible person of the Branch.
- Physical access should be restricted, visitors log must exist and to be maintained for server room.
- Access authorization list must be maintained and reviewed on regular basis.
- Servers which contain/store valuable computing resources of the bank should be maintained properly to prevent any kind of unauthorized intrusion or damage to it.

22.2 Environmental Security

- Desktop screen must be locked and Server must have password protected screen saver that should activate after 10 seconds.
- Administrative password of **Operating System** and **Database** should be written in sealed envelop and kept in vault.
- User creation request form should be maintained.
- Provision to replace the server within quickest possible time in case of any disaster.
- Server room should be air-conditioned.
- Water leakage precaution & water drainage system from air condition should be in place.
- Power Generator should be in place to continue banking operations in case of power failure.
- UPS should be in place to provide uninterrupted power supply to the server during power failure.
- Proper attention must be given on overloading electrical outlets with too many devices.
- Power supply system and other support units should be separated from production site and placed in secure area to reduce the risks from environmental threats.
- Power supply from source (Main Distribution Board or Generator) to data center should be dedicated (Electrical outlets from these power sources for any other devices must be restricted and monitored to avoid the risk of overloading)
- Channel alongside the wall prepared to allow all the cabling to be in neat and safe position with the layout of power supply and data cables
- Proper earthing of electricity should be ensured
- Address and telephone or mobile numbers of all contact persons (e.g. fire service, police station, service providers, vendors and all ICT/ responsible personnel) should be available to cope with any emergency situation.

22.3 Fire Protection

- Power distribution board for the PC with a **circuit breaker** should be placed outside the enclosure and covered with a box under lock and key **held by the Operator.**
- Power and other connecting cables for PCs must be kept secured from physical damage.
- UPS for backup power supply to be placed in the enclosure.
- Power supply of the PC should be switched off before leaving the branch.

- Fire extinguishers with expiry date mentioned, to be placed beside the power distribution board. This must be maintained and reviewed on an annual basis.
- Proper earthing of electricity shall be ensured.

23. Physical Security Guideline for Tier-3

23.1 Computer room Access

- The PC running the Branch Banking software must be placed in a secured area/ in a glass enclosure with lock and key and held by a responsible person in the Branch.
- Access authorization list must be maintained and reviewed on regular basis.

23.2 Environmental Security

- Operator must have the desktop password only known to him and kept written in a sealed envelope in the vault.
- PC must have password-protected screensaver which should activate after 1 minute of inactivity.

23.3 Physical Security for Desktop and Laptop computers

- Desktop and laptop computer should be connected to UPS to prevent damage to data and hardware.
- When leaving a desktop or laptop computer unattended, users shall apply the "*Lock Workstation*" feature (ctrl/alt/delete, enter) where systems allow.
- Password protected screen saver should be used to protect desktop and laptop from unauthorized access.
- Automatic screen saver should be activated after a period of inactivity. This period should not be more than five (5) minutes.
- Laptop computers that store confidential or sensitive information must have encryption technology.
- Desktop and laptop computers and monitors shall be turned off at the end of each workday.
- Laptop computers actively connected to the network or information systems must not be left unattended.
- Laptop computers, computer media and any other forms of removable storage (e.g. diskettes, CD ROMs, zip disks, PDAs, flash drives) shall be stored in a secure location or locked cabinet when not in use.
- Other information storage media containing confidential data such as paper, files, tapes, etc. shall be stored in a secure location or locked cabinet when not in use.

- Individual users shall not install or download software applications and/or executable files to any desktop or laptop computer without prior authorization.
- 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).
- Any kind of viruses should be reported immediately.
- Viruses shall not be deleted without expert assistance unless instructed by the IT & MIS Division.
- User identification (name) and authentication (password) shall be required to access all desktop and laptop whenever turned on or restarted.
- Standard virus detection software must be installed on all desktop and laptop computers, mobile, and remote devices and shall be configured to check files when read and routinely scan the system for viruses.
- 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.)
- On holiday occasions computers should be removed from floors and away from windows.

23.4 Fire Protection

- Preventive measures shall be taken to protect computer room from short circuits.
- Power and other connecting cables for PCs must be kept secured from physical damage.
- Power supply of the PC shall be switched off before leaving the branch.
- Fire extinguishers with expiry date shall be placed beside the power distribution board. This must be maintained and checked on an annual basis.
- Proper earthing of electricity shall be ensured.

Data and equipment should be protected from internal and external threats. Data, the most valuable asset for Bank's operations, should be protected from any level of intruder. To avoid fraud and forgery and to prevent unauthorized access, data and equipment should be maintained in a secured environment.

24. Information Security Policy

Access control consists of collection of mechanisms that specify what user can do on the system. There can be logical control, administrative control and physical control. Logical control includes the use of access control software such as firewalls, proxy servers, anti-virus software, passwords, smart card/biometrics, encryption, audit trails, intrusion detection system etc. Administrative controls

include security awareness training, separation of duties, security reviews and audits, rotation of duties etc. Physical control includes Identification Badges, memory cards Guard keys, locks, biometrics etc.

Access control policy for information system are as follows:

24.1.1 User Access Management: Formal procedure should be in place to control the allocation of access rights to information systems. The procedure should cover all stages in life cycle of user access, from the initial registration of new users to the final de-registration of users. Care should be taken for allocation of privileged access rights. Time to time review of user access rights is to be monitored. Again monitoring of system access by the system administrator is to be ensured.

24.1.2 User Account maintenance – creating users, groups, user-accounts, deleting user-accounts, modifying user accounts etc. on the system.

24.2 Password Control

- Passwords should be maintained with utmost secrecy to prevent unauthorized persons from any inappropriate use of ICT resource.
- The password should be minimum six characters having combination of upper-lower case, number & special characters and should be kept strictly secret.
    - Administrative password of Operating System, Database and Banking Application should be kept in sealed envelope and kept in a safe custody (centralized/decentralized)
- Password is to be locked for three consecutive invalid attempts.
- The password should be changed in every 30 days.
- Password maintenance is to be enabled to allow same password be used again only after using at least 4 different password.
- Password should be masked i.e. not visible.
- The terminal inactive time should be set 10 minutes.
- Sensitive password should be kept in sealed envelope with movement records.
- Operating time schedule for the user is to be fixed where necessary.
- Audit trail should be available to review the user profile for maintenance purpose.

24.3 User ID Maintenance

- Each user should be assigned to unique user ID and valid password and hard copies should be kept safely.
- The user ID should be locked after 3 consecutive invalid attempts.
- There should be control mechanism to ensure that user IDs and passwords are not same.
- The user ID form describing access privileges is to be approved by appropriate authority.
- User ID should be locked within 24 hours when user has been transferred or left the Bank.

24.4 File/System/application access management:

24.4.1 Input Data validation: Data input to application system should be validated to ensure that it is correct and appropriate. The input checks should be applied to business transactions, standing data and parameter tables.

24.4.2 Output data validation: Data output from an application system should be validated to ensure that processing of information is correct and appropriate.

24.4.3 Data encryption: Data encryption should be considered for the protection of highly sensitive or valuable data. The level of protection provided by encryption should depend on the strength of the underlying cryptographic algorithm, size of key space, length of key and the secure management of the key type.

24.4.4 Change control procedure: In order to minimize the corruption of information systems, there should be strict control over the implementation of changes. Formal change control procedures are to be implemented. The control procedures should ensure that security and security procedures are not compromised, that support programmers are given access only to those parts of the system that are necessary for their work and that formal interdisciplinary agreement and approval for any change are obtained.

24.5 Security monitoring & investigation

- Monitor physical security (through VDR)
- Access risks on a particular system (OS environment & user needs)
- Monitor network security (through software)
- Monitor denial of service attacks
- Track logins and logouts
- Perform security audit

24.6 Performance optimization & reporting

- Process and memory management
- Monitoring CPU performance
- Monitoring Hard disk /memory performance
- Monitoring input/output performance
- Monitoring Ethernet traffic etc
- Error detection & correction
- Troubleshooting & client support
- Backup file retention

24.7 Asset tracking

Inventory of all kinds of assets, such as information assets, hardware, software, licenses etc must be maintained for keeping track of all these assets. All data, equipment and associated storage media must be destroyed or overwritten before sale, disposal or reissue.

This covers hardware, software & peripherals changes, relocations and maintenance, for which a detailed inventory of assets should be maintained. The assets can be classified as follows:

24.7.1 **Information Assets:** Database and data files, system documentation, user manuals, training materials, operational and support procedures, continuity plans, fallback arrangements, archived information.

24.7.2 **Software assets:** Application software, system software, development tools and utilities.

24.7.3 **Physical Assets:** computers equipments (processor, monitors, laptops, modems), communication equipment (routers, PABXs, fax machines, answering machines), magnetic media (tapes and disks), other technical equipments (power supplies, air conditioning units) furniture, accommodation.

24.7.4 **Services Agreements:** computing and communication services, general utilities (heating, lighting ,power, air-conditioning).

24.8 Secure Disposal of equipments

The Bank's data cannot be compromised through careless disposal of equipments. It should be noted that 'deleted data' could easily be retrieved from storage media. So storage devices containing very highly sensitive data should be physically destroyed or securely overwritten, which is different from the ordinary 'delete' function. All items of equipments containing storage media e.g. fixed hard disks should be checked to ensure that any sensitive data and licensed software are moved or overwritten prior to disposal. Damaged storage devices containing very sensitive data may require a risk assessment to determine if the items should be destroyed, repaired or discarded.

25. Input Control :

- The system should not allow the person making the entry i.e. the creator/teller of the entry and the checker of the entry to be same and they should not have the authority to modify it.
- Any change in the entry should be done by Supervisor/Modifier.
- For any entry, final approval should be given by the authenticator i.e. section in charge.
- Master authority for all jobs should be kept with the manager.
- Audit trail must be clearly marked with user ID and date-time stamp.
- The system should restrict from being accessed specially to sensitive data/fields.

26. Network security :

The network design and its security should be implemented under documented plan and network access control as well as physical security for the network equipments should be ensured.

- The network design and its security should be implemented under documented plan.
- Physical security for the network equipments should be ensured.
  - Access should be controlled.
  - Network equipments shall be housed in a secure environment.
- Unauthorized access and electronic tampering is to be controlled strictly.
- Groups of information services, users, and information systems shall be segregated in networks e.g VLAN.
- Security of the network should be under dual administrative control.
- Firewalls should be placed for any external connectivity.
- Fallback connectivity for WAN should be ensured.
- There should be mechanism to detect unauthorized intrusion in the network.
- Data encryption should be used for data traveling through WAN.
- Connection of personal laptop to official LAN or wireless modem with laptops must be secured.

26.1 Network Access Control:

The Bank may use public or private network. The Bank must ensure appropriate security characteristics such as confidentiality, integrity and availability of business applications. Large networks should be divided into separate physical and logical domains. In this case control within the network, segregation of information services, users and information system should be considered. Following controls should be imposed:

27.1.1 Appropriate interfaces between networked services

27.1.2 Appropriate authentication mechanisms shall be maintained for remote users and equipments.

27.1.3 Control of user access to information services.

27. Data Encryption

- Any mechanism to encrypt and decrypt sensitive data traveling through WAN or public network should be in place.

28. Virus Protection

- All computer users must take steps to avoid viruses and if virus is detected, immediate action is to be taken to neutralize its effect on the computer system.
- Licensed anti-virus must be installed and enabled in each server, computer whether connected to LAN or not.
- Virus auto protection mode should be enabled in computer.
- The anti-virus should be updated regularly.
- All users must be trained / aware about computer viruses and their protection mechanism
- A system should be in place to scan all incoming e-mails for viruses.
- All computers in the network should get updated signature of anti-virus software automatically from the server.

29. Internet and E-mail Policy

Email must be used carefully to avoid viruses and to avoid releasing confidential material. Agrani Bank's website should be used to display only bank related information and the contents should not be modified without proper authorization.

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

Following should be considered for all official e-mails:

- A formal authorization process is to be followed for the allocation of official email addresses at the *agranibank.org* domain to the employees of the Bank.
- Email attachments having *.vbs / .exe / .api* extensions or any other file of executable nature shall not be exchanged or downloaded by employees of the Bank.
- No employee shall exchange proprietary data over email except within the Head Office network, without prior authorization from the information asset owner as per the asset inventory list.
- Employees shall not make any communication of information pertaining to religion, politics or other personal opinions, which are not job-related.
- Employees shall not exchange any obscene messages or information using e-mail.
- Employees must exercise utmost caution when sending any email from inside to an outside network.
- Sensitive information will not be forwarded via any means, unless that email is critical to business and is encrypted.
- All access to e-mail system and internet will be obtained only through official request

- Concerned department should perform regular review and monitoring of e-mail service
- All attachments with the incoming e-mail messages should be monitored especially for viruses
- The mail server should have latest anti-virus signature.

Agrani Bank's website may be maintained either by itself or by any outside vendor. Following matters should be taken care of for Bank's website operation.

- The materials displayed in the Bank's website shall not be modified, altered, changed without appropriate authorization
- The Bank's website should not be used for any illegal, immoral or unethical purposes.
- The website should not contain any obscene material or any material subversive of the state, religion, society or community.
- Material displayed in website should not violate any copyright, trademark or other proprietary rights of any other entity.

30. Transaction through alternative channels

30.1 Service through Mobile

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

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

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

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

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

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

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

Bank shall comply with 'Regulatory Compliance' requirements of the country. Proper documentation of security practices, guidelines, methods and procedures used in such mobile services shall be maintained and updated.

30.2 Internet Banking

Information involved in internet banking passing over public networks shall be protected from fraudulent activity, contract dispute, and unauthorized disclosure and modification.

Therefore, bank shall establish following control procedures:

I-banking standards shall be included in the Bank's ICT Security Policy.
Network and Database administrator shall ensure the security issues of I-banking.

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

Bank shall ensure real time security log for unauthorized access.

Bank shall define technology security protocols for 1. banking solutions like PKI (Public Key Infrastructure), SSL (Secured Socket Layer), 2. FA (Two Factor Authentication), RSA, VASCO etc.

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

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

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

b) Searching for back door traps in the programs.

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

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

e) Checking the weaknesses of the infrastructure.

f) Taking control of ports.

g) Cause application crash.

h) Injecting malicious codes to application and database servers.

All applications of bank shall have proper record keeping facilities for legal purposes.

Bank may keep all received and sent messages in restricted form.

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

30.3 Payment Cards

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

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

31. Business Continuity and Disaster Recovery Policy

Business continuity management reduces damage caused by disasters and security failures, which may be caused by natural disasters, accidents, equipment failures and deliberate actions, to an acceptable level through a combination of preventative and recovery measures.

The consequences of disaster, security failures and loss of services should be analyzed. Contingency plans should be developed and implemented to ensure that critical process could be restored within the required time scale. The plans, in turn, should be maintained and practiced as an integrated component of all other management processes and be accepted as such by staff members, suppliers and contractors. Finally, the Bank will establish policies to ensure business continuity and a disaster recovery plan will be developed for individual locations. Availability of all sorts of measures like mirroring, embedded data backup system, establishment of DRS etc should be ensured.

31.1 Business Continuity Plan : (BCP)

- Bank must have a Business Continuity Plan addressing the recovery of disaster to continue its operation
- Action plan to restore business operations will be within the required time frame, like i) during office hour's disaster, ii) outside office hour's disaster, and iii) immediate and long term plan
- Documents related to BCP should be kept in a secured off-site location (One copy should be stored in the office for ready reference)
- BCP should be tested and reviewed regularly to ensure the effectiveness

Action plan to restore business operation within the required time frame :

31.1.1 During Office hours

- The name address and telephone numbers of the contacting person should be clearly mentioned.
- Grab list of tapes, backups and components should be prepared.
- Emergency exit route map should be drawn and prominently displayed.
- List of emergency contacts like fire, electricity, telephone should be in place.
- All the steps in case of emergency should be written and put in a visible place.

31.1.2 After-office hours

- Ensure work stations and servers properly been shutdown
- Electric main switch has been shut off.
- Server room has been locked.
- Backup has been sent to Disaster Recovery Site/any nearest branch.

31.1.3 Back-up/Restore Plan (BRP)

- Documented backup procedure should be exist
- Creating backup schedule and responsibility list of taking back-up(at all levels of users).
- Daily backup should be taken in duplicate. One should be kept in branch and another to Zonal office. If a Zonal office is at a distant from the branch, it should be kept to a nearest branch.
- If there is no branch nearby, a copy will be kept in the residence of the manager with approval from higher authority.
- Back up media / inventory should be labeled properly indicating contents, date etc and signed by the appropriate authority.
- Backup inventory should be maintained, checked & signed by the supervisor.
- Back up log should be maintained, checked & signed by the supervisor.
- Backup should be sent to off site immediately after taking it.
- Restore of back up should be tested in every three months.
- A log for testing should be maintained.
- The bank should ensure the safety and security of the backup copies of information from not being damaged by natural calamities and theft (if possible to be sent at off-site location)
- The backup should be done periodically considering the cycle of:

  a) Weekly, b) Monthly, c) Yearly or as required by regulatory authority

31.1.4 Operators log :

Computer operators should maintain a log of all work carried out. Operator log should include the following

- System starting and finishing time.
- System errors and corrective actions taken
- Confirmation of the correct handling of data files and computer output.

31.2 Disaster Recovery Plan : (DRP)

Applicable for Tier 1 and Tier 2 :

- Disaster Recovery Site(DRS) is to be developed replicating the data center equipped with compatible hardware and telecommunication equipment and should be located at a distant place (At least 10 km) preferably to different seismic zone.
- Physical and environmental security of DRS is to be maintained.
- Information security is to be properly maintained through fall back and DR recovery process.
- DR test should be carried out at least once a year and tested copy of DR plan is to be preserved off-site.
    - DR site should be equipped with compatible hardware and telecommunication equipments to support the critical services of the business operation in the event of a disaster
    - An up-to-date and tested copy of the DR plan securely should be held off-site (DR plan should exist for all the critical services where DR requirement is approved by the business)
    - DR test documentation should include at a minimum:

      a) Scope, b) Plan, and c) Test Result.

As a general rule:

- The business continuity plan has to be properly maintained and should be audited by the IT Division at periodic intervals.
- Restored log should be maintained and should be audited by IT Division.

32. Software License Management & Maintenance Agreement

The following should be undertaken in connection with all maintenance agreements:

- Perform an inventory of software licenses in place as of a particular date.
- Develop & maintain a software license inventory database to include the licenses existing as of the start date and, for software procured through a bidding process or procured directly by the Bank.

- For any program / package provided by bidder / Bank, one original copy should be kept in IT division.
- Maintain data regarding entitlements for software upgrades, enhancements, refreshes, replacements & maintenance.
- Perform periodic audits to gauge compliance with software licensing terms and conditions, e.g., number of valid end users, site license agreements, volume purchase agreements, and other mutually agreed terms.
- Periodically review the price/performance/activity support that the Bank is receiving with regard to software licenses & maintenance agreements

33. Service Provider Management

Agrani Bank obtain goods & services from several external service providers in the following aspects:

Hardware	Procurement, Maintenance
Software	Procurement, Maintenance
WAN/ Web	Connectivity, Maintenance

The policies governing the above services are as follows:

- The bidder/concerned personnel/section/division will be responsible for:
  - obtaining equipment details and for receiving and providing asset management data
  - recording / tracking any hardware, software and peripherals (note: an initial inventory of hardware/software needs to be undertaken to validate and establish the database, and to define the process for tracking hardware and software throughout the life cycle from procurement through disposal, including any changes performed during the useful life of the asset)
  - the initial (baseline) asset inventory of hardware & software, which shall consist of: affixing an inventory tag, inputting the required information into the asset tracking database/file, i.e. configuration of hardware / software & network connectivity, status, location & ownership, vendor name.
  - perform calculations of the database depreciation
  - conduct periodic physical inventory
  - record activities related to troubleshooting/maintenance of hardware in a file/register.
- Service level agreement between the vendor and Bank should be in place
- Annual Maintenance Contract (AMC) with the vendor active and currently in-force should be in place
- All **Service Level Agreements (SLA)** between vendor and the Bank should be executed with clear specification of the following:

  - The bank shall ensure that the equipment does not contain sensitive live data when hardware is taken by the service provider for servicing/repairing

- List of hardware and deliverable services
- Price of Hardware/Software
- Time and Schedule for delivery of the components
- Name and designation of the contacting persons
- Frequency/Schedule of service reporting
- Ownership of the Hardware/Software
- Documentation of Service Log, reviewing event should be maintained.
- Warranties regarding both Hardware and Software should clearly be mentioned with time and nature.
- Roles and responsibilities of the contacting parties
- Time and date of renewal of contract
- Rights of changing of the terms and condition of the contract from Bank's side should clearly be mentioned in the modification clause.
- Geographical location for delivery of services
- Confidentiality clause
- Renewal period
- Modification clause
- Frequency of service reporting
- Termination clause
- Warranties, including service suppliers' employee liabilities, 3rd party liabilities and the related remedies
- Right to have information system audit conducted(internal or external)
- Audits rights from the Bank's side should be specified
- Liability of the supplier and of other third parties (if any) should be mentioned in respect of supply, quantity, quality and services for warranty period and thereafter

- The confidentiality of terms and condition of the contract should be specified
- There should be flexibility of discontinuing the contract in favor of Bank and terms should therefore, be clearly mentioned in the agreement.

33.1 Selection of Service Provider

All procurements should be made in a transparent manner through open and competitive bidding. Where bulk procurement is possible, piecemeal procurements should be avoided. A specific outfit should be established in the headquarters to guide and manage the procurement process. Procurement should be made observing the highest standard of financial propriety 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.

34. Outsourcing

- Outsourcing activities should be evaluated based on the following practices:
  a) Objective behind Outsourcing.

  b) Economic viability

  c) Risk and Security concerns
- Bank will develop a contingency plan for critical outsourced 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)

The Service provider should be selected from bidders considering the following.

- Objectives behind outsourcing
- Reputation of the service provider
- Manpower Strength.
- Financial Strength.
- Work Experience/after sale service.
- The lower value of goods/services.

35. Cross-border System Support

- The bank will 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

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

36. Rules and Regulations for Acquiring IT Hardware / Software / Services

- PPR (Public Procurement Regulations) should be followed.
- Separate teams should be formed for the various aspects of the acquisition: tender document preparation; tender evaluation; and evaluation after completion of work.

37. Systems Maintenance Policy

The bank should establish a support unit responsible for trouble shooting using a mechanism appropriate to ensure efficient handling of the trouble and having facility to keep records of events relating to trouble shooting.

38. Business Process Re-engineering Policy

The management should commission appropriate study to redesign the business processes to achieve improvements in performance, such as cost, quality, service, and speed.

39. Policy Implementation

Failure to adhere to the ICT Policy could result in suspension of usage privileges. Users who violate this policy will be subjected to bank's disciplinary processes and procedures including, but not limited to, those laid down in the existing Service Rules of the bank.

This policy document along with standard operating procedures should be published and made available and accessible to all concerned persons, authorities and organizations related to ICT operations in AGRANI BANK LIMITED. This policy is to be implemented phase-wise starting from the areas of priority to be decided by the management. There should be strict monitoring by the IT Division or concerned authority that the policy is being followed by the concerned persons.

40. Guideline Modification and Up-gradation

Information and Communication Technology (ICT) is continuously changing with rapidly changing global ICT environment. To cope with these changes, the total ICT guideline may be amended / modified and upgraded time to time to make it more efficient and appropriate one.

41. Conclusion

This document sets out the policies taking into account the current and future business environment as well as weighing the technical issues and the alternatives available. It also focuses on the future course of information systems that is implement-able and sustainable. The policy will be supplemented by a time bound action plan to take the ICT agenda forward. To respond to the emerging changes in ICT and also to ensure its continued relevance, the Policy may be amended / modified from time to time.

The End