FINAL YEAR PROJECT

[INFORMATION TECHNOLOGY POLICY FOR ONE BANK LTD]

Submitted By

Md. Mahabur Rahman
ID: 173-17-370
Department of MIS
Daffodil International University

This Report Presented in Partial Fulfillment of the Requirements for the Degree of Masters in Management Information System

Supervised By

Dr. Sheak Rashed Haider Noori
Associate Professor and Associate Head
Department of CSE
Daffodil International University

DAFFODIL INTERNATIONAL UNIVERSITY

DHAKA, BANGLADESH

JULY 2020

APPROVAL

This Thesis titled "**Information Technology Policy for ONE Bank Ltd**", submitted by Md. Mahabur Rahman, ID No: 173-17-370 to the Department of Computer Science and Engineering, Daffodil International University has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of MS in Management Information System and approved as to its style and contents. The presentation has been held on 09 July 2020.

BOARD OF EXAMINERS

Dr. Syed Akhter Hossain **Chairman**

Professor and Head
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

Dr. Md. Ismail Jabiullah **Internal Examiner**

Professor
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

Nazmun Nessa Moon **Internal Examiner**

Assistant Professor
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

Dr. Mohammad Shorif Uddin **External Examiner**

Professor
Department of Computer Science and Engineering
Jahangirnagar University

DECLARATION

I hereby declare that, this project has been done by me under the supervision of **Dr. Sheak Rashed Haider Noori, Associate Professor and Associate Head, Department of CSE**, Daffodil International University. I also declare that neither this project nor any part of this project has been submitted elsewhere for award of any degree or diploma.

Supervised by:

Dr. Sheak Rashed Haider Noori
Associate Professor and Associate Head
Department of CSE
Daffodil International University

Submitted by:

Rahman

(Md. Mahabur Rahman)
ID: 173-17-370
Department of MIS
Daffodil International University

ACKNOWLEDGEMENT

Firstly, I wish to express my heartiest thanks and gratefulness to the almighty Allah, whose divine blessings make me successful to complete this thesis.

Secondly, I would like to acknowledge the constant support and sacrifice of my dear parents towards me from the very beginning of my life. I am really thankful and grateful to them.

I really grateful and wish my profound, my indebtedness to **Dr, Sheak Rashed Haider Noori, Associate Professor and Associate Head**, Department of CSE Daffodil International University, Dhaka. His Deep Knowledge & keen interest in the relevant field helps me lot to carry out the research work and paper work. He always helped me through his scholarly guidance, true encouragement, constructive criticism and valuable advices during the whole time of the research work.

I would like to express my heartiest gratitude and love to **Prof. Dr Syed Akhter Hossain, Chairman** and Head**,** Department of CSE and other faculty members of my department of CSE of Daffodil International University who always gives me courage and support.

Finally, I would like to appreciate my course mates in Daffodil International University, who took part in this discuss while completing the course work.

ABSTRACT

According to the Bangladesh Bank, every Bank and Financial Institution must have an ICT Security policy. This report titled **“Information Technology Policy for One Bank Ltd”** is aimed to provide a complete guideline for the bank. This policy is designed under th direct guidelines of Bangladesh Bank Guideline on ICT (Information and Communication Technology (ICT) Security for Scheduled Banks and Financial Institutions. This guideline is a systematic approach to policies required to be formulated for ensuring security of all online activities of the bank and its information system. The guideline covers all the aspects of the information security related to the banking and financial activities. The provisions of this Guideline are applicable for:

- Information system of all the banks and FIs.
- All activities and operations must ensure the security measurement including facility design, infrastructural and network security, risk ICT risk management and disaster recovery and business continuity planning, data disposal and various intellectual property rights.

Regarding to the protection of the informational assets of the organization an inclusive IT Security Policy must be produced. The authority of the One Bank Limited initiated the process of development of its own “IT Security Policy”. The One Bank Limited considers Information as the most precious and important asset of the organization. Which must be highly secured and safeguarded according to the data protection law. However, intangibility is not the only uniqueness of the informational asset but without the proper security measurements this can be easily used unlawfully without depriving the legitimate owner from its possession. So all aspects of the information security needs to be in the policy list.

All policies are tested at different stages according to the standards and only when a policy pass against all standards and proved that it is successful according to the Bangladesh Banks suggested guidelines then it is implemented.

TABLE OF CONTENTS

CONTENTS **PAGE NO**

1. INTRODUCTION

Since, Information is the most valuable thing in today's world, Information Security is the top priority and most crucial issue for organizations, especially for banking and financial institutions. The bank is responsible for the protection of its information form the unauthorized access, modification, disclosure and omission. These can cause serious trouble for the existence of the organization. Information security mainly about the confidentiality, integrity and availability of the information. A strong and effective security policy can ensure the security of the banks information system. The One Bank Limited is going to design and develop its IT Security Policy under the Bangladesh Banks guideline on ICT security for banks and non-bank financial institutions. This policy will ensure the protection and maintenance of the information and information technological assets. These policies are minimum requirements for the information security and technological adoption.

2. PURPOSE AND SCOPE

The main purpose of this Policy is to set standards and approach to ensure the minimum control requirement over the information and information infrastructure of the One Bank Limited. This means its purpose is to protect the confidential and/or sensitive electronical information of the bank and also to secure the bank's information technological assets. It provides the guidelines to protect the electronic banking system and enhance ICT risk management. It explains the stakeholders' roles and responsibilities of individuals regarding to the information security and data protection.

Information security is not an individual matter rather it is about team effort. Another, purpose of this policy is to aware and train the all users of ICT facilities of the bank. Thus, each employee must follow the policy and will be punished in case of violating the policy rules.

This policy covers the all aspects of the ICT assets security for electronic banking such as illegal access, modification, or destruction of network components, computers, applications and or data owned or operated by the One Bank Limited.

3. DEFINITIONS

Access Control is a mechanism that prevent the unauthorized access to the application, data and e-banking features.

Authorized User means an individual person or a computer or application who has the legitimate access to the Bank's computer network, electronic banking system or data.

Change refers to any kind of adoption of new applications, features or modification of a service policy, updating or removal of existing application or feature or services.

Change Management refers to the management approach which determines when a change is required and how to perform the required change without hampering the regular activities.

Data Center is a physical place with the relevant equipment where all the information and applications are stored and managed.

Data Integrity means that the data is not tempered and intended users can understand the meaning of the data what actually it meant.

Disaster means any unwanted situation or occurrence for what the regular electornic banking or its parts can be affected badly. It might be network failure, hacking attempt and many other things that insist the unavailability of hardware or software resources of the bank.

Firewall is a system to monitor the incoming and outgoing network traffics of a private network or device and decide whether to allow or block the traffic from/to the network or devices.

Information System is a combination of components used to collect, process, store, retrieve and distribute information of the Bank.

Information Technology is the combination of all forms of technologies that are required for electronic data store, process, retrieve, transmit and manipulation.

Network is a collection of inter-linked computers or other devices that are linked for the purpose of sharing resources or exchanging files or enabling electronic communication between those computers or the devices.

Proxy Server used to hide the location and data of actual server form the hackers. It is a server that act as intermediary between the users and their requested resources contained servers.

Scheduled Change is the change that is ready to implement and waiting for the given time to take action or change that is predetermined to occur in a particular time.

Security Breach is incident which occurs unauthorized access to the information on a computer or network or services of an information system.

Sensitive Information are those that are very much important and secret and requires high level of security and protection. If integrity of the sensitive information violates that might cost a bunch for the Bank.

Unscheduled Change is the changes that is not pre-determined rather it required emergency basis for system failure or security breach.

4. ROLES AND RESPONSIBILITIES

4.1 Board of Directors

Approval of the IT Policy is vested with the Board of Directors. They are also responsible for reviewing the changes of the IT Policy from time to time. Board of Directors will review the IT security compliance report that will be prepared by Internal IT. They will also provide guidance and assistance to IT Division in the enforcement of IT Policies.

4.2 ONE Bank Senior Management

The ONE Bank Senior Management will ensure implementation of all application / process specific information standards and provide advice and guidance from time to time regarding the same. They are also responsible for pointing out discrepancies in the standards and for requesting waiver from the Information Technology Division Head to particular standards if that would be in the bank's interest from a regulatory, financial or business driven viewpoint.

4.3 Information Technology Division Head

The ONE Bank Information Technology Division Head is responsible for the timely release of new standards and updates to existing standards, and also liaising with the policies, procedures and standards utility group. The Information Technology Division Head is also the first point of contact (along with Audit) for all security incidents and investigating what actions should be taken to stop such incidents from occurring in the future.

4.4 Network Manager

The ONE Bank Network Manager is responsible for the overall management of network resources like LAN , WAN and Corporate E -mail . He /she will also be responsible for establishing Firewall and related software so as to protect Information Resources from external attack.

4.5 System Administrator

The ONE Bank System Administrator provides first level services on operating systems such as Windows, Linux and UNIX. He /she will also provide use rids and data access rights. He /she will be responsible for the monitoring of access violations and access rights recertification to the application system resources.

4.6 Database Administrator

The ONE Bank Database Administrator is responsible for the installation, configuration and performance tuning of the database system. He/she is also responsible for publishing the backup and, recovery strategy and overall management and monitoring of the storage system.

4.7 Data Center Manager

All responsibility regarding to the management and security of the data center and its resources and operation upon the One Bank Data Center manager. He/she will also be responsible for ensuring the availability of Disaster Recovery Site (DRS) in case of any failure at production end.

4.8 Branch Managers, Other Divisional Heads and Employees

Managers and Divisional Heads will ensure that their employees have access to the information standards in a format that they understand, that they have read them and that they are aware of the implications of non-compliance. Local management and employees must be aware of the security and must maintain the rules and regulations mentioned in this policy. Authority can punish or take legal action for violation of the rules.

4.9 Internal IT Auditor

Internal IT auditor will be responsible for developing an annual information system audit plan as well as monitor the entire system, data extraction, analysis and fraud detection. Internal IT Auditor needs to audit periodically and annually and address the required action to be taken.

4.10 Vendors, Subcontractors and Outsourcers

In the provision of Information Systems services, suppliers must comply with the ONE Bank Information Security Standards as they apply to hardware, software, and related procedures and processes.

The suppliers and other vendors must maintain the One Bank's IT security policy otherwise the bank will take action against them even the bank reserves the right to cancel the agreement with related party.

5. PHYSICAL SECURITY

Necessary control measurements need to be put in place to protect physical access to the bank's ICT infrastructure and resources in line with identified levels of acceptable risk. This can range from simple security measures to complex security measures to protect a user's display screen or a room or facility at server machines location machines to complex security installations. To identify, diminish and foil the impact of unintentional or unauthorized access to the information system physical assets or infrastructure restriction and access control must be imposed.

5.1 Control Standards – Physical Access to Data Center

Data center of One Bank Limited processes, store and transmit the sensitive and important information of the bank usual operations. It is very easy to damage or unethical doings with the information if physical access is possible to information system infrastructure. To ensure the security of the physical access to the ICT infrastructure high level of access restriction and authentication process need to impose. The bank should incorporate the below listed standards:

5.1.1 Card key access for authorized individuals to gain entrance.

5.1.2 Logging of card key access use for audit trail purposes retained for 12 months.

5.1.3 A visitor access log to record non-Data Center personnel visits including vendor, maintenance, and cleaning crew people. All visitors must be escorted while in the Data Center.

5.1.4 Every personnel in the secure zone need to carry a visual identity and without identity any one can be challenged as potential threat to the asset.

5.1.5 Regular review by the Data Center Manager of the authorization list for Data Center access and the Data Center Visitors Log. Personnel should only be afforded access only when required and authorized.

5.1.6 Any kind of electronic devices like mobile phone, photographic, video etc. must not be allowed in the secure zone unless authorized.

5.1.7 Where possible, internal monitoring of data center activity (CCTV) by Data Center Manager or by authorized personnel.

5.1.8 Entering to the datacenter with the mobile phone having built-in camera strictly prohibited.

5.1.9 Appropriate physical construction standards to discourage unauthorized access attempts such as:
- True floor to ceiling Data Center perimeter walls and where appropriate motion detectors in the surrounding areas to detect unauthorized access attempts.
- Automatic door closers on all doors. Doors into the secure area should not be propped open at any time, unless security guard is placed at the door.
- The absence of entrance vulnerabilities such as windows or external hinges on entrance doors to the Data Center.
- Data centers should be moved away from the public areas and also direct access of public vehicles to the data center should be restricted.

5.2 Control Standards - Business Unit Network Server Physical Access

Local area networks (LANs) used by branches of the One Bank to utilize the centralized electronic banking have to maintain following standards to ensure physical access control-

5.2.1 Local network infrastructure must be moved to de physical danger free areas not having public access, fire and water threats etc.

5.2.2 Only authorized Network Administrators can access to the local network infrastructure including servers and this area must be signed as entry restricted.

5.2.3 Required vulnerability and security tests must be performed before installing any software application of hardware changes.

5.2.4 All equipment should be maintained as defined in the manufacturer's guidelines.

5.3 Control Standards - Business Unit End User Workstation Physical Access

5.3.1 Employee workstations must be kept outside of public access and proper security measures to prevent fire, water and other physical need to maintain.

5.3.2 Workstations connected to the network must store sensitive information on file server drives and not local drives. Storing or transferring of sensitive information and files must be restricted by the system and carrying portable storage devices are completely prohibited in to the branch area.

5.3.3 Software to be used on the workstation must be scanned for viruses.

5.3.4 All equipment should be maintained as defined in the manufacturer's guidelines.

5.4 Control Standards - End User Portable Laptop Computers Physical Access

5.4.1 Since portable laptops are highly risky to storing sensitive devices because of having probability of losing or crashing the laptop all information must be stored only into the secure servers only.

5.4.2 All the portable computer device must be protected by disk encryption, antivirus, firewall and other security considerations.

5.4.3 All portable laptops and devices need to locked into a secure locker outside the business hour and devices must be locked with the employee desk in the business hours.

5.4.4 All portable computers that are used for company business must have a "Power - On" password set. The use of passwords must follow the guidelines specified in this document. The only exception to this rule, are those Laptops that have Windows NT installed, and whose Fixed Disk Drives have been partitioned for NTFS, since the user is required to sign on to NT each time the PC is powered on.

5.4.5 When traveling, official laptop carrying is strictly prohibited without the permission and security measures.

5.4.6 All equipment should be maintained as defined in the manufacturer's guidelines.

5.5 Environmental Threats and Controls

5.5.1 Power Backup for emergency situation

Digital information system infrastructure and its supporting environment need sufficient uninterrupted electricity supply to provide consistent service. load shedding and other electrical surges and interference may affect the performance as well as the durability of the information system components like servers, workstations and cooling and alarm systems. Power back up is very much important for the consistent and smooth service and also to avoid any physical damage of the components. At least two different power backup option must be deployed in every branch and also in central data center. Electric or diesel generators, uninterruptable power supply (UPS) or rechargeable digital sensor-based batteries can be used to ensure electrical power backup and 24/7 system uptime. Entire power supply and backup system needs regular checking.

5.5.2 Emergency Power-off Switches

Accidents and emergency situation can arise any time at anywhere. To protect the ICT infrastructure and information system the one Bank data center and all branches must take some precaution. Emergency central shutdown switch, automated circuit breaker etc. must be deployed and protected prom unauthorized access.

5.5.3 Emergency Lighting

In data centers and network server closed areas, automatic emergency automatic lighting should be incorporated for uncertain light out.

5.5.4 Water and Humidity Safety Measures

Since information system environment and infrastructure is water and temperature and humidity sensitive. Water and high temperature can affect the performance and even may damage the components of the information system. Data center must be protected from the unusual water flow and servers needs to established away from water and water sensor and quick action plan should be adopted in order to quick response incase of water sensitivity. On the other hand, server rooms must be well airconditioned and backup cooling system also need to exist. Temperature and humidity sensor and automated air-conditioning system based on the sensor need to implement in order to maintain proper temperature into the server room.

5.5.5 Fire Detection and Fire Suppression

To avoid heavy lose incase of accidental fire, proper measurement needs to be taken in consideration. The One Bank Data Center and local network must be implemented digital and effective fire detection and controlling technology. Smoke and fire detection sensor, alarm must be deployed in potential areas and fire extinguisher, hose pipe and emergency watering system also should be there. To avoid massive loss the alarm system should be associated with the nearest fire service center. Whenever fire will be detected alarm will be bell on the fire service station and they can response quickly. Any kind of smoking is strictly restricted in the datacenter and branch area. No combustible things should be stored inside the data center, server room and or local branches to avoid fire.

5.5.6 Maintain Building Construction Standards

It must be checked and ensured that data center and branches of the One Bank must be build according to the standards of the local authority. The building must contain emergency considerations like fire escape, fire exit, earthquake and flood resistant. Other natural and accidental disaster facing must be contain in the building.

6. LOGICAL SECURITY

Besides the physical security of the data center, network and workstations the logical security is also very much important for the One Bank Limited. The entire information system needs to be secure from any kind of logical security threat. All the components of the Information must use latest version of hardware, software. Latest security patches, regular update of third-party applications must install on a regular basis and also the cyber security team should be formed to find the potential bugs and threats and minimize the effect.

6.1 User Identification and Authentication

The system must be able to identify each individual user uniquely and also able to verify the user identity based on the given credential.

The general requirements for Identification and Authentication are as follows:

6.1.1 Unique user identification must be ensuring. An unique user id, employee id, account number can be provided each user, employee and account holder to identify them easily.

6.1.2 A User should not be assigned with more than one user id on the same application.

6.1.3 Before giving the access to the system every user needs to be authenticated.

6.1.4 For attempting a limited number (3) times with wrong credential the user must be blocked and cannot be unblock without the administrative permission.

6.1.5 A user, user id or account should not be able to logon to the same application / system more than once, at the same time i .e ., Multiple concurrent logons with the same id.

6.1.6 Secret information for authenticating a user never be shared with another user. Like PIN, password or 2FA key.

6.1.7 Password should be encrypted and not recorded in elsewhere without the proper security.

6.1.8 To ensure the security, password must not be less than eight (8) characters.

6.1.9 To make sure that the password is strong enough, it must contain at least one capital letter one small letter, one digit and one special character.

6.1.10 Password must be different from the unique user identifier like username, user id.

6.1.11 Passwords must not be easily guessable and must not be connected with the User in any way.

6.1.12 User needs to change passwords at least every 90 days.

6.1.13 Whenever an employee quite the job his/her access must immediately revoke and also in case of transfer old permissions and access needs to revoked and new one invoked.

6.1.14 Only system administrator can recover forgotten password of a user and 2FA must be implemented for changing the password.

6.2 Data Integrity and Confidentiality

The goals of Data Integrity and Confidentiality are to ensure the continued availability and accessibility of information, to reduce the risk that data may become corrupted by an external influence such as a Virus; and to ensure that client confidentiality is maintained at all times.

6.2.1 Virus Protection

Viruses are nothing but a kind of computer program that are used to gain illegal access to another program or computer or stealing valuable information. These can be used to destroy a computer, application, server even a computer network completely. Its been very much easier to prevent computer viruses rather then cure.

Virus prevention technology, (e.g., virus scanning software) must be implemented for any platform susceptible to viruses. The following scanning procedures must be adhered to:

6.2.1.1 Appropriate Virus protection technology (Anti-virus) need to install and maintain on each device and perform regular update.

6.2.1.2 IT division ensures that every day, at boot up of the PC, memory and boot Sector viruses will be scanned. No files need to be scanned at this stage.

6.2.1.3 IT division shall configure a Virus Shield to scan all accessed files (network, hard disk or floppy disk) whilst the operating system (e.g. Windows) is running.

6.2.1.4 Employees need to be aware of installing unauthenticated application into the computers because that can inject virus unknowingly.

6.2.1.5 Unsafe or external portable disk/storage or diskettes must not use in office computers.

6.2.1.6 Each user shall scan all files of the PC once a week

6.2.1.7 Laptop users should be able to break out of the weekly full file scan so that they can opt to run the scan when they are not using their internal batteries. Laptop users should be educated about the need to run a full virus scans at least once a week. If a user does break-out of a full scan, the PC should continue to try and run a scan every time the PC' is booted until a full scan has been completed.

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

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

6.2.1.10 Laptop users should be notified by E -Mail whenever Virus Signature files need to be updated. The update process should be performed automatically when the Laptop is connected to the LAN.

6.2.2 Spyware Protection

Spyware is a special type of malware infiltrated to the computer for stealing the internet usage information and other sensitive data like cookies. This might be destructive for the Bank’s information system. to prevent spyware installation into the workstations following control mechanism must be adhered to:

6.2.2.1 Every device needs to install legitimate spyware application form the renowned provider.

6.2.2.2 Whenever a spyware is detected into any device of the network the relevant team needs to take necessary action to remove the spyware and make the system functional again and also documented the whole thing.

6.2.2.3 Employees must not install third-party application without the permissions of the cyber security cell.

6.2.2.4 Employees have to regularly perform anti-spyware scan and report any occurrence to the IT division.

6.2.3 Data Encryption

Data encryption is one of some strong data security processes. In encryption the data is transformed into a different form and user having the right secret key can decrypt it and read it. Electronic banking information are very much sensitive and need to store and transmit frequently. If these data are encrypted data will be secured because if someone get the unauthorized access to the information, they cannot read it because of not having the secret key required to decrypt. There are many encryption algorithm and techniques the cyber security division can use an existing encryption technique like Triple Data Encryption Standard (3DES), Blowfish or Twofish Encryption or Advance Encryption Standard (AES) or they can develop a new encryption algorithm for the Bank’s information system.

6.2.3.1 Disk encryption is mandatory for all computers and data transmission.

6.2.3.2 Must use either a strong recommended encryption algorithm like 3DES, Blowfish, Twofish, AES or RSA or a new encryption algorithm must be developed for the One Bank Information system.

6.2.3.3 Encryption Key must be kept secure and length of the key must be according to the encryption algorithm and industry standard.

6.2.4 Information Disclosure

The One Bank Limited is committed to maintain transparency and accountability to its clients. The bank will share all the relevant information related to it and its activities if there is no confidentiality concern associated with it. The bank will not share any information publicly that can be harmful to its clients or that can affect the business of the bank. The bank is committed to follow the rules and regulation of Bangladesh Bank and the government of Bangladesh. The bank is bounded to supply any information demanded by the law forcer agencies of the country. General controls on information disclosure are as follows:

6.2.4.1 Any internal report of the bank is confidential and will not shared publicly.

6.2.4.2 Information regarding to legal advice or agreement upon under processing and matters in legal dispute will not publicly available due to confidentiality of it.

6.2.4.3 The bank will not be going to publicly share documents or information received from outside parties that bank agreed to not share outside of the bank. The One Bank Limited committed to fulfill its agreement and act accordingly.

6.2.4.4 Internal financial information that may or may not affect bank's operations in the capital and financial markets, such as investments, future borrowing estimates and repayment expectation, expected interest rates, return rates or similar market sensitive and financial ratios and financial model related information not approved by the concerned authority of the bank will not be available to the public.

6.2.4.5 The one bank will not share any information of its private sector clients unless their permission. And it never discloses its clients financial, business or proprietary related information.

6.2.4.6 The bank will follow the banking laws and security restrictions and will not share anything that violet such things or that could made undue legislative risk to the bank.

6.2.4.7 Required policies must be applied in the information system design and development to protect privacy, integrity and confidentiality of all electronic data processed by it.

6.2.4.8 Before transferring sensitive data to any authorized user it must be ensure that data is protected with the adequate security measures described in the policy.

7. EMAIL SECURITY

Electronic mail (Email) is a form of modern communication techniques. In email messages transmitted to one electronic mailbox to another box through internet. Email is the most common official communication channel all over the world. The One Bank Limited also provides email facility to its employees to make communication easier. Email may contain sensitive and secrete information and documents. So, email security is very important. To ensure a secure and effective email system following guidelines must be applied-

7.1 One Bank's official email should not be used for personal purpose though it is not prohibited. One should aware of content using in personal purpose.

7.2 Individual employees must use official email from a secure environment and he / she will be responsible for sacrificing that account's security. One should always log out from the account once work is done.

7.3 Employees should not provide any statement or impression on behalf of One Bank Limited without having the authority or legitimate permission to do it. If they give such thing a disclaimer should be included that given impression or statement is sender's personal opinion not the One Bank's.

7.4 Employees must not use unofficial email for official purpose. If any sensitive information or document transmitted from outside emails service providers than One Bank's email service can be punished.

7.5 This policy strictly restricts from doing following things:

- Using One bank's email for personal purpose or intention to harassing someone.
- Email cannot be used to share political purpose.
- Cannot share confidential information.
- Sending emails on behalf of another one without having the written permission.
- Cannot use public email service for official purpose.
- Sharing irrelevant message to a large number of receivers is strictly prohibited.
- Should not use extra large contents in a single email.
- Knowingly share spam or potentially harmful contents in email.

7.6 Confidential and sensitive information (client details and corporate confidential) being sent via E-Mail should be sent as an attachment and not as part of the body of the message.

7.7 Attachments having client's or corporate sensitive information should be password protected.

7.8 All messages which have attachments containing client or corporate sensitive information must be sending with the "Return Receipt" and "High" Priority options set.

7.9 Password secure attachments should have their passwords transmitted to the recipient in a secure manner. The password should not be included as part of the Message text or sent to a fax machine, but should ideally be telephoned through to the recipient in person.

7.10 If message is encrypted then related detailed instruction must be provided at the beginning of email how to decrypt it.

7.11 The identity of the sender of an in -coining message must be clearly established as trusted before the message is copied to any ONE Bank internal network.

7.12 All incoming files must be specifically virus checked.

7.13 For important items, acknowledgement of the e -mail must be done so that the sender can be assured that his/her email is not lost.

7.14 While composing email, punctuation and spelling must be checked carefully as it can reflect organizations reputation. Automatic checking programs, if available, must be used.

8. INTERNET SECURITY

Internet is nothing but combination of worldwide interconnected computer networks following the common standards and protocols set. Internet makes it possible to perform real-time centralized banking through the electronic banking. Since, internet is open to all it must to secure the information system in the internet. Whereas the use of internet can boost up employee's job efficiency and increase Bank's performance, there are also risks of improper uses of internet. Employees must follow the following guidelines while surfing the Internet.

8.1 Internet facility should be provided to limited personnel like Branch Manager , Divisional lead and to some officials specifically authorized by managers , divisional heads

8.2 ONE Bank Limited provides secure workstations with Internet connection for its business purpose only. Employees must not surf the web for personal purpose using the given facility as it can be dangerous for the information security.

8.3 One Bank Limited’s employees should use the internet during the working period only for their job-related needs.

8.4 Employees must not engage in personal chat, email messaging or other things. If it is proven that one violates this rule may get dismissed or will have to be subject to get punishment.

8.5 Using One Bank’s internet facility, its employees cannot start no-job related internet activities.

8.6 Downloading files from unauthenticated web source is forbidden and must perform security check before initiating download and after completing download.

8.7 Without the written permission of the system administrator one cannot install any application into workstation. Employees must not violate the software copyright issue or licensing issue.

8.8 If an employee observe any unusual activities outside the given guideline should immediately inform to the IT division.

8.9 All application has the access to the Internet must be configured individual firewall and proxy setup.

8.10 Using the One Bank Limited's ICT facility for offensive or harassing purpose is subject to legal action.

8.11 Using the Bank's Internet facility personal advertisement or commercial activities strictly prohibited.

8.12 Without ensuring secure encrypted environment no sensitive information like account number, credit card number or PIN should be transmitted over the Internet.

9. NETWORK SECURITIES

One Bank's network need top priority security measures to protect the integrity of this network and to prevent the possible loss associated with the potential security threats. The network needs to be secured form the security breaches, security attacks or potentially harmful things for the Bank. Guidelines for maintaining the network security are listed below-

9.1Bank's IT Division and its Network Department will be responsible for network developing and maintaining infrastructure and its security.

9.2 Network address distribution, IP and protocol configuration, allocation registration etc. maintained centrally by the Network department of IT division.

9.3 Core Banking System (CBS) should run on separate LAN and should not be mixed with the common LAN used for office work.

9.4 To ensure that any network connected component or deployed service do not responsible for compromising the security of another one network department should take necessary action.

9.5 Network engineer should plan and implement the network cabling and wall-sockets. Unused cables and sockets must remove and documented.

9.6 Network manager must perform periodic checking of implemented network and security measures and produce report.

9.7 Network manager have power to investigate suspected security breach and responsible for analyzing the breach and take required security measures to resolve the breach.

9.8 Network equipment need to kept locked and deploy access control to the area.

9.9 Firewalls must be installed and configured.

9.10 To ensure anonymous use of internet and email service proper proxy configuration need to maintain.

9.11 Employees must use the network addresses issued by the network department and should not use other addresses.

9.12 Employees are not allowed to extend or replace network infrastructure or services to the Bank's network without approval from network department of Information Technology division.

9.13 Employees do not have permission to alter hardware devices.

9.14 It is strongly recommended to avoid downloading, installing, or running computer application, scripts or websites that generate security breach or leak security weakness of the bank's network. Only authorized IT division personnel can do these if needed.

10. DISASTER RECOVERIES

Disaster recovery is the process of restarting the business operations after an unexpected occurrence damage or stop the operations. The One Bank Limited's IT disaster recovery plan has two parts, one is 'Disaster Recovery Plan' and other one is 'Data Backup Plan'.

10.1 Disaster Recovery Plan

10.1.1 There must be a separate Disaster Recovery Site other than production site which is at least 10kms away from the production site.

10.1.2 The Information Technology Division should develop a comprehensive disaster recovery plan.
The plan is the combination of following:

- Identifying critical processes and prioritizing these.
- Identifying the required emergency tasks and distribute responsibilities for recovery and continuity.
- Develop a 'Call tree' and list the contact information,
- Should prepare documentation of electronic and/or manual works around and rectification work.
- Train the employees to execute emergency processes and procedures according to plan.
- Prepare separate guidelines and checklists of tasks to assisting different departments and branches.
- Testing the whole plan and evaluate it.
- If medication is needed in the plan then update it according to test result.

10.1.3 Before making the disaster recovery plan an in-depth risk and possible disaster assessment must be performed.

10.1.4 The plan needs regular checking and modification and tested in simulated environment.

10.1.5 The plan must cover the all aspects of important and information system functions and activities.

10.1.6 The plan needs to keep UpToDate to accommodate changing circumstance.

10.1.7 All employees need to be aware of their responsibilities in the recovery plan and trained in simulated environment.

10.2 Data Backup

The goals of Backup are to:

- Ensure the uninterrupted service of the information sytem.
- Minimize the cost of a disruption, e.g., operational error, disaster, or sabotage that causes damage to, or destruction of, information; and
- Provide duplicate up-to-date information for recovery purposes with the same level of integrity and quality

10.2.1 Backup servers needs to established in different geographic location with the necessary security measurements, far enough away from the main site, such that a disaster there is unlikely to affect the safe store.

10.2.2 A replica of the backup server need to maintain on-site for emergency processing and transmission.

10.2.3 Scaleup of the backup criteria need to adjust according to the necessity and importance of the information. The backup cycle might be daily, weekly, monthly and yearly cycle.

10.2.4 Tapes should be sent off-site as soon as possible after the backups have been taken, and NOT left on-site till the next day.

10.2.5 When the technology used to process, store, or communicate information is changed, backup procedures must also be updated.

10.2.6 Frequent periodic test required to ensure that backup is working and recoverable.

11. CHANGE REQUEST MANAGEMENT

The continuous expanding of the One Bank Limited's services its IT infrastructure and information system needs continuous update, extension over the time. Change management helps to plan how the required changes can be done not impacting the continuity of bank's business and regular activities. Here the guidelines for planning maintenance, update and upgrade will be provided.

Because of the information system and IT resources are interdependent, change management is really more complex and critical than other plans. The purpose of this management plan is to identify and predict required changes to make the system more robust and implanting changes without having trouble to the running system.

11.1 Change management policy must be followed in every change made to the One Bank's information system and IT infrastructure. Like hardware change, software change and operating system change or network change.

11.2 A change management committee must be formed and regular meeting needs to arrange to evaluate the change requests.

11.3 Formal manual or electronic change request needs to submit to the change management committee for any change required.

11.4 Scheduled change requests must be submitted with all the change procedures, importance and planned schedule for reviewing by the committee. Because, the committee can evaluate the request against potential failures and threats and make a decision whether change request is allowed or delayed.

11.5 Change Management Committee must approve each individual scheduled change request before change take place.

11.6 The change management committee has the power to approve or deny any request based on the evaluation of provided details and reasons or limitation in planning or timing or negative impact of the change.

11.6 A documented review is mandatory for every approved change request whether change is successful or not.

11.7 A Change log must be maintained by the change management committee to keep track of changes made. The log needs to contain the below listed things:

- Request date, approval date and change implementation date.

- Request maker name and contact details.

- Change type.

- Implementation result, whether success or failed.

11.8 Status of all change requests must be notified to Help Desk.

11.9 Changes must not be incorporated to production environment unless proper User Acceptance Test is done.

11.10 Testing should be done in a separate test environment.

11.11 All the software patches, upgrades that are supplied by Vendor needs to be deployed at test environment prior to implementing in production environment.

12. HARDWARE MANAGEMENT

Hardware management means necessary hardware device installation, upgrading and maintaining the hardware resources of the One Bank Limited. Its really very much important to cope up with the technological advancement in accordance to the cost effectiveness, performance, security and usability issues. Hardware management guidelines are as follows-

12.1 Hardware installation is very critical process, hardware resources can damage or become unusable due to improper attempt of installation. No employee except the one who is authorized to make hardware change allowed to install or change any hardware resource.

12.2 The Bank’s IT divisions hardware managements team will be responsible for maintenance and repair process of damaged or corrupted hardware devices. The team can send the device to third-party for repair if necessary or can decide to completely replace it if economically feasible.

12.3 All portable media ports of the computers must be disabled by the administrative right. In case of any need of using portable media devices prior written approval needs to be obtained from the IT division.

12.4 Hardware team employee will become responsible for all hardware installation and change.

12.5 A hardware fault register should be maintained to record the hardware faults reports and actions taken.

12.6 Any hardware failure or accidental hardware crashes must be reported to the hardware team instantly after occurrence is detected.

12.7 One bank’s procurement policy must be followed in each hardware procurement process.

12.8 Adequate insurance coverage should be provided under the banks insurance policies to minimize the bank’s expense and associated risk.

12.9 Hardware maintenance personnel must always have access to the hardware resource documentation of the bank.

12.10 Information technology hardware inventory management system must be developed and maintained.

12.11 The hardware inventories can be accessed by the authorized personals only and they will be responsible for any kind of risk associated to it.

12.12 Disposal of hardware resources only allowed by the authorized employees of the hardware maintenance team and must consider the following:

- Old devices data must keep for history.

- Hardware resources that are used infrequently may not accidentally disposed by the technical staff.

- Hardware equipment must not be stolen or lost during the disposal.

12.13 Hardware engineers will be responsible for maintenance of the hardware devices owned, leased or licensed by the bank.

13. SYSTEM DEVELOPMENT AND TESTING

All in-house development and testing need to be clone according to the flowing procedure:

13.1 Project initiation

A letter prepared by the user and duly signed by his division head / branch manager should be addressed to the department head of IT Division for commencing any in house software development project.
The letter should be supplemented with:

- Domain Overview

This should describe the procedures of the manual operations to be automated and purpose of the activity.

- Feature List

This should define the features and functionalities to be accommodated in the software.

- Possible Inputs

It should give the input parameters and their data types curd any constraint, regarding, input.

- Expected output

Reports and other output formats should be specified here.

- Related references (if any)

At this stage Head of IT would designate a person to review the user requirements and decide about the feasibility of the project.

13.2 Development Tools Selection

Once the project is found to be feasible project development tools are decided.

13.3 Team Assignment

Head of IT then assign a team with members having knowledge on the tools. A team leader is also selected preferably the one who had done the initial feasibility survey and analysis of the project.

If the project team consists of more than one person then the team members can be assigned with specific jobs like database developer, GUI builder and business logic developers and testers.
It is suggested that if the project is not too small then the team should consist of at least two persons. The tester should not be a member of the development team but separate entity. Any member of the development team can perform more than two roles at the same time except tester . A typical example for clarification is that Mr. X can be GUI Builder as well as Business logic developer for the same project but cannot be tested for that particular project.

13.4 Preliminary Analysis

The Project Head then call for a meeting with the relevant people (users) and if necessary department heads of the department(s) concern to discuss about the detail requirement for the project. After the meeting the Project Head with the help of the project team, would prepare a requirement analysis report. This document should include:

- Project Overview

  - This should elaborate about the concept of the project in detail.

- Functionality List

  - It should describe the functions, procedures and business logic of the project.

- Sample Reports

  - If possible all reports format should be given.

 Sample Screen Shots

- Applicable for large projects but not mandatory if time constraint is high.

 Development Tools

- Should elaborate the DBMS, Report Designer and other tools to be used in the project.

 Deployment Environment

- Would provide the Hardware, Software and Network requirement for deploying the project.

 Risk- Factors and constraints

- This hoist should elaborate about the weak points, dependencies and other causes that can hamper or stop the development of the project.
- Project Head would then sit with the requirement analysis report with the users, discuss it with the users, modify it if necessary, after users' feedback and get it signed by the user and his department head.

13.5 Project Plan Preparation

Once this is done the PL would arrange another meeting with his team and prepare a project plan and schedule with specific time frame. The plans and schedule should be approved by the IT Head.

The project plan should have:

i)System Analysis phase
ii) System Development phase
iii) Coding, Phase
iv) Integration and testing phase

The entire project should be broken down into smaller modules (may be defined as jobs) and the schedule for each job should be detailed with the name of the designated person for accomplishing the job

13.6 System Design Documentation

This document would be used only for internal purpose of IT Division. Since ours is not a Software development firm this documentation should not force any rule and not mandatory. Depending on the time constraint the contents of the documents should be fixed.

This documentation may include:

- Use Case Diagram
- Class Diagram
- Database Schema
- DFD
- ERD
- Data Dictionary

13.7 Coding

Software code and documents should be kept in a dedicated repository machine using Source Safe or CVS and a common directory structure should be maintained.

13.8 Testing

There should be three steps testing of the deliverable. These are:

 Unit Test

- This test is done by the developer and should be completed before Integration test and UAT.

 Integration Test

- Designated tester would be responsible for this job. He should prepare a bug list and forward it to the Project Head. Project Head then assign someone among developers to fix the bug. After the bug is fixed it is re tested by the tester. If the tester is satisfied he should inform it to the Project Head. A sample Bug list is given below:

- SL. DescriptionScenario Report SeverityBug Status Fix No. Date (1-5) Fixer Date

 UAT

- UAT Should is done by the user with the assistance of developers. Once he is satisfied, he should recommend his department head for signing off the project.

13.9 Data Migration

IT Department would be responsible for creating script of data conversion, but users must provide correct data so that it can be flawlessly accommodated in the new database.

13.10 Backup Policy

Source code of the project should be updated oil a weekly basis into the repository and other documents a monthly basis.

13.11 Deployment

Once the UAT is over a copy of the software (only executable) is installed in the production machine after all required environmental setup. Managing the environment (hardware and third-party software) is users' responsibility and configuring the hardware installing the third-party software (OS, DBMS etc.) and the developed software is the responsibility of IT Division. A document detailing environment prerequisite for installation should specified and to be provided to the user.

13.12 Security Measures

i) A dedicated machine should be used as the software code and documentation repository.

ii) Visual Source Safe (VSS) or CVS should be used to control the development of the project.

iii) VSS domain users should be created. Developer should be authorized only with read and write permission.

iv) After project deployment write permission should be withdrawn for developers.

v) No copy of the software can be made except for the purpose of development.

vi) After development of the software all copies except the backup kept in the repository and the production copy should be deleted from

vii) There should be a single exit point for copying the software.

viii) All coding and documentation should have one printed copy (hard copy) and must be kept under direct supervision of Head of IT Division.

14. INTERNET BANKING:

Through Internet Banking our customer will have access to the environment of our Core Banking System; therefore, the System Administrator will put in place appropriate controls to protest network and systems from unauthorized access, fraudulent activity, contract dispute and unapproved disclosure/modification of information / instruction passing over public networks. The controlling measures will cover the following:

14.1 Network and Database Administrator of Information Technology Division will be Responsible for the security of Bank's Internet Banking Application Software.

14.2 Information Technology Division will deploy access control to the information system, application software’s, network addresses, data storage, email system, telephony system owned or operated by the One Bank Limited. Access control must be with traditional industry standards and two factor authentications as well.

14.3 Different real time access request and access logs need to be maintained by the system to identify and prevent unauthorized access attempt by the administrators and security officers.

14.4 Cyber security cell and network team will introduce and deploy various security measurements and protocols for the information system and electronic banking facility of the One Bank Limited. Some standard security measures and protocols are- Public Key Infrastructure (PKI), Secure Socket Layer (SSL), Two Factor Authentication (2-FA), Encryption algorithms like Triple DES (3DES), AES, RSA etc.

14.5 The cyber security cell of the bank will be responsible for monitoring, detecting and preventing the intrusions and attacks on the bank’s private network and information system.

14.6 Employees like information security officer, network security officer, encryption specialist and/or entrusted with similar responsibility will carry out following periodic tests ongoing basis at a frequency approved by Head of Information Technology Division.

a) Password strength test with password cracking tools.
b) Backdoor detection testing for identify and seal backdoors.
c) System accommodation capacity test by attempting Denial Of Service (DoS) and Distributed Denial of Service (DDoS) attack on the electronic banking system.

.

d) Regular checking for common security breaches and security holes in application software like email system.

e) Checking for the unused open ports in the information system servers, network, personal workstations and close if found.

14.7 Information Technology Division will keep proper record of all applications software for legal purposes.

14.8 Security infrastructure and measurements will be maintained by the cyber security cell of the IT division of the bank. Necessary security patches must be developed or collect on a regular basis and install to improve system security. Security applications must be upgraded regularly for better security and control.

15. SERVICE PROVIDER MANAGEMENT

15.1 IT Divisions should perform appropriate due diligence before selecting or contracting with a service provider in respect of security breach, confidentiality, legal terms and conditions, business risk assessment, etc. Country risk and choice of governing law will have to be considered in addition to the above while contracting with Foreign Service Provider.

15.2 Third party service provider must be aware of and comply with this security standard.

15.3 A service level agreement must be completed and executed prior to the commencement of the work.

16. TRANING

16.1 Each employee should be aware of this Information Security Guideline.

16.2 Formal training on Information Security will have to be given to all staff

16.3 Cyber security team members need to be trained periodically to ensure hands on learning about the latest security threats and technologies.

16.4 New employee training must include a cyber security in order to teach the basic responsibilities need to maintain by the employee to maintain security.

17. INTERNAL IT AUDIT

17.1 Necessary tools and applications to perform internal IT audit.

17.2 IT Audit should be conduct at least annually to ensure compliance of this policy.

17.3 The report must be preserved for future reference.

Questionnaire Form

1. General Understanding

Sl. No.	Subject	Implementation		Details Status of implementation	If not implemented, reason and target date of implementation.	Comments from ICCD
		Yes	No			
1.1	Does the bank have an 'ICT Security Policy' which is fully implemented and in compliance with the ICT Security Guideline by Bangladesh Bank?	Yes		Complied with Bangladesh Bank ICT Security Guideline.	Disaster Recovery Site is under construction.	Major issues like establishing Disaster Recovery Site still remaining.
1.2	Does the bank update its 'ICT Security Policy' each year to accommodate the changes in the IT facility and have it approved by the Board of the bank?	Yes		At 2015 we have change ICT Security Policy.	Copy submitted	Please provide a copy of the approval.
1.3	Is there a system administrator available?	Yes		Dedicated system administrator available at IT Division		
1.4	Is the policy containing clear guidelines and responsibilities for various administrative persons?	Yes		Job description of systems, network, database and cyber security administrators already documented		

2. Audit and Controlling measures to mitigate ricks

Sl. No.	Subject	Implementation		Details Status of implementation	If not implemented, reason and target date of implementation.	Comments from ICCD
		Yes	No			
2.1	Does the bank carry out an internal system audit periodically or at least once a year with sufficient ICT skilled persons to find out loop holes and weaknesses in the systems and take appropriate measures to mitigate the risk?	Yes		Internal Audit done periodically		
2.2	Is there any physical IT security audit plan in the policy?	Yes		Physical security audit has already been initiated		
2.3	a) Does a Strong Security System apply to the Account Transfer Process?	Yes		Available in Core Banking Systems		

3. Accounts and Passwords

Sl. No.	Subject	Implementation		Details Status of implementation	If not implemented, reason and target date of implementation.	Comments from ICCD
		Yes	No			
3.1	Does the bank have system error report log, security breach log and system access request log?	Yes		We are complying with all the 9 steps checklist log to ensure the access control. We are using following solutions: Syslog watcher, Check Point, Cisco ASA Firewall, Nagios Server Monitoring Solution and Linux SARG Solution		Please furnish the status of real-time security log 9 for unauthorized access precisely
3.2	Is the bank	Yes		Available, and also		

	has central policy to select a strong password?			mentioned in the ICT Security Policy.		
3.3	Does the bank's information system use password to ensure strong password?	Yes		Available in Core Banking Systems		
3.4	Are passwords changed? If so, how often?	Yes		Its mandatory to change password after each three months.		

4. Physical Security

Sl. No.	Subject	Implementation		Details Status of implementation	If not implemented, reason and target date of implementation.	Comments from ICCD
		Yes	No			
4.1	Does the bank have guidelines in the policy regarding to the physical security of the ICT assets?	Yes		Physical security is partly available and will be regularized soon.		
4.2	Are there procedures for restricting access in the data center/computer rooms?	Yes		Access point is electronically restricted and even manual register is available		
4.3	Are there locking system enable for the portable workstations, laptops and other devices?	Yes		Keep in safe site		
4.4	Are hardware components of	Yes		Locked properly		

	the bank secured from unauthorized access?			keep in safe site		
4.5	Is unused hardware components stored in a safe place?	Yes		Locked and safe in hardware inventory and only authorized persons can access them.		
4.6	Does gate pass required for moving hardware devices from one place to another?	Yes		Gate pass is properly maintained		

5. On Hardware

Sl. No.	Subject	Implementation		Details Status of implementation	If not implemented, reason and target date of implementation.	Comments from ICCD
		Yes	No			
5.1	Are interdependent hardware devices able to continue work even when one of them faulted?	Yes		Redundant Hardware is available for all mission critical service i.e. CBS, BACH, Email systems. CBS system is running with Active-Passive mode with clustering system where down on one system will not affect the operation. Email Server running Active-Active mode with load balancing. BACH is working with manual redundancy system.		Please specify in a more elaborate manner.

6. On Software

Sl. No.	Subject	Implementation		Details Status of implementation	If not implemented, reason and target date of implementation.	Comments from ICCD
		Yes	No			
6.1	Are there backup installation files of the applications if reinstallation is required?	Yes		License software is available for all data center hardware. For User Level we are working to implement Licensing with different vendors while cost effectiveness is the main concern		Not in all segments.
6.2	Is the Bank's developer team easily reachable for reporting faults and bugs?	Yes		Locally developed software and support is done by In House developer team of ITD.		

7. On Environmental Failures

Sl. No.	Subject	Implementation		Details Status of implementation	If not implemented, reason and target date of implementation.	Comments from ICCD
		Yes	No			
7.1	Does the data center and branches have proper safety measures from environmental and accidental dangers like fire, water, humidity etc?	Yes		Before installing any equipment, we always consider said issue		
7.2	Do emergency power backup	Yes		UPS protect our servers and		Only available in

	available in data center and branches?			workstation during out of PDB with three level generator backups. In CHQ and Branch level Users Desktops and Devices are under offline UPS for each user while generators are on backup.		the data center

8. On Network and Configuration Security

Sl. No.	Subject	Implementation		Details Status of implementation	If not implemented, reason and target date of implementation.	Comments
		Yes	No			
8.1	Does the network department produce a compete network map to guide the engineers?	Yes		Network Map/diagram is already implemented		
8.2	Does the Bank have inventory facility for hardware devices?	Yes		Updated inventory is maintained by ITD		Sometimes not updated.
8.3	Are all the jacks directed to a port as followed by the network map?	Yes		Port map is implemented and displayed in Data Center. Document Available		Mapping documents to be submitted.
8.4	Is the bank have a network access policy and guidelines for its	Yes		Network Security Policy is in the place		

	employees?					

9. On to Web Servers and Email

Sl. No.	Subject	Implementation		Details Status of implementation	If not implemented, reason and target date of implementation.	Comments from ICCD
		Yes	No			
9.1	Does the bank’s web servers configure to allows request only through port 80?	Yes		Allow port 80 only for web server		
9.2	Does the network address translator installed to protect webservers form the external access?	Yes		Reject for all external user also ICMP request		
9.3	Is the bank’s servers able to check whether request is valid or fake?	Yes		Authenticate only for respective service		
9.4	Have testing data, files and documents removed before system is going to live?	Yes		All things are removed from the testing area after going live		

10. On FTP Servers

Sl. No.	Subject	Implementation		Details Status of implementation	If not implemented, reason and target date of implementation.	Comments from ICCD
		Yes	No			
10.1	Does FTS servers have proper authentication service?	Yes		User name and password mandatory		
10.2	Is this traffic encrypted/secured?	Yes		Encrypted and secured by router		
10.3	Are read or write or both permissions set for each individual user to determine the what the user can do with the FTP server?	Yes		FTP Server is being used for data sharing purpose across OBL and contains both the Read and Write Permission. FTP server is regularly monitored and removed the unnecessary files.		Please specify.

11. On Disaster Planning

Sl. No.	Subject	Implementation		Details Status of implementation	If not implemented, reason and target date of implementation.	Comments from ICCD
		Yes	No			
11.1	Does the bank has any written disaster management planning on how to react with the emergency moments of	Yes		According to the Business continuity Plan if On-Site workstation is failed then user can access the system by using others work station with the username and		Please specify in a more elaborate manner.

	disaster?			password provide to him. In case of failure all the workstation in a branch, users are requested to use the workstation of nearest available branch.		
11.2	Does the bank have a backup plan for continuing its operation while the information system goes down?	Yes		Continue service by redundant server. DR is under construction		

12. On Backup and Recovery

Sl. No.	Subject	Implementation		Details Status of implementation	If not implemented, reason and target date of implementation.	Comments from ICCD
		Yes	No			
12.1	Are backup servers established in different safe place from the actual servers?	Yes		Backup servers are in different safe places and the locations of these are hidden due to security reason.		By using public transport as mentioned in the early reports.
12.2	Are the servers and files safe on operation centers?	Yes		Kept secured in location.		
12.3	Does data, files and documents backed up on a regular basis?	Yes		Take backup on regular basis		
12.4	Does there are off-site media	Yes		At Dhanmondi Branch		

	storage facility?					
12.5	Is the environment of the backup servers' locations safe from temperature, humidity, water and power outage?	Yes		Maintained properly, we used the cartridge again and it's tested.		

13. On Training

Sl. No.	Subject	Implementation		Details Status of implementation	If not implemented, reason and target date of implementation.	Comments from ICCD
		Yes	No			
13.1	Does the bank need new IT officers to review and prepare IT related documents?		No	Yes, but under different delegation as and where applicable and security documents are accessible by the respective officials		IT security documents to be accessed by IT Officials under different delegation.
13.2	Does the employees of the OBL aware of their responsibilities regarding to the system security?	Yes		IT officials aware about the matter and update our officials about any changes		
13.3	Does the bank authority consider that frequent trainings and workshops are required for the general employees?	Yes		Noted for compliance, within this year		Please ensure the targeted/tentative time.

14. Host based firewall

Sl. No.	**Subject**	**Implementation**		**Details Status of implementation**	**If not implemented, reason and target date of implementation.**	**Comments from ICCD**
		Yes	No			
14.1	Does security compromises for sensitive data storage protected?	Yes		We protect all critical data by using Check Point, Cisco ASA Firewall, Nagios Server Monitoring		Please explain precisely.
14.2	Is it possible to detect and monitor unauthorized access attempt to sensitive information?	Yes		Since Implemented. Monitored by Syslog watcher, Nagios Server Monitoring		Is that possible to monitor accessing critical data?
14.3	Does the OBL's workforce is enough to maintain each individual device firewall configurations?	Yes		Staff is Available in ITD		

15. Antivirus Software

Sl. No.	**Subject**	**Implementation**		**Details Status of implementation**	**If not implemented, reason and target date of implementation.**	**Comments from ICCD**
		Yes	No			
15.1	Are hardware and software resources updated regularly?	Yes		Update regularly		

16. Cross Border System Support

Sl. No.	Subject	Implementation		Details Status of implementation	If not implemented, reason and target date of implementation.	Comments from ICCD
		Yes	No			
16.1	Is there any resolution have been taken to ensure the continuity of regular activities of the bank on unavoidable circumstances like natural disaster, accidental emergency, or local diplomacy changes?	Yes		Agreement is available for Core Banking Database. Since we provide yearly service charge only respective vendor		We didn't find any cross-border /tri-party agreement during last inspection.

Should the policy is enough?

According to the recommendation from the External Examiner, Dr. Mohammad Shorif Uddin, Professor, Department of Computer Science and Engineering, Jahangirnagar University, I have analyzed the policy and found that the policy is not enough to antagonize all the security threats available. I also have found the following limitations:

- According to the Bangladesh Bank ICT Policy, the composed policy is subject to be updated in regular basis. After going through the policy, we find the missing guideline for Mobile Banking process. Since, day by day mCommerce transactions are getting increased, security challenges regarding to this type of transaction also increased. Mobile banking is also very promising turnoff of modern banking. It is growing popularity and proved to be very promising from the revenue point of view. So, there should be existed a clear guideline for mbanking.

- One of the most important missing security challenges of the proposed ICT security policy is there is no guide line about how ensure clients awareness about the information security and sensitivity. This might cause unrecoverable loss to the One Bank Limited.

- Another lacking of this policy is incompatible with the cyber security challenges associated with the international crimes since Internet makes electronic banking boundary-less. The policy has a scope to update its vision about cyber security and information sharing trends.

- There is limitation of security requirements for the Bank's business process. There is a scope to update the security measures involves with the bank's business.

- The bank needs to take evaluation from the external consultant's and service providers.

- This policy does not contain policy about some very important aspects of information security like, corporate website security standards, privacy policy for client's fillable data forms, information disclosure policy for the clients.

- My findings reveal that, the electronic service deliver channel is the most insecure and challenging among the services delivery channels the OBL using.
- Telephony banking is also less effective in accordance with the security aspects. I have found no clear guideline for the phone (IVR) banking in the policy.

If we can overcome the above limitations of the policy, we may provide better security to the Banks information systems. But still as I have already mentioned, the security policies are subject to be supervised repeatedly. We must keep evaluate the process and make fine-tuning if necessary. We find the similar opinion from the Bangladesh Bank ICT Policy guideline.

REFERENCES:

- Bangladesh Bank ICT policy 2015
- https://www.bb.org.bd/mediaroom/circulars/fid/guidelinev2ictsb.pdf
- https://www.bb.org.bd/aboutus/regulationguideline/brpd/guideline_v3_ict.pdf
- https://icb.gov.bd/pdf/ICT_SECURY_POLICY_15.pdf
- http://www.fintechbd.com/it-security-and-information-system-audit-in-banks/
- https://www.csoonline.com/article/2112402/physical-security-19-ways-to-build-physical-security-into-a-data-center.html
- https://www.thefinancialexpress.com.bd/views/cyber-security-in-banks-protecting-email-communications-1548169943
- https://blog.gigamon.com/2019/06/13/what-is-network-security-14-tools-and-techniques-to-know/

Final_Thesis_paper_Mahabub_173_17_370_Full.doc

ORIGINALITY REPORT

4%	3%	0%	3%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Daffodil International University Student Paper	3%
2	www.fintechbd.com Internet Source	<1%
3	dspace.daffodilvarsity.edu.bd:8080 Internet Source	<1%
4	Submitted to University of Rajshahi Student Paper	<1%
5	Sushil K. Sharma, Jatinder N.D. Gupta. "chapter 29 Information Security Policies", IGI Global, 2009 Publication	<1%
6	lionnews00.blogspot.com Internet Source	<1%
7	www.mod.uk Internet Source	<1%

Exclude quotes	On	Exclude matches	< 10 words
Exclude bibliography	On		