بسم الله الرحمن الرحيم

(In the name of Allah, The Most Benevolent, The Most Merciful.)

ICT Policy

Millennium Information Solution Limited

Version 2.0

MILLENNIUM
information solution ltd.

Document Details and Version Information

Version	Date	Prepared by	Approved By	Remarks
1.0	2017			
1.2	2020			
2.0	2020			

Table Of Contents

Chapter 1

1. Introduction

Millennium Information Solution Limited (MISL) is a Bangladeshi Origin Global Multinational engaged in software development, marketing, deployment and support services: primarily focusing on Islamic Fintech, Internal Audit and HR domain. This document serves as a physical proof of the guidelines which are in practice and accommodates the policies that are being perpetually implemented in MISLs daily operations. This also serves as a minimum requirement for the level of security measures that is in practice at MISL as part of its Information Security Management Systems.

1.1 Objectives

This policy defines minimum controls in place for Millennium Information Solution.

The primary objectives of the policies are:

1.1.1. Devise a standard ICT Security Policy and ICT Security Management approach.

1.1.2. Devise a secured setup of MISLs ICT infrastructure.

1.1.3. Establish a secured environment for the development and processing of data.

1.1.4. Establish a holistic approach for ICT Risk management.

1.1.5. Establish a procedure for Business Impact Analysis in conjunction with ICT Risk Management.

1.1.6. Aware stakeholders' roles and responsibilities for the protection of information.

1.1.7. To prioritize information and ICT systems and associated risks those need to be mitigated.

1.1.8. Establish appropriate project management approach.

1.1.9. Aware and train the users for achieving the business objectives.

1.1.10. Define procedure for periodic review of the policy.

1.1.11. Ensure the best practices (industry standard) of the usage of technology that is not limited to this policy.

1.1.12. Analyze security risks against faster adoption of Bring-Your-Own-Devices (BYOD).

1.1.13. Prepare Procurement policy for IT Infrastructure of MISL

Chapter 2

2. ICT Strategy

ICT Strategy must ensure that the ICT functions and operations are efficiently and effectively managed. MISL shall be aware of the capabilities of ICT and be able to appreciate and recognize opportunities and risks of possible abuses. They have to ensure maintenance of appropriate systems documentations, particularly for systems, which support financial transactions and reporting. They have to contribute in ICT security planning to ensure that resources are allocated consistent with business objectives and to ensure that sufficient and qualified technical staff are employed so that continuance of the ICT operation area is unlikely to be seriously at risk. ICT Security Management deals with Roles and Responsibilities, ICT Security Policy, Documentation, Internal and External Information System Audit, Training and Awareness, Insurance or Risk coverage fund. The scope of this document is moderated through the best practices of Shariah and global regulators and adapted for use as per the environmental requirements of Bangladesh.

2.1 Roles and Responsibilities

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

2.1.1 Roles and responsibilities of Board of Directors

1. Approving ICT strategy and policy documents.
2. Ensuring that the management has placed an effective planning process.
3. Endorsing that the ICT strategy is indeed aligned with business strategy.
4. Ensuring that the ICT organizational structure complements the business model and its direction.
5. Ensuring ICT investments represent a balance of risks and benefits and acceptable budgets.
6. Ensure compliance status of ICT Security Policy.
7. Review the ICT Policy Annually for upgradation or enhancement.

8. Assign person/persons who will be calling the formation of ICT Steering Committee and ICT Security Committee.

2.1.2 Roles and responsibilities of CEO

1. Act as a convenor to form ICT Steering Committee
2. Act as a convenor to form ICT Security Committee.
3. To propose, present and get approval of the aforementioned committees from the Board of Directors.
4. Endorse all project management plan (PMP) and its execution.
5. Maintain collaboration and cooperation among Project Manager, CTO, Business Development Officer and Head Quality Assurance.

2.1.3 Roles and responsibilities of ICT Steering Committee

ICT Steering Committee needs to be formed with representatives from related Business units.

1. Monitor management methods to determine and achieve strategic goals
2. Aware about exposure towards ICT risks and controls
3. Provide guidance related to risk, funding, or sourcing
4. Ensure project priorities and assessing feasibility for ICT proposals
5. Ensure that all critical projects have a component for “project risk management”
6. Consult and advise on the selection of technology within standards
7. Ensure that vulnerability assessments of new technology is performed
8. Ensure compliance to regulatory and statutory requirements
9. Provide direction to architecture design and ensure that the ICT
10. Architecture reflects the need for legislative and regulatory compliance
11. Ensuring clear scope and Terms of Reference
12. Conflict resolution.
13. Ensuring the committee achieves pre-defined objectives/targets.

2.1.4 Roles and responsibilities of ICT Security Committee

ICT Security Committee needs to be formed with representatives from ICT, ICT Security, Risk, Compliance and Business units.

1. Ensure development and implementation of ICT security objectives, ICT security related policies and procedures.
2. Provide ongoing management support to the Information security processes.
3. Ensure continued compliance with the business objectives, regulatory and legal requirements related to ICT security.
4. Support to formulate ICT risk management framework/process and to establish acceptable ICT risk thresholds/ICT risk appetite and assurance requirements.
5. Periodic review and provide approval for modification in ICT Security processes.

2.2 ICT Policy, Standard and Procedure

1. The policy covers common technologies such as computers and peripherals, data and network, applications and other specialized ICT resources. MISLs' service delivery depends on availability, reliability and integrity of its information technology system. MISL must adopt appropriate controls to protect its information system. The senior management of the MISL must express commitment to ICT security by ensuring continuous awareness and training programs for each level of staff and stakeholders.
2. The policy requires regular update to deal with evolving changes in the ICT
    a. environment both within MISL and overall industry.
3. MISL shall engage ICT security professionals employed in separate ICT security departments/units/cells for improved and impartial dealing with security incidents, policy documentation, inherent ICT risks, risk treatments and other relevant activities.

2.3 Documentation

1. MISL shall have an updated organogram for its departments.
2. Each individual within the department/division/unit/section shall have approved Job Description (JD) with fallback resource person.
3. MISL shall maintain updated "Operating Procedure" for all ICT functional activities (e.g. Backup Management, Database Management, Network Management, Scheduling Processes, System Start-up, Shut-down, Restart and Recovery).
4. MISL shall have approved relevant requisition/acknowledgement forms for different requests/operation/services.

5. MISL shall maintain detailed design documents for all ICT critical systems/services (e.g. Network design, Power Layout for Data Center, etc.).

2.4 Internal Information System Audit

1. Internal Information System (IS) audit shall be carried out by Internal Audit Department of MISL.
2. Internal IS audit shall be conducted by personnel with sufficient IS Audit expertise and skills. Engagement of certified IS auditor having adequate audit experience in this area of technology will be appreciated.
3. MISL may use Computer-Assisted-Auditing Tools (CAATs) to perform IS Audit planning, monitoring/auditing, control assessment, data extraction/ analysis, fraud detection/prevention and management.
4. An annual system audit plan shall be developed covering critical/major technology-based services/processes and ICT infrastructure including operational branches.
5. Internal Information System audit shall be done periodically at least once a year. The report must be preserved for regulators as and when required. MISL shall also ensure that audit issues are properly tracked and, in particular, completely recorded, adequately followed up and satisfactorily rectified.

2.5 External Information System Audit

1. MISL may engage external auditor(s) for their information systems auditing in-line with their regular financial audit.
2. The audit report shall be preserved for regulators as and when required.

2.6 Standard Certification

1. MISL may obtain industry standard certification related to their Information System Security, Quality of ICT Service Delivery, Business Continuity Management, etc.

2.7 Security Awareness and Training

1. As technology evolves rapidly, MISL shall ensure that all relevant personnel are getting proper training, education, updates and awareness of the ICT security activities as relevant with their job function.
2. MISL shall also ensure the minimum level of Business Foundation Training for ICT personnel.
3. MISL shall arrange security awareness training/workshop for all staff.
4. MISL shall ensure adequate training/awareness facilities for the IS Audit team considering any new services and technological changes.

2.8 Planning and Innovation

1. MISL shall have a formal Planning and Innovation process consisting of all relevant stakeholders and experts.

2.9 Procurement Policy

1. MISL shall implement its ICT and Overall Procurement through the global best practices.
2. MISL shall assign a Procurement expert who will lead a committee in conjunction with representatives of strategic management to conduct need analysis, devise, implement, maintain and perpetually update the Procurement Policy, actions and methodology

Chapter 3

3. ICT Risk Management

ICT risk is a component of the overall risk universe of an enterprise. Other risks MISL or MISL faces include strategic risk, environmental risk, market risk, credit risk, operational risk, compliance risk, etc. In many enterprises, ICT related risk is considered to be a component of operational risk. However, even strategic risk can have an ICT component itself, especially where ICT is the key enabler of new business initiatives. The same applies for credit risk, where poor ICT security can lead to lower credit ratings. It is better not to depict ICT risk with a hierarchic dependency on one of the other risk categories.

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

3.1 ICT Risk Governance

1. MISL shall form an ICT Risk Management Committee to govern overall ICT risks and relevant mitigation measures.
2. The MISL shall define the Risk Appetite (amount of risk the MISL is prepared to accept to achieve its objectives) in terms of combinations of frequency and magnitude of a risk to absorb loss e.g: financial loss, reputation damage.
3. MISL shall define the Risk Tolerance (tolerable deviation from the level set by the risk appetite definition) having approval from the board/Risk Management Committee and clearly communicated to all stakeholders.
4. MISL shall review and approve risk appetite and tolerance changes over time; especially for new technology, new organizational structure, new business strategy and other factors require the enterprise to reassess its risk portfolio at a regular interval.
5. MISL shall define the risk responsibilities to individuals for ensuring successful completion.
6. MISL shall define the risk accountability applied to those who owned the required resources and have the authority to approve the execution and/or accept the outcome of an activity within specific ICT Risk processes. Ownership of risk stays with the owner or custodian whoever is in a better position to mitigate the identified risk for that specific ICT asset.

7. MISL shall acknowledge all risks by Risk Awareness so that those are well understood and known and recognized as the means to manage them.
8. MISL shall contribute to executive management's understanding of the actual exposure to ICT risk by Open Communication, enabling definition of appropriate and informed risk responses.
9. MISL shall be aware amongst all internal stakeholders of the importance of integrating risk and opportunity in their daily duties.
10. MISL shall be transparent to external stakeholders regarding the actual level of risk and risk management processes in use.
11. MISL shall begin Risk-aware Culture from the top with board and executives, who set direction, communicate risk-aware decision making and reward effective risk management behaviors.

3.2 ICT Risk Assessment

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

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

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

1. MISL shall establish business impact analysis needs to understand the effects of adverse events. MISL may practice several techniques and options that can help them to describe ICT risks in business terms.
2. MISL shall practice the development and use of Risk Scenarios technique to identify the important and relevant risks amongst all. The developed risk scenarios can be used during risk analysis where frequency and impact of the scenario are assessed.

3.3 ICT Risk Response

Risk response is to bring measured risk in line with the defined risk tolerance level for the organization. In other words, a response needs to be defined such that as much future residual

risk as possible (usually depending on budgets available) falls within risk tolerance limits. When the analysis shows risks deviating from the defined tolerance levels, a response needs to be defined. This response can be any of the four possible ways such as Risk Avoidance, Risk Reduction/Mitigation, Risk Sharing/Transfer and Risk Acceptance.

1. MISL shall develop a set of metrics to serve as risk indicators. Indicators for risks with high business impact are most likely to be Key Risk Indicators (KRIs).
2. MISL shall give effort to implement, measure and report different indicators that are equivalent in sensitivity.
3. Selection of the right set of KRIs, MISL shall carry out
    a. Provide an early warning for a high risk to take proactive action
    b. Provide a backward-looking view on risk events that have occurred
    c. Enable the documentation and analysis of trends
    d. Provide an indication of the risk's appetite and tolerance through metric setting
    e. Increase the likelihood of achieving the strategic objectives
    f. Assist in continually optimizing the risk governance and management environment

4. MISL shall define risk response to bring risk in line with the defined risk appetite for MISL after risk analysis.

Chapter 4

4. Agile Software Development and DevOps Management Policies

The projects defined as agile will follow the agile development methodology for all MISL Software application solutions, Scrum @ MISL. This is based on the scrum working framework and takes engineering practices from other models into account, such as DevOps.

This methodology will be supported by the use of an ALM platform (Application Lifecycle Management) with tools that include the following features, among others:

- Development planning (releases, sprints, work packages, defects, etc.).
- Documentation, code and binary repositories.
- Requirements and Tests management.
- Unit and function test automation.
- Ongoing integration and rollout.
- Code quality control.

All the documentation generated internally during the course of development will be managed using the tools defined at the start of the project, preferably in the flexible wiki format.
The main characteristics foreseen for this methodology are described according to their life-cycle in the following sections.

The usual events (activities and milestones) for the Scrum @ MISL methodology include the following steps:

Event	Goals
Sprint	Development cycle (lasting from two to four weeks) in which a part of the system is delivered (including all sub-products, such as documentation and tests). The customer may choose to publish the increment delivered by the supplier or not.
Sprint planning	The product owner and the development team decide which part of the product will be produced during the sprint.
Daily Meeting	The development team monitors the sprint and the pertinent corrections. In the event of an overrun, the product owner and the scrum master are notified.
Sprint review	The scrum team and invited external players examine the result from the sprint and review the plan for the following sprints.
Sprint retrospective	The scrum team examines its own performance and plans specific improvements.

4.1 Roles and Responsibilities

Implementation of scrum roles at the MISL fully respects the standard objective and responsibilities for the roles while adapting them to the MISL context, which provides the wide ranges of FinTech, HRMS products & solutions primarily to the BFSI Industries.

The main roles are as follows:

- Product owner (BFSI Customers)
- Proxy product owner (MISL)
- Scrum master (MISL)
- Development team (MISL and / or partner)

4.2 Working Teams and their Management

The scrum model can be implemented with teams contracted in one of two ways: teams for the development of new projects; and application maintenance teams (AM). Below are the differences between them in terms of agile methodologies.

Multidisciplinary teams should include the skills for undertaking the following activities:

- Designing and building a digital service.
- Operating and maintaining a digital service.

The skills needed will change during the life-cycle of the service and support may be received from additional roles.

The entire team, but especially the designers, user researchers and developers, should work together to design, build, test and deliver the product.

Teams for new projects

Teams for new projects should be contracted once the scope of a product or solution service has been defined, before starting development. Definition of the contract requires a prior conceptualisation of the desired system, which will be jointly developed by the PO (Product Owner) at the BFSI Customer and the PPO (Proxy Product Owner) at the MISL. This conceptualisation should include the creation of the following elements:

- An initial backlog defining the scope of the development in terms or work items or packages.
- A delivery plan identifying the deliveries that will be made and which sprints form part of each one.

Application Maintenance teams (AM)

Application maintenance teams (AM) will be contracted a priori and will receive various types of requests (corrective, evolutive and perfective), which will be added to the backlog. Urgent requests will be resolved as soon as possible, in line with the SLA targets. All other requests will

be planned so they can be dealt with in sprints, probably shorter in duration (e.g. two weeks) because the packages will tend to be smaller and more independent.

Coexistence of project teams and AM teams

The coexistence of Scrum teams for developing new products and Scrum teams maintaining those products will have various effects depending on the level of freedom in the contracts with the suppliers and the most suitable option according to the Proxy Product Owner and the Scrum Master. The options are as follows (from most to least suitable):

- The product team includes members from the AM team on a permanent basis in order to work together on the same applications.
- The AM team has an allocated time frame for working with the product team and preparing transferral of the application once delivered to the MISL Deployment and Implementation Teams.
- The AM team does not have an allocated time frame for work during development of the application but does have the frequent increments and the “facts” for preparing the transferral, and may also occasionally take part in the review of sprints.

4.3 Project execution

Agile projects managed by the MISL must be executed according to the following principles, as reflected in the corresponding contract with suppliers:

1. The agile recommendations and methodological guidelines from the MISL as PPO will be followed, as presented in the contract specifications and in the Agile Space of the MISL, as well as any other indications that may be applicable and notified by the Scrum Master, who nonetheless will respect team self-management as a general principle.
2. At the end of each sprint, an agreed deliverable or product increment (software increment) must be available, which will meet the minimum quality requirements defined in the MISL Agile Space. If it is not possible to deliver all the content that is planned, quality will take priority over quantity.
3. Transparency will be required with the Scrum Master (and potentially the PPO) with regard to any possible internal team problems, as well as any external impediments, in order to seek together the best solutions to any structural or individual development problems.

4. Suppliers will use cooperative tools, as well as the baseline methodological rules that favour team interoperability, such as the language, structure and level of detail in the software documentation and other supporting documents.
5. The team responsible for Levels 2 and 3 of incident management will need to have minimum knowledge of the systems and work with the MISL as closely as possible. In the future and depending on the ability to automate rollout of the platform used, it is foreseen that teams will be able to roll out their systems autonomously, in the preproduction and production environments.

Chapter 5

5. ICT Service Management

ICT Service Management focuses on the business deliverables and ICT environment to support and deliver the demands of the organization as well as measuring and demonstrating improvements in the quality of ICT services offered with a reduction in the cost of services in the long term. ICT service management mainly covers the dynamics of technology operation management that includes capacity management, request management, change management, incident and problem management etc. The objective is to set control to achieve the highest level of ICT service quality by minimum operational risk.

5.1 ICT Service Change Management

Change management is achieved by formalizing and documenting the process of change request, authorization, testing, implementation and communication to related stakeholders. Change management process shall consider the following steps:

1. Changes to information processing facilities and systems shall be controlled.
2. MISL shall prepare a Change Request (CR) document which shall cover the detailed requirements of changes and the impact that will have on the business process, security matrix, reporting, interfaces etc.
3. All CR must go through a formal approval process.
4. All changes of business application implemented in the production environment must be governed by a formal documented process (manual/automated) with necessary change details.
5. MISL shall prepare a rollback plan including responsibilities for aborting and recovering from unsuccessful changes and unforeseen events.
6. Provision of an emergency change process to enable quick and controlled implementation of changes needed to resolve an incident, if required.
7. Changes should be communicated to relevant stakeholders as and when required.
8. Audit trail or CR implementation details shall be preserved for future reference.

5.2 Incident Management

An incident is an event that could lead to loss of, or disruption to an organization's operations, functions or standard delivery of ICT services. The organization shall manage such incidents in an effective manner and deploy necessary resources to prevent future recurrence.

1. The organization shall establish an incident management framework with the objective of restoring normal ICT service as quickly as possible following the incident with minimal impact to the business operations. Organization shall also establish roles and responsibilities of staff involved in the incident management process, which includes recording, analyzing, remediating and monitoring incidents.
2. It is important that incidents are accorded with the appropriate severity level. As part of incident analysis, MISL may delegate the function of determining and assigning incident severity levels to a technical helpdesk function. MISL shall train helpdesk staff to determine incidents of high severity level. In addition, criteria used for assessing severity levels of incidents shall be established and documented.
3. MISL shall establish corresponding escalation and resolution procedure where the resolution timeframe is proportionate with the severity level of the incident.
4. The predetermined escalation and response plan for security incidents shall be tested on a periodic basis.
5. The Organization shall form an ICT Emergency Response Team, comprising staff within MISL with necessary technical and operational skills to handle major incidents.
6. In some situations, major incidents may further develop adversely into a crisis. Senior management shall be kept apprised of the development of these incidents so that the decision to activate the disaster recovery plan can be made on a timely basis.
7. The Organization shall keep customers informed of any major incident. Being able to maintain customer confidence throughout a crisis or an emergency situation is of great importance to the reputation and soundness of MISL.
8. As incidents may trail from numerous factors, MISL shall perform a root-cause and impact analysis for major incidents which result in severe disruption of ICT services. MISL shall take remediation actions to prevent the recurrence of similar incidents.
9. The root-cause and impact analysis report shall cover following areas:

a) Root Cause Analysis

i. When did it happen?

ii. Where did it happen?

iii. Why and how did the incident happen?

iv. How often had a similar incident occurred over the last 3 years?

v. What lessons were learnt from this incident?

b) Impact Analysis

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

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

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

c) Corrective and Preventive Measures

i. Immediate corrective action to be taken to address consequences of the incident.

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

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

10. The Organization shall adequately address all incidents within corresponding resolution timeframes and monitor all incidents to their resolution.

5.3 Problem Management

The aim of problem management is to determine and eliminate the root cause to prevent the occurrence of repeated incidents, While the objective of incident management is to restore the ICT service as soon as possible.

1. MISL shall have established automated and/or manual procedure to log and or record the problems.
2. MISL shall have a process of workflow to escalate any problem to a concerned person to get a quick, effective and orderly response.
3. Problem findings and action steps taken during the problem resolution process shall be documented.

4. A trend analysis of past problems may be performed to facilitate the identification and prevention of similar problems.

5.4 Capacity Management

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

1. To ensure that ICT systems and infrastructure are able to support business functions, MISL shall ensure that indicators such as performance, capacity and utilization are monitored and reviewed.
2. MISL shall establish monitoring processes and implement appropriate thresholds to plan and determine additional resources to meet operational and business requirements efficiently.

Chapter 6

6. Infrastructure Security

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

6.1 Asset Management

1. Prior to procuring any new ICT assets, compatibility assessment (with existing system) shall be performed by MISL.
2. All ICT asset procurement shall be complied with the procurement policy of MISL or MISL.
3. All ICT assets shall be clearly identified and labeled. Labeling shall reflect the established classification of assets.
4. MISL shall maintain an ICT asset inventory stating significant details (e.g. owner, custodian, purchase date, location, license number, configuration, etc.).
5. MISL shall review and update the ICT asset inventory periodically.
6. Information system assets shall be adequately protected from unauthorized access, misuse or fraudulent modification, insertion, deletion, substitution, suppression or disclosure.
7. MISL shall establish a Disposal Policy for information system asset protection. All data on equipment and associated storage media must be destroyed or overwritten before sale, disposal or re-issue.
8. MISL shall provide guidelines for the use of portable devices, especially for the usage at outside premises.
9. MISL shall provide policy to return back organizational assets from employees/external parties upon termination of their employment, contract or agreement.
10. MISL shall comply with the terms of all software licenses and shall not use any software that has not been legally purchased or otherwise legitimately obtained.

11. Outsourced software used in production environments shall be subjected to support agreement with the vendor.
12. MISL shall approve a list of Software which will only be used in any computer.
13. Use of unauthorized or pirated software must strictly be prohibited throughout MISL.

6.2 Desktop/Laptop Devices Controls

1. Desktop computers shall be connected to UPS to prevent damage of data and hardware.
2. Before leaving a desktop or laptop computer unattended, users shall apply the "Lock Workstation" feature. If not applied then the device will be automatically locked as per policy of MISL.
3. Confidential or sensitive information that is stored in laptops must be encrypted.
4. Desktop computers, laptops, monitors, etc. shall be turned off at the end of each workday.
5. Laptops, computer media and any other forms of removable storage containing sensitive information (e.g. CD ROMs, Zip disks, PDAs, Flash drives, external harddrives) shall be stored in a secured location or locked cabinet when not in use.
6. Access to USB ports for Desktop/Laptop computers shall be controlled.
7. Other information storage media containing confidential data such as paper, files, tapes, etc. shall be stored in a secured location or locked cabinet when not in use.
8. Individual users must not install or download software applications and/or executable files to any desktop or laptop computer without prior authorization.
9. Desktop and laptop computer users shall not write, compile, copy, knowingly propagate, execute, or attempt to introduce any computer code designed to self replicate, damage, or otherwise hinder the performance of any computer system (e.g. virus, worm, Trojan etc).
10. Any kind of viruses shall be reported immediately.
11. Viruses shall not be cleaned/ deleted without expert assistance unless otherwise instructed.
12. User identification (ID) and authentication (password) shall be required to access all desktops and laptops whenever turned on or restarted.
13. Standard virus detection software must be installed on all desktop and laptop computers and shall be configured to check files when read and routinely scan the system for viruses.
14. Desktop and laptop computers shall be configured to log all significant computer security relevant events. (e.g. password guessing, unauthorized access attempts or modifications to applications or systems software.)

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

6.3 BYOD Controls

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

1. MISL shall conduct a comprehensive risk assessment on the BYOD implementation to ensure that measures adopted sufficiently to mitigate the security risks associated with BYOD.
2. MISL shall not proceed with the BYOD implementation if they are unable to adequately manage the associated security risks.
3. BYOD is associated with a number of information security risks such as:
    a. Loss, disclosure or corruption of corporate data on Personally Owned Devices (PODs);
    b. Incidents involving threats to, or compromise of, the ICT infrastructure and other information assets (e.g. malware infection or hacking) of MISL;
    c. Noncompliance with applicable laws, regulations and obligations (e.g. privacy or piracy);
    d. Intellectual property rights for information created, stored, processed or communicated on PODs in the course of work for the MISL. Due to information security risks associated with BYOD, employees who wish to opt-in to BYOD must be authorized to do so and must not introduce unacceptable risks onto the MISLs' networks by failing to secure their own equipment.

6.4 Server Security Controls

1. Users shall have specific authorization for accessing servers with defined set of privileges.
2. Additional authentication mechanisms shall be used to control access of remote users.
3. MISL shall ensure the security of the file sharing process. File and print shares must be disabled if not required or kept at a minimum where possible.

6.5 Data Center Controls

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

6.5.1 Physical Security

1. Physical security shall be applied to the information processing area or Data Center. DC must be a restricted area and unauthorized access shall be strictly prohibited.
2. MISL shall limit access to DC to authorized staff only. The MISL or MISL shall only grant access to the DC on a need to have basis. Physical access of staff to the DC shall be revoked immediately if it is no longer required.
3. Emergency exit doors shall be available.
4. The physical security of Data Center premises shall be reviewed at least once each year.

6.5.2 Environmental Security

1. Layout design of Data Center including power supply and network connectivity shall be properly documented.
2. Closed Circuit Television (CCTV) camera shall be installed at appropriate positions on all sides for proper monitoring.
3. Data Center shall have dedicated telephone communication.
4. Power supply systems and other support units must be separated from production sites and placed in secure areas to reduce the risks from environmental threats.
5. The following environmental controls shall be installed:
    a. Uninterrupted Power Supply (UPS) with backup units
    b. Backup Power Supply
    c. Temperature and humidity measuring devices
    d. Water leakage precautions and water drainage system from Air Conditioner
    e. Air conditioners with backup units. Industry standard air conditioning system shall be in place to avoid water leakage from the conventional air conditioning system.
    f. Emergency power cut-off switches where applicable
    g. Emergency lighting arrangement
    h. Dehumidifier for humidity control
6. The above mentioned environmental controls shall be regularly tested and maintenance service contract shall be for 24x7 bases.

6.5.3 Fire Prevention

1. Wall, ceiling and door of the Data Center shall be fire-resistant.
2. Fire suppression equipment shall be installed and tested periodically.
3. Automatic fire/smoke alarming systems shall be installed and tested periodically.
4. There shall be a fire detector below the raised floor, if it is raised.
5. Electric cables and data cables in the Data Center must maintain quality and be concealed.
6. Flammable items such as paper, wooden items, plastics, etc. shall not be allowed to store in the Data Center.

6.6 Server/Network Room/Rack Controls

1. Server/network room/rack must have a glass enclosure with lock and key under a responsible person.
2. Physical access shall be restricted, visitors log must exist and to be maintained for the server room.
3. Access authorization list must be maintained and reviewed on a regular basis.
4. Server/network room/rack shall be air-conditioned. Water leakage precautions and water drainage system from the Air Conditioner shall be installed.
5. Power generators shall be in place to continue operations in case of power failure.
6. UPS shall be in place to provide uninterrupted power supply to the server and required devices.

6.7 Networks Security Management

1. MISL shall establish baseline standards to ensure security for Operating Systems, Databases, Network equipment and portable devices which shall meet organization's policy.
2. MISL shall conduct regular enforcement checks to ensure that the baseline standards are applied uniformly and non-compliances are detected and raised for investigation.
3. The Network Design and its security configurations shall be implemented under a documented plan. There shall have different security zones defined in the network design.
4. All types of cables including UTP, fiber, power shall have proper labeling for further corrective or preventive maintenance works.
5. MISL shall ensure physical security of all network equipment.

6. MISL shall deploy firewalls, or other similar measures, within internal networks to minimize the impact of security exposures originating from third party or overseas systems, as well as from the internal trusted network.
7. Secure Login feature (i.e. SSH) shall be enabled in network devices for remote administration purposes. Any unencrypted login option (i.e. TELNET) shall be disabled.
8. MISL shall backup and review rules on network security devices on a regular basis to determine that such rules are appropriate and relevant.
9. The MISL shall change all default passwords of network devices.
10. All unused ports of access switch shall be shut-off by default if otherwise not defined.
11. All communication devices shall be uniquely identifiable with proper authentication.
12. Role-based administration shall be ensured for the servers.

6.8 Internet Access Management

1. Internet access shall be provided to employees according to the approved Internet Access Management Policy.
2. Access to and use of the internet from MISL premises must be secure and must not compromise information security of MISL.
3. Access to the Internet from MISL premises and systems must be routed through secure gateways.
4. Any local connection directly to the Internet from MISL premises or systems, including standalone PCs and laptops, is prohibited unless approved by Information Security.
5. Employees shall be prohibited from establishing their own connection to the Internet using MISLs' systems or premises.
6. Use of locally attached modems with MISLs' systems in order to establish a connection with the Internet or any third-party or public network via broadband, ISDN or PSTN services is prohibited unless specifically approved.
7. Internet access provided by the MISL must not be used to transact any commercial business activity that is not done by the MISL. Personal business interests of staff or other personnel must not be conducted.

6.9 Email Management

1. Email systems shall be used according to MISLs policy.
2. Access to the email system shall only be obtained through official request.
3. Email shall not be used to communicate confidential information to external parties unless encrypted using approved encryption facilities.
4. Employees must consider the confidentiality and sensitivity of all email content, before forwarding email or replying to external parties.
5. Information transmitted by email must not be defamatory, abusive, involve any form of racial or sexual abuse, damage the reputation of the MISL, or contain any material that is harmful to employees, customers, competitors, or others. The willful transmission of any such material is likely to result in disciplinary action.
6. MISL email system is principally provided for business purposes. Personal use of the MISL email system is only allowed under management discretion and requires proper permission; such personal use may be withdrawn or restricted at any time.

7. Corporate email addresses must not be used for any social networking, blogs, groups, forums, etc. unless having management approval.
8. Email transmissions from the MISL must have a disclaimer stating confidentiality of the email content and asking the intended recipient.
9. Concerned department shall perform regular review and monitoring of email services.

6.10 Vulnerability Assessment and Penetration Testing

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

1. MISL shall conduct VAs regularly to detect security vulnerabilities in the ICT environment.
2. MISL shall deploy a combination of automated tools and manual techniques to perform a comprehensive VA. For web-based systems, the scope of VA shall include common web vulnerabilities such as SQL injection, cross-site scripting, etc.
3. MISL shall establish a process to remedy issues identified in VAs and perform subsequent validation of the remediation to validate that gaps are fully addressed.
4. MISL shall carry out penetration tests in order to conduct an in depth evaluation of the security posture of the system through simulations of actual attacks on the system. The MISL shall conduct penetration tests on network infrastructure and internet-based systems periodically or need basis.

Chapter 7

7. Access Control

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

7.1 User Access Management

1. MISL shall only grant user access to ICT systems and networks on a need-to-use basis and within the period when the access is required.
2. MISL shall closely monitor non-employees (contractual, outsourced, or vendor staff) for access restrictions.
3. Each user must have a unique User ID and a valid password.
4. User ID Maintenance form with access privileges shall be duly approved by the appropriate authority.
5. User access shall be locked for unsuccessful login attempts.
6. User access privileges must be kept updated for job status changes.
7. MISL shall ensure that records of user access are uniquely identified and logged for audit and review purposes.
8. MISL shall perform regular reviews of user access privileges to verify that privileges are granted appropriately.

7.2 Password Management

1. MISL shall enforce strong password controls over users' access.
2. Password controls shall include a change of password upon first logon.
3. Password definition parameters shall ensure that minimum password length is maintained according to MISL's Policy (at least 6 characters).
4. Password shall be a combination of at least three of stated criteria like uppercase, lowercase, special characters and numbers.
5. Maximum validity period of password shall not be beyond the number of days permitted in MISL's Policy (maximum 90 days cycle).
6. Parameters to control maximum number of invalid logon attempts shall be specified properly in the system according to the MISL's Policy (maximum 3 consecutive times).

7. Password history maintenance shall be enabled in the system to allow the same passwords to be used again after at least three (3) times.
8. Administrative passwords of Operating System, Database and Business Applications shall be kept in safe custody with a sealed envelope.

Chapter 8

8. Business Continuity and Disaster Management

Business Continuity and Disaster Recovery Management is required for planning of business resiliency for critical incidents, operational risks taken into account for wide area disasters, Data Center disasters and the recovery plan. The primary objective of Business Continuity Plan (BCP) is to enable a MISL to survive in a disaster and to re-establish normal business operations. In order to survive with minimum financial and reputational loss, MISL shall assure that critical operations can resume normal processing within a reasonable time frame. The contingency plan shall cover the business resumption planning and disaster recovery planning. Contingency plans shall also address the backup, recovery and restore process.

8.1 Business Continuity Plan (BCP)

1. MISL must have an approved Business Continuity Plan addressing the recovery from disaster to continue its operation.
2. Approved BCP shall be circulated to all relevant stakeholders. The recipients would receive a copy of the amended plan whenever any amendment or alteration takes place.
3. Documents related to BCP must be kept in a secured off-site location. One copy shall be stored in the office for ready reference.
4. The BCP shall be coordinated with and supported by the Business Impact Analysis (BIA) and the Disaster Recovery Plan (DRP) considering system requirements, processes and interdependencies.
5. BCP shall address the followings:
    a. Action plan to restore business operations within the specified time frame for: i) office hour disaster; ii) outside office hour disaster.
    b. Emergency contacts, addresses and phone numbers of employees, venders and agencies.
    c. Grab list of items such as backup tapes, laptops, flash drives, etc.
    d. Disaster recovery site map.
6. BCP must be tested and reviewed at least once a year to ensure the effectiveness.

7. MISL must have an approved Business Continuity Plan addressing the recovery from disaster to continue its operation.
8. Approved BCP shall be circulated to all relevant stakeholders. The recipients would receive a copy of the amended plan whenever any amendment or alteration takes place.
9. Documents related to BCP must be kept in a secured off-site location. One copy shall be stored in the office for ready reference.
10. The BCP shall be coordinated with and supported by the Business Impact Analysis (BIA) and the Disaster Recovery Plan (DRP) considering system requirements, processes and interdependencies.
11. BCP shall address the followings:
    a. Action plan to restore business operations within the specified time frame for: i) office hour disaster; ii) outside office hour disaster.
    b. Emergency contacts, addresses and phone numbers of employees, venders and agencies.
    c. Grab list of items such as backup tapes, laptops, flash drives, etc.
    d. Disaster recovery site map
12. BCP must be tested and reviewed at least once a year to ensure the effectiveness.

8.2 Disaster Recovery Plan (DRP)

1. MISL must have an approved Disaster Recovery Plan. In formulating and constructing a rapid recovery plan, the MISL shall include a scenario analysis to identify and address various types of contingency scenarios. The MISL or MISL shall consider scenarios such as major system outages which may be caused by system faults, hardware malfunction, operating errors or security incidents as well as a total incapacitation of the primary DC.
2. MISL shall establish a Disaster Recovery Site (DRS) which is geographically separated from the primary site to enable the restoration of critical systems and resumption of business operations when a disruption occurs at the primary site.
3. Physical and environmental security of the DRS and/or Near DC shall be maintained.
4. MISL shall define system recovery and business resumption priorities and establish specific recovery objectives including recovery time objective (RTO) and recovery point objective (RPO) for ICT systems and applications. RTO is the duration of time, from the point of disruption, within which a system shall be restored. RPO refers to the acceptable amount of data loss for an ICT system while a disaster occurs.

5. MISL may explore recovery strategies and technologies such as onsite redundancy and real-time data replication to enhance the MISL's recovery capability.
6. Information Security shall be maintained properly throughout the recovery process.
7. An up-to-date and tested copy of the DR plan shall be securely held off-site. One copy shall be stored in the office for ready reference.
8. MISL shall test and validate at least annually the effectiveness of recovery requirements and the ability of staff to execute the necessary emergency and recovery procedures.
9. The MISL shall involve its concerned teams in the design and execution of comprehensive test cases of the respective applications to verify that recovered systems function properly.
10. DR test documentation shall include at a minimum of Scope, Plan and Test Result. Test reports shall be communicated to management and other stakeholders and preserved for future necessity.

8.3 Data Backup and Restore Management

1. MISL shall develop a data backup and recovery policy. Each application must have a planned, scheduled and documented backup strategy, involving the making of both on- and off-line backups and transfer of backups to secure off-site storage.
2. The frequency of backups taken for information must be determined in line with the classification of the information and the requirements of the business continuity plans for each application.
3. The details of the planned backup schedule for each application must include the retention period for backed-up or archived information and the retention period must be consistent with local legal and regulatory requirements.
4. All media containing backed-up information must be labeled with the information content, backup cycle, backup serial identifier, backup date and classification of the information content.
5. The backup inventory and log sheet shall be maintained, checked and signed by the supervisor.
6. At least one copy of backup shall be kept on-site for the time critical delivery.
7. The process of restoring information from both on- and off-site backup storage must be documented.
8. MISL shall carry out periodic testing and validation of the recovery capability of backup media and assess whether it is adequate and sufficiently effective to support the MISL's recovery process.

Chapter 9

9. Glossary and Acronyms

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

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

References

A. Framework for ICT Policy and Guidelines of Millennium Information Solution
B. Guideline on ICT Security For Banks and FIs 2015 by Bangladesh Bank
C. Information Security Policy Guideline 2014 by GoB.
D. Implementation of the Agile Policy to ICT Projects and Services : Ethical Digital Standards BCN