INFORMATION TECHNOLOGY POLICY

As per RBI Direction

Approved by the Directors of the Board, in the Board meeting held on 17-05-2023

Introduction

This document defines the Information Technology policies within Muthoottu Mini Financiers Ltd (MMFL). All MMFL associates, contractors, partners, and vendors with access to MMFL information assets must comply the policies contained herein. MMFL retains contractual and operational rights for the protection of the Information System Assets when they are under MMFL operational control.

Why Security?

MMFL requires information security in information system environment to protect its information assets, to maintain a competitive advantage in the marketplace, to ensure profitability, and to maintain stake holder's trust and confidence.

Philosophy of Protection

Philosophy of protection provides the intent and direction behind our protection policies, procedures, and control. Our protection philosophy is comprised of three tenets:

1. *Security is everyone's responsibility.*

   Maintaining an effective and efficient security posture for MMFL require a proactive stance on security issues from everyone. Security is not "somebody else problem;" as a member of MMFL you have the responsibility to adhere to the security policies and procedures of the company.

2. *Security permeates the MMFL.*

   Security is not just focused on physical and technical "border control." Rather, MMFL seeks to ensure reasonable and appropriate levels of security awareness and protection throughout our organization and infrastructure. There is no place in our business where security is not a consideration.

3. *Security is a business enabler.*

   Our purpose as a company is "To enable a better way for trusted commerce." A strong security foundation, and maintained, becomes an effective market differentiator for our company. Security has a direct impact on our viability within

the marketplace, and must be treated as a valued commodity. The tenets of our philosophy of protection are mutually supportive; ignoring anyone in favour of another undermines the overall security posture of our organization.

Critical Success Factors

The following factors are critical to the successful implementation of security within MMFL:

- *Comprehensive security policies objectives and initiatives that clearly reflect business objectives.*
- *A security approach that is consistent with MMFL culture*
- *Highly visible support MMFL executive management*
- *Solid understanding of security requirements and risk management practices*
- *Effective communication of information security to all MMFL employees, associates, partners, clients, vendors and developers.*
- *Guidance on information technology policy to all MMFL employees, associates, partners, clients, vendors and developers.*
- *Information security awareness and training*
- *Continual review and measurement of the effectiveness and efficiency of security controls and mechanisms*
- *Timely adjustments to the security posture by addressing deficiencies and by reflecting changes in MMFL business objectives as necessary*

1. Information Technology Organization

Information Technology Strategy Committee is chartered to direct and manage information security governance for the MMFL enterprise. Information Technology Strategy Committee (ITSC) is responsible for policy maintenance activities including reviews and revisions and for monitoring compliance with this policy and may other departments to assist in the enforcement of this policy.

The ITSC is headed by Mr. Manoj Kumar R-Independent Director- Chairperson of the Committee and the members of the committee includes

1. *Mr. Nejimudin C I -Chief Information officer (CIO) - Member*
2. *Mr. Vinodhkumar.C- Chief Technology Officer(CTO)- Member*
3. *Mr. Mathew Muthoottu – Managing Director- Member.*

Information Technology Strategy Committee (ITSC) is the organization, which has ownership of all security policies and procedures. In this context, "ownership" is defined as responsibility for creating, monitoring, and enforcing the administrative, physical, and technical controls MMFL.

ITSE will conduct annual risk assessments in order to determine the level of security risk and the efficacy of security controls within MMFL. The purpose of these risks assessments will be to:

- *Address changes to business requirements and priorities*
- *Consider new threats and vulnerabilities that might exist*
- *Confirm that security controls and mechanisms remain effective and efficient*

ITSE will create all security policies. Security policies will be published and communicated to all MMFL employees, associates, and vendors, as appropriate.

ITSE will review and make necessary changes to the Policy on an annual basis or whenever a major change is made to the MMFL environment or a new technology is deployed. During the review, ITSE will evaluate the following:

- *The overall policy's effectiveness*
- *The costs and impact of security controls and mechanisms on business efficiency.*
- *Changes in technology that affect the adequacy and / or appropriateness of security controls and mechanisms in the environment ITSE will create a repository for the storage of all security policies. This repository must be accessible by all MMFL. associates in some fashion.*

1.1 Role of Committee includes

- *Approving IT strategy and policy documents and ensuring that the management has put an effective strategic planning process in place;*
- *Ascertaining that management has implemented processes and practices that ensure that the IT delivers value to the business;*
- *Ensuring IT investments represent a balance of risks and benefits and that budgets are acceptable;*
- *Monitoring the method that management uses to determine the IT resources needed to achieve strategic goals and provide high-level direction for sourcing and use of IT resources;*
- *Ensuring proper balance of IT investments for sustaining NBFC's growth and becoming aware about exposure towards IT risks and controls.*
- *Review and amend the IT strategies in line with the corporate strategies*
- *Institute an effective governance mechanism and risk management process for all IT outsourced operations*

ITSE will report to the executive leadership team via CIO. The CIO will determine the reporting schedule and formats for ITSE.
Independent Review of Information Security: Internal Audit, or a qualified third party, must periodically review the effectiveness of the MMFL security program and note any deficiencies so that Information System Steering committee can improve the program.

1.2 Responsibilities of CIO

- *Set objectives and strategies for the IT department*
- *Select and implement suitable technology to streamline all internal operations and help optimize their strategic benefits*
- *Plan the implementation of new systems and provide guidance to IT professionals and other staff within the organization*
- *Approve purchases of technological equipment and software and establish partnerships with IT providers*
- *Oversee the technological infrastructure (networks and computer systems) in the organization to ensure optimal performance*
- *Direct and organize IT-related projects*
- *Monitor changes or advancements in technology to discover ways the company can gain competitive advantage*
- *Analyse the costs, value and risks of information technology to advise management and suggest actions*
- *Ensure implementation of IT Policy to the operational level involving IT strategy, value delivery, risk management and IT resource management.*

- *Responsible for formulation, review and monitoring of BCP to ensure continued effectiveness*
- *Focus on improving operational efficiencies and saving costs*
- *Communicate technical issues in business language to the board*
- *Ensure that the company's digital strategy aligns with the business strategy,*

The overall responsibility for ensuring compliance with all security controls as specified by ITSE rest with the CIO.
Individual department heads and team leadership are responsible for implementation of security controls in their respective domain by the direction of ITSE

1.3 Responsibilities of CTO

- *Develop technical aspects of the company's strategy to ensure alignment with its business goals*
- *Discover and implement new technologies that yield competitive advantage*
- *Help departments use technology profitably*
- *Build quality assurance and data protection processes*
- *Monitor KPIs and IT budgets to assess technological performance*
- *Use stakeholders' feedback to inform necessary improvements and adjustments to technology*
- *Maintain current knowledge of technology landscape and developments*
- *Track, analyse and monitor technology performance metrics*
- *Identify new areas of digital marketing opportunities and create plans to implement them*
- *Take the initiative in thought leadership, innovation and creativity*
- *Oversee all system design and changes in system architecture*
- *Delivering the latest tech to customers, both internal and external*
- *Responsible for management of R&D and technological needs of the organization*
- *Oversee the company's data, security, maintenance and network of a company, and help in implementing the company's technical strategy.*
- *Responsible for the engineering team and employing a technical strategy to improve the end product and leveraging new technologies to enhance the product*

2. ACCESS CONTROL

The process for creating, changing and removing users from systems and application should be established. Allowed access rights should be audited and revised periodically. Access to MMFL information asset should be allowed on the basis of business requirement.

2.1 Access Control Methods

2.1.1 Access to data is variously and appropriately controlled according to the data classification.

2.1.2 Access control methods include explicit logon to devices, Windows share and file permissions to files and folders, user account privileges, server and workstation access rights, firewall permissions, network zone and VLAN ACLs, IIS / Apache intranet / extranet authentication rights, MMFL login rights, database access rights, encryption and other methods as necessary.

2.1.3 Access control applies to all MMFL owned networks, servers, workstations, laptops, mobile devices and services run on behalf of MMFL.

2.1.4 Role-based access control (RBAC) will be used as the method to secure access to all file-based/application resources and contained within MMFL.

2.2 Access Approval

All access by any user or system (employee, contractor, business partner, trading member) must be justified by a business reason for why the access is necessary, along with the parameters of access (what classification level, times/dates, from what locations, etc.) Access cannot be simply given to 'everything'. Justifications shall be kept on file for review, as well as forensic purposes.

Users will request access in the following way:

- *A formal access control request is made using an approved form and documentation.*
- *A valid business justification for the access is documented.*
- *Access requests will specify particular systems or information (no general access to all) commensurate with the person's access level.*
- *Access requests must be correctly approved*
- *Request forms should be stored by the administrators and retained until at least 90 days after the person has left the company*

Changes in access must be requested and documented in the same way as original access requests (may be accomplished on the original form as notations and subsequent approval signatures)

2.3 Access Request Form

All access must be requested through an Access Request Form and routed through IT Department. Log register is to be maintained in IT Department server or related systems. Scheduled IT officer is permitted to access the systems with the approval if IT Manager / IT Head.

2.4 User registration

A registration and de-registration procedure shall be used for granting access to all information asset of the company. User should not get access without registration process and in case of violation of being a valid user; user rights should be de-registered with immediate effect.

2.5 User IDs

Each user must have a unique ID that only they should use for logical access. This ID may be used to access several systems but will not be used by anyone else. Employees should not share their unique ID and password. Users are responsible for all actions taken with their unique user ID, whether or not they are the ones who took the actions. Thus, it behoves the user to protect their IDs and passwords. Never give your password to anyone, including your supervisor. User IDs for users who have left the company must be deactivated or deleted. It is permissible to retain a user account for access to the user's data once they have left, but the password must be changed to prevent the user from accessing their account. Data will be recovered and moved as soon as possible, and the account disabled or deleted in this case.

2.6 Password

Password issuing, strength requirements, changing and control will be managed through formal processes.

Password issuing will be managed by the IT Department for employees, associates, contractors, partners, and vendors. Password length, complexity and expiration times will be controlled through Group Policy Objects in Windows/Linux/Application.

2.7 Privilege management

The allocation and use of privileges shall be restricted and controlled. Inappropriate use of system privileges may become a major contributory factor to the failure of systems hence access to critical systems should be filtered in such a way that nobody will be able to take disadvantage of the rights.

2.8 User Account Review

CIO will conduct periodic (at least monthly) audits of all user accounts and disable/delete any accounts that have not been used in the past month. If the user is known to be away from the office (maternity leave, sabbatical, etc.) then the account must be disabled and a notation made as to why and the person's expected return. User accounts that have never been used in the month period must be disabled.

2.9 Review of user access rights

User access rights should be reviewed at regular intervals for effective control over access to data and information. User access to data and information should be reviewed on regular basis to keep updated access control. Transferred or left employees account gets removed in such periodic access audit.

2.10 User Access Termination

Users who leave MMFL will have their access to all systems terminated on their last day, or as soon as possible if they are being terminated for cause. All access must be terminated (through disabling, deleting, or changing the password), including physical access to facilities, and remote access. The user access request form and associated documentation must be used as a reference to ensure that all systems and networks are addressed. The access request form must be annotated that access has been terminated (and how, (e.g. disabling).

3. ASSET MANAGEMENT

This Policy defines the key principles and requirements which will apply to the information assets of the company.

Inventory of Software, Hardware and Information asset shall be maintained and the format should be approved by ITSE. All information asset of the company shall be identified, listed in common format and shall identify the associated vulnerabilities/threats for risk assessment.

This policy ensure.

- *accurate recording of asset information.*
- *accurate recording of asset movements.*
- *all responsible parties are aware of their roles and responsibilities regarding the assets of the organization.*
- *preventative measures are in place to eliminate theft, loss and misuse.*

3.1 Ownership of assets

Ownership and maintenance of inventory shall be assigned to a responsible person/team. ITSE should define the ownership of Inventory to maintain and keep it up to date. Inventory can be maintained in written or electronic form. It should be available to all respective peoples who will use it only for official purpose. Data should be classified and ownership should be defined.

3.2 Acceptable use of assets

Rules for acceptable use of assets shall be defined and communicate to all the users and external parties. ITSE should define the rules for acceptable use of the assets. This gives the guidelines to the asset handler about the maintaining security while handling the assets.

3.3 Information Asset Classification

The Information asset owner must classify all the information assets of MMFL as per its sensitivity and criticality to the organization. Information owners will be responsible for assigning and maintaining appropriate data classifications. Files and electronic mails created by individuals will be owned and classified by them.

All information processed, maintained, stored, and generated by MMFL in the course of normal business operations must be treated as information assets and handled in accordance with the information classification standard.

All sensitive information at MMFL must have a formally assigned information owner, responsible for maintaining the security of their information. The information owner must develop appropriate protective and accountability controls to safeguard their data.

3.4 Information labelling and handling

All the information assets shall be labelled as per the data classification scheme. All assets need to be labelled from the time it is created to the time when it is destroyed. Such labelling shall appear on all manifestation of information.

Violations of this Policy may result in suspension or loss of the violator's use privileges, with respect to MMFL owned Information System Policy. Additional administrative sanctions may apply; up to and including termination of employment or contractor status with the MMFL or expulsion of employees. Civil, criminal and equitable remedies may also apply.

4. PASSWORD MANAGEMENT

The purpose of this policy is to establish a standard for the creation of strong passwords, the protection of those passwords, and the frequency of change. This is to secure and manage the logical access to MMFL information system.

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any MMFL facility, has access to the MMFL network and/or any manner of MMFL information system.

4.1 General Controls

i. *All systems-level passwords (e.g., root, enable, network administrator, application administration accounts, etc.) must be changed at least every 30 days.*
ii. *All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every 90 days and cannot be reused the past 2 passwords.*
iii. *User accounts with access to Loan Management System/Operational Application privileges must have a unique password from all other accounts held by that user.*
iv. *Passwords must not be inserted into email messages or other forms of electronic communication.*
v. *All user-level, system-level, and operational applications access level passwords must conform to the guidelines described below.*

4.2 Guidelines for password construction

- *Minimum password complexity requirement includes, One upper case, One Lower case, one Numeric One special Character and a minimum of 8 characters length.*
- *Not be a dictionary word or proper name.*
- *Not be the same as the User ID.*
- *Expire within a maximum of 90 calendar days.*
- *Not be identical to the previous 2(two) passwords.*
- *Not be transmitted in the clear or plaintext outside the secure location.*
- *Not be displayed when entered.*
- *Ensure passwords are only reset for authorized user.*

4.3 Password Deletion

All passwords that are no longer needed must be deleted or disabled Immediately. This includes, but is not limited to, the following:

- *When a user retires, quits, is reassigned, released, dismissed, etc.*
- *Default passwords shall be changed immediately on all equipment.*
- *Third party accounts, when no longer needed to perform their duties.*

4.4 Password Protection Standards

Do not use your User ID as your password. All passwords are to be treated as sensitive, Confidential MMFL information.

Here is a list of "do not's"

- *Don't reveal a password over the phone to anyone*
- *Don't reveal a password in an mail message*
- *Do not share passwords with anyone.*
- *Don't reveal a password to the boss*
- *Don' talk about a password in front of others*
- *Don't hint at the format of a password*
- *Don't reveal a password on questionnaires or security forms*
- *Don't share a password with family members*
- *Don't reveal a password to a co-worker while on vacation*
- *Don't use the "Remember Password" feature of applications*
- *Don't write passwords down and store them anywhere in your office.*
- *Don't store passwords in a file on ANY computer system unencrypted.*

If someone demands a password, refer them to this document or have them call ITSE member.

If an account or password is suspected to have been compromised, report the incident to ITSE coordinator and change all passwords.

Password cracking or guessing may be performed on a periodic or random basis by the MMFL ITSE Coordinator. If a password is guessed or cracked during one of these scans, the user will be required to change it.

4.5 Remote Access Users

Access to the MMFL networks via remote access is to be controlled by using either a Virtual Private Network (in which a password and user id are required) or a form of advanced authentication (i.e., Biometrics, Tokens, Public Key Infrastructure (PKI), Certificates, etc.).

4.6 Penalties

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5. NETWORK SECURITY

The purpose of this policy is to establish administrative direction, procedural requirements, and technical guidance to ensure the appropriate protection of MMFL information handled by computer networks such as Internet / Intranet / LAN / WAN / External-related systems that are required to be served the interest of MMFL organisation.

This policy applies to all MMFL networks, both the perimeter and the infrastructure, and the parties with which MMFL do businesses.

Business associates and any individual who are accessing the MMFL information system must cooperate to protect the network by securing computers and network devices in order to secure access. In addition, they must certify that the devices connecting to the business unit's network are in compliance with the policies and procedures as established by MMFL Department.

The following rules define the policy regarding access to the MMFL network:

1. *Only authorized people can gain access to MMFL's networks.*

Positive identification is required for system usage. All users must have their identities positively identified with user-IDs and secure passwords or by other means that provide equal or greater security prior to being permitted to use MMFL owned computers.

1. *User-IDs must each uniquely identify a single user. Each computer user-ID must uniquely identify only one user, so as to ensure individual accountability in system logs. Shared or group user-IDs are not permitted.*

2. *Access controls required for remote systems connecting to production systems. All computers that have remote real-time dialogs with MMFL's IT production / test environment systems must run an access control package approved by MMFL IT Department.*

3. *All log-in banners must include security notice. Every log-in screen for multi-user computers must include a special notice. This notice must state:*

   (1) the system may only be accessed by authorized users,

   (2) users who log-in represent that they are authorized to do so.

   (3) unauthorized system usage or abuse is subject to penalties, and

   (4) system usage will be monitored and logged.

4. Security notice in login banner must not disclose system information.

All log-in banners on network-connected MMFL computer systems must simply ask the user to login, providing terse prompts only where essential.

5. Identifying information about the organization, operating system, system configuration, or other internal matters must not be provided until a user's identity has been successfully authenticated.

6. Users must log off before leaving sensitive systems unattended. If the computer system to which users are connected or which they are currently using contains sensitive information, and especially if they have special access rights, such as domain admin or system administrator privileges, users must not leave their computer, workstation, or terminal unattended without first logging-out, locking the workstation, or invoking a password-protected screen saver.

7. Operational, Administrative, and Supporting Technology Services' staff must:

a. Follow policies and procedures, as established by MMFL IT Department, to validate firewall activation, operating system installation, application software security patches and virus protection updates for all devices in the unit's areas of physical or administrative control that are to be, or are configured to utilize network resources that are controlled and managed by MMFL IT Department.

b. Follow policies and procedures, as established by MMFL IT Department, for using automated tools to test devices connected to the business unit's local wired or wireless data network for compliance. Non-compliant devices are to be disconnected, disabled or quarantined until the device is brought into compliance. When devices are not compliant, operating units, or individuals and their information technology staff must employ compensating controls. Units must document compensating controls and/or any exceptions. These must be reviewed, tested, and approved by ITSE.

c. The operating business unit or individual must retain the approved documentation for audits as long as the device is in operation. Any connection to the Internet, or to a national or regional network from a private network operated by an operational, administrative, or support unit, must be made via MMFL network resources.

8. All network access attempts (success or failure) must be logged and retained for auditing.

5.1. Server

5.1.1 Each device must meet the following minimum standards prior to, and after connecting to the data network or support infrastructure:

- *The device must be guarded by an up-to-date and active firewall set to protect it from unauthorized network traffic.*
- *Current operating system and application software with current security patches must be installed.*
- *The device must be protected against malicious or undesired software such as viruses, spyware, or adware.*
- *Access to the device must require appropriate authentication controls such as account identifiers and robust passwords.*
- *The device must be certified and registered by ITSE as equipment that has met all security criteria, prior to connecting to the network.*

5.1.2 Server General Configuration Guidelines

The following items serve as provisioning configuration guidelines for the servers that are managed by ITSE members:

- *Operating System configuration should be in accordance with ITSE approved guidelines.*
- *Services and applications that will not be used must be disabled where practical.*
- *Access to services should be logged and/or protected through access-control methods.*
- *The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements.*
- *Do not use administrator account when a non-privileged account can performed the task.*
- *If a methodology for secure channel connection is available (i.e., technically feasible), privileged access must be performed over secure channels, (e.g., encrypted network connections using SSH or IPsec).*
- *Servers should be physically located in an access-controlled environment.*
- *Servers are specifically prohibited from being operated in uncontrolled cubicle areas.*

5.1.3 Internal network addresses must not be publicly released.

The internal system addresses, configurations, and related system design information systems and users outside the MMFL internal network cannot access this information.

5.1.4 All Internet Web servers must be firewall protected.

All connections between MMFL 's internal networks and the Internet (or any other publicly-accessible computer network) must be protected by a router, firewall, or related access controls approved by ITSE.

5.1.5 In house public servers on Internet must be placed on separate subnets or De-Militarized Zone (DMZ). Internally hosted public Internet servers must be placed on subnets separate from internal networks. It can be either in DMZ or separate subnets. Routers or firewalls must be employed to restrict traffic from the public servers to internal networks.

5.2. ROUTER

5.2.1. All routers within MMFL must meet the following configuration standards:

- *Any user accounts and its authentication are required to be configured on routers must use industry standard methods or standards defined by ITSE.*

- *The enable password on the router must be kept in a secure encrypted form. The router must have the enable password set to the current production router password from the router's support organization*

5.2.2. All routers within organisation must disallow the following:

- *IP directed broadcast. Incoming packets at the router sourced with invalid addresses such as RFC1918 address*
- *TCP small services*
- *UDP small services*
- *All source routing*
- *All web services running on router*

5.2.3. Any external network connections, inbound or outbound, must be authenticated or secured via approved standards.

Before users reach a log-in banner, all inbound lines connected to MMFL internal networks and/or computer systems must pass through an additional access control point, such as a firewall, which has been approved by ITSE. Unless ITSE has first approved the action in writing,

MMFL staff must not enable any trusted host relationships between computers connected to the internal network.

5.2.4. Use Enterprise standardized SNMP (Simple Network Management Protocol).

Routers must be included in the Enterprise Management System with a designated point of contact. Users must have explicit permission by ITSE to access or configure any router. All activities performed on these devices may be logged, and violations of this policy may result in disciplinary action, and may be reported to law enforcement. There is no right to privacy on these devices.

5.2.5 Telnet may never be used across any network to manage a router, unless there is a secure tunnel protecting the entire communication path. SSH is the preferred management protocol.

5.3. FIREWALL

5.3.1 Real-time external network connections require firewalls.

Before reaching a log-in banner, all in-bound real-time external connections to internal networks and/or multi-user computer systems must pass through an additional access control point such as a firewall, gateway, or access server.

- *The functionality of firewalls will be setup to ensure secure Internet connections and the connections to other networks.*
- *Firewall rule-sets must be created for implementing security controls as they pertain to the handling of applications traffic such as web, email and other business processing.*
- *Users, who are at remote locations, must verify that firewall appliances are in place to secure their connections to the Internet and Internet Service Providers before establishing the connection with the network.*

5.3.2 Firewall configuration change requires ITSE permission.

Firewall configuration rules and permissible service rules established by ITSE have been reached after evaluation. These rules must not be changed without first obtaining the permission of ITSE Information Security Management.

- *The IT Department must monitor incident response team reports and security websites for information about current attacks and vulnerabilities.*
- *The firewall policy should be updated as necessary.*
- *A formal process must be used for managing the addition and deletion of firewall rules.*
- *The ITSE must ensure that administrators receive regular training in order to stay current with threats and vulnerabilities.*

5.4. New Installations and Change Management Procedures

All new installations and changes to the configuration of existing equipment and applications must follow the following policies/procedures:

- *New installations must be done via the DMZ Equipment Deployment Process.*
- *Configuration changes must follow the Change Management (CM) Procedures.*
- *must be invited to perform system/application audits prior to the deployment of new services.*
- *must be engaged, either directly or via CM, to approve all new deployments and configuration changes.*

5.5. Equipment Outsourced to External Service Providers

The responsibility for the security of the equipment deployed by external service providers must be clarified in the contract with the service provider and security contacts, and escalation procedures documented. Contracting departments are responsible for third party compliance with this policy.

5.6. Network Management/ Access Requirements

- *To assure the integrity and availability of network services, no other network communications (with the exception of commercial cellular telephony networks or other means of communication after getting prior approval from ITSE) shall be permitted on facilities.*
- *No networking equipment (routers, managed switches, DHCP servers, DNS servers, WINS servers, VPN servers, remote access dial-in servers, wireless access points, hardware firewalls) – shall be permitted without a written exception from ITSE.*
- *No device or program that has the potential to disrupt network service to others is permitted on the Network without prior arrangement with ITSE.*

5.7. Protocol Standards

The management of network protocols shall be performed by information systems administrators and network administrators to assure the efficiency, availability, and security of the common resources.

5.8. Simple Mail Transfer Protocol (SMTP):

- *All email protocol traffic shall utilize the centralized mail gateways. Inbound mail traffic with destination addresses for servers other than those operated by shall utilize a DNS MX record to relay that traffic through the centralized mail gateways. All outbound traffic shall utilize the SMTP gateway.*
- *The use SSL or TLS based communication standards for email client to email server communication is preferred such that the authentication session is the protected transaction.*

5.9. Domain Name Services Protocol (DNS):

- *All hosts on networks shall utilize the DNS systems. All hosts connected to networks receive a muthoottumini.com domain name extension. No host connected to networks shall be addressable by any DNS name other than that provided by MMFL .*
- *No host with a www.muthoottumini.com domain name (and an IP address within the network spaces) will use an IP address outside the MMFL's registered name space without a written exemption from IT Department.*

5.10. Dynamic Host Configuration Protocol (DHCP):

- *All hosts on networks shall either obtain and use a static IP address or use the DHCP service to obtain an assigned IP address. Users shall not use a self-assigned IP address, or operate a DHCP server. The use of bootstrap (BOOTP) shall be governed in the same manner as DCHP.*

5.11. Banned Protocols:

- *IT Department keeps a listing of banned protocols which have shown to interfere with the architecture and management of the network environment.*

5.12. Remote Access

- *Secure remote access must be strictly controlled. Control will be enforced via one-time password authentication or public/private key with strong passphrases.*
- *At no time should any employee provide his or her login or email password to anyone, not even family members.*
- *Employees and contractors with remote access privileges must ensure that their owned or personal computer or workstation, which is remotely connected to the enterprise network is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user.*
- *Employees, contractors and associates with remote access privileges to the network must not use non email accounts or other external resources to conduct NBFC business.*
- *Routers for dedicated Integrated Services Digital Network (ISDN) lines configured for access to the 's network must meet minimum authentication requirements of Challenge-Handshake Authentication Protocol (CHAP).*
- *Reconfiguration of a home user's equipment for the purpose of split-tunnelling or dual homing is not permitted at any time*
- *Frame relay must meet minimum authentication requirements of Data Link Connection Identifier (DLCI) standards.*

- *All hosts that are connected to the internal network via remote access technologies must use the most up-to-date anti-virus software; this includes personal computers.*
- *Third party connections must comply with requirements as stated in the Third Party Agreement.*
- *Personal equipment that is used to connect to the network must meet the requirements of MMFL owned equipment for remote access.*
- *Organizations or individuals who wish to implement non-standard Remote Access solutions to the production network must obtain prior approval from ITSE.*
- *Direct network connections with outside organizations must be approved. The establishment of a direct connection between the systems and computers at external organizations, via the Internet or any other public network, is prohibited unless this connection has first been approved by the ITSE.*
- *Inventory of connections to external networks must be maintained. ITSE must maintain a current inventory of all connections to external networks including telephone networks, extranets, the Internet.*

5.13. VPN

- *It is the responsibility of employees with VPN privileges to ensure that unauthorized users are not allowed access to internal networks.*
- *When actively connected to the network, the VPN will force all traffic to and from the PC over the VPN tunnel: all other traffic will be dropped.*
- *Dual (split) tunnelling is NOT permitted; only one network connection is allowed.*
- *VPN gateways will be set up and managed by ITSE.*
- *All computers connected to the internal networks via VPN or any other technology must use the most up-to-date anti-virus software that is the enterprise standard, this includes personal computer.*
- *VPN users will be automatically disconnected from the network after thirty minutes of inactivity. The user must then logon again to reconnect to the network. Pings or other artificial network processes are not to be used to keep the connection open.*
- *Users of computers that are not owned by the must configure the equipment to comply with VPN and Network policies.*
- *By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of the network, and as such are subject to the same rules and regulations that apply to the MMFL 's owned equipment, i.e., their machines must be configured to comply with ITSE's Security Policies.*

6. PROTECTION AGAINST MALICIOUS CODES

This policy will detail the appropriate measures to take in the event of a virus attack or the discovery of malware on a system or systems. It also highlights the fact that staff must not attempt to circumvent the malicious code detection, prevention and remediation techniques employed and that disciplinary action will be taken against anyone found to be trying to do so.

Every system used or owned by the company must have internationally recognized, centrally managed, antivirus software installed and activated.

Antivirus definition file updates must be deployed through automated means on a daily basis. Systems must be configured so as to prevent users from disabling anti-virus tools.

Portable computers issued and used to house or access company network or services must have Personal Firewall and Anti-virus.

Non-adherence to the Malicious Code Policy and related policies will result in local disciplinary proceedings being implemented.

6.1 Internet and Email Policy

Email, and internet usage assigned to an employee's computer is solely for the purpose of conducting company business. Some job responsibilities at the Company require access to the internet and only people appropriately authorized, for Company purposes, may use the internet to access. This authorization is generally exclusive to decisions that the IT department makes in conjunction with Human Resources.

Any device or computer including, but not limited to, desk phones, smartphones, tablets, laptops, desktop computers, and iPads that the Company provides for your use, should only be used for Company business. Keep in mind that the Company owns the devices and the information in these devices. If the employee leaves the company for any reason, the Company will require that employee should return the equipment on last day of work.

6.2 Internet Usage

Internet use, on Company time, using company-owned devices that are connected to the Company network, is authorized to conduct Company business only. Internet use brings the possibility of breaches of the security of confidential Company information.

Internet use also creates the possibility of contamination to our system via viruses or spyware. Spyware allows unauthorized people, outside of the Company, potential access to Company passwords and other confidential information.

Removing such programs from the Company network requires IT staff to invest time and attention that is better devoted to making technological progress. For this reason, and to assure the use of work time appropriately for work, staff members have to limit internet use.

Additionally, under no circumstances may Company owned computers or other electronic equipment, including devices owned by the employee, be used on Company

time at work to obtain, view, or reach any pornographic, or otherwise immoral, unethical, or non-business-related internet sites. Doing so can lead to disciplinary action up to and including termination of employment.

6.3 Social Media

Employees have limit the use of social media to work-related content and outreach during work hours.

Additionally, employees are prohibited from sharing any confidential information or protected information that belongs to or is about the Company.

In social media participation from work devices or during working hours, social media content that discriminates against any age, race, colour, religion, gender, national origin, disability, or genetic information is prohibited.

Any employee, who participates in social media, who violates this policy will lead to disciplinary action.

6.4 Email Usage at the Company

Email is also to be used for Company business only. Company confidential information must not be shared outside of the Company, without authorization, at any time. Employees are also not to conduct personal business using the Company computer or email.

Please keep this in mind, also, as employee consider forwarding non-business emails to associates, family or friends. Non-business related emails waste company time and attention.

Keep in mind that the Company owns any communication sent via email or that is stored on company equipment. Management and other authorized staff have the right to access any material in your email or on your computer at any time. Please do not consider your electronic communication, storage or access to be private if it is created or stored on work systems.

If you need additional information about the meaning of any of this communication, please reach out to your manager or the CIO for clarification

Disclaimer

The following disclaimer will be added to each outgoing email:

Note: The information contained in this email and any attachments herein are for the sole use of the intended recipient(s) and may contain confidential and/or privileged information. If you are not the intended recipient (or have received this e-mail in error), please notify the sender and delete the message and/or material, immediately. Any unauthorized copying, disclosure or any other unauthorized use of the content of this e-mail, is strictly prohibited and may be unlawful.

7. RISK ASSESSMENT

Information security requirements shall be determined through a methodical assessment of risks. Executive management shall then balance the costs associated with implementing information security controls and mechanisms against the potential harm that could result from a security failure. When conducting risk assessments the following must be considered:

- *Harm to the business as a result of a security failure, considering potential consequences of a loss of confidentiality, integrity and/or availability of information or other assets.*
- *The likelihood of a failure occurring in light of existing threats and vulnerabilities, and the security controls and mechanisms implemented in the system environment.*

Periodic reviews of information security risks and the implemented controls and mechanisms will be conducted annually to:

- *Address changes to business requirements and priorities*
- *Consider new threats and vulnerabilities that might exist*
- *Confirm that security controls and mechanisms remain effective and efficient.*
- *Risks identified by a risk assessment must be mitigated or accepted prior to the system being placed into operation.*
- *Each Information System must have a system security plan, prepared using input from risk, security and vulnerability assessments.*

7.1 Responsibilities

1. *CIO is responsible for ensuring that the entire organization conducts Risk Assessment on Information System and uses the Finance approved process.*
2. *Information System Owners (ISOs) are responsible for ensuring that information systems under their control are assessed for risk and that identified risks are mitigated, transferred or accepted.*
3. *CIO is responsible for implementing systems and specifications to facilitate unit compliance with this policy.*

8. COMMUNICATION AND OPERATION MANGEMENT

8.1 Network Controls

Networks shall be adequately managed and controlled, in order to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit. Network security policy shall serve as a backbone in achieving it.

8.2 Security event logging and auditing

- *Audit logs recording user activities, exceptions (i.e., errors or failures), and information security events should be generated commensurate with the security requirements of the system being monitored. Audit logs should be retained for at least one year.*
- *Enterprise information systems must log system administrator activities, such as the use of privileged accounts (e.g., supervisor, administrator, or root).*
- *Audit logs should be periodically reviewed to detect security violations.*
- *Security event log data must be protected against unauthorized access and alteration.*
- *Clocks of systems being monitored should be synchronized regularly from an accurate time source.*

8.3 Agreements on Information Transfer

Where exchange of information and/or software between MMFL and a third party is necessary, a formal agreement shall be established in this regard.

8.4 Operational Procedures and Responsibilities

8.4.1 Documented Operating Procedures

IT Administrators will ensure operating procedures are used in all, day to day maintenance of the MMFL 's systems and infrastructure in order to ensure the highest possible service from these assets. IT Administrators will ensure these operating procedures are documented to an appropriate level of detail for the intended audience.

8.4.2 Change Management

IT Administrators will ensure all changes to the organizational operational systems are controlled with a formally documented change control procedure. The change control procedure should include references to:

- *A description of the change and business reasons.*

- *Information concerning the testing phase.*
- *Impact assessment including security, operations and risk.*
- *Formal approval process.*
- *Communication to all relevant people of the changes.*
- *Procedures for aborting and rolling back if problems occur.*
- *Process for tracking and audit.*

IT Department will ensure all significant changes to the main infrastructure (e.g. Network, Directories) are assessed for their impact on information security as part of the standard risk assessment.

8.5 Maker Checker Facility

Maker-checker is one of the central principles of authorisation in the information system. The principle of maker and checker means that for each transaction, there must be at least two individuals necessary for its completion. While one individual may create a transaction, the other individual should be involved in confirmation/authorization of the same. Here the segregation of duties plays an important role. In this way, strict control should be kept over system software and data, keeping in mind functional division of labour between all classes of employees in critical operations.

8.6 System Acceptance

1. *Users and IT Department must ensure any new information systems, product upgrades, patches and fixes undergo an appropriate level of testing prior to acceptance and release into the live environment. The acceptance criteria must be clearly identified, agreed and documented and should involve management authorization.*

2. *IT Department must ensure all major system upgrades are thoroughly tested in parallel with the existing system in a safe test environment that duplicates the operational system.*

8.7 Patching

1. *The IT Department will ensure all servers have appropriate critical security patches applied as soon as they become available and have passed the system acceptance testing. All other patches must be applied as appropriate. Patches must be applied to all software on the organization network where appropriate.*

2. The IT Department will adhere to the organization's Patch Management Procedure and keep a full record of which patches have been applied and when.

8.8 Controls against Malicious and Mobile Code

1. *Mobile code represents newer technologies often found in web pages and emails, and includes, but is not limited to:*

- *ActiveX.*
- *Java.*
- *JavaScript.*
- *VBScript.*
- *Macros.*
- *HTTPS.*
- *HTML.*

2. The IT Department will put in place appropriate access controls (e.g. administration / user rights) to prevent installation of software by all users in order to prevent malicious and mobile code.

3. The IT Department will ensure anti-malware software is installed on appropriate points on the network and on hosts.

8.9 Backup

8.9.1. Information Backup

- *The IT Department will ensure regular backups of essential business information are taken to ensure that the organization can recover from a disaster, media failure or error. An appropriate backup cycle will be used and fully documented. Any 3 rd. parties that store organization information must also be required to ensure that the information is backed up*
- *The IT Department will ensure full backup documentation, including a complete record of what has been backed up along with the recovery procedure, is stored at an off-site location in addition to the copy at the main site and be readily accessible. This will be accompanied by an appropriate set of media tapes and stored in a secure area. The remote location will be sufficiently remote to avoid being affected by any disaster that takes place at the main site.*
- *The IT Department will ensure appropriate arrangements must be put in place to ensure future availability of data that is required beyond the lifetime of the backup media.*
- *IT Department will ensure documented procedures are kept for backup tapes that are removed on a regular rotation from organization buildings. Media stores must be kept in a secure environment.*

8.10 Information Restore

The IT Department will ensure full documentation of the recovery procedure is created and stored. Regular restores of information from back up media will be tested to ensure the reliability of the backup media and restore process and this should comply with the agreed change management process.

8.11 Physical Storage Media in Transit

Users must ensure storage media being transported is protected from authorized access, misuse or corruption. Where couriers are required a list of reliable and trusted couriers should be established. If appropriate, physical controls such as encryption or special locked containers should also be used.

8.12 Security of System Documentation

System Administrators must ensure system documentation is protected from authorized access. Examples of the documentation to be protected include, but are not restricted to, descriptions of:

- *Applications.*
- *Processes.*
- *Procedures.*
- *Data structures.*
- *Authorization details*

Effective version control should be applied to all documentation and documentation storage.

8.13 Monitoring

8.13.1 Audit Logging for Restricted Data

The IT Department will ensure audit logs are kept for a minimum of one year which record exceptions and other security related events. As a minimum audit logs must contain the following information:

- *System identity.*
- *User ID.*
- *Successful/Unsuccessful login.*
- *Successful/Unsuccessful logoff.*
- *Unauthorised application access.*

- *Changes to system configurations.*
- *Use of privileged accounts (e.g. account management, policy changes, device configuration).*

The IT Department will ensure access to the logs is protected from unauthorised access that could result in recorded information being altered or deleted. System Administrators will be prevented from erasing or deactivating logs of their own activity.

8.14 Administrator and Operator Logs

The IT Department and System Administrators must maintain a log of the systems activities. The logs should include:

- *Back-up timings and details of exchange of backup tapes.*
- *System event start and finish times and who was involved.*
- *System errors (what, date, time) and corrective action taken.*

The logs should be checked regularly to ensure that the correct procedures are being followed.

8.15 Clock Synchronisation

The IT Department will ensure all computer clocks are synchronised to the GSI time source to ensure the accuracy of all the systems audit logs as they may be needed for incident investigation.

8.16 Network Management

8.16.1 Network Controls

The IT Department will ensure connections to the organization's network infrastructure are made in a controlled manner. Network management is critical to the provision of business and must apply the following controls:

- *Operational responsibility for networks should, where possible be separate from computer operations activities.*
- *There must be clear responsibilities and procedures for the management of remote equipment and users (please refer to the Remote Working Policy and Removable Media Policy.*
- *Where appropriate, controls must be put in place to protect data passing over the network (e.g. encryption).*

The IT Department will ensure the network architecture is documented and stored with configuration settings of all the hardware and software components that make up the network. All components of the network should be recorded in an asset register.

The IT Department will ensure all hosts must be security hardened to an appropriate level. Operating systems will have their network services reviewed, and those services that are not required will be disabled.

8.17 Wireless Networks

The IT Department will ensure wireless networks apply controls to protect data passing over the network and prevent unauthorised access and that encryption is used on the network to prevent information being intercepted. WPA2 should be applied as a minimum.

8.18 Annual Health Check

The CIO will ensure an annual health check of the organization infrastructure systems and facilities is undertaken every 12 months. This health check must include, but is not restricted to, the following:

- *A full penetration test.*
- *A network summary that will identify all IP addressable devices.*
- *Network analysis, including exploitable switches and gateways.*
- *Vulnerability analysis, including patch levels, poor passwords and services used.*
- *Exploitation analysis.*
- *A summary report with recommendations for improvement.*

9. INFORMATION SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE

MMFL shall comply with security requirements while procuring, acquiring, and developing and maintaining new information system.

The policy ensure that security is an integral part of Information Systems throughout all phases of the acquisition, development, and maintenance lifecycle. Security must be considered at every stage of an information system's life cycle (e.g. feasibility, planning, development, implementation, maintenance, retirement and disposal) in order to:

- *Ensure conformance with all appropriate security requirements*
- *Protect enterprise data throughout its life cycle*
- *Facilitate efficient implementation of security controls*
- *Prevent the introduction of new risks when the system is modified*
- *Ensure proper removal of data when the system is retired*

9.1 MIS Reports

Management Information System generated reports for Top Management summarising financial position including operating and non-operating revenues and expenses, cost benefit analysis of segments/verticals, cost of funds, should be included in the application software. Details to file regulatory returns to RBI (COSMOS Returns) should be included in the MIS.

9.2 Capacity Management:

- *The use of information resources shall be planned, prepared, and monitored, and projections shall be made of future capacity requirements to ensure adequate performance.*
- *Procedures shall be developed to respond to audit log storage capacity issues according to the Audit Logging and Monitoring policy.*

9.3 Change Control Management

System changes shall be controlled and monitored by the IT department. After all system changes, it should be reviewed and tested to ensure that there are no adverse effects on organizational operations or security.

9.4 Business Requirements for New Information Systems:

- *Statements of business requirements for new information systems (developed or purchased), or enhancements to existing information systems, shall specify requirements for security controls.*
- *In acquiring new information systems and/or contracting with new vendors, will ensure that the systems/entities are of high reputation and at least*

similar calibre to the current health information exchange vendors and that all such relationships comply with the terms of the ITSE Policies and Policies.

- *Security controls in business requirements shall include:*

  - *Consideration of business value and legal-regulatory-certificatory standards for information assets affected by the new/changed system.*

  - *Consideration of administrative, technical, and physical controls available to support security for the information system.*

  - *Integration of security controls early in requirements specification and system design.*

9.5 Control of Internal Processing:

- *Validation checks shall be incorporated into applications to detect any corruption of information through processing errors or deliberate acts.*

- *MMFL shall define integrity controls and develop a validation checklist.*

9.6 Output Data Validation:

- *Data output from applications and databases shall be validated to ensure that the processing of stored information is correct and appropriate. Both automatic and manual methods of output data validation testing shall be used as appropriate.*

9.7 Control of Production Software:

- *MMFL shall implement procedures to control the installation of software on production/operating systems to minimize the risk of interruptions to, or corruption of those systems.*

- *To minimize the risk of corruption to operational systems, the following procedures shall be implemented:*

  - Only authorized System Administrators shall be allowed to implement approved upgrades to software, applications and program libraries

  - Production systems shall only hold approved programs or executable code (i.e., no development code or compilers).

- *Third party software used in production systems shall be maintained at a level supported by the vendor.*

- *If systems in production are no longer supported by the vendor, MMFL must provide evidence of a formal migration plan and obtain ITSE approval to implement the plan.*

- *Applications and production/operating systems shall be tested for usability, security, and impact prior to release in production.*

- *Production software must comply with the Change Management Policy*

- *Physical or logical access shall be given to a third party for support purposes only when necessary, and only with senior leadership approval. The vendor's activities shall be monitored.*

9.8 Access Control to Program Source Code:

- *Access to program source code and associated items (e.g., designs, specifications, verification plans, validation plans, etc.) shall be strictly controlled, in order to prevent the introduction of unauthorized functionality and to avoid unintentional changes.*

9.9 Outsourced Software Development:

- *The development of software by third parties shall be done under the supervision of ITSE.*
- *The development of software by third parties shall be governed by a contract or a Service Level Agreement (SLA) that includes security requirements.*
- *Independent security and code reviews shall be conducted by an individual with certified security training before bringing new services into production.*

9.10 E-commerce applications

E-commerce applications must be supported based on a flexible, scalable architecture, typically consisting of:

- *Front-end web servers*
- *Mid-tier applications servers*
- *Back-end database servers and back-office servers*

All electronic trading facilities provided to investors and other third parties must use secure session protocols such as SSL to encrypt sessions between browsers and web server to prevent sensitive data (e.g. account details) being intercepted. Strong encryption to protect sensitive data (personal information, credit card details) stored on servers or other systems that might be vulnerable to external access.

No confidential investor information may be stored directly on web servers. Web servers must be physically separate from database servers, and must reside on separate network segments.

All communication between web servers and other components of electronic trading systems must be subjected to firewall mediation and IDS/IPS inspection

9.11 Roles and Responsibilities

ITSE Ensures the application of appropriate operational security controls for an information system; coordinates in the identification, implementation, and assessment of common security controls; plays an active role in developing and updating a system security plan and coordinating with an information system owner any changes to the system and assessing the security impact of those changes. This role may be filled by someone directly involved with the development, maintenance, and/or operation of the information system.

10. BUSINESS CONTINUITY MANAGEMENT

A business continuity management process shall be implemented by MMFL to reduce the disruption caused by disaster and security failures to an acceptable level through a combination of preventive and recovery controls.

This Business Continuity Policy must be observed across the MMFL.

10.1 Business continuity management process

Business Continuity management process shall be developed and shall address the information security requirements for business continuity. ITSE has the responsibility of business continuity management. Managed process should be in place for developing and maintaining business continuity throughout MMFL .

10.2 Business continuity Risk assessment and Development

The events that can cause interruptions to business processes shall be pre identified and shall be followed by a risk assessment to determine the impact of interruptions. Plans shall be developed to maintain or restore operations in the required time scale.

10.3 Plan Maintenance

Business Continuity plans should be tested regularly to ensure that they are up to date and effective. Business continuity plans should be maintained by regular reviews and updates to ensure their continuing effectiveness.

10.4 Principles and Commitments

The Business Continuity Policy shall be based on the following principles and commitments:

1. *The protection and safety of people shall be the first premise and ultimate objective of this Policy, both under normal circumstances and during a crisis resulting from a disaster.*

2. *The designation of representatives in the various areas with appropriate experience and knowledge to actively participate in the preparation, implementation, review, verification and amendment of the Business Continuity Plans.*

3. *The development and implementation of Business Continuity Plans by MMFL, taking into account the internal areas and departments, suppliers and services and using adequate and proportionate systems, resource and procedures.*

4. *The maximisation of the synergies generated through the development and implementation of the Business Continuity Plans in the organization, taking into consideration MMFL common means and resources.*

5. *The adoption of reasonable measures to ensure the operational continuity of processes and activities, based on their criticality as established by the Organization.*

6. *The inclusion of safety and reliability criteria which reasonably ensure the continuity of the critical services provided by third parties, should said services be outsourced.*

7. *The preparation, within the Business Continuity Plans, of appropriate communication procedures, both internal and external, which ensure their correct execution and timely delivery of information to all the interested parties.*

8. *The communication to all the employees of their responsibilities and the procedures that may affect them, within the business continuity framework and through dissemination and training activities.*

9. *The development of a Business Continuity Management System which includes reviews, verifications and amendments of the Business Continuity Plans, either on a regular basis or when significant changes arise, with the aim of continuously improving them.*

10. *The constant willingness to cooperate with the authorities in case of disaster or need, as part of the spirit of service that inspires all MMFL activities and its responsibility towards the business in which it operates.*

10.5 Responsibilities

ITSE shall be responsible for promoting the development and implementation of the Business Continuity Plans of the MMFL, establishing and coordinating business continuity activities, while ensuring the enforcement, dissemination and periodic revision of this Policy.

ITSE shall assume the executive direction and management of those crises resulting from a disaster, which have a multi-entity impact, require extraordinary economic investments or may significantly affect the reputation of the MMFL.

11. IT SERVICE OUTSOURCING

The purpose of this policy that is required to be implemented by MMFL is to establish a comprehensive risk management programme to address the outsourced activities and the relationship with Service Provider. The key purposes of the policy are:

- *To conduct due diligence of the Service Provider to ascertain the credibility and capability of the Service Provider.*
- *To maintain confidentiality of the information that is outsourced.*
- *To ensure compliance with the laws and regulations in force from time to time.*
- *To protect the Company reputation.*
- *To conduct outsourcing of activities in accordance with this policy.*
- *To identify the supervisors and fix their responsibilities.*

11.1 BUSINESS CASE

MMFL will prepare a business case for all new or renegotiated outsourcing arrangements. The business case should include the following information/considerations to allow the Board to make an informed decision on the merits of the proposal.

- Possible efficiency gains by outsourcing the activity
- Clearly defined likely benefits and likely risks
- Possible scenario/s if the activity is not outsourced
- Mechanism in place in MMFL for monitoring the outsourcing arrangements.
- How the proposed outsourcing arrangement aligns with the MMFL's organizational and/or strategic goals.

11.2 ACTIVITIES NOT TO BE OUTSOURCED

Company shall not outsource its core business activities and compliance functions. Core Business activities such as:

- *Loan Management System and monitoring of business activities of*
- *Digitization and conversion of information data*
- *Investment related activities*
- *Know Your Client (KYC) related activities*

An activity shall not be outsourced if it would impair the Board's right to assess, or its ability to supervise, the business of MMFL

Selection of Third Party

The ITSE Coordinator shall exercise due care, skill and diligence in the selection of the third party in order to ensure that the third party has the ability and capacity to undertake the provision of services effectively. The due diligence shall include assessment of:

- *Third Party's resources and capabilities, including financial soundness, to perform the outsourcing work within the timelines fixed*
- *Compatibility of the practices and systems of the Third Party with the intermediary's requirements and objectives*
- *Market feedback of the prospective Third Party business reputation and track record of their services rendered in the past*
- *Level of concentration of the outsourced arrangements with a single Third Party*
- *The environment of the foreign country where the Third Party is located.*

11.3 Tender and procurement processes

- MMFL will conduct a tender (or similar competitive procurement process) for each planned IT Services outsourcing arrangement.
- MMFL will instruct service providers to submit tenders or expressions of interest that are logical, clearly articulated, comprehensive, and demonstrate value for money by responding to criteria set by the MMFL. Such proposals would then be evaluated by the MMFL, considering factors such as:
  - The performance history of each prospective supplier
  - The relative risk of each proposal
  - The flexibility to adapt to possible change over the lifecycle of the property or service
  - Financial considerations including all relevant direct and indirect benefits and costs over the whole service cycle
  - The evaluation of contract options (for example, contract extension options).
- MMFL's IT Head will provide recommendations to the Board of the MMFL as to the preferred provider and the methodology (including execution of a due diligence assessment) used to determine this. This may include:
  - Confirming the credentials of the service provider and its key staff
  - Confirming the financial position of the service provider
  - Obtaining any bank or corporate guarantees required under the contract
  - Viewing and recording any required documentation, e.g. insurance policies
  - Identifying and resolving any intellectual property arrangements
  - Reviewing the physical or intellectual property assets promised by the service

provider for the delivery of the service

- Conducting a final review of the impact of ordinances/regulations, policies and administrative arrangements relating to the service
- Reviewing the service provider's proposed approach to carrying out the procedures including any technical or operational documentation, if necessary
- Reviewing the service provider's procedures on ethical business practice, and confirm the existence and quality of its company code of ethics and staff code of conduct. For example, the codes should cover declarations and avoidance of conflict of interest; and non-disclosure of confidential information.
- Reviewing any taxation or regulatory matters that may be applicable.

- MMFL will enter into a legally binding contract with the successful tenderer/supplier that includes a clause providing RBI with access to the service provider's records and information in relation to MMFL.

11.4 Periodic Risk Assessment, Audit and Reviews

- MMFL will conduct a risk assessment for every outsourced material business activity, develop and implement appropriate risk controls that address any risks identified in the risk assessment, and regularly report to the Board on the status of the risks that have been identified and the effectiveness of the risk controls that have been developed and implemented.
- MMFL will incorporate any outsourcing risks into the MMFL's risk profile.
- MMFL will also have procedures to ensure that all its relevant business units are fully aware of, and comply with, the outsourcing policy and any risk controls that are developed and implemented as a result of a risk assessment.
- MMFL will at least on an annual basis, review the financial and operational condition of the service provider to assess its ability to continue to meet outsourcing obligations.
- MMFL will periodically commission independent audit and expert assessments on the security and control environment of the service provider. Such assessments and reports on the service provider may be performed and prepared by the MMFL's internal or external auditors, or by agents appointed by MMFL.
- MMFL will share the copies of previous audits and assessments of outsourcing service providers to RBI auditors or auditors authorized by RBI during inspection by RBI.

11.5 REPORTING TO REGUALATORS

- MMFL will report to the regulator/RBI, where the scale and nature of functions outsourced are significant, or extensive data sharing is involved across geographic locations as part of technology/process outsourcing and when data pertaining to Indian operations are stored/processed abroad.

11.6 Outsourcing Contracts

All outsourcing arrangements shall be executed only by way of a clearly defined and legally binding written contact with each of the Service Provider.

Care shall be taken to ensure that the outsourcing contract:

a) clearly defines what activities are going to be outsourced, including appropriate service and performance levels;

b) provides for mutual rights, obligations and responsibilities of the Company and the Service Provider, including indemnity by the parties;

c) provides for the liability of the Service Provider to the Company for unsatisfactory performance/other breach of the contract

d) provides for the continuous monitoring and assessment by the Company of the Service Provider so that any necessary corrective measures can be taken up immediately, i.e., the contract shall enable the Company to retain an appropriate level of control over the outsourcing and the right to intervene with appropriate measures to meet legal and regulatory obligations;

e) includes, where necessary, conditions of sub-contracting by the Service Provider, i.e. the contract shall enable Company to maintain a similar control over the risks when a Service Provider outsources to further third parties as in the original direct outsourcing;

f) has unambiguous confidentiality clauses to ensure protection of proprietary and customer data during the tenure of the contract and also after the expiry of the contract;

g) specifies the responsibilities of the Service Provider with respect to the IT security and contingency plans, insurance cover, business continuity and disaster recovery plans, force majeure clause, etc.;

h) provides for preservation of the documents and data by Service Provider;

I) provides for the mechanisms to resolve disputes arising from implementation of the outsourcing contract;

j) provides for termination of the contract, termination rights, transfer of information and exit strategies;

k) addresses additional issues arising from country risks and potential obstacles in exercising oversight and management of the arrangements when Company outsources its activities to foreign Service Provider.

l) *neither prevents nor impedes the Company from meeting its respective regulatory obligations, nor the regulator from exercising its regulatory powers; and*

m) *provides for the Company and /or the regulator or the persons authorized by it to have the ability to inspect, access all books, records and information relevant to the outsourced activity with the Service Provider.*

11.7 Disaster Recovery Plan

a) *Specific contingency plans shall be separately developed for each outsourcing arrangement, as is done in individual business lines.*

b) *The ITSE shall take appropriate steps to assess and address the potential consequence of a business disruption or other problems at the Service Provider level. Notably, it shall consider contingency plans at the Service Provider level; co-ordination of contingency plans at both levels and in the event of non-performance by the Service Provider.*

c) *The ITSE shall ensure that the Service Provider maintains appropriate IT security and robust disaster recovery capabilities.*

4. Periodic tests of the critical security procedures and systems and review of the backup facilities shall be undertaken by the Company to confirm the adequacy of the Service Provider's systems.

11.8 Client Confidentiality

a) *The Company is expected to take appropriate steps to protect its proprietary and confidential customer information and ensure that it is not misused or misappropriated.*

b) *The Company shall prevail upon the Service Provider to ensure that the employees of the Service Provider have limited access to the data handled and only on a "need to know" basis and the Service Provider shall have adequate checks and balances to ensure the same.*

c) *In cases where the Service Provider is providing similar services to multiple entities, the Company shall ensure that adequate care is taken by the Service Provider to build safeguards for data security and confidentiality.*

11.9 Maintenance of Records

a) *The records relating to all activities outsourced shall be preserved centrally so that the same is readily accessible for review by the Board of the Company and / or ITSE, as and when needed.*

b) *Such records shall be regularly updated and may also form part of ITSE review by the management of the Company.*

11.10 Review

a) Regular reviews by internal or external auditors of the outsourcing policies, risk management system and requirements of the regulator shall be mandated by the Board wherever felt necessary.

c) Company shall review the financial and operational capabilities of the third party in order to assess its ability to continue to meet its outsourcing obligations.

12. CRYPTOGRAPHY

MMFL Data Security and the associated Data Handling Procedures establish requirements for the use of encryption techniques to protect sensitive data both at rest and in transit. Cryptographic controls can be used to achieve different information security objectives:

- Confidentiality: using encryption of information to protect sensitive or critical information, either stored or transmitted
- Integrity/authenticity: using digital signature certificates or message authentication codes to verify authenticity or integrity of stored or transmitted sensitive or critical information
- Non-repudiation: using cryptographic techniques to provide evidence of the occurrence of an event or action
- Authentication: using cryptographic techniques to authenticate users and other system entities requesting access or transacting with system users, entities and resources

12.1 Encryption methods for data in motion

The Data Handling Procedures require the transfer of sensitive data through a secure channel. A secure channel is an encrypted network connection.

Various methods of encryption are available and generally built-in to the application. The user should be aware of the data connection being used to transmit sensitive data and if encryption is enabled for that connection.

12.2 Encryption is required for:

The transport of sensitive files (secure FTP, SCP, or VPN usage to encrypt sensitive data for network file access of unencrypted files).

Access to sensitive data via a web site, web application or mobile app. Encryption is required for accessing sensitive data from anything with a web interface, including mobile devices (i.e. use of HTTPS to encrypt sensitive data).

All network traffic for remote access to the virtual desktop environment.

Transport of sensitive data that is part of a database query or web service call (examples SQL query to retrieve or send data from database or a RESTful web service call to retrieve or send data from a cloud application).

Privileged access to network or server equipment for system management purposes.

12.3 Encryption of Email

The Data Handling Procedures require that when emailing some sensitive data the message and attachments be encrypted.

12.4 Use of digital signature certificates

Digital signature certificates are a way to guarantee the authenticity and integrity of an Email message or document.

Users may use a digital signature certificate to digitally sign Email messages.

Users may use a digital signature certificate to digitally sign some types of documents or forms.

12.5 Use and management of SSH keys

Refer to the Standards for the Use of SSH Keys document for guidance on when and how to utilize SSH keys.

12.6 Use and management of SSL digital certificates

WCU web servers (or devices with a web interface) that support secure (HTTPS) connections must have a SSL certificate installed.

.

13. HUMAN RESOURCE

The purpose of this Policy is to ensure that the MMFL and its employees, contractors and third-party users:

- *understand their responsibilities and are suitable for their Roles, in order to reduce the risk of theft, fraud or misuse of Information and Information Technology Assets;*
- *are aware of Information Security threats and concerns and liabilities and are equipped to support Information Security in the course of their normal work in order to reduce the Risk of human error; and*
- *Understand their responsibilities so that employees, contractors, and third party users may exit the MMFL or change employment in an orderly manner.*

13.1 Prior to Employment

13.1.1) A pre-employment screening process must be undertaken by the organization prior to offering employment, to a new employee. Checks must include at least the following:

- *Identity checks (driver's license, passport, bank account in the same name as the employee, etc.)*
- *Reference checks*
- *Confirmation of academic or professional qualifications as appropriate*
- *Criminal records checks for senior positions*

13.1.2) If the employee is being hired through a third party or staffing agency, screening checks in line with those stated above must be implemented by that agency.

13.1.3) Information gathered on potential employees must be secured by all applicable laws and regulations. Access must be limited to 'need to know' basis.

13.1.4) All staff must agree to comply with MMFL IT Security Policy and Standards prior to being granted access to MMFL Information, Communication and Technology systems. Also, staff may be required to sign a Non-Disclosure Agreement if their role requires access to sensitive information.

13.2 During Employment / Enrolment

MMFLIT must create and deliver a security awareness program promoting the importance of security to all employees and students.

The information security awareness program must be created in two distinct parts:

- *General information security awareness.*
- *Information security policy and standards awareness.*

Records of awareness campaigns must be kept detailing the type of information security awareness delivered.

Non-compliance with the IT Security Policy and Standards may result in disciplinary action, consistent with the MMFL disciplinary processes and procedures.

13.3 Termination or Change of Employment

The concerned department / branch manager must immediately notify the MMFLHR Department via an appropriate process upon the resignation or termination of any employee.

Access rights of employees are appropriately modified upon change or termination of employment according to the User Access Management Standard of INFORMATION TECHNOLOGY Policy.

User access rights are reviewed whenever an employee changes roles within the organization. Management is accountable for the review. The review includes cancelling access rights that are no longer needed unless it has been explicitly authorized by the information system owner or authorised delegates.

Upon termination of employment, the employee's access rights must be removed from all systems. All IT assets such as Hardware, keys, ID and physical access cards, software, data, and documentation, manuals must be returned to the concerned Department Head/Branch Head/IT Department.

Managers are responsible for returning all IT assets to MMFL.

It is the policy of the company to ensure that all users joining, moving within or leaving the organization network are properly accounted for and correctly managed in their use of the organization network. Company will not condone the use of any user credentials for anything other than their intended purpose.

It is the responsibility of all employees, consultants, temporary or contract workers to read, fully understand and signify agreement to the MMFL.

13.4 External Users

Users from Partner / Associate organizations, or external consultants brought in for specific purposes, who require direct access to organization systems and information must request user credentials in the same manner as permanent employees via the concerned department/branch manager. Where such access is via a secure login through a purposeful Extranet the user request is to be annotated to reflect this purpose. Once credentials have been granted the remainder of this policy applies.

14. CAPACITY MANAGEMENT

This Policy give guidance on capacity management for the company. It is particularly intended to help and guide those involved in managing business processes or capacity of technology resources and help them understand their responsibilities and obligations according to policy.

Future capacity needs are projected by business area management at least annually and communicated to personnel or agencies responsible for managing and maintaining information technology resources that provide the enabling infrastructure. Significant changes in capacity requirements have budgetary implications.

14.1 Area of Concern

The primary area of concern is the potential for interruption or degradation to the delivery of services. Weaknesses in capacity management processes may reduce the availability services reliant upon information resources.

Many factors amplify these concerns:

- *Business requirements for normal business conditions, maximum capacity, peak demand and failover conditions may be incorrectly estimated.*
- *Specifications for new or enhanced services may contain incomplete or inaccurate capacity requirements.*
- *Implementation of new or significantly enhanced information systems may not have included appropriate capacity testing.*
- *Increased capacity may require acquisition of additional hardware and associated software licenses.*
- *Service Level Agreements may have to be revised when capacity requirements change.*

- *Inadequate capacity may lead to operational interruptions, loss of productivity and a potential loss of information.*
- *Unplanned and unbudgeted capacity requirements may have financial and availability implications.*
- *Monitoring of capacity utilization may be inadequate.*
- *Performance tuning to ensure efficient capacity utilization may be inadequate.*
- *Disaster recovery requirements may not be updated concurrent with changes to system capacity.*

14.2 Intended Outcomes

The policies associated with capacity management are intended to:

- *Ensure the availability and integrity of the information technology infrastructure.*
- *Ensure that the capacity of information technology resources meets current and future business needs.*
- *Ensure that the availability and performance of information resources is maintained at agreed service levels.*
- *Ensure processes for managing capacity utilization and performance are implemented.*

14.3 Responsibilities of CIO

14.3.1 Things to do:

- *Use established processes for estimating and monitoring capacity requirements.*
- *Include capacity requirements in specifications for new or enhanced information systems.*
- *Initiate revisions to Disaster Recovery Plans when capacity requirements change.*
- *Ensure that capacity management testing is done for normal and peak utilization periods.*

14.3.2 Things to avoid:

- *Implementing new or significant changes to information systems prior to completion of capacity tests.*

14.3.3 Things to report:

- *Unexplained degradation or outage of service.*
- *Actual and suspected security incidents and events as required by the Information Incident Management Process.*
- *File a General Incident or Loss Report (GILR) within 24 hours of a security incident.*

14.4 Responsibilities of IT Department

14.4.1 Things to do:

- *Ensure that the Service Level Agreements define capacity requirements.*
- *Ensure capacity requirements are planned, defined, tested and managed throughout the life cycle of information technology resources.*
- *Ensure that capacity is tested during system acceptance.*
- *Ensure Disaster Recovery Plans are updated and tested.*
- *When a security or privacy breach has occurred, review and revise related policies and processes as needed.*

14.4.2 Things to pay attention to:

a. Unanticipated changes to capacity requirements.

Things to establish procedures for:

b. Reviewing and projecting capacity requirements prior to the annual budget cycle.

Things to report:

c. Unexplained degradation or outage of service.

Things to reinforce with personnel:

d. The importance of managing capacity.

e. The importance of understanding and following policies, standards and processes.

f. Ensure the use of the Information Incident Management Process when required.

15. INCIDENT MANAGEMENT

Incident response process must be documented. Incident response plan must be tested for effectiveness through appropriate means such as simulation exercises.

15.1 Information security incidents reporting.

Information security incident management process shall be developed, which shall address the information security requirements. Any event related to information security shall be reported and available for further analysis.

Employees shall report all security weaknesses and software malfunction to IT department.

All employees and customers should be aware of the procedures of reporting the incidents like security breach, threat weaknesses or malfunction that might have an impact on the information security.

15.2 Investigation

Information Technology department should conduct thorough investigations into the root cause of each security incident to:

- *Reprimand, discipline or prosecute those responsible*
- *Update existing security controls or to introduce new ones to prevent a recurrence of the same incident*

15.3 Review

Incident response plans and procedures must be reviewed on annual basis.

16. PHYSICAL AND ENVIRONMENTAL CONTROL

Physical access to information technology processing equipment, media storage areas, and media storage devices and supporting infrastructure (communications, power, and environmental) must be controlled to prevent, detect, and minimize the effects of unauthorized or unintended access to these areas.

MMFL Branches / Departments are required to establish physical and environmental controls for assets under their physical control. Requirements within this policy extend to self-contained facilities such as external data centres, as feasible, and should be considered prior to entering into a contract with an external data centre, workplace, or facility. In conjunction with the Asset Management Policy, physical and environmental controls must follow the minimum requirements established within this policy.

16.1 Physical and Access Controls

Physical and access controls within the organization including branches and department systems will follow the requirements outlined below.

Sl.#	Control	Description
1	Policy and Standards	Develop, document, and disseminate formal physical and environmental protection standards that set criteria for: purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.
2	Physical Access Authorizations and Maintenance	1. Develop and maintain a list of personnel authorized to enter controlled access facilities where information systems reside, and identify those areas in a facility which are designated publicly accessible

		2. Manage the list and all associated logs of access, including: ● *Track names and status of all who have been issued authorized credentials for facility access* ● *Identify and implement regulatory and policy log-retention requirements* ● *Regularly audit the detailed access log(s) of facility* ● *Regularly review the access list, and promptly remove individuals from the facility access list when access is no longer required*
3	*Physical Access Control*	*Enforce physical access controls for all physical access points to the controlled facility. This includes:* ● *Verify individual authorization before granting access* ● *Control entry to the facility using physical access devices and/or guards* ● *Maintain physical-access audit logs* ● *Provide additional controls:* ➢ *Escort visitors and monitor visitor activity* ➢ *Secure keys, combinations, and other physical access devices* ➢ *Inventory physical-access devices annually* ➢ *Conduct routine maintenance checks to verify that devices are functioning properly* ➢ *Change combinations and keys annually or when keys are lost, combinations are compromised, or individuals are transferred or terminated* ➢ *Deactivate or revoke user access credentials upon transfer or termination*
4	*Access Control for Transmission Medium*	*Control physical access to system distribution and transmission lines, for example: (I) lock wiring closets, (ii) disconnect or lock spare jacks; or (iii) protect cabling by conduit or cable trays.*
5	*Access Control for*	*Control physical access to information system output devices to prevent unauthorized*

	Output Devices	*individuals from obtaining the output.*
6	*Monitoring Physical Access*	*Monitor physical access to the controlled facility to detect and respond to physical security incidents, including:* ● *Review physical access logs every 30 days and upon the occurrence of any known physical-access violation* ● *Coordinate the results of the reviews with the departments/branches incident response entity*
7	*Access Records*	● *Maintain visitor-access logs for controlled facilities per the department / branch retention guidelines, and ensure the logs are reviewed regularly.* ● *For information systems designated as High automated mechanisms should be established to facilitate the maintenance and review of visitor-access logs.*

16.2 Environmental Controls

Environmental Controls within MMFL will follow the requirements outlined below.

Sl.#	***Control***	***Description***
1	*Power Equipment and Power Cabling*	*Protect power equipment and power cabling for information assets from damage and destruction.*
2	*Emergency Shutoff*	● *Provide the capability to shut off power to information systems in a facility or individual system components in emergency situations* ● *Place shut-off switches or devices in a defined location to facilitate safe and easy access for personnel, while protecting emergency power shutoff capability from unauthorized activation*
3	*Emergency Power*	● *Provide a short-term uninterruptible power supply (UPS) to utilize if the primary power source fails.* ● *Information systems with a designation of High should be provided with a long-term alternate power supply that can maintain minimum operational capability in the event of an extended loss of the primary power source.*

4	*Emergency Lighting*	● *Employ and maintain automatic emergency lighting for the information systems that activates in the event of a power outage or disruption* ● *Lighting should be provided for emergency exits and evacuation routes within the facility*
5	*Fire Protection*	*Employ and maintain fire suppression and detection devices or systems for the information systems that are supported by an independent energy source such as UPS.* ◆ *Moderate:* ➢ *Employ an automatic fire suppression capability for the information system when the facility is not staffed on a continuous basis* ◆ *High:* ➢ *Employ fire detection devices and systems that activate automatically and notify emergency responders* ➢ *Employ fire suppression devices and systems that activate automatically and notify emergency responders* ➢ *Employ an automatic fire suppression capability for the information system when the facility is not staffed on a continuous basis*
6	*Temperature and Humidity Controls*	*Maintain temperature and humidity levels at operational levels within the facility where the information systems reside, and continuously monitor temperature and humidity levels.*
7	*Water Damage Protection*	*Protect information systems from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel*
8	*Delivery and Removal*	*Authorize, monitor, and control equipment deliveries, moves, and removals from the facility, and maintain records of those moves.*
9	*Alternate Worksite*	*At alternate work sites, employ IT controls, such as a logical and physical access controls, as necessary.*
10	*Location of Information Asset*	*Position information system components within the facility to minimize potential damage from*

	Components	*physical and environmental hazards and to minimize the opportunity for unauthorized access.*
11	*Annual Testing*	*Test environmental systems and emergency sources at least annually to ensure continuous protections are in place.*

17. COMPLIANCE

This policy will enforce the legal requirements that shall be considered to design, operate, use and management of information systems and to abide statutory, regulatory and contractual security requirements.

17.1 Compliance with Legal Requirement

Company shall identity and analyse external regulatory requirements for their impact on its IT function, and take appropriate measures to comply with them.

The following areas shall be covered:

- *Regulators including RBI and other governing body authorities guidelines, especially relating to business trading, e-commerce, information security etc.*
- *Relevant government and/or external requirements (i.e., laws, legislation, guidelines, regulations and standards) pertaining to external relationships and external requirements reviews*
- *Labour laws, especially addressing IT related safety and health (including ergonomics) requirements*
- *Compliance issues relating to IT*
- *Privacy issues especially pertaining to customer related information*
- *Intellectual property rights / software copyright laws*
- *Information systems security requirements, especially relating to use of cryptographic data, and transmission of data*
- *Relevant 'accounting standards/ pronouncements' relating to electronic commerce*

17.2 Identification of applicable legislation

All relevant statutory, regulatory, contractual requirements and responsibilities to meet them shall be defined and documented. Monitoring of local legislation and regulations affecting the company's operations should be done by compliance department.

17.3 Intellectual Property Rights (IPR)

Intellectual property rights such as copyright, design rights, trademarks shall be abide. Non licensed copy of product should not be used. Strong disciplinary action should be taken against any person engaged in the unauthorized copying of software. In addition, any penalties imposed on the company as a result of the breach should be passed on the offending individual.

17.4 Software Copyright

Software products shall be used as per the terms and conditions in license agreement. Proprietary software products are usually supplied under a license agreement that limits the use of the product to specified machines and may limit copying to the creation of back-up copies only. All software used within the company should be purchased and issued in accordance with the license agreements. The company will take strong disciplinary action against any person found to be engaging in the unauthorized copying of software.

17.5 Personal Information

Compliance with local legislation governing the protection of personal information in the jurisdictions covered by the e-commerce application should be identified and followed and must ensure that any personal information collected about investors is used only in ways associated with the company business.

Customer log-on credentials and transactional data traversing public networks must be encrypted by means of commercial grade encryption i.e. at least 128-bit SSL type encryption or equivalent standard.

17.6 Protection of Organizational Records

Important records of the company shall be protected from loss, destruction and falsification. Records may need to be securely retained to meet statutory or regulatory requirements, as well as to support essential business activities. Media used for storage of records should be secured from degradation and should have clear identification of their statutory or regulatory retention period.

17.7 Data protection and privacy of personal information

Company shall determine the applicable regulations and implement appropriate controls for each applicable jurisdiction to reasonably protect the privacy of personal information.

Compliance with data protection legislation requires appropriate management structure and control to ensure the privacy and confidentiality of investor's related information.

18. IS AUDIT POLICY

Purpose of this audit policy is to provide the guidelines to security audit team to conduct a security audit on IT based infrastructure system at various departments of Delhi Govt. Security Audit is done to protect entire system from the most common security threats which includes the following:

- *Access to confidential data*
- *Unauthorized access of the department computers*
- *Password disclosure compromise*
- *Virus infections.*
- *Denial of service attacks*
- *Open ports, which may be accessed from outsiders (Unrestricted modems unnecessarily open ports)*
- *Audits may be conducted to:*
- *Ensure integrity, confidentiality and availability of information and resources*
- *Monitor all security measures to ensure conformance with Delhi Govt. security policies*
- *Investigate security incidents recorded in incident register*

18.1. Responsibility

Audit Policy It is the responsibility CIO to place an appropriate system of internal audit, which provides an independent assessment of security policies. To execute these policies, internal audit should also be done and

reports/documents based on these audit should be generated. The system administrator or the nodal officer will be responsible for internal Audit within the department and operations of their sub dept.

When requested and for the purpose of performing an audit, any access needed will be provided to members of External Audit team. This access may include:

- *User level and/or system level access to any computing or communications device*
- *Access to information (electronic, hardcopy, etc.) that may be produced, transmitted or stored on respective Dept. equipment or premises*
- *Access to work areas (labs, offices, cubicles, storage areas, etc.)*
- *Access to reports / documents created during internal audit.*
- *Access to interactively monitor and log traffic on networks*