

**MUSCCO LIMITED**

**INFORMATION TECHNOLOGY POLICY**

|  |  |  |
| --- | --- | --- |
| Date of Change | Author | Summary of Change |
| 10 September 2021 | Daniel Imfa | Initial Creation |
| 12 October 2021 | Uchizi Nkhata | Editing |
| Approved By: |  |  |
| Date Approved: |  |  |

Version 1.1 (9th September 2021)

**Table of Contents**

1.0 OVERVIEW......................................................................................................... 3

2.0 SCOPE................................................................................................................ 3

3.0 POLICY MANAGEMENT FRAMEWORK ............................................................ 3

3.1 IT Steering Committee ........................................................................................ 3  
3.2 IT Steering Committee Charter............................................................................ 4

4.0 POLICIES............................................................................................................ 6

4.1 Acceptable Use Policy......................................................................................... 6  
4.2 Password Policy.................................................................................................. 7  
4.3 System Access Control Policy ............................................................................. 9  
4.4 Internet Access & Usage Policy ......................................................................... 11  
4.5 Electronic Communication Policies.................................................................... 12  
4.6 Bring Your Own Device (BYOD) Policy............................................................. 13  
4.7 Data Security Policy........................................................................................... 15  
4.8 Change Management Policies............................................................................ 17  
4.9 Asset Management Policies................................................................................ 18  
4.10 Data Retention Policy...................................................................................... 18

4.11 Emergency Management of Information Technology ………………………….... 19

4.12 Data Protection Policy …………………………………………………………….…20

5.0 ENFORCEMENT ............................................................................................. 25

6.0 REVISION HISTORY......................................................................................... 25

APPENDIX A: USER DECLARATION........................................................................ 18

1. **OVERVIEW**

The purpose of this document is to provide guidelines for safeguarding information resources of the organization and to mitigate operational risks associated with the use of corporate computing resources.

Malawi union of Savings and Credit Co-operatives (MUSCCO) electronic media, computer equipment, and communication systems, including, but not limited to, computers, computer networks, electronic mail (e-mail), Internet access and systems, smart phones, tablets, telephone systems and equipment, voice mail, fax equipment, hardware, software, user identifications, passwords, and all data, files and other applications (“Company equipment and systems”), are the property of MUSCCO. All materials and information created, transmitted or stored on or through these systems are the property of MUSCCO and may be accessed or monitored by authorized personnel at any time. MUSCCO has the right to enter or access any and all MUSCCO equipment or systems at any time without notice in order to inspect or review any and all data. Employee Personal devices accessing MUSCCO information and systems will also be bound by these policies.

The policies defined in this document must be adhered to by all staff and wherever possible must be enforced in all computer systems deployed at each owned MUSCCO Network sites. These sets of policies have been developed from best practices from international standards and will form the reference point for all IT systems audits.

1. **SCOPE**

The contents of this policy document are applicable to all corporate computing resources (hardware, software, business applications, and corporate data) and information in the form of hard or soft copy, at all levels of sensitivity, and whether information is obtained, created, or maintained by the organization.

The policy also applies to all automated technology, manual or electronic transfer of information currently in existence and to any automated technology or information system planned for use in the future and to all computer and data communication systems owned by and/or administered by the organization.

This policy applies to all MUSCCO staff, service providers, visitors, temporary staff and contractors who have been given access to any computing resources within the organization.

1. **POLICY MANAGEMENT FRAMEWORK**
   1. **IT Steering Committee**

MUSCCO shall establish a Management Committee known as IT Steering Committee composed of at minimum the following: the IT Officer and the IT Manager from IT department, Head of Co-operative Development and Projects Head of Finance, HR and Administration, and CEO. This committee will meet at least quarterly to:

* Review progress on closure of all internal & external IT audit findings
* Review and approve amendments to this policy document
* Review and approve technology projects and expenditure
* Review the IT strategic plan and endorse any changes to the plan

The IT Manager has ultimate responsibility for the implementation of this policy document.

Where applicable, local laws supersedes the policies defined in this document.

* 1. **IT Steering Committee**

The IT Steering Committee charter aims to establish a governance structure that promotes and supports the effective use of information technology in the organization’s operational activities.

The IT Steering Committee is charged with identifying, prioritizing, and proposing tactical and strategic IT initiatives.

This charter specifies the purpose, responsibilities, membership, and conduct of the IT Steering Committee.

**The Charter**

**Name**: IT Steering Committee

|  |  |
| --- | --- |
| **Purpose**: | To ensure that IT initiatives and proposed projects help the organization achieve its strategic goals and objectives. |

**Responsibilities:**

1. Adopt and disseminate guiding principles for using IT within the organization
2. Adopt and disseminate standard processes for developing, submitting, reviewing, prioritizing and acting on proposed IT initiatives.
3. Encourage IT initiatives that provide the organization with a competitive advantage in the SACCO industry
4. Align applications of IT with the organization’s strategic goals and tactical objectives.
5. Receive, review, prioritize and make decisions about proposed IT initiatives.
6. Review and approve IT procurement cost and procedures, and pre-approve all major IT expenditure
7. Allocate resources or make recommendations about resources required to implement  
   proposed IT initiatives.
8. Minimize the risks associated with providing individuals with access to digital data and IT systems.
9. Resolve issues or conflicts that, if unresolved, would jeopardize the successful completion of approved IT initiatives.

**Authority:**

The IT Steering Committee advises about current and future IT‐related issues and initiatives and submits recommendations to members of the Board when appropriate.

**Membership:**

* IT Officer
* IT Manager
* Head of Finance, HR and Administration
* Head of Co-operative Development and Projects
* CEO

**Meetings:**

The IT Steering Committee will meet at least quarterly when necessary and as often as needed to accomplish its duties. However, the committee is expected to meet at least once every quarter in a year to review IT department audits.

**Reporting:**

Regularly reports to the Board about activities, issues, and related  
recommendations. In addition, publish meeting agendas, minutes and supporting documents so that members of the Board are aware of the work and recommendations of the committee.

**Committee Ground Rules**

Each committee meeting must have the following roles assigned which may be assigned on a time-basis and cycled through committee members.

**1. The Chair Person**

* The CEO shall Chair the Committee or delegated function
* Propose an agenda for each meeting using input from the committee members.
* Ensure that the meeting agenda and any relevant materials are distributed to all  
  members of the committee at least two working days prior to the meeting.
* Maintain the focus on meeting topics.
* Ensure the meetings begin and end on time.
* Serve as the liaison to the Board

**2. The Secretary**

* Maintain minutes of all meetings in hard copy and in an appropriate electronic format.
* Provide a list of action items. For each action item identify the description, which is responsible and the estimated completion date.
* Distribute the minutes and action items for all meetings within five business days after the meeting.

Meetings will begin and end on time.

Discussion about sensitive or controversial topics will be treated confidentially.

Confidential information shared remains confidential.

Members will judge ideas, not people.

Practice consensus team decisions.

Members are expected to attend every meeting; members should contact Chair prior to the meeting if attendance is not possible.

Members should contribute to the achievement of the goals and objectives

1. **POLICIES**
   1. **Acceptable Use Policy**
      1. MUSCCO equipment and systems are to be used primarily for MUSCCO business, and personal use should be kept to a reasonable minimum. All data, including Internet data, which is composed, transmitted, or received via MUSCCO equipment and systems, may be subject to disclosure to law enforcement or other third parties. Consequently, employees should always ensure that the business information contained in Internet email messages and other transmissions is accurate, appropriate, ethical, and lawful. MUSCCO has access to all e-mail communications, including all Internet sites visited by each employee and may review e-mail messages in connection with internal audits or investigations or for other business purposes.
      2. Music and video files required for business purposes will be allocated a dedicated area on corporate servers. Any such files found in unauthorized locations, or found to have been obtained illegally, will be deleted without notice.
      3. All software installed on company equipment must conform to the organization’s software standards and to be recommended by IT Manager and approved by the CEO.
      4. Users must not read, modify, delete, or copy a file belonging to another user without permission from the owner of the file. Unless general user access is clearly provided, the ability to read, modify, delete or copy a file belonging to another user does not imply permission to actually perform these activities.
      5. Users must not install software on their personal computers, network servers, or other machines without first receiving advance authorization to do so from the IT Manager / IT Officer.
      6. Any software or hardware tools that can be used to breach systems security is strictly prohibited, unless authorized by the IT Manager / IT Officer for security testing purpose or fraud detection.
      7. Information gathered about customers or potential customers, such as phone number and address, must be used for corporate purposes only.
      8. Customer information may not be disclosed to third-parties without explicit authorization by the customer or as required by law and must always be approved by the IT Manager or designate
      9. Users and visitors may not smoke, eat, or drink next to the computer machines or other IT equipment.
      10. Removable media (pen drives etc…) may not be used on any IT equipment without being checked for malicious software and approved by the IT department.
      11. Virus scanning software must be continuously enabled on all local area network (LAN) equipment (servers and other computer equipment on the network).
      12. Without specific written approval from IT Manager / CEO, system administrators (IT Officer) must not grant privileges beyond the user job functions and responsibilities.
      13. All user ID creation, deletion, and privilege change activity performed by systems administrators must be securely logged and available for audit.
      14. Every administrative transaction in all computer systems must be segregated to ensure that no one person completes the transaction from beginning to end.
      15. System privileges must be defined so that non-production staff (internal auditors, information security officers, programmers, computer operators, etc.) are not permitted to update production business information.
      16. Games software may not be stored on any computer system. Any games found on any ofthe company’s computers or servers will be uninstalled and/or deleted without notice. Persons responsible for the installation of games on any corporate computer system will face an appropriate disciplinary action.
      17. Any material viewed as offensive or potentially illegal, will be removed from computer systems without notice.
      18. Use of other organization’s trademarks or service marks in any external publication requires authorization from the IT Manager or designate.
      19. Staff must not work under the influence of drugs (whether prescribed or not) or alcohol.
      20. Non-compliance with information security policies, standards or procedures has grounds for disciplinary action up to and including termination.
   2. **Password Policy**
      1. Never record passwords on paper or in electronic devices like cell phones or Personal Device Accessories (PDAs)
      2. Passwords must be sent separately from user IDs if delivered by regular e-mail and must have no indications of the content of the message
      3. Never share your password with anyone – you will be held accountable for misuse of your account
      4. Never hint at the format of your password verbally or electronically
      5. Never use the "Remember Password" feature of application programs such as Internet Explorer, your email program, or any other program.
      6. Passwords must be difficult to guess. This means that passwords must not be related to one’s job or personal life. For example, a car license number, a spouse’s name, or fragments of an address must not be used. This also means passwords must not be a word found in any dictionary or some part of speech. For example, proper names, places, technical terms, and slang must not be used.
      7. Be careful about letting someone see you type your password.
      8. If your password is suspected to have been compromised, report the incident to IT Department and change your password immediately.
      9. Passwords MUST contain at least one alphabetic and one non-alphabetic character. Nonalphabetic characters include numbers (0-9) and punctuation and other symbols (e.g. ! ”, #,$, %, &).
      10. Be aware that passwords are usually case sensitive
      11. Do not construct fixed passwords by combining a set of characters that do not change, witha set of characters that predictably change.
      12. Do not perform any activity with user IDs belonging to other users and do not allow otherusers to use your logon credentials to perform any activity in any computer system
      13. Passwords must not be written down in any place where unauthorized persons might discover them.
      14. For the sake of accountability, passwords must not be shared (the only exception is thelocal administrator account for desktop and laptop computers)
      15. Passwords must not be stored in readable form in batch files, automatic login scripts, software macros, or hard-coded in developed software
      16. All devices on the internal network (e.g. routers, firewalls, access control servers) musthave unique passwords
      17. Default passwords on all devices must be changed before installing in production environment
      18. Administrator or root password on servers and security & network devices MUST be changed every 30 days
      19. Any staff who uses passwords, security keys and other access codes with administrator rights or its access equivalent must sign a responsibility statement.
      20. Minimum Password Length shall be 8 characters
      21. Password complexity or strong passwords must be enabled
      22. Password history must be restricted to 3
      23. Concurrent logon to any single application/system must be disabled
      24. User account will be locked after 3 failed login attempts
      25. Locked accounts must only be cleared by Administrator
      26. Password protected screen savers must be enabled and must activate 10 minutes of user inactivity.
      27. All passwords must be transmitted in encrypted form – not clear text
      28. The display and printing of passwords must be masked, suppressed or otherwise obscuredso that unauthorized parties will not be able to observe
      29. All workstations must have a common local administrator password, to avoid problems anddelays during the set-up of devices and applications.
   3. **System Access Control Policy**
      1. Access to all computer systems must be approved by Departmental Head of the user and authorized by the IT Officer /IT Manager.
      2. Every user must have a unique user ID and password to access any MUSCCO computer system.
      3. Anonymous user IDs must not be assigned to users.
      4. Guest user IDs must always be disabled.
      5. All user IDs must identify their owner and must follow the convention, the first letter of the owner’s given name and surname. For example, for Dorothy Mambulasa the user ID must be“Dmambulasa”
      6. All users must log out of systems at the end of each day.
      7. Users must log out of a computer before leaving it, or lock the computer if they are leaving the computer for a short time.
      8. Access rights of terminated staff must initially be disabled for a minimum of 30 days prior to receiving instructions from the appropriate department head to dispose of the data.
      9. Users must not attempt to gain unauthorized access to any other information systems, or in any way damage, alter, or disrupt the operations of the systems. Likewise, users must not capture or otherwise obtain passwords, encryption keys, access cards, or any other electronic control mechanism, which could permit unauthorized entry.
      10. Access to systems for non-employees must be accompanied by a non-disclosure  
          agreement and authorized by the IT Manager / IT Officer.
      11. Access to the organization’s Data Centre is restricted only to IT staff. All access to these areas by other staff and visitors are by permission granted only by the IT Officer/IT Manager and must be accompanied by IT staff at all time.
      12. Access to IT server room should be restricted by use of key entry or biometric  
          authentication entry system.
      13. Staff resignations or dismissals must be reported to the IT department immediately by IT Manager and profile disabled from the IT system by IT.
      14. Access privileges to corporate data must be defined for each category of user for all systems and approved by department heads and IT Manager or designate
      15. Remote access to any network resource must be through encrypted channels.
      16. All third-party remote access to the organization’s internal computer systems must be jointly approved by the IT Manager and Head of Heaf of Finance, HR and Administration. Access must be enabled only for the time period required to accomplish approved tasks.
      17. All in-bound real-time external connections to the organization’s networks must pass a firewall or security device.
      18. The use of direct database access utilities to corporate business systems is not permitted unless specifically approved by the IT Officer.
      19. Use of corporate business applications must be via the applications menus. Users must not be allowed to invoke system level commands.
      20. All computer systems running business applications must include logs which record user session activity including user IDs, log-in date and time, logout date and time, modifications to privileges of users and system start-up and shut-down events.
      21. Security logs of business applications must be retained as per data retention policy of theorganization and reviewed at least once every week.
      22. Production environments must be kept separate from test environments. This separation must be achieved via physically separate computer systems.
      23. 4.3.23 All computer and communications equipment must have an asset identification tag andregistered accordingly in the organization’s hardware asset list.
      24. The organizations computer and communications equipment, including storage media, must not be moved or relocated, within or outside the organization’s premises, without the prior approval of the IT Officer /IT Manager and person responsible for security of that premises.
      25. Users may not lend out company equipment (personal computers, handheld computers,transportable computers, personal digital assistants (PDAs), smart phones, or any other devices used for business activities) as these may contain sensitive information.
      26. The IT Department must maintain a current inventory of all hardware indicating date of purchase, warranty expiration date, location of equipment and user to which the equipmentis assigned to.
      27. The IT department must maintain a current inventory of all corporate software indicatingdate of purchase, license details, maintenance support agreements/SLA, cost of softwareand user installations
      28. The IT Department must maintain a current inventory of all connections to external  
          networks including telephone networks, Electronic Data Interchange networks, intranets, extranets and the Internet.
      29. Systems administrators are only authorized to examine private user files to handle emergencies such as virus infestations and system crashes. Whenever user files are examined in this manner, the involved user(s) must be notified. After problem has beenresolved, all copies of such files made by the administrator must be promptly destroyed.
      30. In all cases where a member of the IT department is involuntarily terminated, access to allsystems for this member must be immediately terminated. Close supervision ofthemember’s departure from the organization’s premises is required to safeguard theorganizations’ information assets and as a security precautionary measure.
      31. When employees, consultants and contractors terminate their relationship with the MUSCCO,all the MUSCCO’s property must be returned. This includes portable computers, External hard drives, phones, portable Wi-Fi gadgets, and the like.
   4. **Internet Access & Usage Policy**
      1. Downloading free software and/or pornographic materials are strictly prohibited. Users who breach this policy will face disciplinary action and may be dismissed from the organization
      2. Users must not advertise, promote, present, or otherwise make statements about the organization’s product and services on the Internet without the prior approval of the Marketing Officer or equivalent authority.
      3. All Internet gateways must be protected by a firewall device which is in accordance withcorporate hardware standards.
      4. All software or documents downloaded from the Internet must be screened with virus detection software.
      5. Users must not upload software which has been licensed by a third party, or software which has been developed internally to any computer via the Internet unless authorized by the IT Office or equivalent authority.
      6. A web content filtering device must be installed to control user access to the Internet
      7. Users who discover they have inadvertently visited a website that contains sexually explicit, racist, or other potentially offensive material must immediately disconnect from that website.
      8. All corporate Internet web pages must conform to layout standards, navigation standards, legal wording standards, and similar requirements specified by MUSCCO Network.
      9. User access must be controlled to ensure optimum and economic use of the Internet.Theremust be justification and an approval process for access to the Internet.
      10. Internet access for users shall be terminated if the access is abused or used in a way thatthreatens the integrity of the organization’s systems.
      11. Internet use must be for corporate purposes. Use for personal reasons must be during out of work hours.
   5. **Electronic Communication Policy**
      1. The use of Skype and/or Yahoo Messenger is restricted to key staff who can demonstrate abusiness need for its use. Approval is required from a department headand subsequentlyauthorized by the IT Officer.
      2. All employees must be assigned a corporate electronic mail account.
      3. All electronic mail accounts must adhere to the organization’s Password Policy.
      4. It is prohibited to send or receive electronic mail from accounts assigned to other individuals.
      5. Forwarding of chain-mail or unsolicited e-mail is prohibited.
      6. Electronic mail messages may be monitored for internal policy compliance, suspectedcriminal activity and other systems management reasons. Approval is required from the IT Manager or a designate for such monitoring to take place
      7. It is prohibited to send the following file types as an attachment to electronic mail messages(music, video clips, images, etc.) unless work related.
      8. Personal email use is not recommended.
      9. The size of electronic mail attachments is limited to 5 megabytes. This limit when reached will either block the email from being sent or strip the e-mail message of its attachment while notifying sender or recipient of action taken. Exception to lift this limit will be grantedon a case by case basis depending on seniority of requester or the business criticality ofthe email to be sent.
      10. Electronic mail systems are not intended for archival storage of important information. Theonus is on users to archive mail messages if not stored in a central location on server.
      11. Electronic mail systems are intended to be used primarily for business purposes. Any personal use must not interfere with normal business activities
      12. The corporate email system must not be used for criminal acts, terrorism, or other activities against the law of the land.
      13. Broadcast facilities found in electronic mail systems (such as the use of distribution lists such as “everyone@” may only be used with authorization from department heads or executive management of the organization.
      14. All outbound electronic mail must contain the sender’s first and last name, job title, organizational unit, and telephone number. This should be presented in the signature ofeach user.
      15. Users’ identities on electronic communications must not be misrepresented, obscured, suppressed, or replaced. The user name, electronic mail address, organizational affiliation, and related information included with message or postings must reflect the actual originator of the message or postings.
      16. Confidentiality and Disclaimer information should be indicated at the bottom of every outbound message in the email system.
      17. All outbound email communications must reflect well on the organization’s reputation and public image. Inflammatory, defamatory, harassing, disruptive communications, “spamming” and “flaming” are strictly prohibited.
      18. Users are prohibited from sending or forwarding any messages that may be considered to be defamatory, harassing, or explicitly sexual and is likely to offend on the basis of race, gender, national origin, sexual orientation, religion, political beliefs, or disability.
      19. It is prohibited to use electronic mail, other electronic systems (fax, dial-up devices), or any other communication systems for the distribution of unsolicited advertising material.
      20. The organization reserves the right to disclose electronic mail to law enforcement officials without prior notice to the users who may send or receive such messages.
      21. All electronic mail sent through corporate infrastructure is subject to corporate archival policy.
      22. Only applications that comply with the organization’s software standards may be used for reading and sending electronic mail
      23. Recipients of unsolicited email (also known as spam) must notify the IT department who will take steps to prevent further transmissions.
      24. External e-mail addresses must not be included in internal distribution lists without approval from MUSCCO Senior Management.
   6. **Bring Your Own Device (BYOD) Policy**
      1. MUSCCO issues all employees standard technology equipment relevant to their role or job function.However, MUSCCO also supports employee use of personally owned smartphones, tablets, and laptops of their choosing at work for their convenience. MUSCCO reserves the right to revoke this privilege if users do not abide by the policies and procedures outlined below.
      2. This policy does not apply to systems which maintain valuable, private, or sensitive customer centric data and information or any content deemed confidential by national regulators. MUSCCO will provide purpose-specific equipment, software and networks for staff working in such situations
      3. MUSCCO employees must agree to the terms and conditions set forth in this policy in order to be able to connect their devices to MUSCCO network.

* Smartphones including iPhone, Android, Blackberry and Windows phones are allowed
* Tablets including iPad, Windows and Android are allowed
* General device support and connectivity issues are not supported by IT; employees should contact the device manufacturer or their carrier for operating system or hardware-related issues.
* Employees must follow documented IT general setup procedures (if applicable) in order to self-configure their device to access MUSCCO systems. IT will not provide support on personal devices.
* Employees must ensure that all software on their device has been acquired legally and does not violate copyright laws.
* Employees are required to maintain the corporate standard software on these devices as defined by IT. If a personal device becomes their primary productivity device (e.g. laptop) MUSCCO may provide this software to the employee. However, any software provided to employee is licensed and owned by MUSCCO and will need to be removed from personal owned equipment at termination of employment or ending use of this device.
* Any information developed on behalf of MUSCCO (e.g. presentations, memos, documents,spreadsheets, etc) is the property of MUSCCO. Employees must ensure that this information is not maintained only on the local device. Such information must be saved on centrallyaccessible MUSCCO storage services such as file shares or online storage repositories (e.g. google workspace, dropbox, icloud etc)
* MUSCCO will not reimburse the employee the cost of the device
* MUSCCO employees required to use the device as part of core job responsibilities may be eligible for employer compensation when the device gets damaged in the course of being used for business purposes.
* Any software purchases or paid downloads from Application stores will not be reimbursed unless pre-approved by management
* MUSCCO may require installation of security or remote management software on any personal device accessing MUSCCO systems.
* The device must lock itself with a password or PIN if it is idle for at least 10 minutes.
* In order to prevent unauthorized access, devices must be password protected using the features of the device and including the strong password already required to access MUSCCO network.
* Rooted (Android) or jailbroken (iOS) devices are strictly forbidden from accessing the  
  network.
* Employees’ access to company data is limited based on user profiles defined by IT and automatically enforced.
* The employee’s device may be remotely wiped if 1) the device is lost, 2) the employee terminates his or her employment, 3) IT detects a data or policy breach, a virus or similar threat to the security of MUSCCO’s data and technology infrastructure.

While IT will take precaution to prevent the employee’s personal data from being lost in the event itmust remote wipe a device, it is the employee’s responsibility to take additional precautions, suchas backing up photos email, contacts, etc. MUSCCO will not be held accountable if such information iswiped from a device

* MUSCCO reserves the right to disconnect devices or disable services without advanced notification.
* Lost or stolen devices must be reported to MUSCCO within 24 hours. Employees are responsible for notifying their mobile carrier immediately upon loss of a device if they are not on a managed MUSCCO service contract.
* The employee is expected to use his or her devices in an ethical manner at all times and adhere to MUSCCO’s Technology Acceptable Use Policy.
* The employee is personally liable for all costs associated with his or her device.
* The employee understands, and will not hold MUSCCO accountable, for the partial or complete loss of company and personal data due to an operating system crash, errors, bugs,viruses, malware, and/or other software or hardware failures, or programming errors thatrender the device unusable.
* Employees should not text or email while driving and, should use hands-free talking while driving.
  1. **Data Security Policy**

4.7.1 All corporate information systems equipment or storage media provided to any third partymust be physically inspected by the IT Department to ensure that sensitive information has been removed.

4.7.2 All server rooms must have adequately maintained fire detection/suppression, air  
conditioning, humidity control, dust control, or other computing environment protectionsystems to ensure uninterrupted service to business operations.

4.7.3 All PCs and workstations must be fitted with uninterruptible power supply (UPS) systems,electrical power filters, or surge suppressers which have been approved by the Head of ITand are in accordance with corporate hardware standards.

4.7.4 All server rooms must have adequate backup power (generator and UPSs) to maintainbanking operations in the event of main power failure.

4.7.5 Computer equipment must not be placed under air conditioners

4.7.6 All computer equipment (including for servers, computers, air conditioners, powerequipment, telecom and network equipment, copiers, printers, fax machines, scanners,PABX, etc) must regularly undergo hardware maintenance to ensure full shelf life andprotect corporate data.

4.7.7 All departments must maintain an up-to-date Backup Control List to identify data that needsto be backed up and at what frequency to back up the data.

4.7.8 Each department Head is responsible for presenting department data required to bebacked up and expected to be recovered in the event of a disaster indicating clearly thelevel of importance to guide recovery priorities for IT. All staff have access to google workspace where they have access of up to 50GB of space on google drive which they must backup their data.

4.7.9 Backup of user data is the full responsibility of the equipment user. IT departmentwill provide guidelines to assist users in ensuring adequate backup and security of these equipment.

4.7.10 All software must be copied prior to its initial usage and original or master copies must bestored in a safe and secure location.

4.7.11 Labels should be used for every back up disk, tape or other storage media, detailinginformation backed up and backup date.

4.7.12 Backups of essential business information and software must be stored in an  
environmentally-protected and access-controlled site

4.7.13 Backup media contents stored off-site must be encrypted or password protected.

4.7.14 The offsite backup systems must contain up-to-date copies of data on productions ystems.

4.7.15. A copy of the IT Disaster Recovery Plan must be available at the disaster recovery site

4.7.16 All IT staff must be conversant with the contents of the IT Disaster Recovery Plan document

4.7.17 Documents related to IT Disaster Recovery must be updated at all times

4.7.18 Disaster Recovery procedures must be tested at least once a year to ensure reliability andsuccessful recovery of critical corporate systems

4.7.19 IT Disaster recovery sites must be located at least 15 kilometres away from the primary data centre.

4.7.20 Information in electronic form must be retained as dictated by local banking laws and regulations.

4.7.21 Backup expertise in critical business systems areas must exist within the IT support team toprevent undue interruptions in systems service

4.7.22 The internal system addresses, configurations, and related systems design information orthe MUSCCO networked computer systems must not be displayed and must be kept out ofreach from unauthorized staff.

4.7.23 All firewalls used to protect the MUSCCO’s internal network are configured on router/switch level separate from computers.

4.7.24 Unless prior approval of the Head of IT has been obtained, users may not establish internetor any other external network connections which could allow another company’s users togain access to the MUSCCO systems and information.

4.7.25 Personal Digital Assistants (PDAs), handheld computers, smart phones, digital camerasand other handheld devices must not be used for the MUSCCO business information unlessthey have first been configured with necessary controls and approved for such use by the IT Officer. Exceptions will be made for calendars, address books, to do tasks, and storedconnection information such as telephone numbers and IP addresses.

4.7.26 Users of corporate portable computers (such as laptops and palmtops) must not leavethese computers unattended at any time in the car or at public places without adequatesecurity to prevent loss of company property and information.

4.7.27 All portables, laptops, notebooks, and other transportable computers containing MUSCCO’ssensitive information must consistently employ both hard disk encryptions for all files aswell as boot protection.

4.7.28 Users who have been assigned corporate portable computers must check these  
equipment when travelling by any transport either land, water or air. These computers must remain in the possession of thetraveller as hand luggage, unless restricted by airport security regulations.

4.7.29 Users of portable computers (notebooks, netbooks, PDAs, smart phones) are responsiblefor ensuring regular backups of their devices to protect loss of company data.

4.7.30 All corporate data stored on the network must have a designated owner who will determineappropriate sensitivity classifications. Data owners must make decisions about who will bepermitted to access the information, and the uses to which this information will be put.

* 1. **Management Policy**

4.8.1 All changes to corporate computer systems must be reviewed by the steering committee in conjunction with the change request or and the implementer.

4.8.2 All changes must be tested in a test environment prior to implementation.

4.8.3 The following procedure must be followed for all changes to corporate computer systems:

* The request may come from any member of staff and will require authorization from the relevant Department Head or Manager (via e-Mail or Helpdesk system)
* IT Personnel must fill out a Change Request (CR) form and present to the requestor’s Manager to sign off
* Personnel who receives the request must present the signed CR form to the IT Officer to review and authorise.
* The IT Officer must clarify & confirm the required changes and invite other team members (where necessary) to review the implementation of the change.i.e. IT Personnel will proceed with implementing the requested change in a TEST environment prior to the agreed implementation time
* IT Officer must verify that the expected results have been achieved in the TESTenvironment together with the Change Requester. IT Officer will require the Change Requester to sign the CR form indicatingsatisfaction with the test results.
* Test results shall be reviewed and signed off by Change Requester and Head of ITbefore implementation in the production environment.
* Prior to implementing the change on the “live” system, backup the “live” system.
* Notify users of the system prior to implementing the required change
* Implementing the required change at the agreed time
* Re-confirm functionality on the live system with the Change Requester
* Notify Change Requester and his/her authorizing Manager via e-mail that the requestedchange has been successfully implemented
* File the completed paper copy of the fully completed CR form plus any supportingdocumentation
  1. **Asset Management Policy**

4.9.1 All computers, communication equipment, and other computer-systems-related hardware must be included in a comprehensive inventory system to monitor and account for its location, cost, movement, usage and accountability.

4.9.2 Hardware and equipment must have up-to-date property tags to account for their existence during physical inventory. The tag should include the serial number.

4.9.3 Adequate insurance coverage must be obtained for all computer equipment at all branches.

4.9.4 When disposed of, all secret, confidential, or private information in hardcopy or electronic form (paper, microfilm, microfiche, handwritten notes, CDs, tapes, files etc.) must be either shredded or incinerated.

4.9.5 Computer equipment can only be disposed off with explicit authorization from the IT Manager and IT Officer

4.9.6 Acquisition of hardware or software from third party vendors should be approved by the IT Steering committee who may choose to evaluate 3 short listed providers or select preferred provider for the year

4.9.7 All software acquired from third parties must have a maintenance agreement and a service level agreement for support

4.9.8 All software developed for the organization must have documentation that includes at least a business case approved by the IT Steering Committee, a signed Terms of Reference, source code for the development, and testing plan signed off by the business owner of the application.

4.9.9 A formal change control process is required for all business applications deployed to the production environment.

* 1. **Data Retention Policy**

4.10.1 This I.T Policy on Data retention and archiving is limited to whatever is retained in electronic form, what company policy prescribes that it must be retained in electronic format, whatever statutory regulation or legislation requires that it must be retained

4.10.2 Permanent retention of all documents is undesirable, thus appropriate disposal is advised to avoid unnecessary/excessive use of electronic storage space for personal data and to ease access to required documents by reducing clutter.

4.10.3 Any decision whether to retain or dispose of electronic shall be taken in accordance with the retention laws and statutory obligations in Malawi.

4.10.4 A review should always be carried out and documented before final decision to expunge any expired data.

4.10.5 When undertaking data asset disposal under no circumstances should the MUSCCO’s electronic storage media be simply binned. Storage media and computer hard drives marked for disposal should be physically destroyed or irreversibly erased of all data by the designate MUSCCO IT Officer. Best practice is that if steps are taken to make data virtually impossible to retrieve, then this will be regarded as equivalent to deletion.

4.10.6 A certificate of deletion shall be filed by the deleting officer for the device(s).

4.10.7 The Following below shall be considered before final decision to dispose of or retain Data:

a. has the Data set been appraised?

b. Is retention required to fulfil statutory or other regulatory requirements?  
c. Is retention required to evidence events in the case of dispute?  
d. Is retention required to meet the operational needs of MUSCCO?  
e. Is retention required because the document or record is of historic interest or intrinsic value?

4.10.8. Recommended retention Periods for various Data Sets

|  |  |
| --- | --- |
| **Type of record** | **Suggested retention period** |
| Company records | Permanent |
| Financial Records | 10 years after transaction |
| Customer Information | 10 years after transaction |
|  |  |
| General email correspondence | 6 months unless likely that it will need to be retained for longer |
| Property records, trust deeds | Permanent |
| Any information private to any individual | Destroy when no longer required |
| All Other Data | As advised by appropriate policy or respective line management in absence of company policy |

* 1. **Emergency Management of Information Technology**

This policy provides guidelines for emergency management of all information technology within the business.

### 4.11.1 IT Hardware Failure

* Where there is failure of any of the business’s hardware, this must be referred to IT Officer immediately.
* It is the responsibility of IT Officer to decide relevant actions that should be undertaken in the event of IT hardware failure.
* It is the responsibility of IT Officer to undertake tests on planned emergency procedures quarterly to ensure that all planned emergency procedures are appropriate and minimize disruption to business operations.

### 4.11.2 Teller Disruptions

In the event that a Teller system is disrupted, the following actions must be immediately undertaken:

* System provider to be notified
* IT Officer must be notified immediately
* All Teller transactions to be halted until a solution is found

### 4.11.3 Virus or other security breach

* In the event that the business’s information technology is compromised by software virus or malware, such breaches are to be reported to IT Officer immediately.
* IT Officer is responsible for ensuring that any security breach is dealt with within one hour to minimize disruption to business operations.
  1. **Data protection policy**

**4.12.1 Introduction**

MUSCCO needs to gather and use certain information about individuals.

These can include customers, suppliers, business contacts, employees and other people the organization has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the company’s data protection standards — and to comply with the law.

**4.12.2 Why this policy exists**

This data protection policy ensures MUSCCO:

* Complies with data protection law and follow good practice
* Protects the rights of staff, customers and partners
* Is open about how it stores and processes individuals’ data
* Protects itself from the risks of a data breach

**4.12.3 Data protection law**

Data Protection describes how MUSCCO— must collect handle and store personal information.

These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

Data Protection is underpinned by seven important principles. These say that personal data must:

* Be processed fairly and lawfully
* Be obtained only for specific, lawful purposes
* Be adequate, relevant and not excessive
* Be accurate and kept up to date
* Not be held for any longer than necessary
* Processed in accordance with the rights of data subjects
* Be protected in appropriate ways

**4.12.4 People, risks and responsibilities**

**4.12.5 Policy scope**

This policy applies to:

* The head office of MUSCCO
* All branches of MUSCCO
* All staff and volunteers of MUSCCO
* All contractors, suppliers and other people working on behalf of MUSCCO

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of Data Protection. This can include:

* Names of individuals
* Postal addresses
* Email addresses
* Telephone numbers
* …plus any other information relating to individuals

**4.12.6 Data protection risks**

This policy helps to protect MUSCCO from some very real data security risks, including:

* Breaches of confidentiality. For instance, information being given out inappropriately.
* Failing to offer choice. For instance, all individuals should be free to choose how the company uses data relating to them.
* Reputational damage. For instance, the company could suffer if hackers successfully gained access to sensitive data.

**4.12.7 Responsibilities**

Everyone who works for or with MUSCCO has some responsibility for ensuring data is collected, stored and handled appropriately.

Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility:

* The board of directors is ultimately responsible for ensuring that MUSCCO meets its legal obligations.
* The IT Manager, is responsible for:
  + Keeping the board updated about data protection responsibilities, risks and issues.
  + Reviewing all data protection procedures and related policies, in line with an agreed schedule.
  + Arranging data protection training and advice for the people covered by this policy.
  + Handling data protection questions from staff and anyone else covered by this policy.
  + Checking and approving any contracts or agreements with third parties that may handle the company’s sensitive data.
* The **IT Officer,** is responsible for:
  + Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
  + Performing regular checks and scans to ensure security hardware and software is functioning properly.
  + Evaluating any third-party services the company is considering using to store or process data. For instance, cloud computing services.
* The **Marketing & Member Services Officer,** is responsible for:
  + Approving any data protection statements attached to communications such as emails and letters.
  + Addressing any data protection queries from journalists or media outlets like newspapers.
  + Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.
  + Dealing with requests from individuals to see the data MUSCCO LIMITED holds about them (also called ‘subject access requests’).

**4.12.8 General staff guidelines**

* The only people able to access data covered by this policy should be those who need it for their work.
* Data should not be shared informally. When access to confidential information is required, employees can request it from their line managers.
* MUSCCO LIMITED will provide training to all employees to help them understand their responsibilities when handling data.
* Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
* In particular, strong passwords must be used and they should never be shared.
* Personal data should not be disclosed to unauthorised people, either within the company or externally.
* Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.
* Employees should request help from their line manager or the IT Manager if they are unsure about any aspect of data protection.

**4.12.9 Data storage**

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the IT Officer.

When data is **stored on paper,** it should be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

* When not required, the paper or files should be kept in a locked drawer or filing cabinet.
* Employees should make sure paper and printouts are not left where unauthorised people could see them, like on a printer.
* Data printouts should be shredded and disposed of securely when no longer required.

When data is **stored electronically**, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

* Data should be **protected by strong passwords** that are changed regularly and never shared between employees.
* If data is **stored on removable media** (like a USB, External Hard Drives, CD or DVD), these should be kept locked away securely when not being used.
* Data should only be stored on **designated drives and servers**, and should only be uploaded to an **approved cloud computing services**.
* Servers containing personal data should be **sited in a secure location**, away from general office space.
* Data should be **backed up frequently**. Those backups should be tested regularly, in line with the company’s standard backup procedures.
* Data should **never be saved directly** to laptops or other mobile devices like tablets or smart phones.
* All computers containing data should be protected by **approved security software and a firewall**.

**4.12.10 Data use**

Personal data is of no value to MUSCCO LIMITED unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

* When working with personal data, employees should ensure **the screens of their computers are always locked** when left unattended.
* Personal data **should not be shared informally**. In particular, it should never be sent by email, as this form of communication is not secure.
* Data must be **encrypted before being transferred electronically**. The IT officer can explain how to send data to authorised external contacts.
* Employees **should not save copies of personal data to their own computers.** Always access and update the central copy of any data.

**4.12.11 Data accuracy**

The law requires MUSCCO LIMITED to take reasonable steps to ensure data is kept accurate and up to date.

The more important it is that the personal data is accurate, the greater the effort MUSCCO LIMITED should put into ensuring its accuracy.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

* Data will be held in **as few places as necessary**. Staff should not create any unnecessary additional data sets.
* Staff should **take every opportunity to ensure data is updated.** For instance, by confirming a customer’s details when they call.
* MUSCCO LIMITED will make it **easy for data subjects to update the information** MUSCCO LIMITED holds about them. For instance, via KYC Update forms.
* Data should be **updated as inaccuracies are discovered**. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.
* It is the Marketing & Member Services Officer’s responsibility to ensure **marketing databases are checked against industry suppression files** every six months.

**4.12.12 Subject access requests**

All individuals who are the subject of personal data held by MUSCCO LIMITED are entitled to:

* Ask **what information** the company holds about them and why.
* Ask **how to gain access** to it.
* Be informed **how to keep it up to date.**
* Be informed how the company is **meeting its data protection obligations**.

If an individual contacts the company requesting this information, this is called a subject access request.

Subject access requests from individuals should be made by email, phone call, office visit, by requesting the attention of a Marketing & Member Services Officer. The Marketing & Member Services Officer can supply a standard request form.

Marketing & Member Services Officer will aim to provide the relevant data within 14 days.

Marketing & Member Services Officer will always verify the identity of anyone making a subject access request before handing over any information.

**4.12.13 Disclosing data for other reasons**

In certain circumstances, Data Protection allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, MUSCCO LIMITED will disclose requested data. However, the Marketing & Member Services Officer will ensure the request is legitimate, seeking assistance from the IT Manager and from the company’s legal advisers where necessary.

**4.12.14 providing information**

MUSCCO LIMITED aims to ensure that individuals are aware that their data is being processed, and that they understand:

* How the data is being used
* How to exercise their rights

To these ends, the company has a privacy statement, setting out how data relating to individuals is used by the company.

[This is available on request.]

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

**6.0 REVISION HISTORY**

|  |  |  |
| --- | --- | --- |
| Date of Change | Author | Summary of Change |
| 10 September 2021 | Daniel Imfa | Initial Creation |
| 12 October 2021 | Uchizi Nkhata | Editing |
|  |  |  |

**APPENDIX A: USER DECLARATION**

**NAME :…………………………………………………………………….**

**DEPARTMENT :…………………………………………………………………….**

**DECLARATION**

I have read and understood the IT Policy Manual in its entirety and therefore agree to adhere to all the policies defined in the manual.

I accept the responsibility to regularly review the manual to keep abreast of updates as they are issued.

If found to have violated this policy, I understand and agree that I may be subject to disciplinary action, up to and including termination of employment

**Name :**

**Signature:**

**Date :**