MUKUBA UNIVERSITY

INFORMATION AND COMMUNICATION TECHNOLOGY POLICIES

Prepared By

CENTRE FOR INFORMATION AND COMMUNICATION TECHNOLOGY

(April 2021)

Contents

1.0 INTRODUCTION

Mukuba University is one of the major Higher Education institutions in Zambia developing human resources in Sciences, Technology, Engineering and Mathematics.

Mukuba University Information and Communication Technology (ICT) resources are designed to ensure that the University achieves its Vision, Mission and Strategic Objectives.

The move toward global knowledge society require a fundamental shift in thinking about the methodology in the provision of education and research. ICTs have already begun to exert massive transformation of education systems in both developed and developing countries as illustrated by the following scenarios:

- Integration of digital technology (software and hardware systems) into the teaching and learning process has given students more options than ever before to decide where, how, and when they pursue their studies. For example, through online portals, students can use their smartphones and other mobile devices to gain access to homework assignments and grades, or attend classroom lectures or participate in a tutorial remotely through the use of video technology.

- Distance education universities are now quoted on the stock exchange, the best teachers in the world are becoming available anywhere at the click of a button while 'Lifelong Just-In-Time Learning' has become the order of the day.

- Access to Virtual Libraries, Virtual Laboratories, High Performance Computers are becoming big source of information, especially in developing countries where physical literature and ICT infrastructure are not only scarce, but unaffordable to most students and researchers.

- The Internet and other digital connections, act as gateway where academic staff, researchers, students and librarians can access and share world knowledge and learning materials, they provide facilities where local research is published, and disseminated world-wide, and enables networking among researchers, promoting discourse and dialogue on shared topics and challenges.

Mukuba University has invested and will continue to invest in ICTs in order to strategically support the teaching, learning, research outreach, and professional services as well as enhance business process efficiencies within the University. The cost of ICT investment is substantial and the technology rapidly changes. It is thus of utmost important that the institution deploys and manages ICT resources strategically for maximum benefit (value for money) and for competitive advantage.

The University has connectivity to the Internet and thus is able to access many opportunities offered by today's information societies.

Access to computers, computing systems and networks owned by the University imposes certain responsibilities and obligations and is subject to university policies, ethics and local laws. It is important that these ICT resources are used for the purpose for which they are intended.

The use of these resources is a privilege that is extended to qualified members of all the University community. All users of these resources must comply with specific policies and guidelines governing their use, and act responsibly while using shared computing and network resources.

This set of policies are aimed at optimizing and securing usage of both logical and physical ICT infrastructures, as well as effective and efficient deployment of the infrastructures and services.

The policies fall under two categories, General Policies, which provide guidelines on acceptable use, responsible use of ICT services and handling of information accessible or provided through platforms provided by Mukuba University and Technical Policies which address guidelines on technical requirements in implementing and managing ICT infrastructure and services.

2.0 GENERAL POLICIES

The general policies provide guidelines on acceptable use, responsible use of ICT services and handling of information accessible or provided through platforms provided by Mukuba University.

2.1.0 ACCEPTABLE USE POLICY

2.1.1 Overview

Mukuba University's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to Mukuba University's established culture of openness, trust and integrity. Mukuba University is committed to protecting Mukuba University's employees, partners and the institution from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network/user accounts providing electronic mail, Web Portals, and FTP, are the property of Mukuba University. These systems are to be used for business purposes in serving the interests of the institution, and of our clients and customers in the course of normal operations.

Effective security is a team effort involving the participation and support of every Mukuba University employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

2.1.2 Purpose

The purpose of this policy is to outline the acceptable use of computer systems and equipment at Mukuba University. These rules are in place to protect the employee and Mukuba University. Inappropriate use exposes Mukuba University to risks including virus attacks, compromise of network systems and services, and possible litigations.

2.1.3 Scope

This policy applies to employees, contractors, consultants, temporaries, and other workers at Mukuba University, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by Mukuba University.

2.1.3 Policy

2.3.3.1 **General Use and Ownership**

i) While Mukuba University's network/system administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the institution's systems remains the property of Mukuba University. The need to protect Mukuba University's network is of utmost importance, however, management cannot completely guarantee the confidentiality of information stored on any network device belonging to Mukuba University. Users should therefore engage in safe computing practices including but not limited to establishing appropriate access restrictions for their accounts, guarding their passwords, changing them regularly, and by backing up critical files when appropriate.

ii) Employees and students are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees and students should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or head of department or CICT.

iii) Mukuba University recommends that any information that users consider sensitive or vulnerable be encrypted. For guidelines on information classification, refer to Mukuba University's Information Sensitivity Policy. For guidelines on encrypting email and documents, refer to Encryption Policy.

iv) For security and network maintenance purposes, authorized individuals within Mukuba University may monitor equipment, systems and network traffic at any time, per Mukuba University's Audit Policy.

v) Mukuba University reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

2.1.3.2 **Security and Proprietary Information**

i) The user interface for information contained on Internet/Intranet/Extranet-related systems should be classified as either confidential or not confidential. Examples of confidential information include but are not limited to: company private, corporate strategies, competitor sensitive, trade secrets, specifications, customer lists, and research data. Employees should take all necessary steps to prevent unauthorized access to this information.

ii) Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. System level passwords should be changed quarterly, user level passwords should be changed every six months.

iii) All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off when the host will be unattended.

iv) Use encryption of information in compliance with Mukuba University's Encryption Policy.

v) Because information contained on portable computers is especially vulnerable, special care should be exercised. Protect laptops in accordance with the "Laptop Security Tips".

vi) Postings by employees from a Mukuba University email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Mukuba University, unless posting is in the course of business duties.

vii) All hosts used by the employee that are connected to the Mukuba University Internet/Intranet/Extranet, whether owned by the employee or Mukuba University, shall be continually executing approved virus-scanning software with a current virus database.

viii) Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

2.1.3.3 **Bring Your Own Device (BYOD)**

i) Employees who prefer to use their personally-owned IT equipment for work purposes must secure corporate data to the same extent as on corporate ICT equipment, and must not introduce unacceptable risks (such as malware) onto the corporate networks by failing to secure their own equipment

ii) BYOD users must use appropriate forms of user authentication approved by Information Security, such as user IDs, passwords and authentication devices.

iii) The following classes or types of corporate data are not suitable for BYOD and are not permitted on PODs:

    a) Anything classified SECRET or CONFIDENTIAL;
    b) Other currently unclassified but highly valuable or sensitive corporate information which is likely to be classified as SECRET or CONFIDENTIAL;

iv) The University has the right to control its information. This includes the right to backup, retrieve, modify, determine access and/or delete corporate data without reference to the owner or user of the device.

v) The University has the right to seize and forensically examine any device within the University premises believed to contain, or to have contained, corporate data where necessary for investigatory or control purposes.

vi) Suitable antivirus software must be properly installed and running on all devices.

vii) Any device used to access, store or process sensitive information must encrypt data transferred over the network (e.g. using SSL or a VPN)

viii) Devices used for BYOD will receive limited support on a 'best endeavours' basis for academic purposes only.

ix) While employees have a reasonable expectation of privacy over their personal information on their own equipment, the University's right to control its data and manage devices may occasionally result in support personnel unintentionally gaining access to their personal information. To reduce the possibility of such disclosure, device users are advised to keep their personal data separate from University data on the device in separate directories, clearly named (e.g. "Private" and "BYOD").

x) Care should be taken to avoid infringement of other people's privacy rights, for example use of someone else's devices to make unauthorized audio-visual recordings at work.

2.1.3.4 **Unacceptable Use**

The following activities are, in general, prohibited. Employees and students may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services). Under no circumstances is an employee or student of Mukuba University authorized to engage in any activity that is illegal under local, or international law while utilizing Mukuba University-owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

i) Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Mukuba University.

ii) Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Mukuba University or the end user does not have an active license is strictly prohibited.

iii) Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. CICT should be consulted prior to export of any material that is in question.

iv) Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

v) Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

vi) Using a Mukuba University computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.

vii) Making fraudulent offers of products, items, or services originating from any Mukuba University account.

viii) Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

ix) Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee or student is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

x) Port scanning or security scanning is expressly prohibited unless prior notification to Mukuba University is made.

xi) Executing any form of network monitoring which will intercept data not intended for the employee's or student's host, unless this activity is a part of the employee's normal job/duty.

xii) Circumventing user authentication or security of any host, network or account.

xiii) Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).

xiv) Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

xv) Providing information about, or lists of, Mukuba University employees to parties outside Mukuba University.

2.1.4 Enforcement

Any employee or student found to have violated this policy may be subject to disciplinary action, up to and including termination of employment or expulsion from the University in case of students.

2.2.0 RESPONSIBLE USE OF INFORMATION TECHNOLOGY POLICY

2.2.1 Overview

Information and Communication Technology provides important and critical means for both public and private communication at Mukuba University. Access to information technology is essential to Mukuba University's mission of providing the students, faculty and staff with educational and research resources of the highest quality.

The principle of academic freedom shall apply to public communication in all these forms of communication, as well as in the transmission of information in both the physical and virtual environments, however, users and systems administrators shall respect the privacy of person-to-person communications in all forms including telephone, electronic mail and file transfers, video and graphics, and television to the fullest extent possible under applicable law and policy.

The preservation of those resources for Mukuba University community requires that each staff member, student or other authorized user comply with institutional policies, responsible use of technical resources and applicable laws.

Authorized users of ICT resources shall be faculty, staff, student and other affiliated individuals or organizations authorized through CICT.

2.2.2 Purpose

The purpose of this policy is to outline the responsible use of information hosted on ICT systems at Mukuba University. These rules are in place to protect the employee and Mukuba University. Inappropriate use exposes Mukuba University to risks such as of loss of institution's integrity, loss of strategic data and including litigations.

2.2.3 Scope

This policy applies to employees, contractors, consultants, temporaries, and other workers at Mukuba University, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by Mukuba University.

2.2.4 Policy

Notwithstanding the geographical location of the user, authorized use of University-owned or operated computing and network resources shall be consistent with the teaching, learning, research and public service mission of Mukuba University and consistent with this policy.

2.2.4.1 Subject to requirements of network administration, Mukuba University shall not monitor or restrict the content of material posted on university-owned computers, or transported across its networks. However, Mukuba University reserves the right to:

i) Limit access to its networks and remove access to content or to material residing on or transmitted on university-owned computers or networks when severe circumstances arise (i.e., evidence of a reported violation of applicable university policies, contractual).

ii) Determination of violations shall be made in accordance with established applicable due process procedures (i.e., student code of conduct, collective bargaining agreement, academic and administrative grievances and appeals policies, as appropriate).

iii) In the normal course of system maintenance, both preventative and troubleshooting, staff members operating the computer systems may be required to view files. Staff shall be required to maintain the confidentiality and privacy of information in such files unless otherwise required by law or university policy.

iv) Upon reasonable cause for suspicion, to access all aspects of its computing systems and networks, including individual login sessions to determine if a user is violating this policy or state laws.

2.2.4.2 A university member who stores or distributes copyrighted material must be the copyright holder or have the permission of the copyright holder as required under law. This

includes duplication of audios, videos, pictures, illustrations, computer software, and all other information for educational use or any other purpose.

2.2.4.3 No user may, under any circumstances, use Mukuba University computing equipment, software or networks to harass or defame any other person or organization.

2.2.4.4 Security and privacy of e-mail.

i) Access:- The university recognizes the private nature of electronic mail communications. The university may access such files in the course of its normal supervision of the network or system (i.e., backing up of electronic messaging material), or when severe circumstances arise (i.e., evidence of reported violations of policies or laws). Accordingly, the private nature of electronic mail communications sent or received by users on any computer system owned or operated by the university shall be maintained, subject to the technology limitations of Mukuba University's electronic systems and in a manner consistent with the University polices, and local laws.

ii) Public records request:- From time to time the university may receive requests pursuant to local laws. When such requests are for access to a user's e-mail files, the university will make a good faith effort to notify the affected user. A good faith effort may include, though not be limited to, an e-mail message sent to the affected user's university e-mail address or telephone notice, including a message left on the university-based voice mail system.

2.2.4.5 Administration of responsible use of Information Technology

To ensure compliance with the University policy on responsible use of information technology, the following will apply:-

i) University assigned accounts (UserID). Computer and network access accounts are for the personal use of that individual only. Accounts are to be used for the university-related activities for which they are assigned.

ii) Sharing of access. Computer accounts. Passwords, and other types of authorization are assigned to individual users and should not be shared with others. Individual users are responsible for the use of their accounts. If an account is shared or the password divulged, the holder of the account may lose all account privileges and be held personally responsible for any actions that arise from the misuse of the account.

iii) Unauthorized access. Individual users may not run or otherwise configure software or hardware to intentionally allow access by unauthorized users.

iv) Termination of access. When individual users cease being a member of the campus community (i.e., withdraw, student, or terminate employment or otherwise leave the university), or if an individual user is assigned a new position and/or responsibilities within Mukuba University, access authorization may be reviewed. Users must not use facilities, accounts, access codes, privileges or information for which they are not authorized.

v) Circumventing security. Users are prohibited from attempting to circumvent or subvert any system's security measures. Users are prohibited from using any computer program or device to intercept or decode passwords or similar access control information.

vi) Breaching security. Deliberate attempts to degrade the performance of a computer system or network or to deprive authorized personnel of resources or access to any Mukuba University computer or network is prohibited. Breach of security includes, but is not limited to, the following:

(a) Creating or knowingly propagating viruses;
(b) Hacking;
(c) Password cracking;
(d) Unauthorized viewing of other's files;
(e) Willful modification of hardware and software installations.

vii) Abuse of campus computer resources is prohibited and includes, but is not limited to:
(a) Unauthorized monitoring. A user may not use computer resources for unauthorized monitoring of electronic communications.
(b) Spamming. Posting a personal or private commercial message to multiple list servers, distribution lists or news groups with the intention of reaching as many users as possible is prohibited.
(c) Private commercial purposes. The computing and networking resources of campus shall not be used for personal or private commercial purposes or for financial gain.

2.2.4.6 Guidelines on Anti-Virus Process

Recommended processes to prevent virus problems:

i) Always run the institutional standard, supported anti-virus software is available from the institution download site. Download and run the current version; download and install anti-virus software updates as they become available.

ii) NEVER open any files or macros attached to an email from an unknown, suspicious or untrustworthy source. Delete these attachments immediately, then "double delete" them by emptying your Trash.

iii) Delete spam, chain, and other junk email without forwarding, inline with Mukuba University's Acceptable Use Policy.

iv) Never download files from unknown or suspicious sources.

v) Avoid direct disk sharing with read/write access unless there is absolutely a business requirement to do so.

vi) Always scan a flash/Hard drive from an unknown source for viruses before using it.

vii) Back-up critical data and system configurations on a regular basis and store the data in a safe place.

viii) If lab testing conflicts with anti-virus software, run the anti-virus utility to ensure a clean machine, disable the software, then run the lab test. After the lab test, enable the anti-

virus software. When the anti-virus software is disabled, do not run any applications that could transfer a virus, e.g., email or file sharing. If in doubt Contact CICT for assistance.

New viruses are discovered almost every day. Periodically check the "*Lab Anti-Virus Guidelines"* for updates or contact CICT.

2.2.5 Enforcement

Users who violate this policy may be denied access to university computing resources and may be subject to other penalties and disciplinary action, both within and outside of the university. The university may temporarily suspend or block access to an account, prior to the initiation or completion of such procedures, when it reasonably appears necessary to do so in order to protect the integrity, security or functionality of university or other computing resources or to protect the university from liability. The university may also refer suspected violations of applicable law to appropriate law enforcement agencies.

2.3.0 ELECTRONIC COMMUNICATIONS POLICY

2.3.1 Overview

Mukuba University is committed to using the most advanced technologies available to communicate with all its stakeholders and general public. It recognizes an expanding reliance on electronic communication among students, faculty, staff, and the administration due to the convenience, speed, cost-effectiveness, and environmental advantages of using electronic communication.

2.3.2 Purpose

The electronic communications policy will provide procedures and regulations to govern the use of electronic communications between the university and its stakeholders. Electronic communications may include, but are not limited to, electronic mail, electronic bulletin boards, and information portals.

2.3.3 Scope

This policy covers appropriate use of any communications platform sent from a Mukuba University registered account such as email address or and applies to all employees, vendors, and agents operating on behalf of Mukuba University.

2.3.4 Policy

2.3.4.1 **E-mail Accounts will be assigned to:**

i) All New students, upon registration for any programme offered by Mukuba University

ii) All Members of members of staff.

iii) Partners and agents operating on behalf of Mukuba University may, depending on the nature of collaboration.

2.3.4.2 **Student Email Accounts;-**

i) Mukuba University will maintain a student's email account for the life of the student to facilitate communication as an alumnus, or until such time that a former student requests that the account be closed.

ii) A university-assigned student email account shall be an official university means of communication with all students at Mukuba University. Students are responsible for all information sent to them via their university assigned email account. If a student chooses to forward their university email account, he or she is responsible for all information, including attachments, sent to any other email account.

iii) The student is expected use the University electronic communications, which include, but are not limited to, email and information portals. To stay current with university information, students are expected to check their official university email account and other electronic communications on a frequent and consistent basis. Recognizing that some communications may be time-critical, the University recommends that electronic communications be checked minimally twice a week.

iv) Distribution of mass communication to all students or targeted communication to a specific subset of students shall be restricted to Mukuba University departments for university business. External requests will not be honored.

v) A faculty may determine how email and other electronic communications will be used in their classes and it is recommended that faculty expectations of all electronic communication requirements be specified in their course syllabus. Faculty should expect that students are accessing official electronic communications and should use such communications for their courses accordingly.

2.3.4.3 **Prohibited Use :-**

Mukuba University email system shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any emails with this content from any Mukuba University employee should report the matter to CICT immediately.

2.3.4.4 **Prohibited E-mail and Electronic Communications Activities:-**

i) Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).

ii) Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.

iii) Unauthorized use, or forging, of email header information.

iv) Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

v) Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

vi) Use of unsolicited email originating from within Mukuba University's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Mukuba University or connected via Mukuba University's network.

vii) Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

2.3.4.5 **Personal Use:-**
Using a reasonable amount of Mukuba University resources for personal emails is acceptable, but non-work related email shall be saved in a separate folder from work related email. Sending chain letters or joke emails from a Mukuba University email account is prohibited. Virus or other malware warnings and mass mailings from Mukuba University shall be approved by CICT before sending. These restrictions also apply to the forwarding of mail received by a Mukuba University employee.

2.3.4.6 **Monitoring:-**
Mukuba University employees shall have no expectation of privacy in anything they store, send or receive on the company's email system. Mukuba University may monitor messages without prior notice. Mukuba University is not obliged to monitor email messages.

2.3.5 Enforcement
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.
Any student found to have violated this policy may be subject to disciplinary action, up to and including suspension or expulsion from Mukuba University.

2.4.0 SOCIAL MEDIA POLICY

2.4.1 Overview
The term "social media" refers to a set of online tools that supports social interaction among users. These include but not restricted to Facebook, Twitter, Flicker, YouTube, Instagram, TikTok etc. Social media has radically changed the way we communicate and interact. It offers opportunities to connect and engage with a range of key stakeholder groups including prospective and current students, alumni, staff, donors, partners, research collaborators and friends of the University.

Mukuba University currently has social media presence on Facebook, and Twitter and is in, the process of broadening presence through other social media networks. The University welcomes the use of social media to facilitate knowledge and information sharing, among users and the general public.

2.4.2 Purpose

This Policy is intended to assist the University to achieve maximum benefits while minimizing risks of social media networking. This Policy aims to exert positive influence and help shape the online social behavior of the University community in physical and virtual spaces while using facilities that are owned and/or controlled by the University. The University recognizes that inappropriate use of social media has the potential to damage its image, reputation since the lines between personal position and institutional position can be blurred on social media platforms.

This Policy outlines the University's position on the appropriate use of social media by members of its community. It seeks to clarify how best to enhance and protect personal and professional reputations when participating in social media. It serves to facilitate and encourage the proper use of social media while sensitizing users about the risks of antisocial activity with a view to protecting the University from liability that may be incurred when members of the community misuse the University's Information and Communications Technology (ICT) systems.

2.4.3 Scope

The policy applies to all Mukuba University employees and students including all personnel affiliated with third parties. It also applies to all Mukuba University Social Media Sites and to the activities permitted by these sites, whether they are current or future. Examples include weblog posts (blogging), event updates, news updates, chats, discussion boards/posts, photo/video sharing, music and radio broadcasts and gaming.

2.4.4 Policy

2.4.4.1 **Use of Mukuba University Marks:-**

Mukuba University Marks include; The Mukuba University name, and all other words, logos, signs or any other marks whether registered or not, that belong to or are associated with Mukuba University.

i) Use of Mukuba University Marks without permission is illegal. CICT Directorate is the authorized agency (acting on behalf of the University Registrar) from which persons or entities wishing to use Mukuba University Marks should seek permission.

ii) Mukuba University Marks shall only be used on social media sites designated as "Mukuba University Social Media Sites"

Applicable Laws:- Persons making postings shall respect the laws relating to copyright and other intellectual property rights, defamation, privacy, and other applicable laws.

2.4.4.2 **Content:-** Compliance with other Mukuba University policies

i) Information published on social media sites should conform to all applicable Mukuba University policies, including but not limited to:
   - Acceptable Use Policy
   - Acceptable Information and Communication,
   - Electronic Mail and Messaging Services Policy
   - Policy on Intellectual Property

- Policy on Gender Issues
- Web Publishing Policy

ii) Content posted by users shall conform to the University's principles of confidentiality and information disclosure which are included in the relevant rules and regulations for both staff and students. Considerations when discussing work-related activities on social media taking into account the following guidelines:-
   a) Content posted on any social media site should conform to the tenets of good taste.
   b) There shall be no posting of biased statements on matters such as politics, religion, race, gender, sexual orientation, nationality or disability.
   c) There shall be no posting of statements that contain obscenities or vulgarities or that can cause anxiety and panic.
   d) Statements posted should follow Mukuba University's non-biased position and be respectful at all times.

iii) Users should note that all Mukuba University Social Media Sites represent Mukuba University. Therefore, content providers must ensure that information placed on any Mukuba University Social Media Site is accurate and represents the values of the University.

iv) Users are reminded of their duties and obligations to maintain staff, student and third party confidentiality and shall not use social media sites to transmit or discuss confidential information.

2.4.4.3 **Compliance Requirements**

i) This policy does not include matters related to the use of social media to support teaching and learning at Mukuba University.

ii) Mukuba University entities, lecturers or other personnel interested in supporting their taught courses with social media should not initially seek to establish separate social media accounts, but should first determine whether existing facilities may be utilized and should contact CICT.

iii) Mukuba University entities, lecturers or other personnel already using social media for teaching and learning should have their sites reviewed/assessed by CICT to ensure compliance with the University's policies.

iv) Mukuba University entities, lecturers or other personnel already using social media for purposes other than teaching and learning should have their sites reviewed/assessed by CICT.

v) Any user desirous of using social media should consult CICT for appropriate guidance prior to use.

2.4.5 Enforcement

Where there is evidence of misuse of social media, Mukuba University may restrict or prohibit the use of its ICT resources and/or, where appropriate, and may apply other penalties and disciplinary action, both within and outside of the university.

2.5.0 WEB PUBLISHING POLICY

2.5.1 Overview

Mukuba University's web presence is essential to its mission of teaching, learning, research and public service. However, any information published to a web server can potentially be viewed, copied, and redistributed by anyone who can access it via a web browser.

Specific requirements for the proper protection and handling of sensitive and confidential information in any medium by members of Mukuba University community are described in the University's Information Sensitivity policy document.

This Web Publishing Policy document is not intended as a style guide for the look and feel of web pages, nor does it address areas of web page design or branding

2.5.2 Purpose

The University's Web Publishing Policy seeks to establish standards and guidelines that will:-

Support the vision, mission, goals and values of the University.
Facilitate the official business of the University and appropriate online transactions while maintaining the necessary level of security and privacy.
Facilitate advancement of Mukuba University's unique institutional brand identity, as defined in the Mukuba University positioning platform.
Outline mechanisms for maintaining the integrity and security of confidential/sensitive information that for legitimate business or pedagogical reasons must be stored on or accessed via a campus web server.
Assist web publishers in developing sites that comply with university policies, rules, and regulations, and all applicable laws.
Outline Web Account creation procedures to ensure that only those individuals with proper authorization can publish content to web servers in the mukuba.edu.zm domain.

2.5.3 Scope

This policy document applies to:

i) Mukuba University's official website, http://www.mukuba.edu.zm

ii) All web pages located on servers within the mukuba.edu.zm domain.

iii) University-affiliated sites outside of the montclair.edu domain using approved Mukuba University trademarked or copyrighted materials, images, logos, etc.

iv) Web pages of Application Service Providers (ASPs) or vendors that have contracted with the University to deliver online services. Examples include, but are not limited to, online learning management systems and vendor "portals" for procurement of equipment, services, and supplies.

v) Faculty, staff, and student pages located on any server or device connected to the Campus network that is capable of delivering web content.

vi) Individuals who have been assigned custodial rights to a departmental web publishing account.

2.5.4 Policy

Web publishers are responsible for the content of the pages they publish and are expected to abide by the highest standards of quality and responsibility. These responsibilities apply to all publishers, whether they are campuses, departments, student or employee organizations, or individuals.

i) All web content must conform to the University's Information Sensitivity Policy document. Among other things, this means that sensitive University information including, but not limited to, student records, financial records, or any other confidential or private information may not be displayed on publicly-accessible web pages or stored on a web server in unencrypted form.

ii) Web pages may only be published to a server on the campus network using an CICT-authorized user account. Examples of authorized user accounts and any departmental or application-specific logins created by CICT for the purposes of web content publishing.

iii) All accounts used for web publishing shall conform to the University's Account Management and Password Policies.

iv) Any website or online form that requests a username and password for authentication must do so over a secure (SSL/TLS) connection for both the username/password entry and the actual form submission process.

v) A web site's home page should clearly identify the person or unit responsible for its creation and maintenance. It is recommended that any sub-pages linked from the site's home page should contain similar information.

2.5.4.1 Campus and Departmental Web Pages

Non-CICT web servers that are maintained and operated by a campus or department are subject to all University policies regarding server configuration, security, account management, and content as defined in the following policy documents:

i) Network Connectivity Policy

ii) Account Management Policy

iii) Password Management Policy

iv) Information Sensitivity Policy

Departments choosing to maintain web sites on independent servers are responsible for the security and maintenance of the servers and web sites.

At the University's discretion, Campus and Departmental web server may be included in the University's overall search engine indexing and website statistics gathering processes.

2.5.4.2 Personal Web Pages

There are numerous services available on the campus community that facilitate the publishing of personal web pages. Some examples include:

i) Mukuba University Web "public html" folders available to all faculty, staff, and students with an active Mukuba University NetID.

ii) Faculty/staff cover pages on the main University website.

iii) The Online Learning Management System (course content, student portfolios, discussion groups.)

iv) Various college and departmental web servers that allow personal web pages.

v) Personal computers with web server software installed (note: access to these web servers is restricted by the University's firewall to on-campus traffic only.)

Individuals who utilize one or more of the above services to publish web content are subject to all of the policies herein, as well as all other University computing policies, and laws

2.5.4.3 Copyright

i) All web publishers are required to respect the intellectual and creative property rights of others and abide by all applicable policies and guidelines for fair use of copyrighted materials.

ii) Copyright and ownership of internet materials, whether original or derived works, created or developed by Mukuba University staff, faculty or students are prescribed by Mukuba University contractual agreements or policies regarding intellectual property.

iii) No web page can contain any copyrighted or trademarked material without permission except as permitted by law. Photographs, drawings, video clips or sound clips may not be used on a page without permission of the person who created them or the entity owning the rights except as permitted by law.

iv) Limited commercial sponsorship is permitted on web sites covered by this policy if all of the following conditions are met:

   a) The commercial entity must be sponsored by a department or unit of the university;

   b) A commercial sponsorship agreement must be signed by the commercial entity, approved at the Registrar level and reviewed by university counsel;

   c) Commercial sponsorship must meet the requirements set forth in the appropriate section of the guide to web standards.

   d) Use of logos, trademarks or other identifying elements not associated with the University should be avoided except as noted in paragraph (a) to (c) above. Hosting of commercial sponsor's web pages or web sites is prohibited.

2.5.4.4 Online forms and Transactional Web Pages

Campuses, departments, and administrative units have a legitimate need to collect and process information using online forms and transactional web pages. Some examples include online registration, applications for financial aid, post graduate applications, event/seminar registration, and surveys. The following rules apply to any online form or transactional web page, whether it is hosted on an CICT operated web server, campus or departmental web server, or an individual's web server.

i) Individual (personal) web pages may NOT be used to gather personally identifiable information such Mukuba University's NetIDs and passwords, social security numbers, home address, or any other personal identity information as defined by applicable laws.

ii) Campuses, departments, and administrative units needing to gather personal identity information may only do so using web forms or transaction systems that have been provided by CICT for this purpose or have been evaluated by CICT for security and privacy compliance.

iii) Any online form or transactional website must clearly state on the site what will be done with the information collected, and provide a link to the University's Privacy Policy.

iv) All transactional websites must comply with University policies regarding server configuration, security, account management, and content, as defined in i), ii) and iii) above.

v) Online forms and transactional websites should only collect the minimum amount of information that is required to complete the form or transaction.

vi) Where possible, give users the option of not identifying themselves.

vii) Clearly state who is collecting the information and provide context so that users are aware why it is being collected.

viii) Use and disclose personal information only for the primary purpose for which it was collected, and in accordance with the University's Information Sensitivity policy.

2.5.5 Enforcement

Users who violate this policy may be denied access to university computing resources and may be subject to other penalties and disciplinary action, both within and outside of the university. Violations will normally be handled through the university disciplinary procedures applicable to the relevant user.

All requirements and restrictions in any other Mukuba University policies remain in force and are not considered superseded by this policy.

2.6.0 INFORMATION SENSITIVITY POLICY

2.6.1 Overview

The information covered in these guidelines includes, but is not limited to, information that is either stored or shared via any means. This includes: electronic information, information on paper, and information shared orally or visually (such as telephone and video conferencing).

All employees should familiarize themselves with the information labeling and handling guidelines of the University. It should be noted that the sensitivity level definitions were created as guidelines and to emphasize common sense steps that you can take to protect Mukuba University Confidential information (e.g., Mukuba University Confidential information should not be left unattended in conference rooms).

Questions about the proper classification of a specific piece of information should be addressed to the Dean, Head of Department or Registrar.

2.6.2 Purpose

The Information Sensitivity Policy is intended to help employees determine what information can be disclosed to non-employees, as well as the relative sensitivity of information that should not be disclosed outside of Mukuba University without proper authorization.

2.6.3 Scope

All Mukuba University information is categorized into two main classifications:

i) Mukuba University Public

ii) Mukuba University Confidential

Mukuba University Public information is information that has been declared public knowledge by someone with the authority to do so, and can freely be given to anyone without any possible damage to Mukuba University.

Mukuba University Confidential contains all other information. It is a continuum, in that it is understood that some information is more sensitive than other information, and should be protected in a more secure manner. Included is information that should be protected very closely, such as trade secrets, development programs, potential acquisition targets, and other information integral to the success of our company. Also included in Mukuba University Confidential is information that is less critical, such as telephone directories, general institution information, personnel information, etc., which does not require as stringent a degree of protection.

A subset of Mukuba University Confidential information is "Mukuba University Third Party Confidential" information. This is confidential information belonging or pertaining to another corporation which has been entrusted to Mukuba University by that company under non-disclosure agreements and other contracts. Examples of this type of information include everything from joint development efforts to vendor lists, customer orders, and supplier information. Information in this category ranges from extremely sensitive to information about

the fact that we've connected a supplier/vendor into Mukuba University's network to support our operations.

Mukuba University personnel are encouraged to use common sense judgment in securing Mukuba University Confidential information to the proper extent. If an employee is uncertain of the sensitivity of a particular piece of information, he/she should contact their Head of Department or Registrar.

2.6.4 Policy

The Sensitivity Guidelines below provides details on how to protect information at varying sensitivity levels. Use these guidelines as a reference only, as Mukuba University Confidential information in each column may necessitate more or less stringent measures of protection depending upon the circumstances and the nature of the Mukuba University Confidential information in question.

2.6.4.1 Minimal Sensitivity:

General institution information; some personnel and technical information, and intellectual property.

Marking guidelines for information in hardcopy or electronic form.

Marking is at the discretion of the owner or custodian of the information. If marking is desired, the words *"Mukuba University Confidential"* may be written or designated in a conspicuous place on or in the information in question. Other labels that may be used include *"Mukuba University Proprietary"* or similar labels at the discretion of your school or business unit. Even if no marking is present, Mukuba University information is presumed to be *"Mukuba University Confidential"* unless expressly determined to be Mukuba University Public information by a Mukuba University employee with authority to do so. Any of these markings may be used with the additional annotation of *"3rd Party Confidential"*.

i) **Access:** Mukuba University employees, contractors, people with a business need to know.

ii) **Distribution within Mukuba University:** Standard interoffice mail, approved electronic mail and electronic file transmission methods.

iii) **Distribution outside of Mukuba University internal mail**: Hard Copies, Postal mail and other public or private carriers, approved electronic mail and electronic file transmission methods.

iv) **Electronic distribution:** No restrictions to approved recipients within Mukuba University, but should be encrypted or sent via a private link to approved recipients outside of Mukuba University premises.

v) **Storage:** Keep from view of unauthorized people; erase whiteboards, do not leave in view on tabletop. Machines should be administered with security in mind. Protect from loss; electronic information should have individual access controls where possible and appropriate.

vi) **Disposal/Destruction:** Deposit outdated paper information in specially marked disposal bins on Mukuba University premises; ***electronic data should be expunged. Reliably erase or physically destroy media.***

2.6.4.2 More Sensitivity:
This will comprise detailed curricular of programs, Business, financial, technical, and most personnel information.

Marking guidelines for information in hardcopy or electronic form.

As the sensitivity level of the information increases, you may, in addition or instead of marking the information *"Mukuba University Confidential" or "Mukuba University Proprietary"*, wish to label the information *"Mukuba University Internal Use Only" or* other similar labels at the discretion of the school or department to denote a more sensitive level of information. Any of these markings may be used with the additional annotation of *"3rd Party Confidential"*. However, marking is discretionary at all times.

i) **Access**: Mukuba University employees and non-employees with signed non-disclosure agreements who have a business need to know.

ii) **Distribution outside of Mukuba University internal mail**: Sent via Postal mail or approved private carriers.

iii) **Storage:** Individual access controls are highly recommended for electronic information.

iv) **Disposal/Destruction:** In specially marked disposal bins on Mukuba University premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media.

2.6.4.3 **Most Sensitive:**
All information related to examinations, Trade secrets & marketing, operational, personnel, financial, source code, & technical information integral to the success of the University

Marking guidelines for information in hardcopy or electronic form.

To indicate that Mukuba University Confidential information is very sensitive, you may should label the information *"Mukuba University Internal: Registered and Restricted", "Mukuba University Confidential", "Mukuba University Private and Confidential" or* similar labels at the discretion of the school or department. Any of these markings may be used with the additional annotation of *"3rd Party Confidential"*. Once again, this type of Mukuba University Confidential information need not be marked, but users should be aware that this information is very sensitive and be protected as such.

i) **Access:** Only those individuals (Mukuba University employees and non-employees) designated with approved access and signed non-disclosure agreements.

ii) **Distribution within Mukuba University:** Delivered direct - signature required, envelopes stamped confidential, or approved electronic file transmission methods.

iii) **Distribution outside of Mukuba University internal mail:** Delivered direct; signature required; approved private carriers.

iv) **Electronic distribution:** No restrictions to approved recipients within Mukuba University, but it is highly recommended that all information be strongly encrypted.

v) **Storage:** Individual access controls are very highly recommended for electronic information. Physical security is generally used, and information should be stored in a physically secured computer.

vi) **Disposal/Destruction:** Strongly Encouraged: In specially marked disposal bins on Mukuba University premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media.

2.6.4.4 Appropriate measures

Mukuba University Information System Resources include, but are not limited to, all computers, their data and programs, as well as all paper information and any information at the Internal Use Only level and above.

To minimize risk to Mukuba University from an outside business connection. Mukuba University computer use by external personnel and unauthorized personnel must be restricted so that, in the event of an attempt to access Mukuba University institution information, the amount of information at risk is minimized.

i) **Configuration of Mukuba University-to-other business connections**

Connections shall be set up to allow other businesses to see only what they need to see. This involves setting up both applications and network configurations to allow access to only what is necessary.

ii) **Approved Electronic File Transmission Methods**

Includes supported FTP clients and Web browsers.

iii) **Approved Electronic Mail**

Includes all mail systems supported by the CICT

iv) **Approved Encrypted email and files**

Techniques include the use of DES and PGP. DES encryption is available via many different public domain packages on all platforms. Contact CICT for more details.

v) **Expunge**

To reliably erase or expunge data on a PC or Mac you must use a separate program to overwrite data. Otherwise, the PC or Mac's normal erasure routine keeps the data intact until overwritten. The same thing happens on computers running UNIX, however, data is much more difficult to retrieve on UNIX systems.

vi) **Individual Access Controls**

Individual Access Controls are methods of electronically protecting files from being accessed by people other than those specifically designated by the owner. On UNIX machines, this is

accomplished by careful use of the chmod command (use *man chmod* to find out more about it). On Mac's and PC's, this includes using passwords on screensavers, such as Disklock.

vii) **Insecure Internet Links**
Insecure Internet Links are all network links that originate from a locale or travel over lines that are not totally under the control of Mukuba University.

viii) **Encryption**
Secure Mukuba University Sensitive information in accordance with the *Encryption Policy*. International issues regarding encryption are complex. Follow institution guidelines on export controls on cryptography, and consult CICT for further guidance.

ix) **One Time Password Authentication**
One Time Password Authentication on Internet connections is accomplished by using a one-time password token to connect to Mukuba University's internal network over the Internet. Contact your support organization for more information on how to set this up.

x) **Physical Security**
Physical security means either having actual possession of a computer at all times, or locking the computer in an unusable state to an object that is immovable. Methods of accomplishing this include having a special key to unlock the computer so it can be used, thereby ensuring that the computer cannot be simply rebooted to get around the protection. If it is a laptop or other portable computer, never leave it alone in a conference room, hotel room or on an airplane seat, etc. Make arrangements to lock the device in a hotel safe, or take it with you. In the office, always use a lockdown cable. When leaving the office for the day, secure the laptop and any other sensitive material in a locked drawer or cabinet.

2.6.5 Enforcement

Penalty for deliberate or inadvertent disclosure: Any employee or student found to have violated this policy may be subject to disciplinary action up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

3.0 CICT TECHNICAL POLICIES

The ICT Technical Policies provide guidelines on implementation and management of ICT services by CICT to ensure security, operational efficiency and effectiveness.

3.1.0 PASSWORD POLICY

3.1.1 Purpose

This policy forms part of information governance policy framework. Passwords are a key method in protecting the data for which we are responsible. Good password choices defend the institution from loss or theft of data and protect you from impersonation and identity theft.

3.1.2 Scope

This Policy applies to, but is not limited to, all staff, students, partners, contractual third parties and agents of the university. The policy sets out the minimum standards everyone must adhere to when making decisions about passwords.

3.1.3 Policy

3.1.3.1 General Passwords Protection Standards

i) A Password must be at least 6 Characters long and contain characters from three of the following four categories:
   - English uppercase characters (A through Z)
   - English lowercase characters (a through z)
   - Numbers 0 to 9
   - Non-alphabetic characters (for example,!, $, #, %)'

ii) Always use different passwords from the ones you use in your personal life or for other organisations.

iii) Always use different passwords for the various systems within the organisation.

iv) Do not share your passwords with anyone, including administrative assistants or secretaries.

v) All passwords are to be treated as sensitive, confidential information. (Exceptions to this are during ICT Support sessions, where the password must be changed afterwards).

vi) Passwords should never be written down or stored on-line without encryption.

vii) Do not reveal a password in email, chat, or other electronic communication. Do not reveal a password on questionnaires or security forms.

viii) If an unauthorised person requests a password, or there are other suspicious circumstances, do not provide the password. Report the request immediately to the CICT Service Desk.

ix) If an account or password compromise is suspected, the password must be changed and the incident reported to the CICT Service Desk promptly.

x) Occasionally, for troubleshooting purposes an ICT Technician may temporarily change a user's password to something both the ICT Technician and the user know in order to assist with support or diagnosis as a short term measure. All password reset requests must be recorded by CICT.

3.1.3.2 System Administrative Passwords

System administrative passwords for Mukuba University ICT Services and facilities are to be generated and managed by the CICT Officers responsible for ICT Service, facility or infrastructure management.

i) Administrative passwords must be kept secret from any person who is not responsible for the management of an ICT Service, facility or infrastructure item.

ii) All administrative passwords must meet the following minimum standard in construction:
- Contain eight **(8)** characters or more; and
- English uppercase characters (A through Z)
- English lowercase characters (a through z)
- Numbers 0 to 9
- Non-alphabetic characters such as ?,!, $, #, %,@

iii) Administrative passwords will have a maximum age of six (6) months and will be changed during the closest administrative windows.

iv) Administrative passwords must not be used on multiple occasions, and where possible systems should monitor password history. Upon change of the administrative password, a new random password should be generated following the rules defined in this Procedure.

v) Administrative passwords must be kept in a secure, locked space, accessible only by members of the University who have been appointed to a systems administration role.

vi) Administrative passwords must be changed if the following events occur:
   a) Breach of system, or administrative account, through external/internal attack, or compromised external connection;
   b) Member of the systems administrator team leaves the University, or transfers to another faculty or department;
   c) Unauthorised access to password storage space;
   d) Improper storage, or handling, of administrative passwords;
   e) Password ageing window is met.

3.1.4 Enforcement

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

3.2.0 BACKUP AND RECOVERY POLICY

3.2.1 Purpose

The purpose of this policy is to ensure that procedures and processes are defined for backup and recovery of data and files to ensure uninterrupted continuity of the business of the University. A backup policy sets forth the importance of data and system backups, defines the ground rules for planning, executing and validating backups and includes specific activities to ensure that critical data is backed up to secure storage media located in a secure location.

3.2.2 Scope

Mukuba University Backup and Recovery Policy defines the objectives, accountability, and application of backup and recovery of data held in the technology environment of all University Schools, departments and units. The Policy sets schedules whereby information from business applications such as Oracle, Microsoft SQL, email server databases and user files are copied to disk/cloud to ensure data recoverability in the event of accidental data deletion, corrupted information or some kind of a system outage

This document applies to the entire information security management system scope, and to all personal data processing activities.

The policy addresses the following key areas:

i) To define and apply a clear backup and restore standard for all University's information systems.

ii) To define backup and recovery standards per data prioritization.

iii) To prevent the loss of data in the case of an accidental deletion or corruption of data, system failure, or disaster.

iv) To permit timely restoration of information and business processes, should such events occur.

v) To manage secure backup and restoration processes and the media employed in the process.

vi) To set the retention periods of information contained within system level backups designed for recoverability and provide a point-in-time snapshot of information as it existed during the time-period defined by system backup policies.

3.2.3 Policy

Performing proper backup, storage, and handling of data is necessary for all departments to achieve their objectives.

Users of this policy are staff of CICT who must accurately follow the policy and protect the availability, confidentiality, and integrity of data.

3.2.3.1 BACKUP SERVICES AND CONTROLS

The policy applies to the following services and controls:-

i) Corporate file services:
   - Mukuba University's Sensitive / Confidential institution data.
   - Mukuba University's Sensitive / Confidential customer data.

ii) Corporate source control services:
   - Mukuba University's intellectual property data.

iii) Corporate configuration files:
   - Network device configuration files (e.g.: WiFi Router, WiFi Access Points, Institution Firewall, Managed Switches, Routers.)

iv) Corporate internal services:
   - Critical services configurations.
   - Critical resources OS system states.

v) Customers' production applications:
   - These are Mukuba University's hosted application production deployments serving customers' needs and holding customer's data.

3.2.3.2 Protection of Backup Data.

i) The appropriate team must perform backups for data they are responsible to protect.

ii) Backup copies must be stored in an environmentally-protected and access-controlled secure location offsite from the location of the originating asset.

iii) Stored copies must be stored with a short description that includes the following information; Backup date / Resource name / type of backup method (Full/Incremental)

iv) Stored copies of data must be made available upon authorized request.

v) The request for stored data must be approved by an authorized person nominated by a Director/Manager in the appropriate department. Requests for stored data must include:
   a) A completed form that outlines the specifics of the request, including what copy is being requested, where and when the requester would like it delivered, and why they are requesting the copy.
   b) Acknowledgement that the backup copy will be returned or destroyed promptly upon completion of its use.
   c) Submission of a return receipt as evidence that the backup copy has been returned.

vi) A record of physical and logical movements of backup media must be maintained. This includes the following information:
   a) All identification information relating to the requested copies.
   b) Purpose of the request.
   c) Information about person requesting the copy.
   d) Authorization for the request.
   e) Where the copy will be held while it is out of storage.
   f) When the copy was released from storage.
   g) When the copy will be returned to storage

vii) Backup copies must be maintained in accordance with Mukuba University's Retention and Disposal Schedule for backup copies, or as stipulated by specific customer requirements or laws. The schedule will determine the status of the information, as to whether it can be disposed, cycled back into production, or remain in archive storage

3.2.3.3 Disposal of Backup Media

All backup media must be appropriately disposed of. Prior to retirement and disposal, CICT will ensure that:

i) The media no longer contains active or backup images.

ii) The media's current or former contents cannot be read or recovered by an unauthorized party.

iii) As with all backup media, CICT will ensure the physical destruction of media prior to disposal in accordance with University disposal policy and laws

3.2.3.4 Backup Recovery Capability Checks

All relevant department backups should be verified periodically, and a report created on its ability to recover data (relevant for Logical/Cloud based backup procedure). On a quarterly basis, log information generated from each backup job will be reviewed for the following purposes:-

i) To check for and correct errors.

ii) To monitor the duration of the backup job.

iii) To optimize backup performance where possible.

iv) CICT will identify problems and take corrective action to reduce any risks associated with failed backups.

v) Random test restores will be done once every 6 months in order to verify that backups have been successful.

vi) CICT will maintain records demonstrating the review of logs and test restores so as to demonstrate compliance with this policy for auditing purposes.

vii) Every quarter the Backup Operators shall report on its ability to recover data (relevant for physical storage media).

viii) CICT will conduct a Backup recovery exercise. The ability to recover data shall be measured by ability to retrieve backup media sample (copies). The ability or inability to recover data shall be reported to the departments via the quarterly Directors reporting process.

3.2.3.5 Backup Schedules

CICT is responsible for backing up internally-hosted institution information systems. The unit should maintain the following backup schedule:-

i) Network file shares:
- Weekly Full backup
- Daily Incremental backup

ii) Source control:
- Daily Incremental backup
- Weekly Full backup

iii) Configuration files:
- Monthly Full backup
- Relevant backup initiated by configuration changes.

iv) Internal services and data (license server, etc.):
- Daily Incremental backup
- Weekly Full backup

v) CORE Production Systems
- Backed up via Windows/Amazon/Oracle Relational Databases Automated Backups.
- Backup retention period 31 days.
- Amazon RDS automated backup provides an ability to restore to any point in time during backup, a prior retention period up to 5 minutes.

vi) Application System
- Hourly DB transaction log backup.
- Daily ERP System Volume Snapshot.
- Weekly Full backup saved on ERP System volume (local disk).
- Weekly on disk backups retention period 1 week.
- Effective combined backup retention period is 31 days.

vii) Governance Risk and Compliance Applications
- Hourly DB transaction log backup.
- Daily ERP Volume Snapshot.
- Weekly Full backup saved on ERP volume (local disk).
- Weekly on disk backups retention period 1 week.
- Effective combined backup retention period is 31 days.

3.2.4 Enforcement

CICT is responsible for executing this policy.

3.3.0 LAB ANTI-VIRUS POLICY

3.3.1 Purpose
To establish requirements which must be met by all computers connected to Mukuba University lab networks to ensure effective virus detection and prevention.

3.3.2 Scope
This policy applies to all Mukuba University lab computers that are PC-based or utilize PC-file directory sharing. This includes, but is not limited to, desktop computers, laptop computers, file/ftp/tftp/proxy servers, and any PC based lab equipment such as traffic generators.

3.3.3 Policy
All Mukuba University PC-based lab computers must have Mukuba University's standard, supported anti-virus software installed and scheduled to run at regular intervals. In addition, the anti-virus software and the virus pattern files must be kept up-to-date. Virus-infected computers must be removed from the network until they are verified as virus-free. IT End-User Administrators are responsible for creating procedures that ensure anti-virus software is run at regular intervals, and computers are verified as virus-free. Any activities with the intention to create and/or distribute malicious programs into Mukuba University's networks (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) are prohibited, in accordance with the *Acceptable Use Policy*.

Refer to "*Lab Anti-Virus Guidelines"* to help prevent virus problems.

Noted exceptions: Machines with operating systems other than those based on Microsoft products are excepted at the current time.

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

3.4.0 DATABASE (DB) PASSWORD POLICY

3.4.1 Purpose
This policy states the requirements for securely storing and retrieving database usernames and passwords (i.e., database credentials) for use by a program that will access a database running on one of Mukuba University's networks.

Computer programs running on Mukuba University's networks often require the use of one of the many internal database servers. In order to access one of these databases, a program must authenticate to the database by presenting acceptable credentials. The database privileges that

the credentials are meant to restrict can be compromised when the credentials are improperly stored.

3.4.2 Scope

This policy applies to all software that will access a Mukuba University, multi-user production database.

3.4.3 Policy

3.4.3.1 General

In order to maintain the security of Mukuba University's internal databases, access by software programs must be granted only after authentication with credentials. The credentials used for this authentication must not reside in the main, executing body of the program's source code in clear text. Database credentials must not be stored in a location that can be accessed through a web server.

3.4.3.2 Storage of Data Base User Names and Passwords

i) Database user names and passwords may be stored in a file separate from the executing body of the program's code. This file must not be world readable.

ii) Database credentials may reside on the database server. In this case, a hash number identifying the credentials may be stored in the executing body of the program's code.

iii) Database credentials may be stored as part of an authentication server (i.e., an entitlement directory), such as an LDAP server used for user authentication. Database authentication may occur on behalf of a program as part of the user authentication process at the authentication server. In this case, there is no need for programmatic use of database credentials.

iv) Database credentials may not reside in the documents tree of a web server.

v) Pass through authentication (i.e., Oracle OPS$ authentication) must not allow access to the database based solely upon a remote user's authentication on the remote host.

vi) Passwords or pass phrases used to access a database must adhere to the *Password Policy*.

3.4.3.3 Retrieval of Database User Names and Passwords

i) If stored in a file that is not source code, then database user names and passwords must be read from the file immediately prior to use. Immediately following database authentication, the memory containing the user name and password must be released or cleared.

ii) The scope into which you may store database credentials must be physically separated from the other areas of your code, e.g., the credentials must be in a separate source file. The file that contains the credentials must contain no other code but the credentials (i.e., the user name and password) and any functions, routines, or methods that will be used to access the credentials.

iii) For languages that execute from source code, the credentials' source file must not reside in the same browseable or executable file directory tree in which the executing body of code resides.

3.4.3.4 Access to Database User Names and Passwords

i) Every program or every collection of programs implementing a single business function must have unique database credentials. Sharing of credentials between programs is not allowed.

ii) Database passwords used by programs are system-level passwords as defined by the *Password Policy*.

iii) Developer groups must have a process in place to ensure that database passwords are controlled and changed in accordance with the *Password Policy*. This process must include a method for restricting knowledge of database passwords to a need-to-know basis.

3.4.4 Enforcement

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

3.5.0 ENCRYPTION POLICY

3.5.1 Purpose

The purpose of this policy is to provide guidance that limits the use of encryption to those algorithms that have received substantial public review and have been proven to work effectively. Additionally, this policy provides direction to ensure that local regulations are followed, and legal authority is granted for the dissemination and use of encryption technologies outside of the country.

3.5.2 Scope

This policy applies to all Mukuba University employees and affiliates.

3.5.3 Policy

Proven, standard algorithms such as DES, Blowfish, RSA, RC5 and IDEA should be used as the basis for encryption technologies. These algorithms represent the actual cipher used for an approved application. For example, Network Associate's Pretty Good Privacy (PGP) uses a combination of IDEA and RSA or Diffie-Hellman, while Secure Socket Layer (SSL) uses RSA encryption. Symmetric cryptosystem key lengths must be at least 56 bits. Asymmetric crypto-system keys must be of a length that yields equivalent strength. Mukuba University’s key length requirements will be reviewed annually and upgraded as technology allows.

The use of proprietary encryption algorithms is not allowed for any purpose, unless reviewed by qualified experts outside of the vendor in question and approved by Mukuba University as per encryption technology laws of the country.

3.5.4 Enforcement

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

3.6.0 ICT SECURITY POLICY

3.6.1 Purpose

The purpose of this document is to specify the security requirements of Mukuba University's ICT Services and Facilities to ensure the availability and integrity of information assets and supporting infrastructure.

3.6.2 Scope

This policy applies to all Mukuba University staff, students and associates. It outlines procedures to minimize the exposure of Mukuba University to risk, ensure the security of ICT Services and Facilities, information assets and associated infrastructure and provide direction and support for ICT Security Management.

3.6.3 Policy

It is the University's policy that the ICT Services, Facilities and Infrastructure it manages, inclusive of all electronic information, shall be appropriately secured against breaches of confidentiality and integrity of information or interruptions to the availability of the ICT services, facilities and infrastructure.

3.6.3.1 Access Control

Mukuba University provides public and university ICT Services. Public ICT Services are considered to be those available to non-University personnel including, but not limited to, the University's publicly available web site and some services offered by the University Library. University ICT Services include all ICT Services offered in support of learning, teaching and research, and operational business and all ICT Facilities and Infrastructure which support those ICT Services.

iii) Access to ICT Services and Facilities

University ICT Services are considered to be those offered to University members in support of learning, teaching research and business operations. Access to these ICT services, and supporting ICT facilities and infrastructure is restricted to Authorised Users

only. The conditions of access to University ICT Services for Authorised Users are defined in Acceptable Use and Responsible Use Policies.

ii) Logical Access to ICT Services, Facilities and Infrastructure
All access to University ICT Services and Facilities must incorporate appropriate authentication controls refer to Password Policy.

iii) Operating System Access Control
Where technically feasible, password protected inactivity time-outs shall be implemented for terminals and workstations. The period of inactivity shall be no longer than twenty minutes in publicly accessible areas. Where a workstation is not publicly accessible, inactivity time-outs may be extended beyond twenty minutes. Security mechanisms at the operating system level shall be used to restrict access to computer resources. The mechanisms must be capable of:

- Identifying and verifying the identity and, if necessary, the terminal or location of each Authorised User
- Recording successful and failed system accesses
- Providing appropriate means for authentication. If a password management system is used, it shall enforce the use of strong passwords
- Where appropriate, restricting the connection times of Users.

iv) Application Systems Security
Facilities shall be used to restrict access within application systems. Logical access to software and information shall be restricted to Authorised Users. Application systems shall:

- Control user access to application system functions
- Provide protection from unauthorised access by any software or device utility that is capable of overriding system or application access controls
- Not compromise the security of other systems or applications.

v) Network Access
Access to the University's ICT Services, Facilities and Infrastructure is limited to Authorised Users except where limited access is provided to the public. Devices which are considered or known to send generally undesirable transmissions are to be blocked from access to the University network.

vi) External Access to University Resources
The encryption of outbound communications must be commensurate with the level of classification of information that is being sent. Refer to Information Sensitivity and Encryption Policies.

vii) Physical Access to ICT Services, Facilities and Infrastructure.
Physical access to ICT Facilities is managed through the University's security arrangements. Access to buildings and computing laboratories is at the discretion of the relevant facility administrators. Hosting of ICT Facilities and Infrastructure on campus must be undertaken as per the provisions of the ICT physical security procedure.

a) All communications rooms and cabinets (Server Rooms) shall be locked at all times.
b) Entry to communications rooms and cabinets (Server Rooms), and interference with ICT network equipment is strictly prohibited.

c) Other than in an emergency, access to communications rooms, cabinets (Server Rooms) and ICT network equipment shall be restricted to designated members of staff of CICT.
d) Access to the server room, system console and server or drives of the production servers shall be restricted to authorised specialised CICT staff only
e) Contractors shall observe any specific access conditions which apply within the areas in which they will be working. These access conditions include, in all cases, that contractors working in main server rooms shall be accompanied by appropriate University ICT personnel.

viii) Security of Information Assets
Information assets within the University must have a nominated custodian. This Data Custodian will be responsible for implementing this policy in relation to the information assets for which they are accountable.

ix) Data Archiving and Recovery
All Mukuba University Corporate and Research data shall be archived as per the requirements of applicable legislations and University policy.

3.6.3.2 Monitoring of ICT Services, Facilities and Infrastructure

Mukuba University provides members with access to ICT Services, Facilities and Infrastructure in support of teaching and learning, research activities, and in support of University business. These services, facilities and infrastructure are provided on condition that members meet the requirements described in the ICT Security Framework. ICT Security. In order to ensure compliance with University Policies, Procedures and Guidelines and relevant State legislation, the University may collect information related to the use of ICT services, facilities and infrastructure.

i) Usage of ICT Services, Facilities, and Infrastructure shall be monitored Information related to the usage of ICT Services, Facilities and Infrastructure may be consulted to investigate and ensure compliance with legislation and policies, or may be used for the purposes of: operations, maintenance, audit, quality of service, identifying inappropriate, excessive or unauthorized usage and for the purpose of litigation and criminal investigation. System logs and audit trails from application systems, networks, and computer systems shall, where appropriate, be aggregated and filtered to assist in the identification of incidents. To ensure the accuracy of and the ability to compare audit logs, procedures shall be in place to ensure all systems have synchronized clocks.

ii) Monitoring of University Members.
Monitoring of University staff, students and associates shall be carried out only in accordance with appropriate legislation, regulation and policies.

iii) Development and Modification of Facilities and Services ICT Services.
Facilities and Infrastructure are controlled by a Senior CICT Officer. No changes may be made to any ICT services, facilities or infrastructure without the approval of a Senior CICT Officer. Any authorised changes to ICT services, facilities and infrastructure must meet the requirements set out in this policy and other relevant University policies.

3.6.3.3 Development of Services and Facilities

Development of new of Mukuba University ICT services and facilities must be approved by an appropriate Senior CICT Officer.

3.6.3.4 Modifications of ICT Services and Facilities and ICT Infrastructure

Modifications to ICT services, facilities and infrastructure must be made by an authorized ICT Officer. Infrastructure failing to meet these specifications may only be connected following approval from CICT. The current status and configuration of any ICT service, facility or infrastructure item should also be recorded.

3.6.3.5 ICT Security Governance

The ICT Security Framework provides guidance and control over ICT services, facilities and infrastructure and defines the rights and responsibilities of University members in their use of ICT services and facilities.

The ICT Security Framework is subject to change, via a process of review and revision, to ensure ICT Security Risks are mitigated and that the framework remains relevant to the strategic goals of the University. Processes of risk assessment, audit, and incident management and response will provide input into the review and revision cycle, and the framework will align with the Business Continuity Processes of the University.

i) Risk Management

Mukuba University Risk Management Policy defines the processes adopted by the University in identifying, analysing, prioritising and treating risks. The ICT Security Framework adopts the University's processes and regular Risk Management activities will be undertaken. Where the Risk Management process requires changes to be made to the ICT Security Framework, these changes will be performed as part of the review and revision cycle of the ICT Security Framework.

Risk assessment activities will occur:

a) annually
b) after a serious ICT Security incident that highlights vulnerabilities
c) when cumulative updates indicate that the risk assessment requires a review
d) when an event, or series of events indicate(s) that a review is required (i.e. these could include incidents, events elsewhere, changes to business operations etc.)
e) where Infrastructure changes, such as technology and/or software upgrades;
f) following a change in business requirements
g) following a change in University Ordinances, Rules or Policies
h) following a change in legislation.

ii) Audit

Audit of ICT Security controls and the ICT Security Framework will occur in line with the requirements of the University Internal Audit. The results of any audit of the ICT Security Framework, or part thereof, may be used for review and revision, or may be used to assess compliance with the ICT Security Framework.

iii) Business Continuity Planning

The ICT Security Framework will align with the Business Continuity Plans of the University. The ICT Security Framework will meet the Business Continuity requirements by ensuring the application of appropriate security and availability controls on ICT Services, Facilities and Infrastructure.

iv) Disaster Recovery Planning

All critical ICT Services covered under the ICT Security Framework will be supported by disaster recovery plans. Disaster recovery plans for ICT Facilities and Infrastructure that support critical ICT Services will also be required under the ICT Security Framework. Disaster recovery planning will be performed in conjunction with the University's Business Continuity Planning processes, however it is also mandatory for any critical ICT Service, Facility of Infrastructure item not covered under that process. Refer to Backup and Recovery Policy

v) Incident Response Procedure

The ICT Security Framework will align with the Critical Incident Response Procedures of the University and of IT Services. The Framework will meet the ICT Security requirements of those processes, and will compliment and facilitate the action plans of those documents.

vi) Security Incident Management Procedure

Security Incident Management Procedures will cover any breach of the ICT Security Framework. Procedures may vary depending on the severity of the incident, but can include:

a) evaluation of an incident
b) classification of an incident
c) investigation procedures
d) escalation processes
e) notification of appropriate people regarding the incident
f) immediate mitigation processes
g) review procedures regarding the incident itself, the wider risks involved, and effect on the ICT Security Framework.

vii) Information Privacy

Related to the use of University of ICT Services and Facilities is collected and may be consulted to ensure compliance with University policies, procedures and guidelines, and relevant State and Federal legislation. This information may be accessed for purposes of investigating allegations of misuse. Information may be provided to law enforcement agencies where necessary to investigate or report suspected unlawful activity, as per the University Privacy Policy.

3.6.4 Enforcement

Breaches Breach of this policy may result in disciplinary actions, as provided for under the applicable Employment Agreements and ordinances. Staff, students and associates learning of any violation of this policy are obligated to bring this matter to the attention of an appropriate staff member within the University without delay.

3.7.0 REMOTE ACCESS POLICY

3.7.1 Purpose
The purpose of this policy is to define standards for connecting to Mukuba University's network from any host. These standards are designed to minimize the potential exposure to Mukuba University from damages which may result from unauthorized use of Mukuba University resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical Mukuba University internal systems, etc.

3.7.2 Scope
This policy applies to all Mukuba University employees, contractors, vendors and agents with a Mukuba University-owned or personally-owned computer or workstation used to connect to the Mukuba University network. This policy applies to remote access connections used to do work on behalf of Mukuba University, including reading or sending email and viewing intranet web resources.

Remote access implementations that are covered by this policy include, but are not limited to, dial-in modems, frame relay, ISDN, DSL, VPN, SSH, and cable modems, etc.

3.7.3 Policy
It is the responsibility of Mukuba University employees, contractors, vendors and agents with remote access privileges to Mukuba University's network to ensure that their remote access connection is given the same consideration as the user's on-site connection to Mukuba University. General access to the Internet for recreational use by immediate household members through the Mukuba University Network on personal computers is permitted for employees that have flat-rate services. A Mukuba University employee is responsible to ensure the family member does not violate any Mukuba University policies, does not perform illegal activities, and does not use the access for outside business interests. The employee of Mukuba University bears responsibility for the consequences should the access be misused.

3.7.3.1 Please review the following policies for details of protecting information when accessing the institution network via remote access methods, and acceptable use of Mukuba University's network:

i) *Encryption Policy*
ii) *Remote Access Policy*
iii) *Wireless Communications Policy*
iv) *Acceptable Use Policy*

For additional information regarding Mukuba University's remote access connection options, including how to order or disconnect service, cost comparisons, troubleshooting, etc., go to the Remote Access Services website.

3.7.3.2 **Requirements**

i) Secure remote access must be strictly controlled. Control will be enforced via one-time password authentication or public/private keys with strong pass-phrases. For information on creating a strong pass-phrase. Refer to the Password Policy.

ii) At no time should any Mukuba University employee provide their login or email password to anyone, not even family members.

iii) Mukuba University employees and contractors with remote access privileges must ensure that their Mukuba University-owned or personal computer or workstation, which is remotely connected to Mukuba University's 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.

iv) Mukuba University employees and contractors with remote access privileges to Mukuba University's network must not use non-Mukuba University email accounts (i.e., Hotmail, Yahoo, Gmail), or other external resources to conduct Mukuba University business, thereby ensuring that official business is never confused with personal business.

v) Routers for dedicated ISDN lines configured for access to the Mukuba University network must meet minimum authentication requirements of CHAP.

vi) Reconfiguration of a home user's equipment for the purpose of split-tunneling or dual homing is not permitted at any time.

vii) Frame Relay must meet minimum authentication requirements of DLCI standards.

viii) Non-standard hardware configurations must be approved by Remote Access Services, and CICT must approve security configurations for access to hardware.

ix) All hosts that are connected to Mukuba University internal networks via remote access technologies must use the most up-to-date anti-virus software (place url to institution software site here), this includes personal computers. Third party connections must comply with requirements as stated in the *Third Party Agreement.*

x) Personal equipment that is used to connect to Mukuba University's networks must meet the requirements of Mukuba University-owned equipment for remote access.

xi) Organizations or individuals who wish to implement non-standard Remote Access solutions to the Mukuba University production network must obtain prior approval from CICT.

3.7.4 Enforcement

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

3.8.0 WIRELESS COMMUNICATION POLICY

3.8.1 Purpose

This policy prohibits access to Mukuba University networks via unsecured wireless communication mechanisms. Only wireless systems that meet the criteria of this policy or have

been granted an exclusive waiver by CICT are approved for connectivity to Mukuba University's networks.

3.8.2 Scope

This policy covers all wireless data communication devices (e.g., personal computers, cellular phones, PDAs, etc.) connected to any of Mukuba University's internal networks. This includes any form of wireless communication device capable of transmitting packet data. Wireless devices and/or networks without any connectivity to Mukuba University's networks do not fall under the purview of this policy.

3.8.3 Policy

3.8.3.1 Register Access Points and Cards

All wireless Access Points / Base Stations connected to the University's network must be registered and approved by CICT. These Access Points / Base Stations are subject to periodic penetration tests and audits. All wireless Network Interface Cards (i.e., PC cards) used in University laptop or desktop computers must be registered with CICT

3.8.3.2 Approved Technology

All wireless LAN access must use corporate-approved vendor products and security configurations.

3.8.3.3 VPN Encryption and Authentication

All computers with wireless LAN devices must utilize a University-approved Virtual Private Network (VPN) configured to drop all unauthenticated and unencrypted traffic. To comply with this policy, wireless implementations must maintain point to point hardware encryption of at least 56 bits. All implementations must support a hardware address that can be registered and tracked, i.e., a MAC address. All implementations must support and employ strong user authentication which checks against an external database such as TACACS+, RADIUS or something similar.

3.8.3.4 Setting the SSID

The SSID shall be configured so that it does not contain any identifying information about the organization, such as the company name, division title, employee name, or product identifier.

3.8.4 Enforcement

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

3.9.0 DE-MILITARIZED ZONE (DMZ) LAB SECURITY POLICY

3.9.1 Purpose

This policy establishes information security requirements for all networks and equipment deployed in Mukuba University labs located on the "De-Militarized Zone" (DMZ). Adherence

to these requirements will minimize the potential risk to Mukuba University from the damage to public image caused by unauthorized use of Mukuba University resources, and the loss of sensitive/institution confidential data and intellectual property.

3.9.2 Scope

Mukuba University Lab networks and devices (including but not limited to routers, switches, hosts, etc.) that are Internet facing and located outside Mukuba University Internet firewalls are considered part of the DMZ Labs and are subject to this policy. This includes DMZ Labs in primary Internet Service Provider (ISP) locations and remote locations. All existing and future equipment, which falls under the scope of this policy, must be configured according to the referenced documents. This policy does not apply to labs residing inside Mukuba University's Internet firewalls. Standards for these labs are defined in the *Internal Lab Security Policy*

3.9.3 Policy

3.9.3.1 Ownership and Responsibilities

i) All new DMZ Labs must present a business justification with sign-off at the business unit Vice President level. Mukuba University must keep the business justifications on file.

ii) Lab owning organizations are responsible for assigning lab managers, point of contact (POC), and back up POC, for each lab. The lab owners must maintain up to date POC information with Mukuba University. Lab managers or their backup must be available around-the-clock for emergencies.

iii) Changes to the connectivity and/or purpose of existing DMZ Labs and establishment of new DMZ Labs must be requested through a Mukuba University Network Support Organization and approved by Mukuba University.

iv) All ISP connections must be maintained by a Mukuba University Network Support Organization.

v) A Network Support Organization must maintain a firewall device between the DMZ Lab(s) and the Internet.

vi) The Network Support Organization and Mukuba University reserve the right to interrupt lab connections if a security concern exists.

vii) The DMZ Lab will provide and maintain network devices deployed in the DMZ Lab up to the Network Support Organization point of demarcation.

viii) The Network Support Organization must record all DMZ Lab address spaces and current contact information.

ix) The DMZ Lab Managers are ultimately responsible for their DMZ Labs complying with this policy.

x) Immediate access to equipment and system logs must be granted to members of Mukuba University and the Network Support Organization upon request.

xi) Individual lab accounts must be deleted within three (3) days when access is no longer authorized. Group account passwords must comply with the *Password Policy* and must be changed within three (3) days from a change in the group membership.

xii) Mukuba University will address non-compliance waiver requests on a case-by-case basis.

3.9.3.2 General Configuration Requirements

i) Production resources must not depend upon resources on the DMZ Lab networks.

ii) DMZ Labs must not be connected to Mukuba University's internal networks, either directly or via a wireless connection.

iii) DMZ Labs should be in a physically separate room from any internal networks. If this is not possible, the equipment must be in a locked rack with limited access. In addition, the Lab Manager must maintain a list of who has access to the equipment.

iv) Lab Managers are responsible for complying with the following related policies:
- *Password Policy*
- *Wireless Communications Policy*
- *Lab Anti-Virus Policy*

v) The Network Support Organization maintained firewall devices must be configured in accordance with least-access principles and the DMZ Lab business needs. All firewall filters will be maintained by Mukuba University.

vi) The firewall device must be the only access point between the DMZ Lab and the rest of Mukuba University's networks and/or the Internet. Any form of cross-connection which bypasses the firewall device is strictly prohibited.

vii) Original firewall configurations and any changes thereto must be reviewed and approved by Mukuba University (including both general configurations and rule sets). Mukuba University may require additional security measures as needed.

viii) Traffic from DMZ Labs to the Mukuba University internal network, including VPN access, falls under the *Remote Access Policy*

ix) All routers and switches not used for testing and/or training must conform to the DMZ Router and Switch standardization documents.

x) Operating systems of all hosts internal to the DMZ Lab running Internet Services must be configured to the secure host installation and configuration standards. (Add url link to site where your internal configuration standards are kept).

xi) Current applicable security patches/hot-fixes for any applications that are Internet services must be applied. Administrative owner groups must have processes in place to stay current on appropriate patches/hotfixes.

xii) All applicable security patches/hot-fixes recommended by the vendor must be installed. Administrative owner groups must have processes in place to stay current on appropriate patches/hotfixes.

xiii) Services and applications not serving business requirements must be disabled.

xiv) Mukuba University Confidential information is prohibited on equipment in labs where non-Mukuba University personnel have physical access (e.g., training labs), in accordance with the *Information Sensitivity Policy*

xv) Remote administration must be performed over secure channels (e.g., encrypted network connections using SSH or IPSEC) or console access independent from the DMZ networks.

3.9.4 Enforcement

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

3.10.0 INTERNET DE-MILITARIZED ZONE (DMZ) EQUIPMENT POLICY

3.10.1 Purpose

The purpose of this policy is to define standards to be met by all equipment owned and/or operated by Mukuba University located outside Mukuba University's Internet firewalls. These standards are designed to minimize the potential exposure to Mukuba University from the loss of sensitive or institution confidential data, intellectual property, damage to public image etc., which may follow from unauthorized use of Mukuba University resources.

Devices that are Internet facing and outside the Mukuba University firewall are considered part of the "de-militarized zone" and are subject to this policy. These devices (network and host) are particularly vulnerable to attack from the Internet since they reside outside the institution firewalls.

The policy defines the following standards:

i) Ownership responsibility

ii) Secure configuration requirements

iii) Operational requirements

iv) Change control requirement

3.10.2 Scope

All equipment or devices deployed in a DMZ owned and/or operated by Mukuba University (including hosts, routers, switches, etc.) and/or registered in any Domain Name System (DNS) domain owned by Mukuba University, must follow this policy.

This policy also covers any host device outsourced or hosted at external/third-party service providers, if that equipment resides in the Mukuba University domain or appears to be owned by Mukuba University.

All new equipment which falls under the scope of this policy must be configured according to the referenced configuration documents, unless a waiver is obtained from CICT. All existing and future equipment deployed on Mukuba University's un-trusted networks must comply with this policy.

3.10.3 Policy

3.10.3.1 Ownership and Responsibilities

Equipment and applications within the scope of this policy must be administered by support groups approved by CICT for DMZ system, application, and/or network management.

Support groups will be responsible for the following:

i) Equipment must be documented in the institution wide enterprise management system. At a minimum, the following information is required:
   - Host contacts and location.
   - Hardware and operating system/version.
   - Main functions and applications.
   - Password groups for privileged passwords.
   - Network interfaces must have appropriate Domain Name Server records (minimum of A and PTR records).
   - Password groups must be maintained in accordance with the institution wide password management system/process.
   - Immediate access to equipment and system logs must be granted to members of CICT upon demand, per the *Audit Policy*.
   - Changes to existing equipment and deployment of new equipment must follow and institution's change management processes/procedures.

To verify compliance with this policy, CICT will periodically audit DMZ equipment per the *Audit Policy*.

3.10.3.2 General Configuration Policy

All equipment must comply with the following configuration policy:

i) Hardware, operating systems, services and applications must be approved by CICT as part of the pre-deployment review phase.
ii) Operating system configuration must be done according to the secure host and router installation and configuration standards.

iii) All patches/hot-fixes recommended by the equipment vendor and CICT must be installed. This applies to all services installed, even though those services may be temporarily or permanently disabled. Administrative owner groups must have processes in place to stay current on appropriate patches/hotfixes.

iv) Services and applications not serving business requirements must be disabled.

v) Trust relationships between systems may only be introduced according to business requirements, must be documented, and must be approved by CICT.

vi) Services and applications not for general access must be restricted by access control lists.

vii) Insecure services or protocols (as determined by CICT) must be replaced with more secure equivalents whenever such exist.

viii) Remote administration must be performed over secure channels (e.g., encrypted network connections using SSH or IPSEC) or console access independent from the DMZ networks. Where a methodology for secure channel connections is not available, one-time passwords (DES/SofToken) must be used for all access levels.

ix) All host content updates must occur over secure channels.

x) Security-related events must be logged and audit trails saved to CICT approved logs. Security related events include (but are not limited to) the following:
   a) User login failures.
   b) Failure to obtain privileged access.
   c) Access policy violations.
   d) CICT will address non-compliance waiver requests on a case-by-case basis and approve waivers if justified.

3.10.3.3 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:

i) New installations must be done via the *DMZ Equipment Deployment Process*.

ii) Configuration changes must follow the Change Management (CM) Procedures.

iii) CICT must be invited to perform system/application audits prior to the deployment of new services.

iv) CICT must be engaged, either directly or via CM, to approve all new deployments and configuration changes.

3.10.3.4 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.

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

External service providers found to have violated this policy may be subject to financial penalties, up to and including termination of contract.

3.11.0 ROUTER SECURITY POLICY

3.11.1 Purpose

This document describes a required minimal security configuration for all routers and switches connecting to a production network or used in a production capacity at or on behalf of Mukuba University.

3.11.2 Scope

All routers and switches connected to Mukuba University production networks are affected. Routers and switches within internal, secured labs are not affected. Routers and switches within DMZ areas fall under the *Internet DMZ Equipment Policy*.

3.11.3 Policy

Every router must meet the following configuration standards:

3.11.3.1 No local user accounts are configured on the router. Routers must use TACACS+ for all user authentication.

3.11.3.2 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.

3.11.3.3 Disallow the following:

i) IP directed broadcasts

ii) Incoming packets at the router sourced with invalid addresses such as RFC2103 address

iii) TCP small services

iv) UDP small services

v) All source routing

vi) All web services running on router

3.11.3.4 Use corporate standardized SNMP community strings.

3.11.3.5 Access rules are to be added as business needs arise.

3.11.3.6 The router must be included in the corporate enterprise management system with a designated point of contact.

3.11.3.7 Each router must have the following statement posted in clear view:

> "UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED. You must have explicit permission to access or configure this device. All activities performed on this device 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 this device."

3.11.4 Enforcement

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

4.0 TERMS AND DEFINITIONS

Access:
Connection of University, personal or third party owned Devices to ICT Infrastructure facilities via a direct or indirect connection method. Such connection methods could include but are not restricted to:- LAN/MAN/WAN network connections (eg Ethernet); Wireless network connections; Remote access via a third party such as a contracted ISP with trusted access to the University network; Connection via VPN (Virtual Private Networking) technology; and Connection to any systems, services and applications.

Access Control List (ACL):
Lists kept by routers to control access to or from the router for a number of services (for example, to prevent packets with a certain IP address from leaving a particular interface on the router).

Account:
A combination of a username (identifier) and password allocated by an ICT Officer to an Authorised User (the account owner) to access ICT Services, Facilities and Infrastructure.

Anti-Virus Software:
A software package designed to identify and remove known or potential computer viruses, and associated software including but not limited to virus definition files.

Asymmetric Cryptosystem:
A method of encryption in which two different keys are used: one for encrypting and one for decrypting the data (e.g., public-key encryption).

Authorised User:
An individual who has been granted access to University ICT Services under one or more of the following categories:- A current member of the governing body of the University; A currently employed officer or employee of the University; A currently-enrolled student of the University; Any person granted access to use Mukuba University ICT Services including, but not limited to:- A contractor undertaking work for the University under the provisions of a legal contract; A member of a collaborative venture in which the University is a partner

Business Critical Production Server*:*
A server that is critical to the continued business operations of the institution.

CHAP:
Challenge Handshake Authentication Protocol is an authentication method that uses a one-way hashing function. DLCIData Link Connection Identifier (DLCI) is a unique number assigned to a Permanent Virtual Circuit (PVC) end point in a frame relay network. DLCI identifies a particular PVC endpoint within a user's access channel in a frame relay network, and has local significance only to that channel.

Computer language:
A language used to generate programs.

Credentials:
Something you know (e.g., a password or pass phrase), and/or something that identifies you (e.g., a user name, a fingerprint, voiceprint, retina print). Something you know and something that identifies you are presented for authentication.

Dial-in Modem:
A peripheral device that connects computers to each other for sending communications via the telephone lines. The modem modulates the digital data of computers into analog signals to send over the telephone lines, then demodulates back into digital signals to be read by the computer on the other end; thus the name "modem" for modulator/demodulator.

DMZ (de-militarized zone):
Any un-trusted network connected to, but separated from, Mukuba University's network by a firewall, used for external (Internet/partner, etc.) access from within Mukuba University, or to provide information to external parties. Only DMZ networks connecting to the Internet fall under the scope of this policy.

DSL:
Digital Subscriber Line (DSL) is a form of high-speed Internet access competing with cable modems. DSL works over standard phone lines and supports data speeds of over 2 Mbps downstream (to the user) and slower speeds upstream (to the Internet).

Dual Homing:
Having concurrent connectivity to more than one network from a computer or network device. Examples include: Being logged into the institution network via a local Ethernet connection, and dialing into AOL or other Internet service provider (ISP). Being on a Mukuba University-provided Remote Access home network, and connecting to another network, such as a spouse's remote access. Configuring an ISDN router to dial into Mukuba University and an ISP, depending on packet destination.

Encryption:
The process of transforming information using an algorithm to render it unreadable to those without special knowledge. It is a method of securing sensitive information in accordance with the *Encryption Policy*. A "*Proprietary Encryption*" is an algorithm that has not been made public and/or has not withstood public scrutiny. The developer of the algorithm could be a vendor, an individual, or the government.

End Host Device:
An electronic device which can be connected to a network via the allocation of a network address to that device's MAC address such that this forms the only active network connection on that device. End Host Devices include, but are not limited to:- Desktop computers; Laptops; Workstations; Servers; Network Printers; Telecommunications equipment; Wireless Devices; and other network aware devices

Expunge:
To reliably erase or expunge data on a PC or Mac you must use a separate program to overwrite data, supplied as a part of Norton Utilities. Otherwise, the PC or Mac's normal erasure routine keeps the data intact until overwritten. The same thing happens on UNIX machines, but data is much more difficult to retrieve on UNIX systems

Firewall:
A device that controls access between networks., such as a PIX, a router with access control lists, or a similar security device approved by Mukuba University.

FTP:
File Transfer Protocol is a standard Internet protocol for transmitting files between computers on the Internet over TCP/IP connections. FTP is a client-server protocol where a client will ask for a file, and a local or remote server will provide it.

Frame Relay:
A method of communication that incrementally can go from the speed of an ISDN to the speed of a T1 line. Frame Relay has a flat-rate billing charge instead of a per time usage. Frame Relay connects via the telephone company's network.

Gateways:
Gateways are ICT Services for connecting privately owned devices which have been authorized through CICT.

Hash:
An algorithmically generated number that identifies a datum or its location.

ICT Infrastructure:
All electronic communication devices, networks, data storage, software, licenses, hardware, end-host devices, network connections to external resources such as ZAMREN and the Internet

Internally Connected Lab:
A lab within Mukuba University's firewall and connected to the institution production network.

Internet Services:
Services running on devices that are reachable from other devices across a network. Major Internet services include DNS, FTP, HTTP, etc.

ISDN:
Integrated Services Digital Network. It is a design for a completely digital telephone/telecommunications network to carry voice, data, images and video.

Lab Network:
A "lab network" is defined as any network used for the purposes of testing, demonstrations, training, etc. Any network that is stand-alone or firewalled off from the production network(s) and whose impairment will not cause direct loss to Mukuba University nor affect the production network

LDAP:
Lightweight Directory Access Protocol, a set of protocols for accessing information directories.

Least Access Principle:
Access to services, hosts, and networks is restricted unless otherwise permitted.

Module:
A collection of computer language instructions grouped together either logically or physically. A module may also be called a package or a class, depending upon which computer language is used.

Name Space:
A logical area of code in which the declared symbolic names are known and outside of which these names are not visible.

Network Support Organization:
Any Mukuba University-approved support organization that manages the networking of non-lab networks.

Network Support Organization Point of Demarcation:
The point at which the networking responsibility transfers from a Network Support Organization to the DMZ Lab. Usually a router or firewall.

One Time Password Authentication:
One Time Password Authentication on Internet connections is accomplished by using a one time password (OTP) token to connect to Mukuba University's internal network over the Internet.

Private Link:
A Private Link is an electronic communications path that Mukuba University has control over it's entire distance. For example, all Mukuba University networks are connected via a private link. A computer with modem connected via a standard land line (not cell phone) to another computer have established a private link. ISDN lines to employee's homes is a private link. Mukuba University also has established private links to other companies, so that all email correspondence can be sent in a more secure manner. Companies which Mukuba University has established private links include all announced acquisitions and some short-term temporary links

Production Network:
The "production network" is the network used in the daily business of Mukuba University. Any network connected to the corporate backbone, either directly or indirectly, which lacks an intervening firewall device. Any network whose impairment would result in direct loss of functionality to Mukuba University employees or impact their ability to do work.

Physical Security:
Physical security means either having actual possession of a computer at all times, or locking the computer in an unusable state to an object that is immovable. Methods of accomplishing this include having a special key to unlock the computer so it can be used, thereby ensuring that the computer cannot be simply rebooted to get around the protection. If it is a laptop or other portable computer, never leave it alone in a conference room, hotel room or on an airplane seat, etc. Make arrangements to lock the device in a hotel safe, or take it with you. In the office, always use a lockdown cable. When leaving the office for the day, secure the laptop and any other sensitive material in a locked drawer or cabinet.

Remote Access:
Any access to Mukuba University's network through a non-Mukuba University controlled network, device, or medium.

Secure Channel:
Out-of-band console management or channels using strong encryption according to the *Encryption Policy*. Non-encrypted channels must use strong user authentication (one-time passwords).

Spam:
Unauthorized and/or unsolicited electronic mass mailings.

Split-tunneling:
Simultaneous direct access to a non-Mukuba University network (such as the Internet, or a home network) from a remote device (PC, PDA, WAP phone, etc.) while connected into Mukuba University's network via a VPN tunnel.

SSL:
Secure Sockets Layer, is an encryption-based Internet security protocol. It is designed to ensure privacy, authentication, and data integrity in Internet communications.

SSID:
Service Set Identifier, is a technical term for the name given to a wireless network to distinguish it from other networks in the surrounding neighbourhood.

Symmetric Cryptosystem:
A method of encryption in which the same key is used for both encryption and decryption of the data.

Un-Trusted Network:
Any network firewalled off from the institution network to avoid impairment of production resources from irregular network traffic (lab networks), unauthorized access (partner networks, the Internet etc.), or anything else identified as a potential threat to those resources.

URL:
Uniform Resource Locator, is an address of a given unique resource on the Web. It's a text string that refers the user to a location of a web page or another resource (such as a program or a graphic document).

User Authentication:
A method by which the user of a wireless system can be verified as a legitimate user independent of the computer or operating system being used.

VPN:
Virtual Private Network (VPN) is a method for accessing a remote network via "tunneling" through the Internet.