The Open University of Tanzania

ICT Security Policy and Procedures

April, 2014

ICT Security Policy and Procedures

April, 2014

The Open University of Tanzania
P. O. Box 23409
DAR ES SALAAM
TANZANIA
Fax (255) 022-2668759
Website http://www.out.ac.tz

The Open University of Tanzania
Kawawa Road
P.O. Box 23409
Dar es Salaam
TANZANIA.

CONTENTS

Preface

Among the twenty key strategic objectives identified by The Open University of Tanzania in its vision towards delivery of affordable quality education through open and distance learning is the support and development of the ICT function within the University. In this connection, some of the objectives of the Strategic Plan for 2013/14 and 2017/18 are to: Improve Information and Communication Technology (ICT) infrastructure and services enhance teaching and learning and enhance research, consultancy and publications capacity through the use of ICT.

Clearly, this is a challenge that must be taken on board with vigour and gusto; with a clear vision and plan and with a commitment from all concerned including students, staff and management. Against this background, the Institute of Educational and Management Technologies (IEMT) -- acting on behalf of the University -- has taken its mandate of developing a blueprint that will guide in the development, implementation, and effective use of the ICT services at the University. This document is an improved version of the draft policy and procedures developed in 2006.

The ICT Security policy and procedures covers all information that are electronically generated, received, stored, printed, scanned, and typed. This document therefore seeks to provide guidelines for compliance, acceptable and secure use of information communication technology by both OUT staff, students and other OUT stakeholders.

The readers of this document are advised to refer to University strategic plan document and ICT Policy Plan document. The practices described in the ICT security policy and procedures, are in line with the University ICT policies and Master Plan guidelines.

I take this opportunity to thank the University participatory organs, and in particular, the Management Committee, The Finance and Planning Committee, The Senate and The OUT Council for thoroughly discussing this document at different stages.

Prof. Tolly Mbwette
Vice Chancellor
Open University of Tanzania

Dar-es-Salaam
April, 2014

Acknowledgements

On behalf of the OUT Management, I wish to thank all who played critical role and those who have -- in one way or another, played a role in the production of this ICT Security policy and procedures document. Special thanks are extended to the OUT management for their excellent contributions during the process of scrutiny and approval of this ICT security policy and procedures document.

It is the hope of the OUT management that staff, students and other OUT stakeholders will read and familiarize themselves with the revised ICT Security Policy and Procedures, so as to make most of what exists in the institution more secure.

Prof. Modest Varisanga
Deputy Vice Chancellor (LT & RS)
The Open University of Tanzania

Dar es Salaam
April, 2014

List of Abbreviations and Acronyms

DIEMT	Director Institute of Educational and Management Technologies
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
FINMIS	Financial Management Information System
FTP	File Transfer Protocol
HRMIS	Human Resource Management Information System
HTTP	Hypertext Transfer Protocol
ICT	Information and Communication Technology
IP	Internet Protocol
IEMT	Institute of Educational and Management Technologies
ISO	International Standard Organization
IT	Information Technology
LAN	Local Area Network
LMS	Learning Management System
MAN	Metropolitan Area Network
ODL	Open and Distance Learning
OUT	Open University of Tanzania
PC	Personal Computer
POP3	Post Office Protocol 3
SARIS	Student Academic Register Information System
SMTP	Simple Mail Transfer Protocol
SSH	Secure Shell
VPN	Virtual Private Network
WAN	Wide Area Network
WINS	Windows Internet Name Service

Introduction

The Open University of Tanzania (OUT) is an Open and Distance Learning (ODL) institution offering Certificates, Diplomas and Degrees courses. Education delivery is attained through various means of communication such as print media (study materials), Information management, network - supported by electronic platforms correspondence, enhanced face-to face, special seminars, contact programmes or a combination of any such means.

In accordance with its broader strategic objectives of Teaching, Research and Consultancy, OUT has procured and implemented at various coordination and regional centers, information and communication technologies (ICTs) that are used to create, process, store, share and disseminate data and information. These assets represent a significant economic investment by OUT. The data and information resources they create, store and disseminate could well be priceless and irreplaceable. Their continued availability in furtherance of the OUT's business is of paramount importance, hence, there is a compelling need to secure and control access to them.

Users of the university electronic systems and other stakeholders have expectations of privacy for their personal data gathered by The Open University of Tanzania in the normal course of business. Therefore there is a reasonable expectation from users that OUT would institute control to conserve the privacy of personal information. Confidentiality, Integrity and Availability of information is demanded by the university rules and regulations. Since OUT operates on a broad spectrum of the local and foreign communities by means of distance education, misuse of the institution's ICT assets could degrade its goodwill and reputation.

OUT acknowledges that there is a well-founded requirement to maintain the confidentiality, integrity and availability of its electronic data and information. Such assets must be protected from unauthorized access and intrusions, malicious misuse, inadvertent compromise and intentional damage or destruction. Accordingly, OUT is obliged to ensure that the appropriate security measures are enacted for all electronic data and information, as well as ICT equipment and processes in its domain of ownership and control.

The ICT security policy and procedures are developed as per the University ICT Policy and ICT Master Plan 2009/10 – 2013/14 to address security standards, procedures and guidelines in accordance with ISO 7799 standard.

Purpose

This security policy and procedures is prepared for the direction and use of personnel engaged in the implementation, support and use of the OUT's ICT systems and the services delivered thereon. It is intended to inform:

a) The development and implementations of rules, guidelines and code of practice to secure the OUT's systems and services.

b) The development of mechanisms that will help the University to reduce its legal risk brought about by an increasingly internal ICT usage and interconnected world.

c) The OUT community about the rules and practices pertaining to confidentiality and security of the University's ICT resources;

d) Custodians of the University ICT systems and services about their responsibilities with respect to the preservation of these systems and sanctions for non-compliance.

Scope

The policy and procedures apply to staff, students and all others granted user of the university information or related assets and defines their responsibility for the protection and appropriate use of the university information, applications, computer systems and networks. This policy applies to the mitigation of the following categories of risks:

a) Computer system availability

b) Conservation of University ICT assets

c) Confidentiality and Integrity of university data and information

d) Efficient use of University ICT resources.

The policy and procedures covers the following security domains:

a) The physical security of all computing and communication premises, computer communication equipments and appliances, transmission paths and computer peripherals.

b) The physical security of all storage media for data, system software, application software and documentation.

c) Physical security of power systems supplying electrical power to network communication and computer systems.

d) The logical security of data, information and information processing resources such as databases, computer programs, email records, servers, routers, switches and other network appliances.

Part 1

ICT Security Policy

1.1 Introduction

The purpose of this section is to guide developers and users of information and ICT resources on appropriate standards to be adopted at the University. In order for this policy to be employed effectively it is essential that those in a managerial position at The Open University of Tanzania are personally fully aware of it and apply it in their own use of ICT.

1.2 Roles and Responsibilities

ICTs are provided and deployed by the OUT to support the operational University core functions of Teaching and Learning, Research and Publications, and Consultancy and community services. They are intended to be used primarily as business tools and provide other support services.

1.3 General Control

The ICTs deployed are the property of OUT. Therefore the Vice Chancellor is the custodian of all ICT facilities and services owned by the University.

IEMT through DVC responsible to learning technologies oversee the implementation of the ICT security policy, make recommendations to DVC (LR & RS) and Vice Chancellor and report on ICT security matters. Deans/Directors/head of departments have the key responsibility within the context of this policy. Computer users are responsible for ensuring that others users do not use their privileges.

1.4 Roles

1.4.1 Deputy Vice Chancellor Learning Technologies and Regional Services

a) Take appropriate action in order to prevent breaches of the Policy.

b) Ensure that the Policy is appropriate for the protection of the University interests.

c) To ensure all students, staff and any other university stakeholders are aware of and comply with this policy.

1.4.2 Institute of Educational and Management Technologies

a) Account for all ICTs and information resources in their area of jurisdiction that is connected to the OUT networks by one or other means.

b) Provide and maintain a database of unique identifiers for all network-connected ICT assets.

c) Assess the security risk of all ICT systems and apply such security systems and processes as are consistent with mitigation of this risk.

d) Provide and/or commission the physical security of all enterprise servers, databases, backbone network switches and ICT management, teaching and learning platforms.

e) Procure, implement and maintain the logical security systems as are necessary to protect University electronic data and information assets from misuse, damage, loss or unauthorized access.

f) Develop, document and publish the ICT security guidelines in accordance with and informed by best practice.

g) Promote a security awareness campaign for users of University ICT systems and collaborate with functional departments to design and deliver end user security awareness training.

1.4.3 Deans/Directors/Heads of Departments with Functional Ownership of Data and Information Resources

a) Assess the security risk to data and information resources developed, generated and produced in their operations.

b) Determine the confidentiality requirements for data and information resources developed, generated and produced by their departments.

c) Collaborate with Institute of Educational and Management Technologies to develop and implement procedures that establish and manage privilege to access confidential data and information resources.

d) Ensure every user in their jurisdiction and span of control is informed of the security requirement

1.5 Responsibilities

a) The Vice Chancellor is responsible for ensuring that the University has adequate information security, and that the ICT policy is observed. The Vice Chancellor delegates responsibility for approving and reviewing information access and related matters to the ICT steering committee.

b) The DVC (LT &RS) is responsible for ensuring that staff, students and visitors only use ICT when they have agreed to abide by the policy. This includes staff working in collaborative partner institutions who have access to the University systems. The staff will be responsible for handling any disciplinary issues that arise and proactively investigating any suspected breaches.

c) The Director of the Institute of Educational and Management Technologies shall be responsible and accountable for all aspects of the design, implementation, administration and maintenance of all ICT security systems and the processes and procedures by which these operate. The Director has the duty to immediately suspend privilege, access and service to any user in breach of this policy pending further enquiry. Such restrictions as applied are subject to review by the appropriate superior university authority.

d) Deans, Directors and Heads of departments are responsible for enforcing the application of the security policies covering ICTs, data and information resources and for setting out local guidelines and practice documents. They are also responsible in notifying students and staff of information security practices relating to students and staff respectively.

e) Computer Users of the ICT services are responsible for maintaining the security of their interfaces to University owned ICTs, data and information resources by complying with university policies, the applicable university rules and regulations.

f) University Visitors are responsible in liaising with IEMT to determine rules governing identity management and access to ICT services and ensure that the guidelines are being followed when accessing any university ICT resources.

1.6 Access Control Management

Users of University ICTs, data and information resources shall be limited to OUT students, staff and other approved persons, for purposes that advance the objectives of teaching, learning, research, outreach and administration. These classes of users must be known to and defined in the existing gateway systems such as Human Resource Management Information System (HRMIS) for staff, Student Academic Record Information System (SARIS) or Learning Management System (LMS) for students. Any exception must be authorized by respective authority in conjunction with a head of department.

Users of the University ICT systems shall be allowed to access the systems and information appropriate to their educational and business needs through computer accounts. Passwords shall be used to validate users' identities.

1.7 Physical Security and Integrity of Systems

Appropriate barriers and controls governing the physical access to, and the maintenance of, the integrity of critical University ICT assets must be deployed commensurate with the risks identified. These risks include identified natural and environmental hazards. Barriers and controls include, but not limited to, electronic access control to servers and critical network infrastructure, installation of grillwork surrounding and enclosing video systems, fire suppression, and power management systems. Physical ICT asset include but not limited to multifunction devices, servers, communication switches, personal computers, cameras, printers, multimedia projectors, scanners, and media containing software, books and manuals.

1.8 Logical Security and Integrity of Systems

Authentication and authorization functions must be employed for all users of University electronic data and information resources. A central authentication database shall be established for all users. Procedures to manage access, authentication and authorization shall be developed to support and manage these activities. Such processes and procedures include but shall not be limited to user passwords for network and application access, biometric access mechanism and electronic key devices. For the purpose of this paragraph, computer and other electronic processes are deemed to be users.

1.8.1 Software Upgrades

All computers, switches, routers and other network-attached devices shall have the most recent approved and released software security patches installed as soon as they are generally available.

1.8 2 Malware Control

Malware is a common feature of globally connected networks. Personnel engaged in the implementation and support of the OUT's ICT systems shall take all appropriate steps to protect its ICT assets from damage, compromise or loss of confidentiality. For the purposes of this policy, malware is defined as software agents that by their action deny users the maximum capabilities of the ICT systems, compromise the security and confidentiality of university data and information or destroy or damage university ICT assets. Malware may be represented by but not limited to spyware, viruses, worms and spam.

1.8.3 Network Interconnections

Interconnections among networks are unavoidable in the ordinary course of business. These interconnections are portals for unauthorized access and entry to University networks and pose significant risk to the security of university data and information resources. Therefore all network interconnections shall be guarded, and audited by processes and such perimeter defense and intrusion detection systems, as are appropriate to manage and mitigate these risks.

1.8.4 Access to Business Critical Systems

The University is dependent on several of its major systems for its daily operations. Breaches to their unavailability for any significant period of time, could reduce the service delivery capability or place the institution in disrepute. Such systems may include the SARIS, LMS, FINMIS, HRMIS etc. Notwithstanding the general security safeguards enunciated before, these business-critical systems shall be provided with an elevated level of security. These additional measures shall include, but not limited to, internal firewalls, secondary access challenges and biometric access controls. When the security requirements are stringent enough, internal isolation of the network segment to which such systems are attached is the final consideration.

1.9 Awareness and Training

The University recognises the need for all the University ICT systems users to be aware of the ICT security threats and concerns. The IEMT will provide training programmes to enable staff and students to be better informed of the ICT security and to understand their responsibilities in the process.

The University will ensure that the ICT security policy can be accessed by all students and staff. For students, small booklets summarising what they are supposed to adhere to which will be extracted from this policy and procedure shall be prepared and made available. This shall form one of the agenda during the students' orientation.

1.10 Compliance and Exceptions

Compliance with this policy is mandatory. Each user must understand his/her role and responsibilities regarding information security issues, and protecting OUT's information asset. Any non-compliance with this security policy that results in the compromise of OUT information confidentiality, integrity and/or availability may result in disciplinary action and possible prosecution under applicable law. Any compromise or suspected compromise of this policy must be reported.

Exceptions to this policy will only be granted if an appropriate business justification for the exception is approved and the person requesting exception fully accepts the additional risk posed by the exception. The business justification describing the reason for the exception must be documented in writing, and submitted for approval by the director Institute of Educational and Management Technologies

1.11 Enforcement

This policy applies to all users of the University ICT systems and resources. It is a violation of this policy to fail to comply with security practices described in the ICT security policy and procedures. Any user who fails to adhere to the policy and procedures will be subject to penalties and disciplinary action, both within and outside the University. Violations will be handled through the University disciplinary procedures as provided for in various rules and regulations.

The University may temporarily suspend, block or restrict access to ICT resources when it reasonably appears necessary to do so in order to protect the integrity, security or functionality of University. The University may also refer suspected violations of applicable law to appropriate law enforcement agencies where necessary.

1.12 Confidentiality

The University requires that the architecture, processes and procedures surrounding applications must be such that confidentiality of University data and information is protected. Users of the University supplied or supported applications must be advised of the procedures required to maintain privacy of the University data and information.

1.12.1 Right to Monitor ICT System

Notwithstanding OUT's acknowledgement of an inherent right to privacy by users of the University-provided ICT systems, the University reserves the right to monitor, audit and interdict all electronic payloads traversing its networks or stored on its systems in furtherance of its duty to secure and retain the confidentiality of its data and information resources.

1.12.2 Localized Policies

Notwithstanding the broad elements of this policy, OUT departments may establish or seek to establish complementary policies, standards, guidelines or procedures that refine or extend the provisions of this policy and to meet specific local needs. In any event, such extensions shall comply with university regulations, ordinances and national laws.

1.12. 3 Disposal of ICT Equipments

The Institute of Educational and Management Technologies (IEMT) is mandated with the monitoring of acquisition and management of disposal of all university equipments. The University through the board of survey will develop guidelines and make recommendations for useful life spans of different equipment, salvaging, storing, donating, trashing and disposing of obsolete information technology products.

All University user (academic and administrative) units are required to avail obsolete ICT equipment to the IEMT for inspection and recommendations to the University board of survey.

Part 2

ICT Security Procedures

2.1 Introduction

The purpose of this section is to define procedures to implement the ICT security policy in part 1 of this document. It provides advice and guidance in the area of University ICT security, and put in place procedures and/or guidelines to minimize the risk associated with the use of ICT. It is meant to translate the policy into implementation in form of guidelines and procedures.

2.2 Information Systems Usage Guidelines

OUT provides Internet/Intranet access to students and staff for university business use only. The following procedures will guide staff and students to determine proper business Information systems resources usage.

2.2.1 Users and Computers Accounts

a) A staff member or a student is not allowed to share his/her account with somebody else.

b) In the use of the OUT computers the home directory for a user account must not be in the root or usr file system

c) Each user’s home directory has write to access by specific user only

d) Any user logins that have not been used for more than three months will be terminated and the data associated with that login will be archived for a maximum of six months.

e) Regular review of authorized users and their privileges shall be carried out.

f) Group login accounts are not allowed.

g) Guest accounts will be deleted or disabled within a week after expiry of its validity.

h) Retired/terminated/dismissed/suspended student or staff user accounts shall be disabled immediately.

i) Any authorized personal computer or laptop to be used on the system will have its own account.

j) Only registered personal computers and laptops can be used to gain access to the system.

k) All new ICT equipment should be reported by users to IEMT for purposes of registration.

2.2.2 Password/Pass Phrase

a) Every account must have a password/pass phrase. Administrators require passwords for every active login without exception. Users must be informed of the proper password requirements. The importance of selecting a password that is not easily determined by others (e.g. birth date, first name).

b) Users are required to enter their usernames and passwords/pass phrases in order to login to the system.

c) User password/pass phrase length must be a minimum of six characters and a system administrator password must have a minimum of eight characters (preferably a combination of numbers and characters).

d) The maximum password/pass phrase lifetime will be set. A shorter period is recommended for system administrator accounts. The last 5 passwords may not be reused.

e) All equipment and software supplied with default passwords for predefined system accounts will have to be changed immediately upon installation or upgrade.

f) Administrators will restrict the use of vendor logins. The administrator may activate a password for a vendor for a specific amount of time and for limited privileges. The administrator shall keep a record of these vendor login requests in the form of a log specifying date, time, group, and purpose of use.

g) A unique password must be assigned to each new account and each user must change his/her password immediately when using the account for the first time.

h) An authorized password checker programme will be run periodically

i) Passwords should not be communicated via e-mails

j) Password ageing should be used wherever and whenever possible. The longer a static password is used, the greater the chance that it can be compromised via a password analyzer, a personal watching keystrokes, etc.

k) Any Unix system will require a password when booting a single-user. If the console to a Unix system is not in a physically secure area, an intruder may gain root access by crashing the system and rebooting single-user. Ideally, a UNIX system should boot multi-user and password should be required when booting single-user.

l) The password to a user's account is the key to the security of information, and more generally the integrity of the University’s information systems. A user is responsible for all activities and possible misuse originating from his or her account and it is important that the password is not disclosed to anyone else, whether intentionally or accidentally.

m) Password should not be written down or permanently stored on a machine or in a database. Use Pass phrase which is easy to remember so that it cannot be easily guessed by others.

n) A user should log off from his/her computer when he/she leaves even if it is for a short time. That is Do not log in and leave your computer un-attended. Remember when you log into the system, you are responsible for all transactions thereafter, up to when you log off.

o) If a user has forgotten his/her password or must have it reset by the administrator, he/she must do it in person. (Note: Administrator does not know users passwords and has no right to know them. He/she has only the capability of re-setting passwords).

p) Users are not allowed to share their identifications and passwords. If there is a requirement to grant access to an outside user, that user must follow appropriate procedures to apply for access.

q) Both the system and application programmes must incorporate multiple levels of password protection where possible.

2.2.3 User Logins

a) All users, including system administrators must login using their personal computers (or computers they are entitled to use)

b) All logins and logouts are recorded in the system accounting file

c) There is time-out for terminal inactivity

d) Information describing previous successful and unsuccessful account login activity is displayed following successful login to help users to determine if there have been any unauthorized attempts to gain access to their accounts

e) All login failures are recorded

f) A maximum of three consecutive failed login attempts is allowed after which the account is locked out

g) An alert message is sent to the security administrator in the event of repeated login failure

h) When dial-in connections are broken, the login session is automatically terminated by the system

i) All logouts clear the terminal screen

2.2.4 The Root Account

(a) The root password is changed on an unannounced basis at least every 30 days

(b) Systems that have the capability should disable remote root login, except for the console

(c) The root password is not known by anyone other than the system administrator.

(d) For security reasons, the root password is kept in a secure storage device to which unauthorized access can be readily detected. A lock box (safe) containing a sealed envelope for each password would meet the requirements. The box is located where the administrator can notice if it had been opened. The use of this password during emergency situations is logged. In addition, once someone uses the password other than the administrator, it should be changed.

(e) Availability of the root login is limited. The administrator should ensure that the root login is only available at the console or at a secure terminal

(f) A secure method of becoming super-user is used. All administrators should login as themselves first and then **su** to root rather than login as root directly. This provides an audit trail of the root usage

2.2.5 General Usage

(a) When sensitive information is stored on a backup medium, precautions must be taken to ensure the storage is secure. Particular care should be taken to ensure physical security.

(b) Access to sensitive information should be strictly controlled when temporary staff, consultant or fieldwork students are employed.

(c) Confidential information is not to be transmitted over the Internet without proper encryption.

(d) Transmission of harassing, discriminatory or otherwise objectionable E-mail or files (as determined by the recipient) is strictly prohibited.

(e) Disruptive behavior such as introducing viruses or intentionally destroying or modifying files on the network is strictly prohibited.

(f) Any personal use of the network for commercial or illegal activity is strictly prohibited.

(g) Transmission of any religious or political messages is strictly prohibited.

(h) The usage of the University ICT resources should confirm to the University Mission and Vision and not otherwise.

2.3 Guidelines for Network Usage

The University network is critical to the University's mission, goals and operations. The purpose of these guidelines is to establish requirements for use and protection of the University network and the information transmitted via that network. Network users and administrators are responsible for following the security requirements set, and immediately reports suspected security violations to the Director Institute of Educational and Management Technologies (DIEMT).

The University network refers to those devices and communication pathways that form the campus computer and data communications infrastructure. University departments and individuals that make use of the University network and computing equipment connected to the networks are responsible for keeping the network and departmental workstations secure in accordance with this policy.

Due to the critical nature and function of the University network, the design, operation and maintenance of the network is delegated exclusively to Institute of Educational and Management Technologies (IEMT).

2.3.1 Basic Security Measures

All network users are responsible for implementing the following basic security measures with respect to their workstations:

(a) Installing a current version of anti-virus software.

(b) Running an operating system that has been recently updated and patched.

(c) Uploading all vendor-recommended security updates to their computers when prompted to do so by Patch link.

(d) Utilizing a personal firewall as recommended.

(e) Users of the University's Virtual Private Network or Wireless Network must install anti-virus software, an updated and patched operating system, and a personal firewall.

(f) Following all security measures and requirements as set forth in the ICT Security Policy and procedures.

(g) Encrypting laptop computers and other mobile devices containing confidential information.

(h) Downloading of online movies is strictly prohibited especially movies that conflict with organization objectives.

(i) Downloading from torrent website can cause harm to university network by inducing virus and malware hence should be avoided.

2.3.2 Additional Security Requirements for Wireless Network and Virtual Private Network Usage

Security threats increase when using remote access such as a Wireless Network or the Virtual Private Network (VPN). Thus, all wireless and VPN connections and transmissions are logged by Network infrastructure, and are subject to scanning by approved officials.

VPN users may use the VPN only under the following stipulations;

(a) IEMT shall limit access to the VPN to individuals who have a justifiable administrative, business, academic or research need to access University-owned systems from a remote or wireless location.

(b) VPN users who require privileged access to administrative University systems must receive written approval from their department head before access to VPN services will be granted.

(c) VPN users must use the VPN client in accordance with all university policies.

The administrator of a server for University network-connected computers is responsible for the security of that system. The administrator must monitor and log accesses and keep other system logs that could be useful in establishing the identities and actions of people, programs and processes that might use the system to breach network or system security. All servers that provide access to the University network or Internet services must require user authentication in order to restrict access. Units that operate publicly accessible computers connected to the University network must implement safe guards against network abuse appropriate to the network access available to users of those systems.

2.3.3 Information Security

(a) Data that is considered confidential must not be publicly accessible. System administrators are responsible for reasonably securing these systems so as to reduce the threat to the University as a whole.

(b) As network data transmissions are not secure, confidential data should either be encrypted separately before transmission, or a secure network transmission protocol that provides encryption automatically should be used.

(c) Departments may require individual users to be responsible for their own machines.

2.3.4 Management of Security Violations

(a) In the event IEMT judges that a LAN, a network device, or an individual user presents an immediate security risk to the University network equipment, software, or data, IEMT Network section may terminate or restrict network connection without notice.

(b) Attacks on the University network or systems are detected by University network and system administrators. Severe or ongoing attacks (such as an onslaught of unsolicited mail) may require that the source of the attack be blocked from the University network.

(c) Staff/student/visitors account that may be found as a source of attack to any University communication system shall be blocked from the use of university resources.

(d) IEMT may block a specific network address, port or application in order to protect the University against attack, or take other action as it deems necessary.

2.4 Network Documentation Guidelines

The network documentation guidelines define the level of network documentation required such as documentation of which switch ports connect to what rooms and computers. It defines who will have access to read network documentation and who will have access to change it. It also defines who will be notified when changes are made to the network. It is designed to provide for network stability by ensuring that network documentation is complete and up-to-date. This policy shall complement disaster management and recovery by ensuring that documentation is available in the event that systems should need to be rebuilt. This ICT security policy and procedures will help reduce troubleshooting time by ensuring that appropriate personnel are notified when changes are made to the network.

2.4.1 Documentation

The network structure and configuration shall be documented to provide the following information:

(a) IP addresses of all devices on the network with static IP addresses.

(b) Server documentation on all servers as outlined in the "Server Documentation" document.

(c) Network drawings showing:

   i. The locations and IP addresses of all switches, routers, and firewalls on the network.
   ii. The various security zones on the network and devices that control access between them.
   iii. The locations of every network drop and the associated switch and port on the switch supplying that connection.
   iv. The interrelationship between all network devices showing lines running between the network devices.
   v. All subnets on the network and their relationships including the range of IP addresses on all subnets and net-mask information.
   vi. All wide area network (WAN) or metropolitan area network (MAN) information including network devices connecting them and IP addresses of connecting devices.

(d) Configuration information on all network devices including (Switches, Routers, and Firewalls).

(e) Configuration shall include but not limited to:

   i. IP Address
   ii. Net-mask
   iii. Default gateway
   iv. DNS server IP addresses for primary and secondary DNS servers.
   v. Any relevant server information.

(f) Network connection information including:

   i. Types of connection to the internet or other WAN/MAN including T1, T3 frame relay.

ii. Provider of internet/WAN/MAN connection and contact information for sales and support.
iii. Configuration information including net-mask, network ID, and gateway.
iv. Physical location of where the cabling enters the building and circuit number.
v. DHCP server settings showing:
vi. Range of IP addresses assigned by all DHCP servers on all subnets.
vii. Subnet mask, default gateway, DNS server settings, WINS server settings assigned by all DHCP servers on all subnets.
viii. Lease duration time.

2.4.2 Accessing the Network Documentation

Network personnel and some ICT security staff shall have full access to all network documentation. The networking staff shall have the ability to read and modify network documentation. ICT security staff shall have access to read and suggest changes of network documentation to the network personnel. The Help desk staff shall have read access to network documentation.

2.4.3 Change Notifications

The help desk staff, server administration staff, application developers, and IEMT management shall be notified when network changes are made including.

(a) Reboot of a network device including switches, routers, and firewalls.

(b) Changes of rules or configuration of a network device including switches, routers, and firewalls.

(c) Upgrades to any software on any network device.

(d) Additions of any software on any network device.

(e) Changes to any servers which perform significant network functions whether configuration or upgrade changes are made. These servers will include (DHCP, DNS, Domain controllers and WINS)

(f) Notification shall be through email to designated groups of people.

2.4.4 Documentation Review

Institute of Educational and Management Technologies shall ensure that network documentation is kept up-to-date by performing a monthly review of documentation or designating a staff member to perform a review. The remedy or help desk requests within the last month shall be reviewed to help determine whether any network changes were made. Also any current or completed projects affecting network settings should be reviewed to determine whether there were any network changes made to support the project.

2.4.5 Storage Location

The entire OUT network documentation shall be kept in both hardcopy form and electronic form in a minimum of two places. It should be kept in two facilities (located in different OUT branches and in special software fireproof safe) so that if one facility is destroyed, information from the other facility may be used to help construct the ICT infrastructure. Information in both facilities should be updated monthly at the time of the documentation review.

2.5 Information Systems Documentation Guideline

In order for the OUT to maintain an effective operation and continue to retrieve data in the operating environment changes over time, the IEMT will be required to keep full documentation of the following;

(a) Hardware and software, including brand names, version numbers and dates of installation, upgrades, replacements, and conversions.

(b) Data structure and content, including the file layout and data dictionaries.

(c) Operating procedures, including methods for scanning or entering data; revising, updating, or expunging records; indexing; backing up disks, tapes, etc.; testing the readability of records; applying safeguards to prevent tampering and unauthorized access to protected information; and carrying out the disposition of original records.

To provide audit trails, IEMT should document procedures for logging and tracking. Full documentation of operating procedures will contribute to the legal acceptability of records management program and will help to make the data produced from optical disks admissible as evidence in legal proceedings.

2.6 Server Documentation Guidelines

These guidelines define the requirements for server documentation such as configuration information and services that are running. It defines who will have access to read server documentation and who will have access to change it. It also defines who will be notified when changes are made to the servers. It is designed to provide for network stability by ensuring that network documentation is complete and current. This ICT security procedure shall complement disaster management and recovery by ensuring that documentation is available in the event that systems should need to be rebuilt. This policy will help reduce troubleshooting time by ensuring that appropriate personnel are notified when changes are made to any servers.

2.6.1 Documentation Requirements

For all servers, a list of items that must be documented and reviewed on a monthly basis will be prepared in order to keep the OUT network secure. This list of information about every server shall be created as servers are added to the network and updated/checked every month. The list shall include but not limited to;

(a) Server name

(b) Server location

(c) The function or purpose of the server.

(d) Hardware components of the system including the make and model of each part of the system.

(e) List of software running on the server including operating system, programmes, and services running on the server.

(f) Configuration information about how the server is configured will include:

   i. Event logging settings
   ii. A comprehensive list of services that are running.
   iii. Configuration of any security lockdown tool or setting
   iv. Account settings
   v. Configuration and settings of software running on the server.

(g) Types of data stored on the server.

(h) The owners (department/functions) of the data stored on the server.

(i) Login restriction shall be in such a way that, users can only login to the servers remotely.

(j) The sensitivity of data stored on the server.

(k) Data on the server that should be backed up along with its location.

(l) Users or groups with access to data stored on the server.

(m) Administrators on the server with a list of rights of each administrator.

(n) The authentication process and protocols used for authentication for users of data on the server.

(o) The authentication process and protocols used for authentication for administrators on the server.

(p) Data encryption requirements.

(q) Authentication encryption requirements.

(r) List of users accessing data from remote locations and type of media they access data through such as internet or private network.

(s) List of administrators administering the server from remote locations and type of media they access the server through such as internet or private network (where applicable).

(t) Intrusion detection and prevention method used on the server.

(u) Latest patch to operating system and each service running.

(v) Groups or individuals with physical access to the area the server is in and the type of access, such as key or card access.

(w) Emergency recovery disk and date of last update.

(x) Disaster recovery plan and location of backup data.

(y) For the mail Server Documentation the following should be included;

    i. Account size limit where the person receives warnings about mailbox size
    ii. Account size limit where the person cannot send mail anymore.
    iii. Account size limit where the person cannot receive mail anymore.

2.6.2 Accessing the Servers

Authorized ICT server administration staff shall have full read and change access to server documentation for the server or servers they are tasked with administering. The ICT networking staff, ICT security staff, application development staff (in-house), and help desk staff shall have the ability to read all server documentation.

2.6.3 Change Notification

The help desk staff, network administration staff, application developer staff, and IT management shall be notified when changes are made to servers. Notification shall be through email to designated groups of people.

2.6.4 Documentation Review

IEMT shall ensure that server documentation is kept current by performing a monthly review of documentation or designating a staff member to perform a review. The remedy or help desk requests within the last month should be reviewed to help determine whether any server changes were made. Also any current or completed projects affecting server settings should be reviewed to determine whether there were any server changes made to support the project.

2.6.5 Storage Location

Server documentation shall be kept in both written form and electronic form in a minimum of two places. It should be kept in two facilities (located in different OUT region office) so that if one facility is destroyed, information from the other facility may be used to help construct the ICT infrastructure. Information in both facilities should be updated monthly at the time of the documentation review.

2.7 Personnel Security

Personnel security covers not only permanent and temporary staff of the University, but extends to contractors, consultants and other individuals working on the University's premises or using the University's information and information processing assets.

2.7.1 Job Descriptions

To reduce the risks resulting from errors or intentional or unintentional breach of security, all staff (permanent, part time, consultants) should be made aware of their responsibilities/obligations for implementing and maintaining effective information security controls. Clear roles and responsibilities for the security of information and information systems, should be developed and documented in their job descriptions.

2.7.2 Segregation of Duties

In the development of job descriptions, it is important to ensure that no individual has the ability to both commit and conceal an accidental or intentional breach of information security. This is best achieved by the segregation of incompatible duties or knowledge so that collusion between two or more personnel is required to conceal a security breach. Where segregation of duties is not practical, there should be adequate supervision and review of activities.

2.7.3 Recruitment

Personnel employed in the administration, operation and support of information assets or in the handling of sensitive data are often in positions of trust. They have specialist technical knowledge and business insight that places them in a unique position to abuse their job roles. More stringent screening processes should be utilized during recruitment of these personnel. Where necessary references and previous employment details of applicants should be validated and police or other security checks should be performed on applicants for sensitive positions.

2.7. 4 Termination

The University shall inform IEMT about terminated staff to be blocked from accessing University systems because a terminated staff that still has access to University's information systems is a security threat. The same measures shall be applied to suspended students through the Dean’s office. Retired staff and graduate students should be allowed to continue accessing university ICT services for a period of 30 days from the date of a staff has retired or student graduation. University associates should be allowed to continue accessing the university ICT resources for the rest of their lifetime.

2.7.5 Terms and Conditions of Employment

The terms and conditions of employment should include the Staff’s responsibilities for information security either within or outside the University, as well as the consequences of non-compliance to information security policy and procedures. As part of the terms and conditions of employment, all personnel should be required to sign confidentiality and security policy agreements (see appendix 3, 4 & 5).

2.7.6 Security Awareness and Training

Adequate training of all staff is critical to the effective implementation of information security. Security awareness and training activities should be ongoing to further demonstrate management’s commitment to information security. Information security policy and procedures are of little use unless they are understood and observed by the personnel who are affected by them. The University shall be proactive in communicating its expectations and requirements to its member of staff and students, as well as in prescribing disciplinary action for non-compliance. It is not sufficient to publish policy and assume that staff and students are aware of them, it is important to ensure that staff and students will read them and will adhere to them.

(a) Both members of staff and students shall be made aware of the importance of the information processes, the associated threats, vulnerabilities and risks and to understand why controls are needed.

(b) Members of staff and students shall be appropriately trained to perform their tasks, prior to access to systems and information being granted. Different levels of training may be required to match the requirements of their jobs.

(c) Security officers may require specialized security training or education. Periodic information security awareness seminars for staff and students shall be conducted to advice them of industry developments in information security and of new security initiatives within the University, to present case studies, and to reinforce the need for security and for complying with the university policy and procedures.

2.7.7 Working with Third Party

Controls should be in place in order to minimize the security of organizational information processing facilities and ICT assets accessed by third parties.

(a) Where there is a business need for such third part access, a detailed risk assessment should be carried out to determine security implications and control requirements.

(b) If agreed to work with the third party, controls should be agreed and defined in a contract with the third party.

(c) Third party access may also involve other participants. Contracts offering third party access should include conditions for their access.

(d) Any outsourcing arrangements should address the risks, security controls and procedures for information systems, networks and/or desk top environments in the contract between the parties.

2.8 Antivirus and Spam Management

2.8.1 Proposed Best Practices for the University

(a) For standalone PCs, the antivirus software loaded into PCs should be automatically enabled for checking viruses and updating virus definition files.

(b) The centralized server antivirus should be deployed with capability to check for viruses in all the computers automatically.

(c) The antivirus software should auto-update virus signatures automatically from the service providers or the centralized server, as and when an update of signature or virus engine is available.

(d) Weekly analysis of the log files should be done to obtain a profile of viruses’ infections and the infected computers.

(e) Unneeded services should be turned off and removed. By default many operating systems install auxiliary services that are not critical e.g. an FTP, SSH or a web server.

(f) The mail server is one of the easiest routes for virus attack through e-mail attachments. Mail server should be configured to block or remove email that contains attachments that are commonly used to spread viruses, such as .vbs, .bat, .exe, .pif, and .scr files.

(g) The mail servers should be configured to reject mails from servers that have open relays, the database of such servers can be accessed from various sites like mail-abuse.org.

(h) Mail servers should be equipped with appropriate software to filter out junk mails.

(i) All students and staff must be made aware of the potential threat of viruses and the various mechanisms through which they propagate.

(j) Staff must be trained not to open attachments unless they are expecting them.

(k) The latest patches for operating systems, as well as web browsers have to be applied or else simply visiting a compromised web site can cause infection to the system.

(l) If a blended threat exploits one or more network services, disable or block access to those services until a patch is applied.

(m) Always keep patch level up-to-date, especially on computers that host public services and are accessible through the firewall. Such as HTTP, FTP, mail and DNS services.

(n) Since all online viruses arrive from the internet, good antivirus software should be loaded at the logical gateway of the network.

(o) In the case of a virus attack the following steps are required to be taken.

   i. Disconnect the computer from the network
   ii. Contact ICT help desk

(p) The notified expert should perform the following action on the infected work station.

   i. Determine the type of virus
   ii. Isolate all infected systems
   iii. Clean the infected file
   iv. In case of failure of the process above, the file should be deleted from the work station.
   v. In case of failure of the above, the work station should be removed from the network and remedial action taken.

(q) Spam should be managed appropriately as follows

i. Don't put explicit email addresses in out-of-office messages.
ii. Don't open spam emails - you may confirm through web links that your email address is valid.
iii. If you do open a spam, never reply or click web links, even those inviting you to be "taken off the list". Again this only confirms that your email is valid.

(r) Incidence profile including all reported problems and how they were handled should be kept at all time.

2.8.2 Anti-virus Deployment

(a) An antivirus server should be deployed and all the workstations should have the corresponding antivirus client. It is recommended that all these clients be configured from the central antivirus server for routine tasks such as Updating of antivirus signatures, scheduled scanning of the client workstations. The management of the client workstations should be done centrally from the antivirus server in order to have a centralized monitoring of all the activities.

(b) Antivirus with latest update should be installed to all Laptop, standalone computers and servers.

(c) All the traffic entering the network should be routed via an antivirus gateway application for monitoring all the types of traffic flowing through the network, whether be it HTTP, FTP, SMTP or POP3. This ensures that the risk of any virus entering the network is greatly reduced. A firewall with Anti-virus support will give addition security for the network.

2.8.3 Communications and Operations Management

Unauthorized access to University network may result in damage, corruption, and loss of confidentiality of University information. The University management must audit the security strength of the third part before engaging in business with them. The Connection to a third part network can not only introduce viruses but can destroy business operations.

2.8.4 Separation of Development and Operational Facilities

Development and testing activities may cause unintended changes to software and information if they share the same computing environment. Separating development, test and operational facilities is therefore recommended to reduce the risk of accidental change or unauthorized access to operational software and business data.

2.8.5 System Planning and Acceptance

Projection of future capacity requirements should be made, to reduce the risk of system overload. In addition, the operational requirements of new systems should be established, documented and tested prior to their acceptance and use.

2.8.6 Internet Connectivity

OUT network shall be connected to the outside world as follows;

(a) There shall be only one gateway to and from the internet

(b) There shall be only one gateway to and from the internet

(c) All OUT regional offices shall be connected to the Internet through the OUT's VPN. The end date for the current connections and the near future connections will be set by the University once all regional offices are connected to the VPN as proposed in the ICT Master plan.

2.8.7 Remote Access

Any remote access to the OUT network using either dial-up, VPN, or any other remote access technology must be approved by the Director of IEMT after review.

2.8.8 Remote Computer Requirements

OUT clients and other remote users shall be advised on keeping their computers installed with up-to-date anti-virus products. Portable devices shall not be allowed to connect to the university network unless clearance is given by IEMT.

2.8.9 Wireless Connectivity (Hotspots)

Members of staff, students and visitors shall be allowed to use their PCs/Laptops in hotspots environment after being registered by IEMT.

2.9 User Privilege Guidelines

These user privilege guidelines define the privileges various users are allowed to have, when working with the University's information systems. These guidelines are designed to minimize risk to University resources and data to the minimum allowable by establishing the privileges of users of data and equipment on the network while still allowing users to perform their duties without undue inconvenience. Only users with special need for additional access shall be allowed to change system settings and install programmes that are not operating system programs. This is because many malicious software such adware or spyware may be installed in a subtle manner by tricking the user or the installation may be completely transparent to the computer user. If the user does not have the ability to install programmes or change settings to a more vulnerable setting, most of these potential security problems can be prevented.

2.9.1 Main Categories of Privileges

There are three main categories of users on a computer or network. These categories include:

(a) **Students –** All students will be assigned to restricted user account, except during practical sessions in predetermined students' labs where the privileges shall be in such a way that student are able to carry out their practical. .

(b) **Restricted user -** Can operate the computer and save documents but can't save system settings. By default all OUT staff fall under this group. All non-technical staff and some technical staff will be in this group. Only with special assignment will be granted one of the following privileges.

(c) **Standard user (power user) -** Can change many system settings and install programmes that don't affect OS system files. This group shall include back-up operators, helpdesk operators etc.

   i. **Backup operator -** Allowed to read data on the domain for the purpose of saving files to backup media. This group cannot write all data on the domain.
   ii. **Account operator -** Can manage and view information about user accounts on the domain.
   iii. **Server operator -** Has full privileges on servers including reading and writing of data, installing programmes, and changing settings.

(d) **Administrators -** Have complete access to read and write any data on the system and add or remove any programmes or change system settings. This group shall include Domain administrators, Network administrator etc, Database administrators will only have full access to the database that they administer.

(e) **Domain administrator** - Has full privileges on all computers in the domain including servers and workstations. Privileges include reading and writing data, installing programmes, and changing settings.

2.10 Guidelines for E-mails

E-mail and other electronic information systems will, in accordance with the University's ICT policy and master plan, reduce the need for paper-based communication. The University makes available e-mail systems for use by its staff and students and encourages the appropriate use of e-mail as an alternative to paper based communication.

2.10.1 Responsible Use of E-mail

Users sending email from OUT owned domain (e.g. firstname.lastname (at) out.ac.tz) are seen as representative of OUT and such should act in a responsible manner.

(a) The sending abusive, offensive, defamatory, racial or sexual content within an email is strictly prohibited.

(b) The sending of email that could be considered libellous to an individual or organisation is strictly prohibited.

2.10.2 Personal Use of E-mail

Uses are permitted to use the OUT email system for personal use providing they adhere to the following:

(a) Personal views are clearly stated as such

(b) Purpose is not for financial gain to the user or other organisation

(c) The use does not contravene the ICT security policy

(d) All personal email must be stored in a folder clearly marked personal.

2.10.3 E-Mail Security

Email is not a secure form of communication and such users must realise that any information sent via E-mail may be seen by other persons. Users are responsible for ensuring they don't compromise information security.

(a) The confidentiality of email cannot be assured and as such users should carry out risk assessment before sending confidential or sensitive information via Email.

(b) Users must not intercept or access other users email without proper grounds and authorization, and accordance with the law.

(c) All e-mail addresses published and displayed on the web must be written with this format firstname.lastname (at) out.ac.tz (an @ sign shall not be seen).

2.10.4 Monitoring and Access to E-mail

The University may at any time permit the inspection, monitoring, or disclosure of email content;

2.10.5 When Required by and Consistent in Law

The University does not automatically comply with all requests for disclosure, but evaluates all such requests against the precise provisions of the laws concerning disclosure and privacy or other applicable laws.

2.10.6 The University Reserves the Right to Monitor Email

(a) In order to carry out system management, problem resolution, maintenance and capacity planning, to correct addressing problems or for similar reasons related to performance or availability of the system.

(b) In order to address security issues including virus management and authorized surveillance, including tracking unauthorized access to a system.

(c) The University may access the content of the email with written authorization of the OUT management

(d) In order to meet time dependent, critical business or operational needs or to carry out records management responsibilities; e.g. to conduct business during a crisis if an employee is absent when information is required as prolonged absence of an employee when information in the user's email is required. The user will generally be informed at earliest opportunity if this form of access is necessary.

2.10.7 Spam

Spam is defined as bulk email communications that are unsolicited and not authorized by the OUT executive. For example an invitation to a personal birthday party sent to the entire OUT community would be considered as a SPAM.

(a) Users are strictly prohibited from sending of spam within the university domain

(b) Users are also strictly prohibited from sending spam form university domain to any other domain worldwide.

2.10.8 Attachments

Network bandwidth is a valuable commodity to the University and such users must be responsible when sending email attachments. Attachments limits for email have been set at 20MB. This is a restriction not a target.

(a) Users must not send harmful or dangerous content as email attachments such as virus or worm.

(b) The sending and forwarding of chain emails is also prohibited.

(c) The sending of multimedia content such as video or music files must be considered carefully, as this can have a serious impact on network bandwidth.

2.10.9 Group Accounts

Group account for various departments and faculties shall be set up as and when they are required.

2.11 Guidelines for Social Networking Sites

The procedures applies to Social Networking site users who have a relationship with OUT, either as a member of staff or student at OUT. Social networking sites include but not limited to Facebook, Myspace, YouTube and Twitter.

2.11.1 Responsible use of Social Networking

The Open University of Tanzania understands the popularity and benefits of social networking sites if used responsibly. Such sites allow for, promote, general communication, online discussion and provide ability to share information about users quickly and easily. In many aspects this can be beneficial to students and staff both in personal and academics terms. By following few simple guidelines Social Networking can be enjoyed by all, safely and productively.

2.11.2 Guidelines for Use of Social Networking

(a) Before signing up to any Social Networking site make sure you have read the terms and conditions for that site, along with their privacy policy. If there is anything you do not understand or are not happy with, do not sign up to the site.

(b) When signing up to a site use only your personal details and not anyone else’s. When filling in your personal details remember that these will be visible to other users. Only enter the details that you are happy with being in the public domain. It is not recommended that you fill in local addresses, telephone numbers or full dates of birth.

(c) If you upload any pictures to your profile, license to use these pictures in many cases is transferred to the Social Networking site in question. This allows the site use the photo how they want to, possibly in marketing and advertising.

(d) You must not post any statement or photos that could damage the reputation of you, your family or that of OUT and its partners. You must not make offensive or derogatory remarks about students members of staff or other individuals, and must not post obscene or derogatory images.

(e) It is important to remember anything you post on Social Networking sites may be visible to anyone, anywhere, at anytime. It is important to be aware of the risks and take steps to protect yourself and your personal information. Posting personal information could potentially lead to unwanted attention and could even contribute to identity fraud. For your own benefit, you should not post details which you might find awkward later, for example something you would not want family members or future employer to see.

(f) It is prohibited to use the same username and password you use for other OUT systems, such as OUT email account.

(g) OUT users of these sites must keep in mind that they could face disciplinary actions by breaching OUT policies. They also could be subject to criminal proceedings if their actions are found illegal. It is now common for employers to search Social Networking sites as a means of screening potential applicants for positions of employment.

2.12 Guidelines for Disposal of ICT Equipments

All information and Technology equipment has an average life span of 3 (Three) years. After 3 years this equipment gets depreciated and obsolete. Obsolete equipment may continue to function during its salvage value for a while before it outlives its usefulness. Wear and tear of obsolete equipment can be hastened by the conditions which the equipment is subjected to like power stability, dust, end user handling and moisture.

ICT equipment that is due to outlive its useful life continues to erode the quality of end user output through regular breakdown until it completely degenerates for disposal. Before disposing of nay hardware, functional components of some ICT equipment like computers may be salvaged to assemble functional equipment like personal computer, which may be re-deployed for use, donation or sale.

2.12. 1 Guidelines for Hardware Disposal

(a) The hardware maintenance team shall periodically conduct maintenance to identify, retire and replace the hardware categorized as at “end-of-life.”

(b) Any user unit wishing to dispose of obsolete ICT equipment should contact the ICT helpdesk which will sent a technical staff to evaluate the hardware and determine the appropriate course of action, according to set guidelines

(c) ICT equipment may be disposed of in the following ways:

i. **Recoveries from offices/labs -** Equipment identified for disposal during the annual stock taking, user requests or hardware audits, from offices /labs may be salvaged and re-assembled. The refurbished computers may be placed in a pool of computers of allocation to new staff or staff in need of computers for. Alternatively the computers may be placed in student computer labs or library for general computing needs (Internet browsing, document production etc).

ii. **Hardware sale -** Obsolete hardware may be sold at salvage value. The University Board of Survey may assess the hardware and advise appropriate market price for the hardware sale. The Board may also advise on the procedures of hardware sales. All hardware for sale should be presented to the hardware workshop for technical inspection to ensure that it does not have any licensed software or university information. The technical staff from hardware workshop will delete all information on the hardware and replace existing software with free equivalents, before the technical inspection.

iii. **Hardware donations -** Obsolete hardware for donation to community outside the university should follow guidelines laid down by the national policies on deployment of used technology equipment and environmental conservation.

iv. **Hardware destruction -** Obsolete hardware that may neither be salvaged, nor sold nor donated may be destroyed. An inventory of hardware that has been destroyed or is due for destruction must be maintained. All hardware destruction should be done in accordance with available hardware destruction statutes or legal requirements.

2.13 Compliance

Particular attention should be paid to proprietary software products which are usually supplied under a license agreement that limits the use of the products to the specified machines and which may have a limit to the creation of back-up copies. This is very essential in order to avoid breaches of any criminal and civil law, statutory, regulatory or contractual obligations and security requirements. The following should be taken care of:

2.13.1 Software Copyright

(a) Acquisition of software products should be centralised and controlled by IEMT even if purchased privately.

(b) Maintaining awareness of the software copyright and acquisition

(c) Maintaining appropriate asset registers (proper documentation)

(d) Maintaining proof and evidence of ownership of licenses, original CDs, manuals, etc.

(e) Ensure that the University has appropriate number of users permitted for each system, and that any maximum number of users permitted is not exceeded.

(f) Carrying out checks that only authorized software and licensed products are installed in PCs used in the OUT LAN and MAN including users or hotspots.

(g) Complying with terms and conditions for software and information obtained from the vendors.

2.13.2 Safeguarding University Records

Some OUT's records may need to be securely retained to meet statutory or regulatory requirements, as well as to support essential OUT's operations. Such records may be required as evidence that an organization operates within statutory or regulatory rules, or to ensure adequate defence against potential civil or criminal action, or to confirm the financial status of the OUT with respect to shareholders and auditors. The time period and data content for information retention should be according to OUT regulations and rules.

2.13.3 Reviews of Security Policy and Technical Compliance

It is important that heads of sections/departments/directorates ensure that all security procedures within their area of responsibility are carried out correctly. In addition, regular reviews (depending on the criticality of the system will be done, this could be weekly or monthly) to ensure compliance with security policy and standards. This review shall include information systems, users, management, owners of the information and information assets.

2.13.4 System Audit Considerations

Audit requirements and activities involving checks on operational systems should be carefully planned and agreed to minimize the risk of disruption to business processes. The following should be observed:

(a) The scope of the checks should be agreed and controlled.

(b) The checks should be limited to read-only access to software and data.

(c) Access other than ready-only should only be allowed for isolated copies of the system files, which should be erased when the audit is completed.

(d) ICT resources for performing the checks should be explicitly identified and made available.

(e) All access should be monitored and logged to produce a reference trail.

(f) All procedures, requirements and responsibilities should be documented.

Important note: It is recommended that access to system audit tools, this means software or data files, should be protected to prevent any possible misuse or compromise. Such tools should be separated from development and operational systems and not held in tape libraries or user areas, unless given an appropriate level of additional protection.

2.14 Physical Security

Physical security is an essential part of a security plan. It forms the basis for all other security efforts, including data security. Physical security refers to the protection of building sites and equipment (and all other information and software contained therein) from theft, vandalism, natural disaster, manmade catastrophes and accidental damage. It requires solid building construction, suitable emergency preparedness, reliable power supplies, adequate climate control, and appropriate protection from intruders. The following are recommended;

(a) Don't arouse unnecessary interest in secure areas - minimize use of location signs

(b) Maximize structural protection. Secured rooms should have fireproof ceilings

(c) Minimize external access. Secured rooms should only have one or two solid, fireproof, and lockable doors. The doors should be observable by security staff. Doors to secure areas should never be left open. Windows should be small and have locks.

(d) Maintain appropriate locks. Keep doors locked when room is not in use. Maintain secure system for keys and combinations. If there is a breach, each compromised lock should be changed.

(e) Alternative physical security strategies. When appropriate, consider the use of window bars, anti-theft cabling (with alarm when cable is disconnected from system), magnetic key cards, and motion detectors.

(f) Be prepared for fire emergencies with appropriate automatic non water fire fighting equipment, and provide appropriate staff training in its use.

(g) Maintain reasonable climate control in secured rooms, with temperature ranges between 50 and 80 degrees Fahrenheit, with a humidity range of 20 - 80% (see also the requirements on the installed systems).

(h) Minimize non-essential materials that could jeopardize a secure room. Examples of non-essential items include: coffee, food, cigarettes, curtains, reams of paper, and other flammables.

(i) Dispose of confidential waste carefully and adequately to maintain confidentiality.

(j) Label confidential information appropriately and ensure suitable security procedures from common carriers when shipping or receiving confidential information.

(k) Keep critical systems separate from general systems.

(l) Store computer equipment in places that cannot be seen or reached from windows and doors, and away from radiators, heating vents, air conditioners, or other work.

(m) Protect cabling, plugs, and other wires from foot traffic.

(n) Keep a secure inventory of equipment and peripheral equipment, with up-to-date logs of manufacturers, models, and serial numbers. Consider videotaping the equipment for insurance purposes.

(o) Lock laptops in secure cabinet when not in use.

(p) Secure laptops to desks with cables when unattended.

(q) Provide and use laptop cover locks.

(r) Log off and lock computers when the operator is not in the vicinity of the computer.

(s) Establish a system to limit and monitor access to equipment areas.

(t) When computers containing sensitive information are being maintained or repaired, be sure that sensitive data is properly pass worded, encrypted, or removed from the computer before maintenance or repair.

(u) Assets with sensitive information should be installed with smoke detectors and security cameras.

Appendices

Appendix 1: Guidelines for Chatting

Recently IEMT staffs have installed messenger software to approximately 80 PCs in out HQ premises. It is noted that, these software are vulnerable to security threats if not used properly and securely. To prevent infection, keep your IM (Instant Messaging) client **updated** and follow these tips:

(a) **Be wary of files sent via IM**, especially those with .exe and .scr extensions, or ones purporting to be games. For best protection, verify with senders before opening.

(b) **Never click an unsolicited link fed via IM** or one lurking in another member's profile or away message.

(c) **Do you know everyone on your buddy or contacts list?** Think carefully about who is on your list. People on IM, like in chat, may not be who they say they are, so a friend of a friend is not necessarily your friend.

(d) **Keep your personal information secret** when talking to someone you doesn't know in the real world. Also think about what visible information you have, for example in your Profile or Member directory.

(e) **Learn how to keep an archive/save a copy of your conversation**, and don't be afraid to tell someone you are saving their conversation.

How to archive/save a copy of your conversations

- Archiving or saving your conversations can provide useful evidence if you come to make a report about something or someone.
- Some versions of Messenger have an option to archive conversations which is easy to switch on, check your preferences or privacy options in the Messenger toolbar for example, under Tools.
- For others that do not offer this option, you can still highlight the conversation with your mouse and copy and paste conversations into a Word document which you can save.

(f) **Learn how to block/ignore people**

- For whatever reason you may wish not to receive messages from a particular person anymore. If this is so you can block this person.

- To do this you right click on the name of the person in the contact list which should give you a range of options and one of these is Block. It will mean that you will not receive messages from this person anymore.
- Block is sometimes called ’Ignore’, and if right-clicking doesn’t work, have a look in your Preferences for this function.

(g) **Keep your username and password private**, and change your password on a regular basis.

(h) **Don’t accept messages from people you don’t know**.

(i) **Don’t reply to abusive messages**. Don’t send abusive messages either. It’s best not to say anything on IM that you wouldn’t say to someone’s face.

(j) **Don’t pass the buck -** if someone you have accepted on your buddy or contacts list is acting weird; don’t pass them on to a friend. You could be putting your friend at risk. Just block them.

(k) Use a nickname (this name must contain an abbreviation OUT in it, to make you easily acceptable with OUT community while chatting)**,** not your real name, and a nickname that is not going to attract the wrong type of attention.

(l) Check your antivirus company's home page or a general virus site, for news on current threats.

(m) For ICT technical staffs in IEMT; upgrade employees' IM clients monthly.

Appendix 2: ICT Laboratory Rules

The Institute of Educational and Management Technologies computer labs are designated for use of current students, faculty, and short course student or staff of the Open University of Tanzania. By using computer in the computer laboratories you agree to abide by this policy.

Purpose

This ICT security policy and procedures establishes requirements for the Computer Labs, to ensure that confidential information and technologies are not compromised, and to ensure that production Services and other University interests are protected from Institute of Educational and Management Technologies computer lab activities.

Scope

This ICT security policy and procedures applies to all IEMT Computer Laboratories, as well as all Authorized Users who use the Computer Lab.

a) No food or drinks allowed in the computer labs.

b) No noises, cell phone use allowed inside the labs.

c) Students are not permitted to install, modify or delete any software on lab computers.

d) Problems with computer lab equipment should be reported to the lab technician immediately.

e) Users should be respectful of other lab users, lab equipment and area at all time in the computer labs

f) Scheduled classes in the labs have priority over all other users.

g) Equipment in the computer labs may not to be removed, modified, relocated, or disassembled without permission of the Lab technician.

h) No signs are allowed in the lab or on the lab doors without first seeking the permission of the Lab Coordinator.

i) Use the dustbin in the computer lab to put all the unwanted materials

j) Reproduction of any copyrighted material (e.g. software, music, video, books, photographs, etc.) is prohibited.

k) Displaying of offensive graphic images by way of Netscape, Internet Explorer or other software is not permitted.

l) Sending/posting harassing messages or repeatedly sending/posting unwanted messages (electronic or paper) to others is prohibited.

m) Intentionally seeking information on, obtaining copies of, or modifying files, tapes, or passwords belonging to other users, or misrepresenting others, unless explicitly authorized to do so by those user, is prohibited.

n) Users are to clean up the area around the computer they used before they leave.

o) Network ports in computer labs are for lab equipment only. No other devices may be connected to them.

p) All traffic between the OUT and the University Computer Lab Networks must go through a Firewall maintained by IEMT. University Computer Lab Networks, wireless or physical, must not circumvent the Firewall.

q) Authorized Users utilizing University Computer Labs are prohibited from engaging in port Scanning, Network Auto-Discovery, Traffic Flooding, and other similar activities that negatively impact the OUT or non-University Networks.

r) Lab coordinators have the right to audit Computer Lab-related data and maintenance processes at any time if necessary, but not limited in-bound and out-bound packets, Firewalls, Network peripherals, etc.

s) Protect your security: Log off the computer before leaving the computer lab.

Appendix 3: Confidentiality and ICT Security Agreement - Staff

OUT regards security and confidentiality of data and information to be of utmost importance. Each staff granted access to data and information holds a position of trust and must preserve the security and confidentiality of the information he/she uses. This form is used to acknowledge and agree receipt of, and compliance with, the OUT Information Security Policy and Procedures.

Acceptable Use Policy Agreement

a) I understand that I am responsible for the security of whatever data I retrieve. I will provide all necessary safeguards to all sensitive and/or confidential information including reproduction or modification of data.

b) I will not access or attempt to gain access to any computer, computer account, network or files without proper and explicit authorization. I will inform the OUT management immediately should I become aware that such access has taken place.

c) I agree that I shall not copy, duplicate (except for backup purposes as part of my job here at OUT), otherwise disclose, or allow anyone else to copy or duplicate any of this information or software;

d) I understand that I am to restrict my retrieval and other computing activities only to data I have been specifically permitted to access as related to my assigned duties and using only functions and utilities which I have been authorized and trained to use.

e) I understand that my account and password are issued for my exclusive use only and I am responsible for the security thereof. I will not authorize or facilitate the use of my account or files by any other person, nor will I disclose my password to any other person.

f) I agree that if I don’t adhere to this policy and procedures, it may result into disciplinary action up to and including dismissal from position, fine and/or imprisonment depending on the terms and conditions of service, rules and regulations or any relevant law.

I have read and understand the above and agree to use the OUT ICT systems and my own devices within these guidelines

Staff name: ____PF Number: _______________

Department:______________________________ User name: ___________________________

Directorate/Regional/Faculty/Institute:

____

Designation:______________________________

Staff signature: ____________________________________

Date: _________________________________

Head of the Department/Section signature:_______________________ (After verification of section (a) above).

Date: _________________________________

This signed acceptance is valid for the period of employment with the OUT, or until a revised statement is deemed to be necessary as determined by the OUT.

Appendix 4: Confidentiality and ICT Security Agreement - Student

OUT regards security and confidentiality of data and information to be of utmost importance. Each student granted access to data and information holds a position of trust and must preserve the security and confidentiality of the information he/she uses. This form is used to acknowledge and agree receipt of, and compliance with, the OUT Information Security Policy and Procedures.

Acceptable Use Policy Agreement

a) I understand that I am responsible for the security of whatever data I retrieve. I will provide all necessary safeguards to all sensitive and/or confidential information including reproduction, destruction or modification of data.

b) I will not access or attempt to gain access to any computer, computer account, network or files without proper and explicit authorization. I will inform the OUT management immediately should I become aware that such access has taken place.

c) I understand that I am to restrict my retrieval and other computing activities only to data I have been specifically permitted to access as related to my assigned privileges as a student and using only functions and utilities which I have been authorized and trained to use.

d) I understand that my account and password are issued for my exclusive use only and I am responsible for the security thereof. I will not authorize or facilitate the use of my account or files by any other person, nor will I divulge my password to any other person.

e) I agree that if I don't adhere to this policy and procedures, it may result into disciplinary action up to and including terminated from studies, fine and/or imprisonment.

I have read and understand the above and agree to use the OUT ICT systems and my own devices within these guidelines

Student name: ___________________________ID No.__________________________

Department:_________________ Faculty: _______________User name: _______________________

Student signature:__________________________________ Date: __________________

Forwarded by:______________________________ Date:____________________________

This signed acceptance is valid for the period of studies with the OUT, or until a revised statement is deemed to be necessary as determined by the OUT.

Appendix 5: Confidentiality and ICT Security Agreement – Visitors/ Sabbatical Staff

The OUT recognizes the use of ICT as an important resource for teaching, learning, research and personal development. It actively encourages visitors to take full advantage of the potential for ICT to enhance development in all areas of the learning, research or any other purpose.

Acceptable Use Policy Agreement

a) I understand that I must use OUT ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

b) I understand that I am responsible for the security of whatever data I retrieve. I will provide all necessary safeguards to all sensitive and/or confidential information including reproduction, destruction or modification of data.

c) I will not access or attempt to gain access to any computer, computer account, network or files without proper and explicit authorization. I will inform the OUT management immediately should I become aware that such access has taken place.

d) I understand that I am to restrict my retrieval and other computing activities only to data I have been specifically permitted to access as related to my assigned privileges as a student and using only functions and utilities which I have been authorized and trained to use.

e) I agree that if I don't adhere to this policy and procedures, it may result into disciplinary action up to and including terminated from studies, fine and/or imprisonment.

I have read and understand the above and agree to use the OUT ICT systems and my own devices within these guidelines

Visitors Name: _________________________ID No.________________________

Reason for visit: ___________________________ Length of stay: _____________________

Visitor's signature: _______________________________ Date: _________________

Forwarded by: ____________________________ Date: __________________________

This signed acceptance is valid for the period of visiting OUT, or until a revised statement is deemed to be necessary as determined by the OUT.

Appendix 6: Confidentiality and ICT Security Agreement - Administrators

I, ………………………………………………………………..………………….
(PRINT FULL FIRST, MIDDLE & SURNAME – BLOCK LETTERS)

a) Acknowledge that I have read and understood the *Whole-of-ICT security policy and procedures*
b) Agree to abide by the requirements for access and use of these ICT resources
c) Acknowledge that the IEMT may authorize access to user logs in the event that there is a perceived threat to the:
    - System security
    - Privacy of staff
    - Privacy of others
    - Legal liability of the OUT.

This signed acceptance is valid for the period of employment with the IEMT - OUT or until a revised statement is deemed to be necessary as determined by the OUT.

Signature: ....

Date: ....

Faculty/Directorate: ....

Position Held: ....

PF No: ....

Note: Use of the full name is important. It must match personnel records. Do not use abbreviated or nicknames unless it is your formal name.

Appendix 7: Confidentiality and ICT Security Agreement – Interns/PT Students

I, …………………………………………………………………..………………….
(PRINT FULL FIRST, MIDDLE & SURNAME – BLOCK LETTERS)

a) Acknowledge that I have read and understood the *Whole-of-ICT security policy and procedures.*
b) Agree to abide by the requirements for access and use of these ICT resources for the whole period that I will be attached at the OUT.

This signed acceptance is valid for the period of ***Practical training/Internship*** at OUT or until a revised statement is deemed to be necessary as determined by the OUT.

Allocated faculty/directorate: ....

Signature: ………………………………..

Date: ……………………………………….

Note: Use of the full name is important. It must match personnel records. Do not use abbreviated or nicknames unless it is your formal name.