



UGANDA TECHNOLOGY AND MANAGEMENT UNIVERSITY

ICT POLICY

I. INTRODUCTION

Uganda Technology and Management University (UTAMU) offers a wide array of computing and networking resources and services to its stakeholders (students, staff and partners). These services are in place to facilitate teaching and learning, research, and administrative activities.

UTAMU is committed to advancing Uganda's development by graduating highly skilled people and by providing technical and technological assistance and service to all sections of the community. UTAMU aspires to become a center for excellence in ICT comparable in standard to the very best in the world. Its niche is in the promotion of innovation in business and technology.

The UTAMU's ICT Policy is a guide on how ICTs shall be used to achieve the goals and aspirations of UTAMU. It highlights how the usage of ICTS shall be implemented, their development and maintenance, the optimal distribution of resources (hardware, software, data and human resources) as well as the safe and healthy utilization of ICTs and the environment. This policy seeks to enumerate the rules necessary to ensure the existence of the highest levels of consistency, control and harmonious interaction with ICT technologies.

II. POLICY STATEMENT

Information and Communication Technologies facilities are simply electrical and mechanical tools that facilitate the storage, manipulation, analysis and transfer of information.

UTAMU is committed to providing safe, effective and efficient usage of ICT facilities by UTAMU stakeholders (Academic and Administrative Staffs, students, Visitors).

UTAMU is committed to training graduates to develop innovative ICT technologies that provide more secure, efficient and effective solutions to the contemporary global challenges.

III. VISION AND MISSION STATEMENTS

The Vision of Uganda Technology and Management University is *"To be a global educational institution for management, science, technology and innovation"* and

The Mission of the university is *"To provide global quality education, Research and innovation critical to economic and human development."*

IV. GUIDING PRINCIPLES FOR THE IMPLEMENTATION OF THE POLICY

The ICT Department, demonstrates an on-going commitment to mainstreaming ICT usage by ensuring that the relevant policies, practices, metrics are in place. Frequent and consistent communication will be issued by the ICT department about tips on how to execute safer, more secure and efficient operations. This will be broadcast to the affected or target audience(s).

IV.1 MAINSTREAMING DIVERSITY

UTAMU supports diversity and does not discriminate against minority entities based on age, gender, race, sexual orientation, religion, political affiliation, e.t.c. Diversity is encouraged in the different spheres like educational preferences, research interests, funding preferences, work-life-balance, performance management, career management and other inclinations or variations.

IV.2 EDUCATION, TRAINING AND KNOWLEDGE BUILDING

UTAMU is committed to continuously re-tool, educate and train all employees, lecturers and administrators in order to improve on institutional practices.

IV.3 SUPPORTIVE WORK PRACTICES AND INSTITUTIONAL CULTURE

UTAMU operates in an open and flexible environment and welcomes people from diverse backgrounds. The work culture at UTAMU is based on the principles of hard work, creativity, fairness and resource optimization.

IV.4 TRANSPARENT RECRUITMENT AND CAREER DEVELOPMENT PRACTICES

UTAMU is committed to fair, transparent and competitive recruitment and promotion of personnel. UTAMU will adopt policies that enable all employees of UTAMU to develop satisfying careers, following the regulations given in the Appointments and Promotions policy.

IV.5 PARTNERING WITH EXTERNAL BODIES

UTAMU seeks to develop relationships with a range of partnering institutions in order to advance mutual interests and to further the development of internal knowledge and capabilities.

V. OBJECTIVES OF THE UTAMU ICT POLICY

The UTAMU ICT Policy contains the following policies, their objectives and strategies:

1. Acceptable Use Policy
2. Electronic Mail Policy
3. Anti-virus and Anti-Spam Policy
4. User Password Policy
5. Data Backup & Restoration Policy
6. Software Use Policy
7. Internet Bandwidth Policy
8. Computer Lab Policy
9. Computer Equipment Policy
10. E-Learning Policy
11. Support Desk Policy

V.1 ACCEPTABLE USE POLICY

The purpose of this policy is to ensure the proper use of UTAMU's ICT facilities, software, services and systems by its employees (academic and administrative), guests and students in an appropriate, responsible, and ethical manner. This policy also applies to the use of privately owned computers or notebooks connected to the University network.

V.1.1 OBJECTIVES

This acceptable use policy has been drawn up with the following objectives:

- To encourage the use of both the Internet and hardware as a conduit for free expression without infringing the rights of others.
- To protect and preserve the privacy of individual users and the public at large.
- To discourage the irresponsible use of hardware and network resources, which use may result in the degradation of service.
- To ensure the security, reliability and privacy of UTAMU's system and network infrastructure.
- To avoid situations that may result in the occurring of any form of civil liability.
- To propagate the image and reputation of UTAMU as a reliable and responsible University.

V.1.2 STRATEGIES

- a) The UTAMU community as a whole must be warned that they must not use the ICT facilities, software, services and systems in any illegal, immoral or otherwise unauthorized manner.
- b) UTAMU reserves the right to monitor and record all activities related to University activities using ICT facilities, software, services and systems.

- a) The Directorate for ICT, Quality assurance and Library services is responsible for the following:
- i. Monitoring network traffic and activities related to University activities
 - ii. Recording all activities related to University activities
 - iii. Putting in place measures to ensure security, reliability, fair use and free expression of users without infringing the rights of others.
 - iv. Ensuring availability of measures to protect and preserve the privacy of individual users and the public at large.
 - v. Disseminating information to sensitize users on irresponsible acts in the use of hardware and network resources, which use may result in the degradation of service.
 - vi. Promoting safety of users and network infrastructure.

V.2 ELECTRONIC MAIL POLICY

As a University, UTAMU commits to provide the members of her community an electronic communication infrastructure that includes computing resources, network connectivity, and software tools for electronic communication (e-mail). The UTAMU's community is reminded that use of e-mail is a privilege, not a right and should be treated as such by all users.

V.2.1 OBJECTIVES

- To ensure the proper use of UTAMU's electronic communication infrastructure system by its employees (academic and non-academic), guests and students.
- To support academic (teaching and learning), research, administrative functions of UTAMU

V.2.2 STRATEGIES

- b) All e-mail communications (and associated attachments, objects, graphics, videos) transmitted or received by UTAMU network are subject to the provision of this policy, regardless of whether the communication was sent or received on a private or UTAMU owned computer.
- c) The Directorate of ICT, Quality assurance and Library services is responsible for the following:
- i. Creating email addresses for new members of the UTAMU community. This also includes access rights e.g. passwords, biometrics, secret questions, e.t.c.

- ii. Disabling email addresses for ex-members of the UTAMU community. In order to allow smooth transition, this will be done after a period of three months.
- iii. Monitoring the electronic mail management usage by its users in a regular or systematic manner. Such monitoring may include tracking addresses of e-mail sent and received, accessing in-box messages, accessing messages in folders, and accessing archived messages. Please note that DIQL reserves the right to monitor such usage from time to time and without prior notice.
- iv. Minimizing any misuse or illegal use of email communications.

d) The mailbox owner is expected to:

- i. Be responsible and liable for all messages sent from their e-mail accounts and ultimately responsible for all activity performed under their account.
- ii. Keep his password secret e.g. by not disclosing it out to another person, frequently changing it, not writing passwords down or using any other processes that facilitate automatic log-on.
- iii. Use only e-mail accounts that they are authorized to use.
- iv. Use email accounts for legal, moral and authorized activities, e.g. by not committing a crime using his/her email account.

e) The mailbox owner is expected to regularly carry out some activities to manage email accounts and documents. This include:

- i. Reading all the new e-mail messages at least once in every 1 or 2 days and replying as soon as possible
- ii. Not letting messages build up in the Inbox and deleting messages as soon they are no longer needed.
- iii. Opening the 'Sent messages' folder at least once a week and deleting old messages that are no longer needed.
- iv. Saving messages that they want to keep onto the hard disk or removable disk.
- v. Logging out of the email account before exiting the application.

f) Mailbox owners are expected to adopt practices that increase privacy and confidentiality of their email communications. They need to be aware of the following:

- i. E-mail messages may be saved indefinitely on the receiving computer.
- ii. Copies of e-mails may be forwarded electronically or printed on paper.

- iii. E-mail messages may be sent to incorrect e-mail addresses or be improperly delivered by an e-mail system or Internet Service Provider (ISP).
 - iv. It may be possible for other people to read or change messages that you send by forwarding it to others.
 - v. New e-mail will be prevented from coming in to the mailbox once the mailbox has reached the maximum allowable storage space.
- g) UTAMU expects members of its community to exhibit acceptable ethical conduct in the use of computing resources. Users are expected to exercise good judgment to ensure that their electronic communications reflect the high ethical standards of the academic community and display mutual respect.

V. 3. ANTI-VIRUS & ANTI-SPAMMING POLICY

V.3.1 OBJECTIVE

To ensure that the University will provide its community with adequate protection from computer viruses, unsolicited and unwanted emails. The university shall invest and deploy anti-virus and anti-spamming software on ICT facilities owned or leased by the University as well as on ICT services outsourced by the University.

V.3.2 STRATEGIES

- a) The Directorate for ICT, Quality assurance and Library services is responsible for the following:
- i. Installing anti-virus software to ensure that all networked computer servers, computers and notebooks used by the University users are protected against virus infections.
 - ii. Installing Anti-Spam software that automatically separates suspected spam from regular mail.
 - iii. Minimizing any misuse or illegal use of email communications.
 - iv. Protecting the community against other malicious attacks like denial of service, spy ware, phishing, e.t.c
- b) Users of University resources are expected to act in the following way:
- i. Report any case of virus, spam or other security risks.
 - ii. Refrain from creating or initiating virus and spam attacks.
 - iii. Use the existing technologies to minimize effects of virus, spam and other attacks.

V.4 USER PASSWORD POLICY

The policy ensures that the user has the minimum standard applied to their user password to support the confidentiality, integrity and security of the University ICT resources. This policy refers to users of university resources that require passwords.

V.4.1 OBJECTIVES

The objectives are to ensure access control to the ICT resources, to communicate the needs to have protection against unauthorized access and to establish an ICT environment that will encourage data sharing and exchange without sacrificing security.

V.4.2 STRATEGIES

- a) The Directorate of ICT, Quality assurance and Library services is responsible for the providing passwords for access to sensitive or controlled environments like email accounts, tests and examinations, restricted rooms, sensitive files and folders as well as various gadgets.
- b) Password holders are expected act in the following way:
 - i. To treat all passwords as private and confidential and not to be divulged, shown or given to any party other than the user.
 - ii. To change passwords on regular basis or at least every six months.
 - iii. To create passwords based on combinations of numeric and alphabetic with a minimum length of 8 characters.
 - iv. To create hard-to-guess passwords e.g. a password not the same as the username, recycled or previous passwords or name which is associated with the user i.e. DOB, company name or horoscope, e.t.c.
 - v. First time users to change the password immediately after he/she has been issued the initial default password.

V.5 DATA BACKUP & RESTORATION POLICY

V.5.1 OBJECTIVES

To define the backup and restoration of data and information associated with the University operations. This policy applies to only staff of the University who create, process and store data and information using the ICT resources. With this policy in place, we can ensure copies of critical data are retained and available in case of disaster, software or hardware failures.

V.5.2 STRATEGIES

- a) The Directorate for ICT, Quality Assurance and Library services is responsible for:
 - i. Performing daily back up for the entire critical corporate database for the entire University.
 - ii. Keeping back up disks in an offsite locked place only known to Vice Chancellor.
 - iii. Clearly marking all back up disks with a name and creation date. This will ease identification.
 - iv. Providing the necessary storage and backup support to staff.
 - v. Periodically testing the backup disks to ensure they are recoverable.

- b) The Individual users shall be responsible for:
 - i. Backing up their own data which is on their own desktop and notebook computers.

V.6 SOFTWARE USE POLICY

V.6.1 OBJECTIVES

To ensure that software that the University adopts provides the service as expected. This includes the financial management software, human resources, academic records and any other software in use.

V.6.2 STRATEGIES

- a) The Heads of units shall:
 - i. Initiate the procurement / adoption of a given software.
 - ii. Report any bugs or mal functions observed on the software.

- b) The Directorate for ICT, Quality Assurance and Library services shall:
 - i. Procure the software after approval from the relevant organs.
 - ii. Procure software licenses after approval from the relevant organs
 - iii. Install the software to on authorized computers or notebooks.
 - iv. Record all installed software in a software directory.

- c) The software users shall:
 - i. Adhere to the rules and regulations set aside for the proper usage of the software.
 - ii. Report to the Head of the relevant unit, any bugs or malfunctions observed on the software.
 - iii. Use the software legally e.g. ensure against copyright infringements on software.

- iv. Install copies of personally owned or free software on University machines, and then report such software to the Directorate of ICT, Quality Assurance and Library services for recording in the software inventory.

V.7 INTERNET BANDWIDTH POLICY

V.6.1 OBJECTIVES

To manage bandwidth use to avoid degradation and ensure network efficacy. Management of Bandwidth resources shall be entrusted to the Directorate of ICT, Quality Assurance and Library services.

V.6.2 STRATEGIES

Bandwidth usage shall be subject to the following:

- a) Internet Bandwidth will not be over utilized as to prevent access to critical information, research and online educational material.
Bandwidth allocation shall be made in the following order:
 - i. UTAMU applications
 - ii. e-mail
 - iii. internet research
- b) Unauthorized persons/users are not allowed to access internet facilities within the campus network
- c) To ensure efficiency and optimal usage by all the users, ICT resources shall be monitored from time to time by the Directorate of ICT, Quality Assurance and Library services.

V.8 COMPUTER LAB POLICY

V.8.1 OBJECTIVE

The main objective is to manage the use of computing lab and to maintain its security.

V.8.2 STRATEGIES

Students are to adhere to the following guidelines while using the computing labs:

- Do not bring food or drink into the computer lab.
- Smoking is not allowed in the computer lab.
- Report problems promptly to the Directorate of ICT, Quality Assurance and Library services.

- Do not alter the configuration of hardware or software. This has been set up to cater for a wide range of users.
- Leave each piece of equipment set up as you found it. Do not remove any items from the computer lab.
- Follow any directions posted in the venue by the staff in the Directorate of ICT, Quality Assurance and Library services.
- Labs are available for use only by University staff and students and authorized external users.
- Unofficial work of a personal, non-profit nature is permitted, provided official work is not affected.
- Non-University related commercial activities are not allowed.
- Do not waste computer resources (e.g. unnecessary printing) or disadvantage other users by monopolizing equipment, network traffic, etc.
- Keep the computer lab clean and free of hazards.
- Do not place software or other files on University computers where these may lead to damage or legal charges (destructive programs such as viruses, pirated software, etc.).
- Do not use the facilities to make unauthorized copies of copyright, licensed or patented material.
- Do not use the facilities to defraud or to create false or misleading information.
- Do not act as though you intend to break the law. Do not attempt to guess an access key or password to gain unauthorized access to local or remote computers.
- Do not attempt to access any areas of any systems for which authority has not been granted.
- Do not attempt to monitor or read another user's files or communications.
- Report unethical activity to University staff promptly.

V.9 COMPUTER EQUIPMENT POLICY

V.9.1 OBJECTIVES

Due to the variety and nature of work performed by staff and students across the entire University, it is not practical and easy to define a standard operating environment for all equipment. This section provides a guide to what is expected of the equipment used by the University community.

V.9.2 STRATEGIES

- a) The Directorate of ICT, Quality Assurance and Library services is responsible for providing the minimum standards for all equipment used by University community. This includes iPhones, netbooks, iPads, desktops, printers, scanners, photocopiers, fax machines, landlines, e.t.c.

b) Standards for Personal Computer Hardware – Desktop

Operating System: Windows 2000
CPU: Genuine Intel® Pentium CPU – 1GHz+
Memory: 256MB+
Hard disk drive: 20.0GB+
1 Parallel Port
1 Serial Port
64MB Graphics (not incorporated in the main RAM)
PCI Bus Architecture, USB connectivity
1.44MB Floppy Disk Drive
Plug & Play BIOS
15" Colour Monitor (1024 x 768 Mhz @ 76hz)
4MB Video card PCI or (preferably) AGP
Keyboard (101 extended key board)
PS/2 Microsoft Mouse
Network card PCI 10/100, RJ45, Wake-on-LAN facility on card and PC Motherboard (if network connectivity required)
Warranty: 3 years, Parts and Labour
No other software installed (including no antivirus, networking, Internet, or ISP software)
Bootable Recovery CD for each PC supplied.
Recovery CD to be produced 'after' PC is configured
UPS with 'User Replaceable' battery

c) Standards for Personal Computers – Notebooks

Genuine Intel® Pentium CPU – 1GHz+
Memory: 256MB SDRAM
Hard disk drive: 20.0GB+
PCI Bus Architecture, USB connectivity
Plug & Play BIOS
1.44MB Floppy Disk Drive
12.1" Colour screen
4MB Video card PCI or (preferably) AGP
Two Type II PCMCIA Card slots
10/100 NIC
Built-in 56K Modem
Availability of " Docking Station".
In-built pointing device and external port
Warranty: 3 years, Parts and Labour
No other software installed (including no antivirus, networking, Internet, or ISP software)

Bootable Recovery CD for each computer (desktop/notebook) supplied. Recovery CD to be produced 'after' laptop is configured Recovery CD from manufacturer.

d) Personal Computer Software

Operating System: Windows NT Workstation 4.0+ with latest Service Pack

Windows 2000 and latest service pack when applicable

Bootable Recovery CD for each computer (desktop/notebook) supplied. Recovery CD to be produced 'after' each computer is configured

Recovery CD from manufacturer.

Additional software products and licenses may be required depending on the planned configuration of the PC.

e) Printers

Hewlett Packard printers, plotters and scanners are the standard. The model purchased will depend

on the requirement, either for portable computing, desktop printing or group printing.

f) Standards for Software

i. Operating Systems

Microsoft Windows XP, Vista, Windows7 Professional

Windows Server (File Server, Application Server)

UBUNTU Open Source

ii. Office Suite

MS Office 2003/2007/2010 Professional

Open Office

iii. Databases

MS SQL Server, MS Access , Oracle.

iv. E-mail Server

MS Exchange Server.

v. E-mail Client

MS Outlook 2003/2007/2010

vi. Browser

MS Internet Explorer ver.6 or greater with latest Service Pack

Firefox Web Browser with latest updates

Google Chrome

vii. Compression utility

WinZip

viii. Anti-virus (Desktop, Fileserver)

Norton's AntiVirus, Avast, MacAfee, E-scan

ix. Backups (Desktop, Fileserver)

V.10 E-LEARNING

Reference to the UTAMU E-Learning Policy

V.11 SUPPORT DESK

Reference UTAMU Support Desk Policy

VI. POLICY VIOLATIONS

- a) The procedure that follows after a violation of this policy is reported or noticed is that:
 - i. The Director of the Directorate for ICT, Quality assurance and Library Services will set up a team to investigate the allegation or suspicion. If it is a student being investigated, The Dean of the School he belongs to must be part of this team. If it is a member of staff being investigated, the Deputy Vice Chancellor must be part of this team.
 - ii. The Director of the Directorate for ICT, Quality assurance and Library Services will temporarily suspend or block access to an account, prior to the initiation or completion of such procedures, when it reasonably appears necessary to do so in order to protect the integrity, security, or functionality of University or other computing ICT resources or to protect the University from liability.
 - iii. After investigations are complete, the findings will be forwarded to the disciplinary committee, which will decide whether the suspect is guilty or not, and which will determine the disciplinary action to be taken.
- b) Users who violate this policy may be denied access to University ICT resources and may be subject to other penalties and disciplinary action, both within and outside of the University. Violations will normally be handled through the University disciplinary procedures applicable to the relevant user.
- c) Any violation of this policy will attract disciplinary action and be handled according to the rules and regulations of the University and the Country in which the act was propagated in.

VII. IMPLEMENTATION AND EVALUATION

VII.1: PLAYERS

The Directorate of ICT, Quality Assurance and Library services is composed of the Director, ICT Manager, ICT System Administrator, Support desk manager, Support desk technician, E-learning Coordinator, Web Master, Librarian and Quality Assurance Manager.

a) Director

Is responsible for the overall activities of the ICT Directorate and the coordination point for all external support escalation services. He/she liaises with other units regarding annual planning of ICT activities; improvements to hardware and software functionalities; any ICT related acquisitions; all ICT budget decisions; coordination of ICT Strategy and ICT Policy; daily, weekly and other, tasking of all ICT staff; coordination with trainers for, and some delivery of, training regarding ICT Policy related training components.

b) ICT System Administrator

Reports to the Director and is responsible for all Server activities including Users, data security (access rights, back ups, antivirus, disaster recovery actioning); LAN configuration; Internet usage; Email accounts and usage; direction to Support Desk Manager with ICT Department Manager approval for system additions and changes at User and non-Server locations; maintenance of the Server based components of any computerized information systems; coordination with external support escalation including remote access to Servers by external support escalation entity; requests to ICT Section Manager for Help Desk staff activities relating to non-Server Systems Administration activities; keep Users informed of ICT Policy issues and system usage changes; acquisition requests to ICT Department Manager.

c) Support Desk Manager

Reports to the Director and is responsible for coordinating all Help/Support Desk activities and ensuring all users are kept informed of status of Help Desk inquiries; task and coordinate other Help Desk staff; ensures all ICT support Desk activities are recorded and updated in the Help Desk Job Register; ensures all help desk problems causing support resolution delays are documented and reported to Director; coordinates with external support escalation entities relating to User hardware and locally installed software both on-site and externally-based support; coordinates with external support escalation entity, in conjunction with ICT System Administrator and under direction from the ICT Department Manager, in relation to on-site system administration activities; maintain ICT Help Desk software and literature libraries; maintain all ICT asset registers; document all requests for acquisition; coordinate acquisition of quotations as directed the ICT Department Manager; coordination with trainers for, and

some delivery of, training regarding training components relating to operating system, locally installed software, and hardware usage; receiving, recording and if necessary actioning Help Desk inquiries when Help Desk Technicians unavailable to do so to ensure prompt response to inquiries (Mon. - Fri. 8:00 - 17:00 including lunchtimes).

d) Support Desk Technicians

Reporting on a day-to-day basis to the ICT Support Desk Manager and is responsible for the delivery of user support for computer hardware and locally installed software; other non-Server system hardware support, ensures receiving, recording and actioning of Help Desk inquiries to ensure prompt response to inquiries (Mon. - Fri. 8:00 – 17:00 including lunchtimes); maintains Help Desk Job Register; delivers user training.

VII.1 Develop the UTAMU's ICT policy

The development of the UTAMU's ICT policy is performed by the Directorate of ICT, Quality Assurance and Library services.

VII.2 Implementation, Evaluation of the UTAMU's ICT policy

The Implementation and evaluation of the of the UTAMU's ICT policy is performed by Directorate of ICT, Quality Assurance and Library services in consultation with the University management.

VII.3 Monitoring and review progress of the UTAMU's ICT policy

The monitoring and reviewing progress of the UTAMU's ICT policy is performed by Directorate of ICT, Quality Assurance and Library services in consultation with the University management.