Appendix C
Usage policies

1. Malawi College of Medicine

Proposed student internet usage agreement

Agreement on use of the College computer & internet facilities

Use of the CoM computing and network resources is a privilege and not a right. As with all privileges, abuses will not be tolerated.

An individual member of the CoM community, faculty, staff or student may be issued a user-id to access one or more CoM computing resources. This user-id will remain valid so long as the individual is associated with the College. The proper use of a user-id is ultimately the responsibility of the individual under whose name it has been assigned. Therefore, guard your passwords and do not share your user-id. The use of another individual's user-id without his/her expressed consent will be viewed as theft.

The College enjoys the use of a direct Internet connection via an international satellite connection. The purpose of this connection is to facilitate the teaching and research conducted at the College through access to relevant information, literature searches and communications with colleagues throughout the world. The bandwidth (capacity) of the Internet link is limited and expensive. It is enough for the intended work, but not for anything else. Inappropriate use of the Internet will be deemed abuse of computer privileges. Examples of inappropriate use include:

- Any type of network games
- The sending of obscene and/or harassing messages to other individuals
- The sending of unapproved bulk mailings
- The unauthorized access or attempted access of another network computer system from CoM computer resources.
- Messaging services
- Programs that uses the Internet in a continuous (streaming) way such as audio or video services
- Downloading large music (MP3 etc.) or video files and storing them on the network
- Visiting Internet sites not related to work**.** These include, but are not limited to, sites of a pornographic nature, violence sites, racist sites, religious sites, etc.

The College does not allow external e-mail accounts, such as Hotmail or Yahoo due to the way that these services take up a lot of the capacity of the Internet link. Official College e-mail addresses have been set up for everyone who needs them. Please contact the IT staff to obtain your user name and password.

Network users should not run any program that causes files to be installed on a workstation or the network. If in any doubt, users should not proceed.

Any action that compromises the integrity of the College network (e.g. hacking) will not be tolerated under any circumstances.

Copyright of materials and intellectual property rights must be respected.

The College puts, as top priority, the security of its network and the safety of its users. Action by any user that compromises these aims in any way will be dealt with very seriously.

It is College policy not to check e-mail randomly but if there are grounds for suspicion of misuse, the account of a user will be frozen and then inspected. The user will be informed that this is happening.

The College reserves the right to examine or delete any files that may be held on its computer system and to monitor any Internet sites visited.

The College will take the following action against an individual who abuses or has gained unauthorized access to computer resources:

The user-id will be immediately inactivated.

The College administrative authorities will be informed.

Actions taken by the administrative authorities will depend on the severity of the computer abuse but will include fines for reconnection where appropriate.

Student's agreement

I have read and understood the College rules for computer use and Internet access. I agree to abide by these rules and to use the College computer system in a responsible way at all times.

Signed: ___________________________ Date: ________________

Full Name: ________________________ Student No: ___________

2. Addis Ababa University

Addis Ababa University Network (AAUNet)
use & security policy (USP)

VERSION CONTROL

REVISION NUMBER	REVISION DATE	MAJOR REVISION(S)
1.0	September 2001	Draft
2.0	March 2002	Draft
3.0	May 2002	First Version Release

2.1 Introduction

2.1.1 Terminology

In this document, unless contrary intention appear, the following terms are used with the meaning stated against the terms.

AAUNet Facility – the University-wide backbone network infrastructure composed of all purchased, rented or leased inventories including:

- Building, Inter-building, campus and inter-campus network links
- network cabling and transmission media up to and including wall outlets and other access points that are connected to the backbone network
- intelligent devices including campus and central servers, workstations, PCs and routers up to and including building switches and intelligent hubs connected to the backbone network
- the operating software used on all such equipment
- the application software loaded on AAUNet
- the people involved in the maintenance and administration of the equipment
- the electronic content and information (transaction and database) that the system hold, process and transfer;
- the documentation associated with the network facility

Account - the login identifier assigned to a user
Broadcast – the transmission of a message to a significant number of user accounts on AAUNet servers.
Commercial Gain - the use of the AAUNet facilities for personal or private commercial purposes or financial gain.
Custodian - a person or organizational unit responsible and accountable for a particular system or a component thereof.
Executive Director – Executive Director of ICTC
Firewall - a device interconnecting computer systems or networks for the purpose of providing the capability to filter network traffic between the interconnected computer systems or

networks.
ICTC – Information & Communications Technology Center of AAU.
Login - the act of accessing a computer system or its associated application systems.
Security Breach - a contravention of the USP.
System Administrator - a person who is authorized as being responsible for the configuration, maintenance, and operation of AAUNet facilities.
Terminal - a physical or virtual device used to access AAUNet.
User – an authorized person who accesses AAUNet facilities whether that access is from within or outside of AAU.
User Account - an account provided for the use of one authorized person for the purposes of accessing AAUNet resources.
User Name: AAUNet system administrators will assign all users a unique "username" based on some derivation of their real name. A username identifies a user on AAUNet.
The University - Addis Ababa University (AAU)

2.1.2 General

Purpose & Scope: AAUNet facilities are owned by Addis Ababa University (AAU) and are provided primarily to support the academic (teaching/learning and research) and administration functions of AAU. The network facilities are provided to students, staff and faculty, and other authorized users to help them advance the educational, scholarly and service missions of AAU.

This document states the Use & Security Policy (USP) of AAUNet facilities. It states the conditions for effective utilization and maximum protection of AAUNet facilities. The rights and responsibilities of users and administrators together with methods for the implementation of the policy are included.

This policy may be supplemented with additional guidelines by campus units which operate their local area networks, provided such guidelines are consistent with this policy.

Official Copy: Official copy of this policy as amended and in force for the time being will be held readily available in the University to users. An up-to-date electronic copy will be available on the University's Official Home Page; and a copy will be filed with the AAU Audit & Inspection Office.

Policy Management: While the formulation and maintenance of the AAUNet USP is the responsibility of ICTC, approval is vested with the President of the University. ICTC is also responsible for providing administrative interpretations of the USP.

Policy Implementation: Each member of the University and any other person who is legally using the network facilities will be responsible for meeting the requirements of the USP and related procedures and standards. As such, Users are expected to read (on routine basis) and abide by this policy and its administrative interpretation as they may be amended form time to time.

Custodianship: While ICTC is the custodian of the AAUNet infrastructure and all central facilities; Faculties, Schools, Departments, Divisions and other elements of AAU will be custodians of network facilities under their management control including shared computing devices. Accordingly, it is the duty of each custodian to take appropriate action to ensure compliance and prevent breaches of USP. Where such action is outside the authority of the custodian, the custodian will notify the appropriate senior officers of the University.

2.2 Security procedures

2.2.1 Physical security

Access to secure areas, including server rooms shall be restricted to authorized staff through the use of passwords, locks or access-control devices.

Visitors to such areas shall be permitted only under the supervision of authorized ICTC staff. Details of visitors including name, time in, time out, and reason for entry shall be recorded in a log.

During non-working hours, secure areas shall be protected against intrusion by appropriate access control, surveillance systems or by security staff.

2.2.2 Hardware

The effect of electrical power outages and fluctuations shall be protected against by the installation of an uninterrupted power supply (UPS) and surge protection devices wherever practical.

AAUNet facilities shall be adequately protected against fire, water and physical damage.

2.2.3 Software

All materials associated with any AAUNet facilities, including software and printed materials, which are not in the public domain, must be treated in accordance with any applicable copyright agreements and restrictions. Such materials must be licensed (if required) in an appropriate manner and may be obtained only in a legal manner from a legal source.

2.2.4 Data security

An appropriate regular back-up schedule shall be implemented to protect all data, software and documentation on AAUNet. A sufficient number of backups of all data, software and documentation shall be stored off-site to protect against major damage at one location.

The backup procedures shall be clearly defined, regularly tested and documented in a Disaster Recovery Plan.

The use of AAUNet facilities supplies the user with information about the computer system, as well as information about the University. This information is essentially private to the University and, in some cases, essential for the user to know in order to carry out useful work. Therefore, a trust relationship exists between the user and the University. Accordingly,

- A user will not use any account or otherwise attempt to gain access to any information that he/she is not authorized to possess.
- A user will not use AAUNet facilities, or otherwise attempt to access any file or device, to disclose information that he/she is not authorized to possess.

2.2.5 Communications

In general, for the purpose of this policy, abuse of any facility at another/remote site accessed from AAUNet is regarded as abuse of AAUNet facility.

The University grants the user a local account. The user can make an outgoing network connection to access (or attempt to access) a remote account, only when

- the user is the holder of the remote account, or
- the provider of the remote computer system recognizes the remote account as a public access account.

The user will access, or attempt to access, remote accounts in a manner that abides by the conditions of use of the remote computer system.

The restrictions on outgoing connections are:

- the provider accepts the type of connection
- only the provider may make a connection, using network management equipment, to AAUNet facilities.

The University may impose any other restrictions on an outgoing connection from any system under that University's control.

A user will inform the University of any details known to the user regarding any violation of this policy.

2.2.6 Internet security

- The Internet will be treated as a potentially hostile environment.
- Access to the Internet will be made only from registered systems.
- Security on these systems will be tightly controlled.
- A firewall will be used on all such systems.
- All data packets and connection requests will be controlled by the firewall.
- Only explicitly permitted traffic is allowed through the firewall.
- All other traffic is rejected.
- All traffic passing through the firewall must be capable of being logged and audited.
- Packet filtering will be used with rules, which keep the risk to a minimum.
- Where possible, access by outside users (e.g. by using modems) will be restricted.

2.2.7 Electronic mail

The University provides electronic mail services to support its academic and administrative functions. This service is available for use in accordance with the applicable rules and regulations. Any use of this service which interferes with these rules and regulations is forbidden.

2.2.8 Web publishing

The University provides web publishing services to support its academic and administrative functions. This service is available for use in accordance with the applicable rules and regulations. Any use of this service which interferes with these rules and regulations is forbidden.

2.3 Users

Authorized users of AAUNet tools and resources include faculty, staff, students, and affiliated individuals or organizations authorized by the President or his/her designee.

A user may be given access to all or a particular part of AAUNet facilities, depending on individual work or study requirements

2.3.1 Rights

Users have a right to privacy while engaged in legitimate activity. This right may on occasion be superseded as indicated in 3.3 below (Privacy). Users also have a right to adequate AAUNet facilities to carry out legitimate activity.

2.3.2 Responsibilities

Users’ responsibilities include:

- being aware of USP and related policies
- ensuring that confidentiality and privacy of data is maintained.
- the safekeeping of their user-id and password.
- ensuring the security of their terminal/workstation by logging off or locking it when it is left unattended.
- compliance with all relevant Regional, Federal and International law
- compliance with the provisions of this policy and all other University policies & procedures
- avoiding excessive use of AAUNet facilities, which may conflict with the rights of others
- compliance with any quotas or limits imposed by the University
- adherence to accepted community standards of expression or ‘netiquette'’, when communicating with other people using any computer system.

The “Usage rules” define the appropriate use of AAUNet facilities. Users are required to read and agree to abide by these rules.

If as an agent/representative of the University, the user has been granted access to external/remote systems, the user agrees to abide by the rules of the remote site.

2.3.3 Privacy

Users have a legitimate expectation to privacy in the carrying out of approved activity.

No user should view, copy, alter, transfer, own or destroy another’s personal electronic files without permission.

The University also has a legitimate right to inspect any data on a computer system on AAUNet (regardless of data ownership), to prevent, detect or minimize unacceptable behavior on that computer system. Where such action is taken, users who have data inspected, and are found to be conforming to this policy, have a legitimate expectation that confidentiality will be preserved. This section formalizes this agreement.

a) The University may monitor or use any account, device, or terminal without notice.

b) The University may inspect, without notice, any data on any resource owned by the University (regardless of data ownership), including electronic mail and other forms of communication.

c) In the course of carrying out computer system auditing operations, the University may access and copy any file on any computer system owned by the University. Subject to all other conditions of this policy, the University is obliged to maintain confidentiality as a result of such access.

d) The University is free to capture and inspect any data on any networking infrastructure owned by the University.

e) The University has the right to give to any appropriate member of the University community, or law enforcement bodies, any information it possesses regarding the use of the University's resources.

The Executive Director will authorize specified staff whose duties include monitoring the use of AAUNet facilities to investigate the suspected security breaches or unauthorized access.

In general, however, the University does not monitor or restrict the content of material transported across AAUNet.

2.4 System administrators

AAUNet system administrators are responsible for:

- Developing, operating and administering the AAUNet facilities in accordance with the USP and related guidelines, and the requirements of users
- Issuing guidelines, with the approval of the Executive Director for the secure operation of the components of AAUNet facilities.
- Maintaining and operating AAUNet facilities in a manner which effectively balances security with users needs to use them free from undue intervention
- Maintaining security awareness by provision of information and training on the USP to users of AAUNet facilities which they manage
- Periodically monitoring and reassessing security measures to ensure their effectiveness and to respond to changes in security requirements
- Reporting all security incidents to the Executive Director immediately when it is known that a breach has occurred.

Each system administrators at a campus level has the authority and responsibility to take actions for the support and security of its respective campus AAUNet facility.

Campus system administrators should restrict actions to their domain of responsibility except by mutual agreement with other affected/concerned campuses.

Campus administrators may adopt additional rules and regulations as required at campus levels to meet specific requirements. Such rules and regulations must however be:

- consistent with the policies of AAU
- be posted in writing or electronically in a manner that is available to all affected users
- and be filed with ICTC.

System administrators at the central level will test and investigate software and action that pose risks to the security of AAUNet facilities, and will as necessary take corrective and/or proactive measures with or without prior notice to campus administrators.

2.5 Security management

2.5.1 Account management

Responsibility: The responsibility for the administration of USP related procedures must be assigned to specific personnel in such a way that the procedures can be implemented and monitored while still guaranteeing that the overall security of AAUNet facilities is not compromised.

> The overall responsibility for the administration of USP rests with the Executive Director.
>
> As part of the security procedures, access to AAUNet facilities must be monitored on a continuing basis and audit trails or access logs maintained.

Detection and prevention of account misuse: It is in the interests of all account holders that the University negates or minimizes any potential or actual security breach. The University may disable an account without notice, regardless of whether the account itself is suspected of misuse.

All other accounts owned by the account holder may also be disabled without notice. The University decides the nature and period of account suspension.

All unsuccessful attempts to logon to AAUNet facilities must be logged and the connection disabled after four unsuccessful attempts.

Terminals which are logged in and inactive for an extended period of time, and which are not being used to process or monitor foreground or background tasks, must be automatically logged off and the details logged for later review.

See 2.7 for more on Account Management.

2.5.2 Password management

Passwords are a primary defense mechanism on AAUNet. Careful selection of passwords improves security. Individual users are responsible for the robustness and maintenance of their own passwords. Individual users are responsible for the defense of any accounts held by them.

When one chooses a password, one should keep in mind that the password should be something that he/she can easily remember but others would be unlikely to guess. All passwords must conform to the following rules.

- Passwords must be used where possible
- A newly-issued password must be changed as soon as possible after issue
- Passwords must be at least 8 characters in length, and could be a mix of alphabetic and special characters.
- Passwords must be changed regularly, within a period determined by the System Administrators.
- Passwords must not be disclosed to others
- Passwords should not be easily associated with a particular user.
- Users will not save passwords electronically within applications as far as practically possible.
- A user who realizes that a password has been compromised shall change the password, if possible. In addition, the user is required to report all details of the breach to the responsible system administrator.
- Passwords shall be checked by the user to ensure that they comply with guidelines and are non-trivial.
- Information on correct selection of passwords shall be readily available and widely distributed.
- The use of automatic logons is discouraged.
- Each password must be personal to a particular user except when the user and another person have shared duties with joint access to the part of AAUNet facilities to which the password relates. Unless under such circumstances, it is an offence for a user to make his/her password available to another person.

2.5.3 Security breaches

Deliberate attempts to degrade the performance of the AAUNet facilities or to deprive authorized personnel of resources or access to any AAUNet facility is prohibited. Breach of security includes, but not limited to, the following: creating or propagating virus, hacking, password grabbing, disc scavenging, etc.

The University will refer any incident involving a possible breach of Regional, Federal or International law to the appropriate authority for investigation. The University will give that authority all reasonable assistance requested.

If a security breach occurs in which a person or organization external to the University is involved as a potential victim of the breach, the University will refer to the external party the details specific to that party.

If a security breach involves facilities strictly internal to the University, the University may follow the appropriate University disciplinary procedures.

2.5.4 Security incident reviews

The person who carries out technical investigation of a security breach shall submit a report to the Executive Director outlining the following details where possible:

- the general nature of the security breach
- the general classification of people involved in the security breach, (such as external users, privileged staff member)

- the AAUNet facility involved in the security breach
- the details of the security breach
- the impact of the security breach
- unrealized, potential consequences of the security breach
- possible courses of action to prevent a repetition of the security breach
- side-effects of those courses of action.

Where appropriate, remedial actions should be taken on the basis of such report.

The following steps are listed in the order that they should be taken. Once a breach is confirmed, these steps should be taken as urgently as possible. If a particular step is not appropriate to the breach, it should simply be skipped.

a) The Executive Director should be notified immediately.

b) The University shall refer any incident involving a possible breach of Regional, Federal or International law, to the appropriate authorities as soon as possible. The University will provide all reasonable assistance to the authorities concerned.

c) If another academic or administrative unit is involved, that unit should be notified as soon as possible, preferably via the Head or an approved representative.

d) If a security breach involves facilities strictly internal to the University, applicable University disciplinary procedures shall be followed.

e) If an organization or person external to the University is involved in any capacity, then the appropriate Government security institutions should be contacted, where it is deemed necessary by the Executive Director.

e) If an organization or person external to the University is involved as a potential victim, then that organization or person should be advised as soon as possible with the details specific to the party.

2.5.5 Security audits

a) Regular auditing procedures shall be carried out on AAUNet facilities to check for conformance to policy. The depth and regularity of each level of audit should be outlined in the local/campus procedures manual.

b) Audit procedures, of any level, may be carried out on any AAUNet facility at the discretion of the University.

c) In the course of the auditing procedure, the University may delete or otherwise modify any data on any AAUNet facility that promotes a contravention of this policy or the host configuration guidelines in the local/campus procedures manual, in order to re-establish system security.

Unauthorized access attempts

All unauthorized access attempts must be noted and logged. The Audit Trail/System Access Log should be reviewed daily, exception reports generated and inspected by the System Administrators and appropriate action taken. A copy of the report of unauthorized access attempts must be produced and kept for future reference.

2.5.6 Disaster recovery

A disaster recovery plan shall be implemented which takes into account the risk assessment, the University's needs and vulnerabilities. The disaster recovery plan shall be documented and tested periodically.

2.5.7 Distributions, review and amendment of security policy

This policy shall be:

- Distributed to designated officers, who shall receive registered copies.
- Reviewed by the ICTC at least annually.
- May be amended as required.
- When amended, each registered copy of the former policy shall be replaced by a copy of the new policy.
- Available on the AAU World Wide Web pages.

2.5.8 Training

The level of security that can be implemented within the University depends to a large extent on the understanding and co-operation of all staff and students. The key to good security is based on staff and student awareness and training.

Personnel and students who have been granted access to AAUNet facilities have a responsibility for the safe keeping of data within their own area of work and or access. Users must be aware of the ways in which the security of data can be enhanced.

To assist users to gain an understanding of how AAUNet security can be enhanced it is necessary to:

- define personnel policies and procedures.
- provide education and appropriate supervision.
- ensure an understanding of confidentiality requirements.

It is essential that all aspects of AAUNet security, including confidentiality, privacy and procedures relating to system access, should be incorporated into formal staff induction procedures for all new staff and be conveyed to existing staff on a regular basis.

Similar training for students shall be provided when they first enroll at the University. Each employee and student, on commencement of employment or education, should be made aware that they must not divulge any information that they may have access to in the normal course of their employment or education. Staff and students must also be made aware that they should not seek access to data that is not required as part of their normal duties.

2.6 Proper usage rules

2.6.1. General

Among others, the major reasons for establishing a usage rule are:

- to keep the security/level of trust of the system;
- to maintain the life of the system;
- to ensure that the secrecy and privacy of other users are kept;
- to ensure that the law of the land and the University are kept.

This section defines the proper usage of AAUNet facilities. Each user is expected to be aware of the rules and regulations. As one cannot claim to be exhaustive, in case of encountering an undefined area we resort to our basic philosophy: “Everything not explicitly allowed is prohibited.”

It should be noted that usage of AAUNet facilities is a privilege and must be treated as such by all users.

By understanding the rationale of the usage rules, users are expected to use AAUNet facilities in a manner which is ethical, lawful, effective and efficient. Failure to abide by these rules will be treated as misconduct and may result in disciplinary action being taken against the offending user(s). Should the violation infringe the laws of the land, the violation may constitute a legal offence.

2.6.2. Rules

The following rules are a guide to the use of AAUNet facilities.

a) The AAUNet facilities are to be utilized for the pursuit, accrual, dissemination, and communication of administrative and academic endeavors pertaining to the University. AAUNet facilities may also be used for interpersonal communications and personal information accrual provided that such uses conform to the moral and ethical principles endorsed by the University and the community it is operating in. Always education and work related tasks take precedence.

b) A user must not use University computing facilities for commercial gain or for commercial gain to a third party without the written permission of the President or his/her designee

c) A user must not attempt to use the facilities for any application that result in any direct cost to AAU

d) A user must only use those facilities which he/she has been authorized to use. Where access to a facility is protected by a password, a user must not make this password available to any other person. A user must not use an account set up for another user nor make any attempt to find out the password of a facility which he/she is not entitled to use. A user must not attempt to find out the password of any other user.

e) A user must respect the privacy and confidentiality of data held on, or reproduced from, AAUNet facilities. Any release of data to those not authorized to receive it is expressly forbidden. Unauthorized release of data may lead to legal action being taken.

f) A use must be aware of the law of copyright as it affects computer software. Copyrighted software may not be copied without the express permission of the copyright owner.

g) A user must not attempt to copy, move, and/or delete data belonging to other users, staff, students or external users, without their express permission.

h) A user may grant other users or groups of users access to your own files by setting the appropriate file protection.

i) A user must not attempt to interfere with the operation of any of the AAUNet facilities.

j) A user must not attempt to subvert the security of any of the AAUNet facilities.

k) A user must not run network-based analysis and attack programs (including running security and cracker tools), or processes that consume significant amount of network resources.

l) A user must not inject or otherwise introduce computer viruses into the AAUNet facilities

m) A user must not attach a modem or any other communication device which will provide an external connection to the AAUNet facilities. Exceptions may be permitted for staff or graduate students working from home or field sites. These must be cleared with the Executive Director.

n) A user must not use the AAUNet facilities that is relying upon computing or networking media belonging to the University to send obscene, offensive or harassing messages.

o) All material a user sends over the network with an identification of his/her affiliation to the University must be presented in a professional manner and uphold the reputation of the University.

p) While using AAUNet, anonymity is not allowed. A user must not, under any circumstance, represent himself/herself as someone else, fictional or real. All user work must be attributable to him/her.

q) A user must not broadcast email messages without prior approval of AAUNet System Administrators

r) A user must, upon request by an authorized member of staff, produce evidence of identity when using any of the AAUNet facilities.

s) A user must not abuse any of the AAUNet facilities. Abuse includes, but is not limited to:

- leaving the laboratory in an untidy or unsightly condition;
- collecting or discarding any output without the owner's permission;
- smoking, eating or drinking in the laboratories;
- stealing paper from printer or storage areas;
- unauthorized server
- unauthorized monitoring
- flooding
- commercial gain
- political advertising or campaigning

t) A user must abide by any relevant instructions given by the System Administrators. Such instructions may be issued by notice displayed near the computer facilities, by letter, by electronic communication, in person or otherwise.

u) If a user has any doubt concerning his/her authority to use any of the AAUNet facilities, he/she should seek advice from system administrators. If users or group of users believe that they should be allowed to practice any of the denied or restricted things by these rules, they may appeal, in writing, to the respective System Administrators or the Executive Director as the case may be.

It is forbidden to register a non-AAU domain for any computer which is connected to the AAUNet without prior approval of the Executive Director.

All AAUNet resources are made available under licence agreements which restrict their use to academic research and teaching. Special arrangements, however, may be made, in some cases, to allow the resources to be used for commercially-sponsored research work, as long as prior arrangements are made. It should be noted that a charge will be made for such use.

User accounts give access to part of the AAUNet resource on the campus in which a user is located. However, users can gain access to the resources on other campuses by making prior arrangement with respective system administrators.

2.6.3. *Incident reporting*

Any system malfunction (denial of services, loss of data, etc.) should immediately be reported to network administration - users may not try to move, repair, configure, modify, or attach unknown external devices.

Suspected proper use violations (including apparent attempt at unauthorized access) must immediately be reported to System Administrators.

2.6.4 *Penalties*

In case of violation, System Administrators are allowed to stop the violator from committing further breaches even by disconnecting the offending device(s) and/or account(s).

Breach of these rules will be treated seriously and the violator will be penalized accordingly. System Administrators should log any violation or the penalties imposed and cede a copy of the log (either in a standard electronic or manual form) to the Executive Director.

Breaches of the security rules will be dealt with as follows:

a) in the case of breaches against guidelines b, c, d, f, j, k, l and n System Administrators will immediately withdraw the user's access privileges to AAUNet for a period not exceeding two months, subject to an appeal to the IT Security Committee, by the user;

b) in the case of breaches against the remainder of the guidelines, or in the case of an appeal under (i), System Administrators shall ascertain or review the facts pertaining to the alleged misuse;

c) in both cases (i and ii above) the System Administrators shall interview the person alleged to have committed the misuse. The person alleged to have committed the misuse may be accompanied by another person, as may the System Administrator. The minutes of the interview meeting should be taken.

d) after the interview, the System Administrator shall inform the alleged person whether or not the allegation is found to be proven. In the event that the allegation is found proven, the System Administrator shall be empowered to:
(a) recover any costs associated with the misuse;
(b) in consultation with the Executive Director, impose a fine comparable to the cost of the repair of the damage/offence. In this case, the offender's access privileges will be withdrawn until the fine has been paid,
(c) withdraw the offender's access privileges for a period not exceeding two calendar months;
(d) inform relevant law enforcement agencies of the facts of the case.

e) The System Administrator shall, in writing, inform the offender of the decision, the penalty imposed and the offender's right of appeal as outlined in item (vi) below. The System Administrator shall also inform the Executive Director and relevant bodies the offence and the penalty imposed.

f) The offender shall have the right of appeal against the System Administrator’s decision and/or the penalty imposed. Should the offender wish to appeal, then the offender should, within 7 days and in writing, appeal to the IT Security Committee.

g) Upon receipt of such an appeal, the IT Security Committee shall consult with the involved System Administrator, the Executive Director, to ascertain the details of the offence. The IT Security Committee may also interview the offender and call for any supporting evidence that is required to reach a decision.

After examining the evidence available, the IT Security Committee may:
(a) instruct the designated System Administrator to exonerate the offender or reduce the fine imposed;
(b) uphold the Administrator's initial finding.
suspend permanently or for as long as necessary the person from the use of all or part of the AAUNet facilities
Refer the case for criminal or civil prosecution

In either case the decision of the IT Security Committee, shall be final.

Misuse or unauthorized use of AAUNet facilities will, in many cases, constitute an offence under the laws of the land. Nothing in the University rules relating to use of these facilities may be taken as in any way diminishing or removing persons' obligations to comply with the law, or their liability to prosecution and punishment under the law.

2.7 Appendix A: user account management

The author has selected these points as a guide.

2.7.1 Account quotas

Accounts have both file and mail quotas. Quotas limit the amount of disk space an account holder can use. If an account holder's disk usage exceeds the quota, he will receive a warning form the system. To avoid exceeding your file quota, periodically delete old files from your account. To avoid exceeding your mail quota, be sure to delete old email messages or save them to another location.

(state the current quota assignment)

Those users performing computation-intensive tasks should contact their Department Chair (or authorized signer) about setting up a research account with more quota.

2.7.2. Assigning accounts and UserIds

Student accounts are assigned at the beginning of each semester, and for the duration of the semester, on the basis of duly authorized lists received from faculty record offices. Where a student drops all courses after registering for the semester, this must be reported immediately to the respective system administrator.

Employees and all other users will be assigned accounts upon receipt of an authorized User Account Request Form.

Retired faculty and staff may also request a network account or request that their current account be retained after retirement by getting authorization from their respective department heads.

Authorized signers are required to check and confirm to System Administrators the status of users authorized by them on a regular basis.

Users are required to have userids and password to have access to available resources on the AAUNet.

Userids are to be created together with temporary passwords that users will later be enabled to change.

A user may belong to a group or more.

Userids must be unique university-wide.

User userids are generated from characters that appear in user names and contain a minimum of 8 characters.

For staff and postgraduate students, the userids are composed of the first (own) name of the individual followed by the first character of the second (father's) name. To further differentiate, as required, related alphabetic characters and/or digits may be suffixed (attached at the end).

For undergraduate and extension students, the first three characters if their names followed by a five-digit number in the range 00001 to 99999 may be used for userids. In this connection, arrangements must be made among campus administrators on specific ranges to be used for each campus user.

Guest accounts must first get approval by the ICTC Executive Director.

2.7.3. Account renewal

Accounts for student users must be renewed every semester.

Accounts for guests, retired faculty must be renewed annually.

System administrators will send renewal notices regularly at the end of the originally specified account period. If system administrators receive no response within a month, the account will be deactivated.

2.7.4. User account deactivation/expiry

Employee or affiliate user account deactivation or expiry will normally occur when the employee leaves AAU and when an affiliate is no longer associated with AAU.

Student account deactivation or expiry will occur if a student is not registered for a semester.

When a user account is deactivated, the user will not be able to log in with the userid or have access to files stored under it. When an account is deactivated, the files are archived and then removed from the host machine. The archived files are kept for a period of 4 months, after which the files will be deleted. As such, users are strongly advised to remove any “personal” information they may have stored on their account prior to ending their relationships with the University. As a courtesy to help users, prior arrangements can be made with system administrators to get user emails forwarded to a different account during the 4 month period.

When a user’s account is revoked their files will be treated in the same way as a deactivated account, their personal email aliases will also be deactivated.

When an employee ceases being a staff of AAU (eg. Withdraw, fired or terminate employment, or otherwise leave AAU), his/her account will be deactivated immediately.

Where an employee is assigned a new position and/or responsibilities within AAU, his/her access authorization must be reviewed. The employee must not use facilities, accounts, access codes, privileges or information for which he/she is not authorized in the new circumstances.

2.7.5 User guideline

Before using your account for the first time, you must activate it. To do this, visit the activation web site (http://www.aau.edu.et?).

When you activate your account you will be required to choose a password. This password in conjunction with your username, allows you to access your account. To ensure privacy, whenever you type a password, the characters will not display on the screen.

Changing a password:
Logging In:
Additional Help
If you need further help,
You can call the help desk (by phone number ….)
You can send email to help@...
You can try walk-in or by-appointment consultation (visit ICTC …)

2.7.6 Some aspects for consideration in the preparation of account/service application forms

Please fill in this form to request user accounts for new users

1. New User

Name
AAU IDNO:
Title
Position
AAU unit
Room number
Telephone number
Group membership
Which Campus
Which Office
Which Standing Committee
Status (PG, UG, staff, …)
Preferred user names (up to three in order of preference):
(preferred user names can only be assigned if not already in use)
Software the user should have access to?
Database the user should have access to?
Printer the user should print to (location and type)?
Other network resources that the user should have access to?
For some services, separate registration may be required.

2. Course web space request

Please fill in this form to request a group id and directory for a course on the AAUNet web server (www.) and to specify or change the members of the group who will be allowed to modify web pages.

Your name:
Your UserId
Your email address
The semester for which you are requesting the space
The name of the course for which you are requesting space
Section number
UserIds of the people to be added to the group

3. Application for direct internet access

Please fill in this form if you would like to be able to access internet directly (rather than through the proxy server) from you own workstation.

Name
Email address
Telephone
Workstation type
Workstation location
IP number
IP name
Charge account
Supervisor usercode

4. Application for dial-in access

Please fill in this form to be able to dial-in to AAUNet. You will need an existing account to charge to.

Name
User code
Password
Email address
The IP number to be used for dialin will be supplied by ICTC

At the end of all application forms

- Declaration of Requester
- I request to use AAUNet resources on the understanding that my use will be for academic teaching, research and/or administrative work.
- I declare that I am/will be a bona fide user of AAUNet resources, and (where applicable) have completed/will complete the appropriate application form(s) requesting access permission.
- I further agree to notify AAUNet system administrators before undertaking my work which has extra funding for computing/internet services
- I also undertake not to divulge passwords to any other persons, unless specifically authorized by AAUNet system administrators, or allow other persons to use my userid.
- I have noted the conditions of AAUNet USP and hereby certify that I agree to abide by them.
- Signature of applicant
- date
- I confirm that this user’s application is valid
- Name (of authorised signer for the requester - supervisor)
- Signature
- date
- Please return the completed form in a “confidential” envelop addressed to:
- Network Administrator ….
- If you have questions about this form, please call ICTC at ext: or email:
- You will receive an e-mail message within 5 days letting you know the details of our response to your request.

Office use only:

The request is: approved or not approved
If approved,

User name:
Group membership:

Date account activated:
System Administrator
Name:
Signature:
Date:

3. Addis Ababa Library IT-related policy

All computing resources at the AAU Libraries exist for the benefit of the students and the staff. With this in mind, we encourage all users to first understand and accept the responsibilities set out by the Library. Here are some of the possible conditions of use in the Library computing resources and the network available in the University. Most of the conditions of use are straightforward common sense, but some are required by law.

3.1 Use of AAUL computing facilities is granted to students for the following purposes

- Completion of course work
- Assigned research and/or limited independent research
- Communicating via e-mail
- Others that are expected to assist the teaching, learning as well as research activities of the University.

3.2 Individuals granted access to computing equipment shall adhere to the following rules and responsibilities

- Students shall not transmit unsolicited information which contains obscene, offensive or discriminatory material to another individual, a mailing list, a news group or a public area on a Library computer. Although mailing list subscribers and/or news group readers are considered to have solicited all postings, students shall not submit entries to news groups and/or mailing lists which are considered inappropriate by the recipients. Repeated transmission of material to a person who finds such transmission offensive, obscene or discriminatory will be treated as harassment and is against AAUL and/or the country regulations. A report will be made to AAU discipline committee for appropriate disciplinary action.
- Users should respect the norm, taboo, & ethics of the society. Browsing unethical web sites, like pornography, is strictly prohibited and cannot be tolerated.
- Use of AAUL computing facilities, including desktop systems, for the purposes of private business activities or other non-educational functions violates the mission of the Library and is not permitted. Students shall not violate the license agreement on any software application installed on AAUL computers.
- Students shall not attempt to gain improper access to any computer system or account, on or off campus. Intentional interception of any electronic communication is considered improper access and may also be in violation of the rule and regulations of the Library.
- Students shall not disturb another user by causing an interruption of service on that person's terminal or workstation or in that person's home directory by either physical activity or remote access.
- Students shall not waste computers or peripheral resources. Using computers for long period of time with out considering the unbalanced supply of resources as compared to the demand is strictly prohibited.

When the above policies are violated, the person responsible for such action will be suspended from access to AAUL computing resources while a review of the situation will be made by Judicial Procedures.

4. Makerere University

4.1 ICT Resource access policy

This access policy has been developed for the general good of all users, and is aimed at ensuring that the University Information and Communication Technology (ICT) resources are utilised efficiently.

Categories of users: Undergraduate students, Postgraduate students, Administrative staff, Academic staff.

Application for Maknet access accounts: Users apply formally to the Help Desk for an account through the Deans/Directors of their faculties/ institutes or Heads of administrative units.

ICT resource users to have a minimum proficiency: Users are required to demonstrate a level of basic computer literacy, before being permitted independent access to ICT resources.

Authorisation levels: Defined by the ICT Implementation Committee (ICTIC - later ICT Steering Committee, ICTSC) according to the University Information Policy.

Cost Recovery: While the University will centrally budget for some aspects of the cost of providing services to users, users may be required to meet part of the cost of services.

Booking usage: Users are required to make a time slot reservation according to a publicised procedure of their user units.

Use of passwords: All accounts shall be password protected.

Privacy of users: Users are advised that monitoring of transactions shall be carried out in the interests of system security.

Resources meant for academic and administrative purposes: All ICT resources are meant for only academic and administrative purposes.

Intellectual property rights: It is the policy of the University to permit and use only freeware or licensed software

Safety: Users must familiarise themselves with the emergency procedures in case of fire that are separately published by the university.

Users should note that all equipment operates at voltages that can lead to fatalities.

No drinks and food of whatever description is permitted in computer rooms.

Physical security of resources: Users are required to register with the supervisor on duty as they enter or leave any computer room.

Equipment may be taken into or removed from any computer room only with the express written permission of relevant Network Administrator or her/his designated representative.

Offensive, malicious and illegal application of facilities: The following will be considered offences and shall lead to suspension or termination of access and disciplinary proceedings.

- Any deliberate attempt to bypass system security
- Deliberate dissemination or transmission of viruses or other code designed to stop or downgrade the operation of the university or other networks
- Permitting another or other persons to gain access to the resources using one's account.
- Unauthorised removal of ICT equipment from any location.
- Use of resources for commercial purposes, unless formally sanctioned at an agreed cost by DICTS.
- Using the resources to access sites that publish pornographic material
- The generation and/or transmission of offensive or harassing materials;
- The deliberate undermining or compromising of the security and/ or integrity of other sites;
- Violation of intellectual property rights.
- The taking of any action that contravenes the law; and other actions that can be interpreted in this general category;

4.2 Guidelines/requirements to access MAKNET

With the establishment of the wireless backbone with a dedicated Internet link, academic and administrative units have the opportunity to use modern communications. It is however necessary for faculties to take some minimum steps in order to gain access. The following guidelines/ requirements for getting connected are based on the general good of the university and the sustainable exploitation of the university information resources.

- The LAN should have reasonable facilities and opportunity for student access, Should have reasonable facilities for staff access, preferably at office level.
- There should be a clearly defined access policy to facilities.
- There should be a senior member of staff who, as an additional assignment, is responsible for the day-to-day management of the computer facilities.
- There should be a technician or other competent person who is or can be trained as a Network Administrator.
- There is a server room, physically secured, normally only accessed by the technician and the DICTS Network Administrator.
- There should be visible and budgeted actions by the Faculty to ensure that computer resources are properly maintained in a clean environment.
- The faculty shall supply a list of users (students and staff) in soft form to DICTS for the assignment of access rights.
- The faculty shall undertake to assume the responsibility for any user based cost recovery charges.