Assam University

Internet /Intranet Usage Policy
Website Usage Policy
and
Email Account Usage Policy

Prepared By

Computer Centre
Assam University Silchar

A. Campus Network Backbone Operations

1. The campus network backbone and its active components are administered, maintained and controlled by Computer centre.
2. Computer Centre operates the campus network backbone such that service levels are maintained as required by the University Sections, departments, and divisions served by the campus network backbone within the constraints of operational best practices.

B. Physical Demarcation of Campus Buildings' Network

1. Physical connectivity of campus buildings already connected to the campus network backbone is the responsibility of Computer Centre.
2. Physical demarcation of newly constructed buildings to the "backbone"is the responsibility of Computer Centre. It essentially means exactly at which location the fiber optic based backbone terminates in the buildings will be decided by the Computer Centre based on the admissibility/approval of the Assam University Authority . The manner in which the building is to be connected to the campus network backbone (whether the type of connectivity should be of fiber optic, wireless or any other media) is also the responsibility of Computer Centre.
3. Computer Centre will consult with the client(s) to ensure that end-user requirements are being met while protecting the integrity of the campus network backbone.
4. It is not the policy of the University to actively monitor Internet activity on the network, it is sometimes necessary to examine such activity when a problem has occurred or as per the reports received from the National knowledge Network (NKN) when optimizing traffic on the University's Internet links.

C. Network Expansion

Major network expansion is also the responsibility of Computer Centre. Every 3 to 5 years on the basis of the requirements of the users departments and the approval of the authority, Computer Centre reviews the existing networking facilities, and need for possible expansion. Network expansion will be carried out by Computer Centre when the university makes the necessary funds available.

D. Wireless Local Area Networks

1. Where access through Fiber Optic/UTP cables is not feasible, in such locations Computer Centre considers providing network connection through wireless connectivity.
2. The entire Assam University Academic campus is Wi-Fi enabled under the MHRD Campus Connect project. Further, Computer Centre is authorized to

consider the applications of Sections, departments, or divisions for the extension of Wi-Fi network with specific approval of the authority.

3. Computer Centre is authorized to restrict network access to the Sections, departments, or divisions through wireless local area networks either via authentication or MAC/IP address restrictions.

E. Electronic logs

Electronic logs that are created as a result of the monitoring of network traffic need only be retained until the administrative need for them ends, at which time they should be destroyed.

F. Global Naming & IP Addressing

Computer Centre is responsible to provide a consistent forum for the allocation of campus network services such as IP addressing and domain name services. Computer Centre monitors the network to ensure that such services are used properly.

G.Providing Net Access IDs and email Accounts

Computer Centre provides User-Ids for Net Access and email accounts to the individual users to enable them to use the campus-wide network and email facilities provided by the university upon receiving the requests from the individuals on prescribed proforma. The prescribed proforma (NKN AND WIFI ACCESS REGISTRATION FORM) is made available to the users through www.ausnkn.in.

H. Network Operation Center

Computer Centre is responsible for the operation of a centralized Network Operation Control Center. The campus network and Internet facilities are available 24 hours a day, 7 days a week. All network failures and excess utilization are reported to the Computer Centre technical staff for problem resolution. The Assam University Campus Network facility is main tained through outsourcing agency. The contact of the technical support staffs are available in the Assam University website. For Wired Network related problems the url is http://www.aus.ac.in/for-wired-network/ ; For Wireless Network related problems the url is http://www.aus.ac.in/for-wireless-network/

Non-intrusive monitoring of campus-wide network traffic on routine basis will be conducted by the Computer Centre. If traffic patterns suggest that system or network security, integrity or network performance has been compromised, Computer Centre will analyse the net traffic offending actions or equipment are identified and protective restrictions are applied until the condition has been rectified or the problem has been resolved. In this process, if need be, a

report will be sent to higher authorities in case the offences are of very serious nature.

I. Network Policy and Technology Standards Implementation

Computer Centre is authorized to take whatever reasonable steps are necessary to ensure compliance with this, and other network related policies that are designed to protect the integrity and security of the campus network backbone.

J. Receiving Complaints

Computer Centre may receive complaints from the user departments through emails or over telephone, if any of the network related problems are noticed by them

Computer Centre may receive complaints from the users if any of the user is not able to access network due to a network related problem at the user end. Such complaints may be generally through phone call to Computer Centre.The designated FMS person from Computer centre receives complaints from the users/COMPUTER CENTER and coordinates with the user/service engineers of the network hardware or with internal technical team to resolve the problem within a reasonable time limit.

K. Scope of Service

Computer Centre will be responsible only for solving the network related problems or services related to the network.

L. Disconnect Authorization

Computer Centre will be constrained to disconnect any Section, department, or division from the campus network backbone whose traffic violates practices set forth in this policy by Computer centre or any network related policy. In the event of a situation where the normal flow of traffic is severely degraded by a Section, department, or division machine or network, Computer centre endeavors to remedy the problem in a manner that has the least adverse impact on the other members of that network. If a Section, department, or division is disconnected, Computer Centre provides the conditions that must be met to be reconnected.

Maintenance of Computer Hardware & Peripherals

A. Maintenance of Computer Hardware & Peripherals

COMPUTER CENTER is responsible for maintenance of the university owned computer systems and peripherals that are either under warranty or annual maintenance contract, and whose responsibility has officially been entrusted to this unit. The maintenance is carried out through outsourcing agency. The technical staffs of the outsourcing agncy are available in Computer Centre on all working days for attending the maintenance related works for Computers and the peripheral devices. The contact phone number s and email-ids of the technical support staffs are available in the Assam university website in the url http://www.aus.ac.in/for-computer-and-peripherals/

B. Receiving Complaints

COMPUTER CENTER may receive complaints from the user departments, if any of the particular computer systems are causing system related problems. COMPUTER CENTER may receive complaints from the users if any of the computer systems or peripherals that are under maintenance through them are having any problems. The designated person in COMPUTER CENTER receives complaints from the users of the computer systems and coordinates with the service engineers of the respective brands of the computer systems (if the same is not covered under AMC) to resolve the problem within a reasonable time limit.

C. Scope of Service

COMPUTER CENTER will be responsible only for solving the hardware related problems or OS or any other application software that were legally purchased by the university and was loaded by the company.

D. Installation of Un-authorised Software

COMPUTER CENTER or its service engineers does not encourage installing any unauthorized software on the computer systems of the users. They are strictly refrain from obliging such requests.

E. Reporting IT Policy Violation Incidents

If COMPUTER CENTER or its service engineers come across any applications that are interfering with the network operations or with the IT policies of the university, such incidents should be brought to the notice of the Computer centre and university authorities.

F. Reporting incidents related to Network

Operations When the network port of any particular computer system is turned off due to virus or related activity that is affecting the network performance, the same will be informed to the corresponding user(s) by COMPUTER CENTER. After taking necessary corrective action at the user end COMPUTER CENTER is informed about the same, so that the port can be turned on by the centre.

G. Rebuilding the Computer System

When the service engineers reformat the computer systems and re-install OS and other application software, care should be taken to give the same hostname, IP address, network Mask, gateway as it was having earlier. Further, after installing the OS all the patches/latest service pack should also be properly installed. In case of anti-virus software, service engineers should make sure that its latest engine and pattern files are also downloaded from the net. Further, before reformatting the hard disk, dump of only the data files should be taken for restoring it back after proper re-installation. Under no circumstances, software files from the infected hard disk dump should be used to write it back on the formatted hard disk.

Responsibilities of Department or Sections

A. User Account Any Centre, department, or Section or other entity can connect to the University network using a legitimate user account (Net Access ID) for the purposes of verification of affiliation with the university. The user account will be provided by Computer centre, upon filling up the prescribed application form available in the website and submitting it online to Computer Centre. Once a user account is allocated for accessing the university's computer systems, network, mail and web services and other technological facilities, that account holder is personally responsible and accountable to the university for all the actions performed using that user account. Hence, users are advised to take reasonable measures such as using complex passwords, not sharing the passwords with others, not writing down the password at a place which is accessible to others, changing the passwords frequently and keeping separate passwords for Net Access Id and for email account ID) to prevent un-authorised use of their user account by others. As a member of Assam University community, when using the university' network facilities and its user account, it becomes user's duty to respect the University's reputation in all his/her electronic dealings within as well as outside the University. It is the duty of the user to know the IT policy of the university and follow the guidelines to make proper use of the university's technology and information resources.

B. Logical Demarcation of Department/ Section/Division Networks

In some cases, Section, department or Division might have created a internal network within their premises. In such cases, the Section, department, or division assumes responsibility for the network service that is provided on all such internal networks on the School, department or divisions of the network backbone. The School, department, or division is also responsible for operating the networks on their side of the network backbone in a manner that does not negatively impact other network segments that are connected to the network backbone.

C. Supply of Information by Section, Department, for Publishing on /updating the Assam University Web Site

Each department, or division should identify at least one person as a Point of Contact (Micro-site Administrator) for updating information in the respective Home page of the Department.
All Schools/ Centers, Departments, or Divisions should provide updated information concerning them periodically (at least once in a month or earlier). Hardcopy of such information duly signed by the competent authority of the (respective Head of the department) at Section, Department, or Division level, may be kept as record for future verification. This policy is applicable for

1. Updating/ Uploading the CV/Biodata of the Departmental faculty
2. Updating/ Uploading the Upcoming events of the department like Seminars. Conferences, Symposiums, etc.
3. Updating/ Uploading the employment notifications under Project vacancies/ Guest faculty, etc.
4. Updating/ Uploading the Tender Notifications of the departments

If any information other than the categories mentioned above are to be updated /Uploaded in the AU website, the Departments, Administration, sections/ Library have to provide these information to the Director Computer Centre with necessary prior approval from the competent authority along with the soft copy of the matter/contents, well in advance. On receiving such information they are uploaded in the AU website by the Website Administrator.

D. Setting up of Wireless Local Area Networks/ Broadband Connectivity

1. This policy applies, in its entirety, to school, department, or division wireless local area networks/broadband connectivity within the academic complex. In

addition to the requirements of this policy, school, departments, or divisions must register each wireless access point with Computer Centre.

2. Obtaining Broadband connections and using the computers alternatively on the broadband and the university campus-wide network is direct violation of the university's IT Policy, as university. IT Policy does not allow broadband connections within the academic complex.
3. School, departments, or divisions must secure permission for the use of radio spectrum from Computer Centre prior to implementation of wireless local area networks.
4. School, departments, or divisions must not operate wireless local area networks with unrestricted access. Network access must be restricted either via authentication or MAC/IP address restrictions. Passwords and data must be encrypted.
5. As inter-building wireless networks are also governed by the University IT Policy, setting up of such wireless .networks should not be undertaken by the Schools/Centers without prior information to Computer Centre.

E. Security

In connecting to the network backbone, a school, department, or division agrees to abide by this Network Usage Policy under the University IT Security Policy. Any network security incidents are resolved by coordination with a Point of Contact (POC) in the originating department. If a POC is not available to contact, the security incident is resolved by disconnecting the offending computer from the network till the compliance is met by the user/POC.

F. Preservation of Network Equipment and Accessories

Routers, Switches, Fiber optic cabling, UTP cabling, connecting inlets to the network, Racks, UPS, and their batteries that are installed at different locations by the university are the property of the university and are maintained by Computer centre.Tampering of these items by the department or individual user comes under violation of IT policy. Tampering includes, but not limited to,

- Removal of network inlet box.
- Removal of UTP cable from the room.
- Opening the rack and changing the connections of the ports either at jack panel level or switch level.
- Taking away the UPS or batteries from the switch room.
- Disturbing the existing network infrastructure as a part of renovation of the location Computer centre will not take any responsibility of getting them rectified and such tampering may result in disconnection of the network to that segment or the individual, until the compliance is met.

G. Additions to the Existing Network

Any addition to the existing network done by Section, department or individual user should strictly adhere to the university network policy and with prior permission from the competent authority and information to Computer centre. University Network policy requires following procedures to be followed for any network expansions:

- All the internal network cabling should be as on date of CAT 6UTP.
- UTP cabling should follow structured cabling standards. No loose and dangling UTP cables be drawn to connect to the network.
- UTP cables should be properly terminated at both ends following the structured cabling standards.
- Only managed switches should be used as far as applicable. Such management module should be web enabled. Managed switches give the facility of managing them through web so that Computer Centre can monitor the health of these switches from their location. Proactive maintenance of the active components are done using Network Management Software (NMS). However, the hardware maintenance of so expanded network segment will be solely the responsibility of the department/individual member. In case of any network problem created by any computer in such network, if the offending computer system is not locatable due to the fact that it is behind an unmanaged hub/switch, the network connection to that hub/switch will be disconnected, till compliance is met by the user/department.
- As managed switches require IP address allocation, the same can be obtained from Computer centre on request.

H. Structured Cabling as a part of New Buildings

All the new buildings that will be constructed in the academic complex here onwards should have the structured cabling included in their building plans like any other wiring such as electrical and telephone cabling, for LAN as apart of the building layout Plan. Engineering Branch may make provisions in their designs for at least one network point in each room. All such network cabling should strictly adhere to the structured cabling standards used for Local Area Networks.

I. Campus Network Services Use Agreement

The “Campus Network Services Use Agreement” should be read by all members of the university who seek network access through the university campus network backbone. This can be found on the Intranet Channel of the university web site. All provisions of this policy are considered to be a part of the Agreement. Any Section, Department or Division or individual who is using the campus network facility , is considered to be accepting the

university IT policy. It is user's responsibility to be aware of the University IT policy. Ignorance of existence of university IT policy is not an excuse for any user's infractions.

J. Enforcement

Computer centre periodically scans the University network for provisions set forth in the Network Use Policy. Failure to comply may result in discontinuance of service to the individual who is responsible for violation of IT policy and guidelines.

Responsibilities of the Administrative Units

Computer centre needs latest information from the Administrative Units of the University for providing network and other IT facilities to the new members of the university and for withdrawal of these facilities from those who are leaving the university, and also for keeping the AU website up-to-date in respect of its contents. The information that is required could be broadly of the following nature:

- Information about New Appointments/Promotions.
- Information about Superannuation /Termination of Services.
- Information of New Enrolments.
- Information on Expiry of Studentship/Removal of Names from the Rolls.
- Any action by the university authorities that makes an individual ineligible for using the university's network facilities.
- Information on Important Events/Developments/Achievements.
- Information on different Rules, Procedures, Facilities

Information related to the items mentioned above should reach Director Computer Centre well in-time. Hard copy of the information that is supplied by the concerned administrative unit duly signed by competent authority along with its soft copy (either on mobile storage devices or mobiles or PDA or by email) should be sent to Computer Centre so as to reach the above designated person.

Guidelines for Desktop Users

These guidelines are meant for all members of the AU Network User Community and users of the University network. Due to the increase in hacker activity on campus, University IT Policy has put together recommendations to strengthen desktop security. The following recommendations include:

1. All desktop computers should have the latest version of antivirus such as Symantec AntiVirus (PC) or Quick Heal or Kaspersky, or any other licensed Anti Virus and should retain the setting that schedules regular updates of virus definitions from the central server at Intrenet.

2. When a desktop computer is installed, all operating system updates and patches should be applied. In addition, operating system updates and patches should be applied regularly, on an ongoing basis. The frequency will be abalance between loss of productivity (while patches are applied) and the need for security. We recommend once in a week cycle for each machine. Whenever possible, security policies should be set at the server level and applied to the desktop machines.

3. All Windows desktops (and OS X or later Macintosh desktops) should have an administrator account that is not used as the regular login account. The login for the administrator account should be changed from the default.

4. The password should be difficult to break. Password, defined as:
   i. must be minimum of 6-8 characters in length
   ii. must include punctuation such as ! $ % & * , . ? + -=
   iii. must start and end with letters
   iv. must not include the characters # @ ' " `
   v. must be new, not used before
   vi. Avoid using your own name, or names of your wife or children, or name of your department, or room No. or house No.etc.
   vii. passwords should be changed periodically and also when suspected that it is known to others.
   viii. Never use ‘NOPASS’ as your password
   ix. Do not leave password blank and
   x. Make it a point to change default passwords given by the software at the time of installation.

5. The password for the user login should follow the same parameters outlined above.

6. The guest account should be disabled.

7. New machines with Windows XP should activate the built-in firewall.

8. All users should consider use of a personal firewall that generally comes along the anti-virus software, if the OS does not have an in-built firewall.

9. All the software on the compromised computer systems should be re-installed from scratch (i.e. erase the hard drive and start fresh from installation disks). When the hard disk of the PC is formatted, the OS and all the application software should be installed from the original CDs of the software. Only the data or document files should be copied from the old hard disk and care should be taken to see that no virus residing in the old hard disk gets into the newly formatted and installed hard disk.

10. Do not install Microsoft IIS or turn on any of its functions unless absolutely necessary.

11. In general, start from a position of security that is most secure (i.e. no shares, no guest access, etc.) and open up services as necessary.

Email Account Use Policy

In an effort to increase the efficient distribution of critical information to all faculty, staff and Ph.D/M.Phil research scholars, and the University's administrators, it is recommended to utilize the university's e-mail services, for formal University communication and for academic & other official purposes. E-mail for formal communications will facilitate the delivery of messages and documents to campus and extended communities or to distinct user groups and individuals. Formal University communications are official notices from the University to faculty, staff and students. These communications may include administrative content, such as human resources information, policy messages, general University messages, official announcements, etc. To receive these notices, it is essential that the e-mail address be kept active by using it regularly. Staff and faculty may use the email facility by logging on to https://mail.aus.ac.in/ with their User ID and password. For obtaining the university's email account, user may contact Computer Centre for email account and default password by submitting an online application in a prescribed proforma available in http://www.aus.ac.in/wp-content/uploads/2018/06/WAR-Form.pdf Users may be aware that by using the email facility, the users are agreeing to abide by the following policies:

1. The facility should be used primarily for academic and official purposes and to a limited extent for personal purposes.
2. Using the facility for illegal/commercial purposes is a direct violation of the university's IT policy and may entail withdrawal of the facility. The illegal use includes, but is not limited to, the unlicensed and illegal copying or distribution of software, sending of unsolicited bulk e-mail messages. And generation of threatening, harassing, abusive, obscene or fraudulent messages/images.
3. While sending large attachments to others, user should make sure that the recipient has email facility that allows him to receive such large attachments.
4. User should keep the mail box used space within about 80% usage threshold, as 'mail box full' or 'mailbox all most full' situation will result in bouncing of the mails, especially when the incoming mail contains large attachments.
5. User should not open any mail or attachment that is from unknown and suspicious source. Even if it is from known source, and if it contains any attachment that is of suspicious nature or looks dubious, user should get confirmation from the sender about its authenticity before opening it. This is very much essential from the point of security of the user's computer, as such messages may contain viruses that have potential to damage the valuable information on your computer.
6. Users should configure messaging software (Outlook Express, etc.,) on the computer that they use on permanent basis, so that periodically they can download the mails in the mailbox on to their computer thereby releasing the disk space on the server. It is user's responsibility to keep a backup of the incoming and outgoing mails of their account.

7. User should not share his/her email account with others, as the individual account holder is personally held accountable, in case of any misuse of that email account.
8. User should refrain from intercepting, or trying to break into others email accounts, as it is infringing the privacy of other users.
9. While using the computers that are shared by other users as well, any email account that was accidentally left open by another user, should be promptly closed without peeping into its contents, by the user who has occupied that computer for its use.
10. Impersonating email account of others will be taken as a serious offence under the university IT security policy.
11. It is ultimately each individual's responsibility to keep their e-mail account free from violations of university's email usage policy.
12. Temporary/ Guest Faculty/ Contractual Staff/ JRF/ RA are required to renew their email account every year
13. Any Spam mail received by the user into INBOX should be forwarded to spam@mail.aus.ac.in
14. Any mail wrongly stamped as SPAM mail should be forwarded ne_cc@aus.ac.in
15. All the mails detected as spam mails go into SPAM_MAIL folder of the respective users' mail accounts. Users are requested to open these folders periodically to check any important mail wrongly stamped as SPAM mail and went into this folder. If so, user may forward that mail ID to ne_cc@aus.ac.in for necessary action to delete from the spam mail category. It is recommended to empty this folder as frequently as possible.

The above laid down policies particularly 1 to 12 are broadly applicable even to the email services that are provided by other sources such as Hotmail.com, Yahoo.com, etc., as long as they are being used from the university's campus network, or by using the resources provided by the university to the individual for official use even from outside.

Mandatory TERMS & CONDITIONS for Obtaining AU Mail Server Email-id:

1. For authentication the User ID & Password will be given only through the given Email address.
2. It is mandatory to change the password after first LOGIN.
3. Computer Centre shall not share any user information with anyone unless authorized.
4. The User shall remain solely Responsible and Accountable for any type of misuse of his/ her account. Any kind of misuse will lead the account to be deactivated whenever needed.
5. Any kind of Misuse may lead to Legal consequences as per IT ACT 2000 and 2008, etc.
6. All actions on internet are punishable in the same manner as if done in the physical space.

UNDERTAKING to be given by the user:

1. I undertake that I would keep my password secret and I also understand that it is my responsibility to maintain its secrecy and I assume full responsibility for the same from the moment the password is given to me.
2. I also understand that if an unauthorized person accesses the account on my password, I will be called to question and would have to own responsibility for the same. I have put my signature onto this application form to acknowledge this accountability/responsibility.

Naming Nomenclature for Creation of Email Account (User-id) for the Research Scholars:

1. While registering Research Scholars the account would be created as: firstnamemiddlename.lastname@aus.ac.in

2. In case the above nomenclature becomes common for more than one scholar then the account would be created as:

   firstnamemiddlename.lastname1@aus.ac.in;
   firstnamemiddlename.lastname2@aus.ac.in; etc.