IT Policies

1.1. Vision, Mission and Goals

Vision: To provide adequate IT Infrastructure and quality support to the academic programs, faculty, administrative staff and students

Mission: Ensure the IT services are reliable, robust, state of art and with highest achievable quality.

Goals :

- Deliver timely and effective responses to users (faculty, staff& students) requirements through teamwork.
- Provide vision, leadership, and a framework for evaluating emerging technologies and implementing proven information technology solution.
- Ensure a reliable and secure data and voice transmission within the campus.
- Ensure effective technical and fiscal management of the Department's operations, resources, technology projects and contracts.

1.2 Policies

These policies apply to the use of computers and networks at CIT, and of computers and networks elsewhere if you use CIT resources to gain access to those computers or networks.

1.2.1. General Policy

- All registered students, faculty and staff have mailing privileges free of charge. Each individual is assigned a email account username and password that provides access to mail resources to assist them in carrying out the instructional, research, and administrative goals of the University.
- Access to CIT's computer facilities (networks, laboratory computer systems, residence hall systems, including software licensed by the University or its agents for use on University systems) is a privilege, not a right. Many members of the University community use these facilities, relying on their availability to accomplish their work and assign environ I.T managements, and to store important and confidential data, including software or computer programs. It is prohibited, and ethically wrong, for individuals to access or attempt to access or

view any account for which they do not have specific authorization; actions which intentionally disrupt, delay, endanger or expose another person's work or University operations are also prohibited. Individuals engaging in such actions will be prosecuted under the internal rules of CIT and applicable criminal statutes of Albanian. Individuals harmed by such actions may also bring civil charges against the person(s) responsible.

- Computing accounts are provided for CIT work only. No commercial activity is permitted unless approved in writing in advance by the Vice President for Finance and Administration

1.2.2. Protect yourself

- Each email account is assigned to a single individual, who is responsible for all usage under that account.
- When prohibited activity is alleged or detected, the University will pursue the owner of the account.
- To protect yourself, prevent unauthorized access by keeping your password a secret.
- There is always the possibility of a system crash, network outage, or some other interruption of your work, which may result in loss of your data, files, or software. Please take steps to minimize your risk by frequently backing up your work.
- If you have special needs, the IT Department may be able to help you work out any necessary extra procedures

1.2.3. Privacy

- In an operational sense, the Network and Telecom Systems unit generally regards files in your account and data on the network as private; that is, employees of the Network and Telecom Systems unit do not routinely look at this information.
- However, the University reserves the right to view or scan any file or software stored on University systems or transmitted over University networks, and will do so periodically to verify that software and hardware are working correctly, to look for particular kinds of data or software (such as computer viruses), or to audit the use of University resources.
- Violations of policy that come to the Network and Telecom Systems unit's attention during these and other activities will be acted upon.
- You should be aware that electronic mail and messages sent through computer networks, including the Internet, may not remain confidential while in transit or on the destination

computer system.

- Your data on University computing systems may be copied to backup devices periodically. Network and Telecom Systems makes reasonable efforts to maintain confidentiality, but if you wish to take further steps, you are advised to encrypt your data.

1.2.4. Copyright

- Software available on computers and networks is not to be copied except as permitted by the applicable software license.
- Respect for intellectual labor and creativity is vital to academic discourse and enterprise. This principal applies to works of all authors and publishers in all media. It encompasses respect for the right to acknowledgement, right to privacy, and right to determine the form, manner, and terms of publication and distribution.
- Because electronic information is volatile and easily reproduced, respect for the work and personal expression of others is especially critical in computer environ I.T managements. Violations of authorial integrity, including plagiarism, invasion of privacy, unauthorized access, and trade secret and copyright violations, may be grounds for sanctions against members of the academic community.

1.2.5. Resources and Facilities Covered by this Policy

- This policy is intended to detail the rules of conduct for users of CIT computing resources, list general prohibitions that apply and point towards additional information that may apply in certain circumstances.
- The use of computer and/or network resources at CIT is a revocable privilege. You must agree to the University's Code of Conduct (see Annex C) and abide by it. If you do not accept the Code, you are ineligible to use the CIT computing and networking facilities.
- All resources managed and overseen by CIT IT Department are covered by this policy, including computing hardware and software, documentation and other reference materials, all data residing on CIT IT Department machines and all institutional data wherever it resides, media such as CD-ROM, tape and other storage devices, and all other possessions of CIT managed by IT Department. Policy coverage will apply even in cases where the management of IT Department has authorized the temporary relocation of resources to areas not normally under the control of IT management (such as a user office or employee's home).

- IT Department considers all temporary and permanent connections via the University network, to be subject to the provisions of this policy. IT Department policy is considered to apply down to the Data Link layer in the protocol stack of user machines, which users connect to the IT Department network. All telephone equipment used by the University shall also be covered by this policy.
- Computing resources not owned or approved by CIT may not be connected to the University's network.
- IT Department reserves the right to monitor the traffic of all transmissions on networks maintained by the department at all times.
- IT Department currently maintains a variety of Linux & NT servers for use. MS Windows NT systems exist to facilitate software distribution and printing for office and student lab environ I.T managements.
- Operating systems currently supported for the desktop Windows 7. There are special requirements for Linux workstations in computer lab. Upgrading will take place in a controlled manner.
- Deans and Directors must request to have items added which are not listed. Software and hardware not on the lists may not be installed or connected to University systems without the approval of the IT Committee. This includes the data and telephone networks.
- All University affiliates (faculty, staff & students) are permitted to use the University network and selected computing resources at all times while the network is available.
- IDF rooms are under the authority and responsibility of the IT Department.
- Everyone within CIT community who uses University computing and communications facilities has the responsibility to use them in an ethical, professional and legal manner.

1.3. IT Support Services

1.3.1. Technical Support

The IT Department provides first level of support through the IT Help Desk. It covers the University network and Hardware related to Finance, Administration & Quasi-Academic Departments only.

- The IT Department provides first level of support through the IT Help Desk.
- It covers the University network and Hardware related to Finance, Administration & Quasi-Academic Departments only.
- The IT Department provides first level support for:
    - The network (e.g., infrastructure, servers, applications on the network, and security).
    - Desktops (e.g., pc's, printers, scanners, etc.) for the Finance and Administration Department only.
- First level support is defined as:
    - De-conflicting incompatibility issues.
    - Hardware add-ons or replacement.
    - Software additions or upgrades.
    - Other simple, IT related issues.
- School Computer Lab Technicians provide first level desktop support for their respective Schools. The IT Help Desk provides second level support. Anything not covered in First level support would require the IT Help Desk to handle. This may take the form of on-site repair, contacting a provider who is responsible for maintenance, or selecting a source to do the work for a fee.

1.3.2. Email Accounts

- User email accounts on IT Department systems are regulated using the following criteria:
    - IT Department management reserves the right to suspend or delete user email accounts earlier than the times specified when compelling reasons exist for such action. In all cases, one the vice-presidents will approve early suspension or deletion of access beforehand.
    - Subject to the limitations of particular systems, IT Department may force the regular changing of passwords on all accounts for all systems. This may occur every 120 days. Passwords cannot be repeated for five consecutive cycles. A cycle is the 120 day period

between password changes.

- Departments are encouraged to notify IT Department immediately about the departure of users from the University when such users have accounts which allow access to administrative data. The HR standard procedure to notify is still exercised, but early notification is critical.
- For security reasons, accounts will be locked out after 5 failed password attempts.
- Concerned users will have to contact IT help desk for account reactivation.

- Account classification and expiration details are contained in the following table:

Classification	Account expiration
undergraduate and graduate students	Graduation or termination of affiliation to CIT
Post-docs	Termination of affiliation to CIT
Retired faculty	Termination of affiliation to CIT
Adjunct faculty	employment duration + 30 days
staff & faculty	employment duration + 120 days
Hourly/wage employees	Termination of employment
Continuing education students	Last day of class or termination
Non-CIT research collaborator	1 year from start date or renewal
Visiting faculty	Duration of visit + 30 days
Contract employee/consultant	Duration of contract + 30 days
Terminated employees	30 days

- Departing staff and faculty are responsible for saving, copying, or forwarding their old emails, bookmarks, files, etc. Once they have departed, the pc will be re-used right away, It will be re-formatted and re-imaged with OS and programs currently supported:
  - If the departing member wishes to purchase their hard drive, this can be arranged.
  - Emails left on the server will be archived off-line after 90 days.

1.4. Prohibited Acts & Proper Resource Utilization

- The IT Department is neither an investigative nor a disciplinary entity in its primary responsibilities. However, in cases where University resources and privileges are abused or otherwise threatened, the department may be asked to take appropriate steps. Immediate revocation of access and subsequent prosecution by the authorities, for example, might be directed. Such revocation may be appealed to the IT committee.
- Another example would be to both discipline and hold accountable an individual who damages IT resources. Improper access or modification of CIT information in a computer system may also bring a stiff penalty.
- Prohibited acts include but are not limited to the following:

- Intentional denial of computing service to other users.
- Exploitation of insecure accounts or resources.
- Attempting to guess, crack or otherwise determine another user's password.
- Interception of network transmissions with hardware or software "sniffers".
- Forging of electronic mail or electronic news or otherwise misrepresent themselves or other individuals in any electronic communication.
- System administrators are not to use their access to examine the private information of other users except in the course of resolving problems and where access to such information is necessary. In these cases, IT staffs are required to seek permission and oversight.
- IT staff may not transfer resources (hardware, software, documentation, etc.) from designated locations without the explicit permission of their supervisor. University Services department shall be notified of the movement and shall update the employee's inventory record accordingly.
- CIT employees or students may not load any software onto their workstations or servers, which has not been purchased or is not free. Software identified as "shareware" should be examined carefully to ensure there is compliance with any licensing requirements. Under no circumstances will software binaries from unknown or illegal sources be placed on workstations or servers.
- Under no circumstances will CIT employees or students share account passwords, key combinations, alarm codes, keys, access cards or any other access control mechanism for any University resource or facility with any individual in a manner inconsistent with the policies established by their supervisor. In the absence of such policies, employees must have the explicit permission of their supervisor to share any access mechanism to any department resource.
- CIT staff or faculty who bring vendors or personal guests into CIT IT facilities must make sure that these guests are escorted at ALL times with care given to protecting CIT equipment, facilities, and information.
- IT management reserves the right to audit University owned workstations and servers without warning for the purpose of verifying software-licensing compliance.
- All computer and network access is denied unless expressly granted. Access is generally granted by the IT Department in the form of computer and network accounts to

registered students, faculty, staff, and others as appropriate for such purposes as research, education (including self-study), or University administration. University accounts are protected by passwords. Deans and Directors must verify the requirement with their signature on the application form.

- Accounts are assigned to individuals and are not to be shared unless specifically authorized. You, the user, are solely responsible for all functions performed from accounts assigned to you. Anything done through your account may be recorded. It is a violation of University Policy to allow others to use your account. It is a violation to use another person's account, with or without that person's permission.
- Your password, used with your account, is the equivalent of your electronic signature. The use of user-id and password authenticates your identity and gives your on-line affirmation the force of a legal document. You should guard your password and account as you would your check book and written signature. It is a violation of this Policy to divulge your password to anyone. It is a violation to attempt to learn the password to another person’s account, whether the attempt is successful or not.
- You may not attempt to disguise your identity, the identity of your account or the machine that you are using. You may not attempt to impersonate another person or organization.
- You may not attempt to monitor other users' data communications; you may not infringe the privacy of others' computer files; you may not read, copy, change, or delete another user's computer files or software without the prior express permission of the owner.
- You may not engage in actions that interfere with the use by others of any computers and networks. Such conduct includes, but is not limited to, the placing of unlawful information on the system; the transmitting of data or programs likely to result in the loss of the recipient's work or system downtime; the sending of "chain letters" or "broadcast" messages to lists or individuals; any other use that causes congestion of the networks or interferes with the work of others.
- You may not engage in actions that threaten or intentionally offend others, such as the use of abusive or obscene language in either public or private messages, or the conveying of threats to individuals or institutions by way of CIT computers and/or networks.

- You may not attempt to bypass computer or network security mechanisms without the prior express permission of the owner of that computer or network system. Possession of tools that bypass security or probe security, or of files that may be used as input or output for such tools, shall be considered as the equivalent to such an attempt.
- You may not alter copy or translate software licensed to another party. You may not make available copyrighted materials without the express permission of the copyright holder. Respect for intellectual labor is vital to the academic discourse. Violations of authorial integrity, plagiarism, invasion of privacy, unauthorized access, and trade secret and copyright violations may be grounds for university sanctions as well as legal prosecution.

- To summarize, access to University computing and communications equipment and facilities may be revoked for reasons including, but not limited to:
  - attacking the security of the system,
  - modifying or divulging private information such as file or mail contents of other users without their consent,
  - modifying or destroying University data, or
  - Using the networks in a manner contrary to the established guidelines.
- Finally, users may not read sensitive information simply because it is accessible to them - because of accidental exposure and/or through the malice of others who have broken into a system or are misusing their access privileges. When sensitive information is recognized as such, it should not be examined further, but reported to the keeper of the materials, if known, or reported to management, if not.

1.5. Storage Usage

- CIT provides limited disk-based storage space for individual faculty, staff, and students, for course-related materials, and for departmental materials. Such space is provided for the University community to use in accordance with the CIT Code of Conduct (See below).
- It is strictly unauthorized to store music and video files on servers for personal use.

1.6. Statement on Obscene Material

- Although there may be difficulty determining what is or is not obscene, students, faculty and staff should know that CIT IT Committee defines "obscene" as that which:
    - Considered as a whole, has as its dominant theme or purpose a shameful or morbid interest in nudity, sexual conduct, sexual excitement, excretory functions or products thereof or sadomasochistic abuse, and which goes substantially beyond customary limits of candor in description or representation of such matters and which, taken as a whole, does not have serious literary, artistic, political, or scientific value.
- The distribution, production, publication or sale of obscene items is illegal in ALBANIAN.
- Further, a student, faculty or staff member distributing obscene material could be subject to criminal prosecution.
- In addition, placing obscene material on a University server violates University policies, including but not limited to the computer usage policy, the employee standards of conduct, and the student standards of conduct. Such violations could result in disciplinary penalties.

1.7. Software Copyright Policy

- Copyright laws protect most software available for use on computers at CIT. Educational institutions are not exempt from the laws covering copyrights. In addition, software is normally protected by a license agreement between the purchaser and the software seller. The software provided through the University for use by faculty, staff, and students may be used only on computing equipment as specified in the various software licenses.
- It is the policy of the University to respect the copyright protections given to software owners by law. It is against University policy for faculty, staff, or students to copy or reproduce any licensed software on University computing equipment, except as expressly permitted by the software license. Also, faculty, staff, and students may not use unauthorized copies of software on University-owned computers or on personal computers housed in University facilities.
- Unauthorized use of software is regarded as a serious matter and any such use is without the consent of CIT and subject to disciplinary action.

1.8. IT Committees

- Three IT sub-committees are in place and have the following responsibilities:
    - Administrative IT Committee: Assessing requirements & technical evaluation. The mission statement for the committee is described below.
    - Academic IT Committee: Advising on purchasing & support of Academic Software.
    - Web Committee.

1.9. IT Policy on Notification of Potential Service Interruptions

- IT Department has in effect a policy governing the way we let you know about activities that have known potential to interrupt access to networks or systems. These would be things like upgrades to the Enterprise Server, server maintenance in a public lab that causes certain software or functions like printing to be unavailable, or planned activity by Facilities Management that affects electrical service to buildings where we have equipment. Some things, like construction crews cutting power lines, are beyond our control and definitely not planned. We will also be letting you know about these when they've interrupted our service, especially if lasting negative affects occur.
- The primary mechanism for notification about service interruptions will be a posting (notice) to the "official-announcements" newsgroup. These notices will be labeled on the subject in one of 3 ways:
    - IT PLANNED DOWNTIME,
    - IT UNPLANNED DOWNTIME, or
    - IT NOTICE OF WORK
- The third category is for activities that we do not anticipate will impact users of our machines or facilities, but which, nevertheless have that potential.
- In the case of planned downtimes or work notices, we will be giving at least 48 hours' advance notice. As soon as possible after an unplanned outage, IT staff will post an item to "official-announcements" which gives a brief description of the extent, duration, and cause of these interruptions and also indicates any ongoing problems that may have resulted. IT staff will notify the IT Computing Help Desk of all downtimes and will provide the Help Desk with information about possible problems caused by these situations along with suggested solutions. Unless otherwise specified, you should call the Help Desk with any questions that you might have.

- In addition to postings in the newsgroup, IT staff in various areas will develop additional, targeted notification procedures, such as mailing and phone lists. Wherever practical we will make those of you on an affected system or network aware of the existence of these lists so that you can identify yourselves or colleagues who should be included as well

1.10. IT Policy on Access to the CIT Network by Third Parties

1.10.1. Purpose

- The university occasionally receives requests for remote connections to its network through either dial up or internet for non-affiliated third parties (e.g., when the vendor implemented Banner). Such requests for network access are typically either from firms that provide computing support services to University departments or from metropolitan area network service providers that offer solutions to University students, faculty, and staff. This policy has been developed to ensure that all such network access requests are treated consistently, fairly, and with a minimum of delay.

1.10.2. Annual Review Process

- Third party network connections will be reviewed on an annual basis. Connections will be reviewed with the requesting departments to determine the usefulness of the connection. Connections that are no longer useful to the requesting department will be terminated at that time. The University does understand that third parties will often need to sign annual contracts with a telephone company and every effort will be made to take this into account during any connection review process.

1.10.3. Policy

- Outside agencies conducting business with the University requiring network communication will usually prefer to conduct this business using the Internet connection. In some cases, however, the University or its departments may be better served by a more direct connection between the University network and the outside agency. Reasons for this may include faster access or a more reliable connection. The following guidelines apply to any request for third-party internet connections to the University network:
    - The University's Department of Information Technology (IT) is responsible for all external connections to the University network. Departments must initiate special connections to outside agencies in a written request to IT Department. The request

must explain the nature of the desired connection, the benefit(s) expected from the connection, as well as date, time, duration and the type of the services (Telnet, Ftp, TCP, UDP, etc.) CIT IT will only open ftp/telnet access for a maximum of "5" external IP addresses, however, through these external IP addresses, no internal ftp/telnet will be allowed either to the host server or to the internal network.

- In general, no direct connection to the University network from non-centrally-contracted third parties providing computing or network support will be allowed.
- The connection must be used solely to provide the improvement in service indicated by the University department in its request. The third-party firm may provide this same set of services to other University departments in addition to the requesting department.
- Agencies with special connections must agree to abide by any and all computing-related policies, especially security and privacy policies, of the University and IT. Violation of any such policy will result in immediate termination of the connection.

1.10.4. Termination of Access

- Access to the University network is a privilege that may be granted or withdrawn by the University at any time. The University may terminate the special connection if it is determined not to be in the University's interest, or a security risk to its' internal network. However, it is generally expected that the University will choose not to remove network access outside of the annual review process unless the connection is being used in violation of one or more of the policies listed above. The University may also impose temporary service interruptions for operational reasons.

1.10.5. Application Procedure

- Sponsoring University departments should submit requests for third-party network access to:

  Information Technology Department
  it@cit.edu.al

  Tirana, Albania

- The request should include a brief description of the service being provided by the third party and the names, e-mail addresses, and phone numbers of firm's administrative and technical contacts.

1.11. Policy Revision

- Since the University is a changing environ I.T managements, and since computer technologies

and network access may be subject to change at any time, the University must reserve the right to update or revise this Policy or implement additional policies in the future. The IT Department will inform users of policy changes; however users share the responsibility of staying informed about and complying with University policy regarding the use of computer and network resources. The Policy will be accessible via the web.

1.11.1. Mission of the Administrative IT Sub-Committee

The Administrative IT Sub-Committee has the responsibility to:

- Seek immediate resolution of existing IT related problems within Administrative Departments.
- Plan for continually improving the overall I.T. platform to ensure Admin. Usesrs have full support to provide quality service.
- Responsibilities:
- 1. Representation of all administrative departments on the committee.
- 2. Problem Solving:
    - Each member of the Committee is assigned the responsibility to report or identify:
        - Shortcomings in the IT support of the areas assigned to the member.
        - Issues related to smooth implementation & interfacing of the university's applications.
    - These identified problems are discussed in the I.T. Sub-Committee, which should decide on a plan of action to resolve each problem.
    - The status of these issues should be communicated to the Committee by the IT representative.
- 3. Planning:
    - The IT Department should provide the Admin. Sub committee with plans for the year that affect Admin. Users.
    - The Admin. I.T. Sub-committee will agree on the best process to ensure minimum disruption to Admin. Users & efficient implementation plans.
    - Ensure that the I.T. strategy developed for the university is in line with the requirements of the departments represented by the committee.
- 4. Training:
    - The committee will be assessing training needs of personnel within the departments represented by the committee.
    - Ensure complete awareness by the represented departments of I.T. available services

and proposed ones.

- 5. Software:
    - The committee will be responsible for assessing software requests & technically evaluating software proposals

1.11.2. Code of Conduct for Use of Computer Services

- The purpose of this document is to establish conditions for use of the University's computing resources and services.
- The computing services at CIT are to be used in a manner that supports the mission of the University in fostering the overall academic climate.
- **Definitions:**
    - The CIT computing services refer to all computers owned or operated by the University and includes hardware, software, data, communication networks associated with these systems and all allied services. The systems range from multi-user systems to personal computers, whether free standing or connected to networks.
    - Users are all students, faculty and staff with privileges on University computing systems and services
- **Code:**
    1. Academic and Professional Ethics. Users must apply standards of normal academic and professional ethics and considerate conduct in the use of all CIT computing systems and services or any other computer system accessed by virtue of their affiliation with CIT. Users agree to and are bound by these and all other applicable rules and regulations, including the student code of conduct and Federal Laws of ALBANIAN.
    2. Identification and Authorization. Users of CIT computing services must be identified either through the physical location of an office computer or through an authorized CIT computer account in the case of multiple user systems. Students may not access or use another person's computer account or allow another person to use his or her account. Users should logout of shared systems and take reasonable precautions to secure access to office or lab computers. CIT computing systems and services may not be used as a means of unauthorized access to computing accounts or systems inside of or outside of the University's systems.
    3. Purpose. Computing services are provided in support of the teaching, research and public service mission of the University and the administrative functions that support

this mission. The unauthorized use of CIT computing services for personal profit or other activities not in furtherance of the mission of the University is prohibited.

- University computing services may be used for personal purposes such as Resume writing, E-mail and Internet (not for chatting), provided that such use does not
  - directly or indirectly interfere with the University operation of computing facilities,
  - burden the University with noticeable incremental cost,
  - interfere with the computer user's employment or other obligations to the University, or
  - violate other University regulations or laws.

4. Copyright and Intellectual Property. Computer users may use only legally obtained, licensed data or software in compliance with license or other agreements and ALBANIAN copyright or intellectual property laws.
   - Respect for intellectual labor and creativity is vital to academic discourse and enterprise. This principle applies to works of all authors and publishers in all media. It encompasses respect for the right to acknowledgement, right to privacy, and right to determine the form, manner and terms of publication and distribution.
   - Because electronic information is volatile and easily reproduced, respect for the work and personal expression of others is especially critical in computer environ I.T managements. Violations of authorial integrity, including plagiarism, invasion of privacy, unauthorized access, and trade secret and copyright violations are grounds for sanctions.
5. Privacy. Computer users must respect the privacy of others by refraining from inspecting, broadcasting, or modifying data files without the consent of the individual or individuals involved.
6. False Identity. University users of e-mail or other electronic communications shall not employ a false identity. Nor may e-mail be sent anonymously with the intent to deceive.
7. Interference: University computing services shall not be used for purposes that could cause or reasonably be expected to cause, directly or indirectly, excessive strain on any computing facilities, or unwarranted or unsolicited interference with others' use of

computing services.

- This provision explicitly prohibits the posting of unsolicited electronic mail to lists of individuals, and the inclusion on electronic mail lists of individuals who have not requested membership on the lists. Students may be required to accept membership in an electronic mailing list for a class in which they are registered or for the purpose of official communications between authorized University personnel and an identified group of students.

8. Improper or Obscene Sites. Accessing or promoting the access of OBSCENE Internet or World Wide Web Sites, including forwarding links to such sites, is strictly forbidden and grounds for strict disciplinary action up to and including expulsion (see below under Enforcement).
9. Harassment. CIT computing services may not be used to harass any individual. Sending obscene, threatening or improper messages to another individual is grounds for strict disciplinary procedures.
    - CIT computing systems and services can ONLY used in a lawful and respectful manner following University codes of conduct and applicable laws of Albanian.
10. Enforcement: Computer activity is monitored by authorized individuals for purposes of maintaining system performance and security. In instances when users are suspected of abuse of computer usage, the contents of user files may also be inspected by an authorized individual and in the case of students the Dean of the student affairs will be notified.
    - Violations of this or University policies governing the use of University computing services may result in restriction or termination of access to University information technology resources. In addition, disciplinary action may be applicable up to and including expulsion.
    - Computer use privileges may be temporarily or permanently revoked pending the outcome of an investigation of misuse, at the discretion of the Vice President for Finance and Administration in collaboration with the President, Vice President for Academic Affairs or, in case of students, Dean of student affairs.

11. Copyright and patents. All data, programs, and files placed on or contained in the University computer systems are subject to the University's copyright, patent, and privacy policies.
12. Take proper care of the equipment entrusted in your care. You will be responsible for any damage caused to the equipment.
13. Use legally software obtained software only. And do not copy for outside use university campus products granted exclusively for campus users at campus.
14. Do not violate security policy.
15. Additional rules may be in effect at specific computer facilities at the discretion of the directors of those facilities.