



Information Technology Policy for Computing, Communication and Social Media

PURPOSE

The University of Hyderabad recognizes the vital role Information Technology plays in the University's missions and related administrative activities as well as the importance in an academic environment of protecting information in all forms. As more information is used and shared in a digital format by students, faculty and staff, both within and outside the University, an increased effort must be made to protect the information and the technology resources that support it. Increased protection of our Computer and Communication resources to assure the usability and availability of those resources is the primary purpose of this policy. The ethical principles that apply to everyday community life also apply to computing and communications. Every user of University of Hyderabad has two basic rights: privacy and a fair share of resources. It is unethical for any other person to violate these rights.

The Policy lays down general guidelines for the use of computing and communication resources. We cannot enumerate all these cases. However, a thumb rule is that any activity which inconveniences users, depletes the computer center resources, or jeopardizes the security of the systems, or violates intellectual property rights of software, amounts to unethical use. Moreover, it should be noted that the punishment set out for various cases can change and can be very severe depending on the view that the University takes of the offence. Faculty, staff, and students with authorized accounts may use the IT facilities for academic purposes, official university business, and for personal purposes so long as such use does not violate any law, University IT policy or IT act of the Government of India.

SCOPE

- **People to Whom Policy Applies:** This Policy applies to everyone who accesses University Information Technology Resources, whether affiliated with the University or not, whether on campus or from remote locations, including but not limited to students, faculty, staff, contractors, consultants, temporary employees, guests, and volunteers. By accessing University Information Technology Resources, the user agrees to comply with this Policy.

Sanjay Sharma

[Signature]

- **Definition of Information Technology Resources:** Information Technology Resources for purposes of this Policy include, but are not limited to, University-owned transmission lines, networks, wireless networks, servers, exchanges, internet connections, terminals, applications, servers and personal computers. Information Technology Resources include those owned by the University and those used by the University under license or contract, including but not limited to information recorded on all types of electronic media, computer hardware and software, paper, computer networks, and telephone systems. Information Technology Resources also includes, but is not limited to, personal computers, servers, wireless networks and other devices not owned by the University but intentionally connected to the University-owned Information Technology Resources (other than temporary legitimate access via the world wide web access) while so connected.
- **Policy change:** As and when it is considered appropriate and new policies or the changes in policy will take effect immediately after a brief announcement by any means, e-mail, printed notices, or through the news groups.

PRIVACY

- On shared computer systems [like servers, HPC systems etc.] every user is assigned an ID. Nobody else should use an ID without explicit permission from the owner.
- All files belong to somebody. They should be assumed to be private and confidential unless the owner has explicitly made them available to others.
- Messages sent to other users should always identify the sender.
- Network traffic both on Intranet/Internet is implicitly private.
- Records, including logs relating to the use of computing and information resources are confidential.

A. Computing

1. Resources

- Nobody should deliberately attempt to degrade or disrupt computing and communication systems performance or to interfere with the work of others. Any attempt to disrupt service or performance on systems on or off campus can result in the loss of network privileges and disciplinary action. The following items are all examples of denial of service attacks, but are not completely inclusive:

Sanjay Sharma



- Mail bombing (sending thousands of mail messages to a group or individual)
 - Ping flooding (launching continuous ping requests at a specific machine)
 - "Smurf attacks"
 - "SYN flooding"
- ii. Loopholes in computer systems or knowledge of a special password should not be used to alter computer systems, obtain extra resources, or take resources from another person. [Reframing of Sentence required].
- iii. Computing equipment owned by academic/administrative units or individuals should be used only with the owner's permission.
- iv. University resources are provided for university purposes. Any use of computing for commercial purposes or personal financial gain must be authorized in advance. While the university makes computer resources available primarily to achieve its goals of education and research, it realizes the need to encourage the personal use of computing for the convenience of the campus community. The extent to which these resources are used for personal reasons is limited to strictly non-profit-oriented tasks. Thus, it is reasonable to allow the use of computing resources for computer mail, document preparation or other activity that can facilitate convenience or enhance productivity. Any personal use of computing resources that produces individual financial gain is prohibited unless permission has been taken and an account has been issued which releases this restriction.
- v. It is unethical to make so excessive a use of system resources [on Servers, HPC systems etc] that other users cannot obtain access to these resources. Examples include excessive use of CPU time during a period of heavy use on a timesharing system, excessive use of disk space on a system that does not limit such utilization, and use of an excessive amount of network bandwidth in an environment of networked personal computers. A novice user might well be unaware that a particular type of action constitutes "excessive use"; but once a system administrator makes him or her aware of the fact that such an action is unreasonable, that user is to be held responsible for any further such infractions.
- vi. Computing and Communication resources are University resources. Theft, mutilation, and abuse of these resources violate the nature and spirit of community and intellectual inquiry.

Sajin Kumar

[Signature]

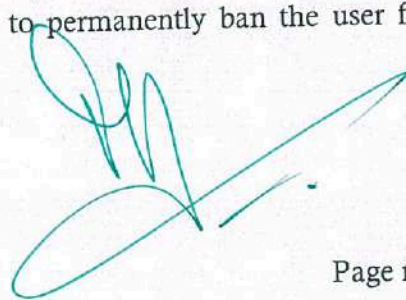
2. System Administration

- i. On rare occasions, computing staff may access others' files, but only when strictly necessary for the maintenance of a system. There may be technical reasons why a small number of system personnel must have access to all information on the system, much as custodial personnel must have keys to all offices in university buildings. Such persons bear a special responsibility not to abuse such privileges. It is improper for them to peruse a user's files for any purpose unrelated to their official functions or to appropriate or divulge any information which the user has protected from general public access.
- ii. If a loophole is found in the security of any computer system, it should be reported to the system administrator and not used for personal gain or to disrupt the work of others.
- iii. Distribution of programs and databases is controlled by the laws of copyright, licensing agreements, and trade secret laws. These must be observed.

3. Security

- i. Users are responsible for the security and integrity of their systems. In cases where a computer is "hacked into", it is recommended that the system be either shut down or be removed from the campus network as soon as possible in order to localize any potential damage and to stop the attack from spreading. In such cases, if the system administrator cannot be contacted in a reasonable time, concerned authority reserves the right to disable the network connection. Once the system administrator is made aware of the situation and agrees to take reasonable steps to ensure that the machine is not compromised, network privileges may be restored.
- ii. In cases where, despite the efforts of the system administrator, the machine continues to pose a security concern, we reserve the right to require that the user switch to a single user OS before allowing the system back onto the campus network.
- iii. In cases where a user's machines habitually cause problems, by action, as a "target" of incoming attacks, or because of a lack of responsible behavior on the owner's part, Computing Centre may initiate action to permanently ban the user from having machines on the campus network.

Sanjay Sharma



4. **Anonymous Mailers:** All electronic communications at University of Hyderabad must accurately identify the sender. Anonymous and masquerading mail forwarders are explicitly prohibited by the IT policy.
5. **Copyright Material [Example Music/Movies Files]:** It is a common misconception that the creation and subsequent distribution of music files is an acceptable activity. The distribution of copyright protected materials is illegal and is in direct violation of the Computing Code of Ethics. Movies which are protected by copyright law, and to which you do not have a license to distribute, should be treated with the same consideration as music files. Copyright material from any website using UoH resources is prohibited.
6. Obscenity material should NEVER be digitally stored, manipulated nor shared.
7. Software Piracy: Distributing licensed software is illegal and constitutes a violation of the Computing Code of Ethics.
8. Backup of critical data should be in compliance with the requirements of IT Act of India.

B. Communications

1. General Guidelines:

- a. It should also be noted that university resources, such as the campus network, are provided for university purposes. Allowing unaffiliated users to have account on campus or dedicated remote access systems could be considered as a violation of this policy.
- b. Bulk emails communicated through G-Apps will be permitted after due approval of the competent authority.
- c. Dynamically assigned IP addresses are considered to be "registered" for the period of the dynamic lease to any device on the communication network.
- d. Under no circumstances may machines be configured with IP addresses that have not been assigned by Computer Centre/CNF. By using an unregistered IP address or an IP addressed to another, you may deprive other users of network service and/or make it considerably more difficult to diagnose network problems on the campus network.

Ranjay Kumar

[Signature]

- e. The servers which have public IP addresses issued to the concerned academic/administrative unit will be liable for any breach of security.
- f. Using a different Ethernet hardware address than is registered with Computer Centre will also result in the machine being removed from the network. Users purchasing new ethernet cards, or who otherwise need to change their hardware address must inform Computer Centre in order to ensure that the information listed above is kept accurate and up-to-date.

2. Routers

- a. Routers are generally used to connect multiple network segments together and should not be necessary for individual users on our campus. If misconfigured, routers can cause severe problems for all users on a network segment. Therefore, all the Wi-Fi AP/Routers are mandated to be configured by the Campus Network Facility. For these reasons, systems connected to the campus network at any site are not permitted to act as routers.
 - b. Most operating systems do not provide routing functionality and are perfectly safe to attach to our network in any configuration. Some operating systems such as Windows/POSIX Machines/Servers have the capability to provide routing functionality; for these operating systems, you should ensure that routing is not configured and are not permitted to be attached to the campus network unless explicit permission is obtained in advance from CC/CNF.
3. Systems on the campus network are not permitted to be configured as DHCP servers. DHCP allows systems to obtain the correct IP address during the boot process. User owned DHCP servers may override the distribution of IP addresses by the official DHCP servers, causing the client system to obtain an incorrect address, denying it access to the network.
4. Domain Names: All registered machines being used for website hosting or for any research activity on the UoH/External network using the domain "uohyd.ac.in", must have the security compliance in place or given access through VPN.
5. Network Traffic: Network traffic should be considered private. Because of this, any "packet sniffing", or other deliberate attempts to read network information which is not intended for your use will be grounds for loss of network privileges for a period of not less than one full semester. In some cases, the loss of privileges may be permanent. Note that it is permissible to run a packet sniffer explicitly configured in non-promiscuous mode (you may sniff packets going to or from your machine). This allows users to explore aspects of networking while protecting the privacy of others.

Sanjay Sharma

6. Buildings on the Campus and dedicated remote access service connections to the campus network, and to the Internet, are provided to allow students, staff and faculty to fully participate in the teaching, research and administrative activities of University of Hyderabad. In general, we encourage individuals to provide useful, interesting and inventive content to the Internet community, so long as it remains feasible for us to do so.
7. It may not remain feasible to provide unlimited connectivity for systems which are not strictly serving the University's missions. Because of this possibility, we reserve the right to request that users reduce the amount of traffic being caused by their service, or where necessary, to remove such systems or services from the campus network. In all but extreme cases, we will contact the owner of the system before removing it from the network.
8. Misconfigured Services: There may be times when a machine is unintentionally misconfigured and subsequently causes a problem on the campus network. In such cases, in order to preserve the best service possible for the majority of the users, the machine will be disconnected from the campus network immediately. The owner of the system in such cases will be notified via electronic mail and via telephone that the machine has been disconnected.
9. The machine will only be allowed back onto the network after the owner notifies Competent Authority or the person who sent the electronic mail, that they have reconfigured the machine, resolving the problem.
10. Network Maintenance: Computer Centre will periodically conduct scans of various areas of the network (subnets) in order to help to maintain a reasonable network environment for the majority of our users. Results of such scanning would help to discover misconfigured systems and may in some cases cause us to discover activity which violates laws, University policies or guidelines. In such cases, action appropriate to the "problem" will be taken.

C. Social Media

1. Ensure others know that your personal account or statements don't represent the University. You shouldn't state or imply that your personal opinions and content are authorized or endorsed by the University. We advise using a disclaimer such as "opinions are my own" to avoid misunderstandings.
2. Avoid sharing intellectual property like trademarks on a personal account without approval. Confidentiality policies and laws always apply.

Rajy Sharma

[Signature]

3. Avoid any defamatory, offensive or derogatory content. It may be considered as a violation of University's anti-harassment policy, if directed towards Students, Faculty, Staff members.
4. Do not use official email addresses to register on social networks, blogs or other online tools utilized for personal use.
5. Refrain from using social media while on work time or on equipment we provide, unless it is work-related as authorized by the University.

D. Punishments for degrees of Improper Behavior:

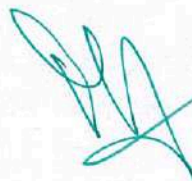
1. Violations of policy will be treated as academic misconduct, misdemeanor, or indiscipline as appropriate.
2. Improper behavior in the use of computer/communication systems is punishable under the general university policies and regulations.
3. The offenses mentioned in this statement range from relatively minor to extremely serious, though even a minor offense may be treated severely if it is repeated or malicious. Most serious of all are offenses that compromise the integrity of the academic process, such as altering grade records or plagiarism. Appropriate disciplinary action depends not only on the nature of the offense, but also on the intent and previous history of the offender.

EXAMPLES: Summary of Punishments for Improper Behavior

Blocking Resources:

1. Playing games using University's computing and communication resources, unless they are related to academic/research activities.
2. Locking the screen of machines belonging to the University.
3. Sending junk/fake mail to all the users.
4. Forwarding chain emails.

Minimum punishment is suspension of computer access facilities for two weeks. Additionally financial fine may also be imposed.



Misusing Facility:

1. Unnecessary downloads from the Internet.
2. Giving accounts to other persons, sometimes outsiders.
3. Storing pornographic material on the disk
4. Viewing pornographic material on terminals
5. Using personal account to do outside (non-institute) work for which the individual is paid.

Minimum punishment is suspension of access facilities for six months and cases being sent to concerned authorities for disciplinary action.

Security related misuse:

1. Breaking security of the systems
2. Trying to capture password of other users
3. Damaging/gaining access to the data of other users

This kind of abuse is taken most seriously. Anyone found involved in these activities will have access being denied for one year. The cases will be sent to concerned authorities for necessary disciplinary action.

Anonymous mail forwarding

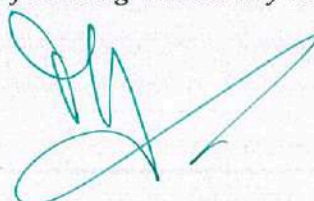
Running of such a service is grounds for removal of campus network privileges for a period of not less than one full semester.

Software related Misuse:

1. Using any kind of software without correct licenses

This kind of abuse is taken most seriously. Anyone found involved in this activity will have access to facilities being denied and will be liable for direct action from the software provider / manufacturer / company for any breach of licensing without any responsibility of the University.

Rajiv Arora



2. Downloading/Distributing copyrighted materials

Users found to be misusing network connections for stated purpose will have their privileges revoked for not less than one full semester and may be subject to disciplinary action.

Network related Misuse:

1. Using an IP address which you have not been assigned or using an ethernet hardware address which is different from the one registered with Computer Centre.

This kind of misuse is grounds for losing your campus network privileges for a period of not less than one full semester.

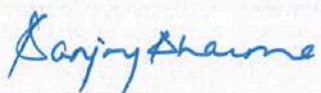
2. No routers are permitted to be attached to any portion of the campus network without approval of Campus Network Facility.

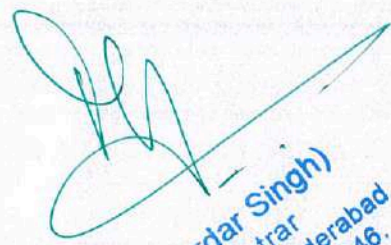
Users who cause problems due to this configuration will face disciplinary action in addition to the loss of network connectivity for the system.

3. Domain Name Violation

Systems violating domain name guidelines will be immediately disconnected from the campus network for a period of not less than one semester.

=== 0 == 0 == 0 ===


Director
COMPUTER CENTRE
Campus Network Facility
University of Hyderabad
Hyderabad-500 046.


(P. Sardar Singh)
Registrar
University of Hyderabad
Hyderabad-500 046.