University of Jammu

Jammu-180006

IT Policy:-Policy for Computer and Network Usage

University of Jammu provides a fully Networked, Computing environment to all the faculty members, researchers, students and staff for their academic use. All the users, using computing and IT-facilities are expected to abide by the certain rules in the form of IT-Policy. These rules are intended to preserve the utility and flexibility of the system, protect the privacy and work of the students and faculty and also to preserve the right to access the international networks to which the system is connected. The policy establishes University-wide strategies and responsibilities for protecting the **Co**nfidentiality, Integrity, and **A**vailability of the information assets that are accessed, created, managed, and/or controlled by the University. Information assets addressed by the policy include data, information systems, computers, network devices, intellectual property, as well as documents. In case of complaints, appropriate action to be taken, will be decided and taken by the competent authority of the University of Jammu. The various aspects covered under the policy are:

1. Faculty, staff, and students with authorized accounts shall be allowed to use the computing and IT facilities for academic purposes, official University business, and for personal purposes so long as such usage:

   a) Does not violate any law, University policy or IT act of the Government of India.
   b) Does not interfere with the performance of the University duties or work of an academic nature.
   c) Does not result in commercial gain or private profit other than that allowed by the University of Jammu.

2. Users are expected to respect the privacy of other users and they may not allow any other person to use their password or share their account. It is the user’s responsibility to protect his/her account from any unauthorized use by changing passwords periodically and using passwords which cannot be easily hacked/cracked by others. Sharing of passwords for any purpose, whatsoever, is strictly prohibited.

3. Any attempt to circumvent system security, guessing others passwords, or in any way gaining unauthorized access to local or network resources is strictly forbidden. Users must not use another person's computing account, attempt to forge an account to identity, or use a false account or e-mail address.

4. Transferring copyrighted materials to or from the University systems without the consent of the owner is a violation of international law. In addition, use of the internet for commercial gain or profit is not allowed. If done so, it will be the sole responsibility of the user.

5. Downloading and installing of new software has to be done with the explicit consent of the respective facility in-charges. Installation of unlicensed software on the University facilities, or on an individual machines connected to the campus network, is strictly prohibited.

6. To the extent possible, users are expected to use only their official email addresses provided by the University of Jammu for official communications with other members of the University.All communication though e-mail can be authenticated if sent through the University domain (@jammuuniversity.in) implying that all other mails sent through other domains may not be considered official and no action can be taken on that..

7. It is forbidden to use electronic mail and other network communications facilities to harass, offend, or annoy other users of the network, including impeding their computing systems, software, or data. Commercial advertising or soliciting using the university resources is strictly prohibited.Spamming/malware/ransomware is strictly disallowed. Subscribing to mailing lists outside the Institute is an individual’s responsibility.

8. Sharing of email accounts for any purpose whatsoever is not allowed. Any special accounts, if need to be set up for conferences and other valid reasons as determined by the university authorities, must have a single designated user.

9. The Centre for IT has assigned an IP address to every computer system connected to the university network. The computer systems in various buildings have been allocated a range of IP addresses using a systematic approach. Therefore, any computer system connected to the network within a building is allocated an IP address only from a particular pool of IP address scheme allotted to that building. Hence, an IP address allocated for a particular computer system should not be used on any other computer even if the other computer belongs to the same individual. If required, an IP address for a new machine should be obtained separately.

10. To the extent possible, users are expected to connect only to the official University wi-fi network i.e. JU wi-fi for wireless access. Setting up of unsecured Wi-Fi systems on the University campus network is strictly prohibited. Securing of University Wi-Fi facility key and IP Address is the prime responsibility of the User. In case of any mishap users shall report the matter to the Centre for IT to block the compromised IP address.

11. The Centre maintains a proper location and corresponding IP address of each system. Hence Computer system, if required, may be moved from one location to another only with the prior written permission from the Centre for IT. Any deviation in this regard may lead to deactivation of the network connection which may be restored only through a written request from the end user after meeting the compliance.

12. All the computers and peripherals should be connected to the electrical points strictly through UPS. Power supply to the UPS should never be switched off, as continuous power supply to UPS ensures its proper charging and backup.

13. Playing of Games in University laboratories or using University facilities for same is strictly prohibited.

14. Display and storage of offensive material like storing pornographic material on the disk, viewing pornographic material on the terminals is strictly disallowed and serious action shall be taken against the offenders.

15. The policy may change as and when it is considered appropriate. New policy or the changes in the existing policy will take effect immediately after incorporating the proposed changes.

16. An employee who leaves the University after retirement/re-employment or otherwise ,can have his e-mail account validated up to six months which may be extended after due approval of the Director IT by another six months with a proper request letter.

17. All Computer systems in the university should have anti-virus software installed, and it should be active at all times. The primary user of a computer system is responsible for keeping the computer system compliant with this virus protection. The user should make sure that the anti-virus is updated and running correctly.

18. As far as possible , all the departments / sections should procure all IT equipment's that comply with the green technology initiatives like energy saving technology, Green packaging etc.

19. Violations of IT-policy shall be treated as academic misconduct or indiscipline and depending upon the nature of the violation, the university authorities may fine or /and take an appropriate action. In extreme cases, the access to the campus network may be completely disabled and the matter be referred to the University authorities.