

## CYBER POLICY

### Guru Jambheshwar University of Science & Technology, Hisar

Networking Cell of GJUS&T, Hisar provides internet facility through its modern and fully equipped network infrastructure. This facility is provided through wireless and wired network media to all faculty, students and staff. For this purpose, Network Cell allocates user ID and password to each and every users at the time of entry in job/course.

Users of Guru Jambheshwar University of Science & Technology, Hisar are expected to abide by the following rules which are intended to preserve the utility and flexibility of the systems, protect the privacy and secure work of student, faculty and staff and to preserve our right to access international network to which our system is connected. In case of any complaints of policy breaching, appropriate action shall be taken by cyber committee consisting of following:

1. Proctor
2. Director (UCIC)
3. Incharge, Networking Cell
4. Chairperson/Branch Officer concerned

#### The policy as follows:

1. Faculty, staff and students with authorized accounts may use the computing and network facilities for academic purposes, official University business, and for personal purposes so long as such use.
  - i. Does not violate any law, University policy or IT act of the Government of India.
  - ii. Does not interfere with performance of GJUS&T, Hisar duties or work of an academic nature.
  - iii. Does not result in commercial gain or private profit other than that allowed by the GJUS&T, Hisar
2. Users are expected to respect the privacy of other users and they **must not allow any other person to use their account and share their account information ( ID and password)**. It is the users responsibility to protect their account from unauthorized access by changing their passwords periodically and using strong passwords. Sharing of passwords for any purpose whatsoever is strictly prohibited. Users may share the required files through sharing software with proper ACL.
3. Any attempt to circumvent system security, guess others' passwords, or in unlawful way to gain unauthorized access to local or network resources is forbidden. Users must not use another person's computing account, attempt to forge an account identity, or use a false account or e-mail address.

1  
Sanghi  
3/9/19  
3/9/19  
3/9/19

3.5.19  
3.9.19


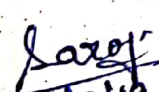


4. Transferring of copyrighted materials to or from the GJUS&T systems without obtaining consent of the authority/owner is a violation of international law. In addition, use of the internet facility for commercial gain or profit is not allowed. If done so, it will be the sole responsibility of the user.
5. Downloading of copyrighted movies/book/games via torrent's or other means is traceable and students are warned that on receipt of any complaints, appropriate fine as deemed fit by cyber committee will be imposed and in case of repeated violation further disciplinary action will be taken. The amount claimed for infringement shall be payable by the user only. University shall not be liable for any of such financial liability.
6. Setting up of any facility requiring password transmission over clear text is prohibited without TLS/SSL encryption.
7. It is forbidden to use electronic mail and other network communication facilities to harass, offend, or annoy other users of the network or outside the network, including impeding their computing systems, software, or data. Neither is any form of commercial advertising, or soliciting allowed. Spamming is strictly **BANNED**. Subscribing to mailing lists outside the Institute is an individual's responsibility.
8. Recreational downloads and peer to peer connections for recreational purposes are **BANNED** unless it is an academic requirement.
9. To the extent possible, users are expected to connect only to the official GJUS&T, Hisar Wi-Fi network for wireless access. Setting up of unsecured Wi-Fi systems, usages of VPN, Socks proxy (Siphon Proxy, Tor Browser, anonymous proxies etc.), Open tunnel Network connection and by passing the GJUS&T, Hisar UTM policy by any means is strictly **BANNED**. Any breach of this rule shall lead to immediate action of blocking the ID for the Semester followed by disciplinary action as decided by the cyber committee.
10. Users are expected to take proper care of network equipment, and are expected to report any malfunction to the staff on duty or to the in-charge of the facility.
11. Display and storage of offensive material like storing pornographic material on the disk, viewing pornographic material on the terminals is strictly **prohibited** and serious action will be taken against offenders.
12. Any other breach, not covered here, shall be decided as per the IT Act of 2000.
13. Every User shall be provided user ID and password ( With single log in only) to use the Internet in university campus.


2  
Sanyu  
3/9/19  
Hans  
3/9/19

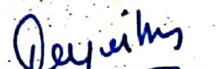
3/9/19  
U  
3.9.19

Rejishy  
3.9.19

14. The students (UG and PG) will be allotted user ID valid till the completion of their course / programme in which they have taken the admission. It will be the responsibility of concerned Chairperson to inform Networking Cell every year about the date of deactivation (Which must not be beyond the last exam date) of user ID's of the outgoing students.
15. The ID's of drop out students will be deactivated immediately. It will be the responsibility of concerned Chairperson to inform Networking Cell immediately about any drop out by students.
16. User ID's of staff and faculty will be for their service period. Upon leaving / transfer outside the campus it will be the responsibility of user to get the ID deactivated after taking NO DUES from Networking Cell. It will be responsibility of concerned HOD/B.O to ensure that the NO DUES has been taken from Networking Cell and user ID has been got deactivated.
17. User ID's of research scholars will be valid till the completion of their Degree. Upon submission of final thesis, it will be the responsibility of user to get the ID deactivated after taking NO DUES from Networking Cell. It will be responsibility of concerned Chairperson / Research Guide to ensure that the NO DUES has been taken from Networking Cell and user ID has been got deactivated.
18. A user can ask for his / her surfing logs with justification which will be provided only after the administrative approval from Honb'le Vice Chancellor. However third party surfing logs shall not be provided in any case in order to avoid the breach of privacy of users.
19. Networking Cell shall retain surfing logs of users for a period of 60 days only. User surfing logs will be provided only on the demand of Police department / Court against the FIR lodged. The following committee will certify and provide the logs in above scenario.
  - Chairperson, CSE
  - Director, UCIC
  - Incharge, Networking Cell
  - Law Officer
  - UTM Dealing Official

 3/5/19  
 Dean, FET  
 3/9/19  
 DSW  
 13/9/19  
 Proctor  
 3/9/19  
 Director, UCIC

 3.9.19  
 Incharge, N/W Cell

 3.9.19  
 T. A.-I