Acceptable Use of Information Technology Resources

The primary purpose of information technology resources at IIITD is to enhance and support the educational mission of IIITD. Access to the Institute's technology resources is a privilege granted to IIITD students, faculty, staff, and approved guests. These resources include hardware, software, computer accounts, local area networks as well as connections to other computer networks via the Internet. Everyone using these resources is responsible for using them in an appropriate, ethical and lawful manner.

All users must refrain from the following activities:

- Using computing resources to violate any Institute policy or regulation, or national, state or local law, e.g. accessing sensitive information for personal use or wider circulation, without consent of the producer of that information or competent authorities.

- Using the Institute computing resources for personal gain or commercial purposes, with the exception of endeavors associated with incubation and entrepreneurship that are duly approved by competent authorities of the institute.

- Accessing, without authorization, any user or group account to read, transfer or change the contents in any way.

- Using computing facilities to send obscene, abusive, threatening, defamatory, or harassing messages.

- Using the resources for activities not directly related to academic or research endeavors in such a way that it causes disruption to other users -- e.g. using applications that generate and transmit unthrottled network traffic (e.g. UDP applications that rely on sending large crafted packets destined to multicast/broadcast addresses), deliberately connecting network equipment using configurations that amplify traffic generation and transmission etc.

- Installing or using pirated software resources on the institute's computing equipment.

- Using computing resources to interfere with the normal operation of the Institute's computing systems, and connected networks including, but not limited to, introducing viruses, sending chain letters to either, or unfairly monopolizing resources that results in the exclusion of others, e.g. running applications without appropriate consent of an instructor/faculty and/or IT staff on institute's computing infrastructure that unduly uses large fraction of computing resources (e.g. RAM, CPU cycles, storage, etc.).

- Illegally downloading and/or sharing copyrighted intellectual property:
    - Illegally downloading and/or sharing copyrighted academic (electronic) material (e.g. e-books) without appropriate written consent of the author(s) or content creator(s), for purposes other than academics.
    - Illegally downloading and/or sharing copyrighted software and/or related artefacts private keys, certificates, authorization serial numbers etc. Such activities are against the spirit of this policy and users are discouraged from such sharing of content.

  Sharing copyrighted content without the permission of the copyright holder, tantamount to breaking the law and the perpetrator may face civil and/or criminal prosecution, in addition to the institute's disciplinary actions and/or penalization (as deemed fit by higher authorities).

  Intentional failure to comply with this policy could be reported to the higher authorities who may in their power take appropriate actions like suspension of user privileges and/or accounts and/or other disciplinary measures.

In addition, all users should comply with the following:

- No user-supplied network equipment may be connected to the campus network without the consent of IT Department. This includes network hubs, network switches, wifi routers, and other similar equipment. Connecting such devices to the IIITD network, without proper configuration, could disrupt network access and performance for others.
- No users should deliberately attempt to interfere or block anti-virus updates, operating system updates, or other activities deemed necessary by Information Technology services to maintain and ensure a safe networking and computing environment.
- Users are responsible for the network and system related activities of their guests (e.g. if the guests install malware infected software on their machines that may infect other users in the network) and should agree to ensure that guests comply with this policy.
- It is strictly prohibited to setup personal/private VPN/SSH gateways for connecting to IIITD LAN from outside, without explicit consent from IT. Such access can be granted to IIITD affiliates and non-affiliates when approved by a IIITD faculty and the IT department.
- Use of profanity, racial slurs, sexual innuendos or pornographic material is strictly discouraged. All IIITD affiliates or non-affiliates hold the right to report such activities or messages to the higher authorities that may take appropriate disciplinary action.
- Each user is responsible for the storage of personal files created on IIITD LAB Computers. IIITD will not be liable, under any circumstances, for files stored on or deleted from its hard disks.

- Users must refrain from installation of unlicensed software on IIITD facilities, or on individual machines connected to the IIITD network, that may possibly interfere with the network access of other users, besides being unlawful. The IT holds the right to report such activities to the higher authorities who may instruct IT to take necessary actions.

- The institute, wherever possible, gives all legitimate users the discretion to determine how to best use the computing resources and facilities within the guidelines of this policy. Users are responsible for their actions, the consequences of those actions, and the consequences of negligent inaction. As such, users whose judgment leads to activities inconsistent with the guidelines of this policy could be reported and thus may face risk of disciplinary action and possible imposition of restrictions. Also the guidelines should be met with letter and the spirit as no such set of ethical/unethical guidelines can be exhaustive.

  Note- Changes to the policy we would be updated via the institute IT website, and also informed to all affiliates via email.

I _____have reviewed the above policies and accept them as stated above.

Roll Number / Employee ID -

Date- Signature