Indore Institute of Management & Research

IT – Policy

Guidelines for Usage of Computing Resources

Opp. IIM , Rau Pithampur Road , Gram Dehri - 453331

Guidelines for Usage of Computing Resources

The Guidelines concerning usage of Computing Resources provided by Institute

Indore Institute of Management & Research provides a strong information technology environment to support its students and faculty in the pursuit of their instructional objectives and teaching. These resources are to be used for educational purposes and to carry out the legitimate business of the Institute.

Understanding that for the Institute to maintain an environment of open access to networked computing resources is important, those who use these facilities must comply with the written policies covering their use as well as the "spirit and intent" of those policies.

Appropriate use of the resources includes instruction, independent study, academic research, and the official work of the offices, departments, recognized student organizations, and the agencies of the Institute. Any activity that intentionally obstructs or hinders the authorized use of campus computing and network resources is prohibited. Examples of inappropriate activities include (but are not limited to):

1. **Interfering with system security or integrity by:**

   • Unauthorized breaking into a system/network and/or accessing data files and programs without authorization.

   • Releasing a virus or other malicious program/software that disables system network performance or hinders other clients.

   • Exploiting security gaps.

   • Hindering/changing supervisory or accounting functions of the systems.

   • Tapping network lines and changing of IP Address.

   Dishonestly moving data from Institute System or through emails that belongs to SGI.

2. **Obstructing users from authorized services by:**

   • Monopolizing computing resources or computer access.

   • Obtaining, possessing, using, or attempting to use someone else's user account or password without notification or permission.

   • Unauthorized Accessing, or attempting to access, another user's data or information without proper authorization.

3. **Email**

   • Sending unsolicited e-mail, junk mail, or propagating chain letters.

• E-mail "bombing", "spamming", etc.

Any activity of a person or group of persons have violent effects upon another person or a social group comes under definition of cyber violence.

4. **Offensive Material**

• Transmitting or storing / sharing offensive material like racial or religious hatred messages, pornography data/pictured/video/audio/text etc.

5. **Forging electronic information**

• Creating, altering, or deleting the attribution of origin (e.g., "From" in e-mail, IP address in headers).

• Sending messages under someone else's address (e.g., hoax messages, even if intended as a joke).

6. IPR Violations: -

Including with software piracy, copyright infringement, trademarks violations, theft of computer source code, patent violations. etc.

Attempting Cyber Squatting- Domain names are also trademarks and protected by ICANN's domain dispute resolution policy and also under trademark laws.

7. Online gambling: -

Any attempt to indulging any form of gambling, betting, money laundering unauthorized money transfer using Institute computing and network resources is Prohibited.

8. Defamation: -Indigenous in any form of online derogatory, defaming , character assassination or degrading any person , Institute , Group , Sector , religion , caste, political party etc is prohibited.

9. Physically damaging a computer system:- Physically damaging a computer or its peripherals either by shock, fire or excess electric supply etc. DESCRIPTIONS of Sample Violations (Not Exclusive).

10. Mishandling email: You must not overload the communications servers; do not abuse your communications
privileges. E-mail is a fast, convenient form of communication. This makes it easy to send mail to multiple recipients and puts a strain on shared systems.

11. Do not help propagate chain e-mail letters: Forwarding chain e- mail is a violation of Institute computing policy. Phrases in the subject line can usually identify chain e-mail, such as "Forward - do not delete," "don't break the chain," etc. Some chain e-mails promise good luck, promise easy money, tell stories and ask for help, or warn of false e-mail viruses. If there are a large number of addresses in the message, chances are very good that it is a chain e- mail. "Get rich quick" schemes will invariably claim to be "completely legal". Do not be fooled. Delete all chain e-mail from your account. Contact IT DEPT. for any clarifications.

12. Do not "bomb" e-mail accounts: Sending numerous or large e- mail messages to one person is considered "e-mail bombing." This may or may not be done in an attempt to disrupt the recipient's network services. Sometimes e-mail "bombs" are used as a method of retaliation. Even if no harm was intended or it was simply a "harmless prank," a e-mail "bomb" can disrupt service to hundreds of users.

13. Copyright Infringements: For your use, the Institute provides many software and data that have been obtained under contracts or licenses stating that they may not be copied cross-assembled, or reverse-compiled. You are responsible for determining whether or not programs or data are restricted in this manner before copying, cross assembling, or reverse-compiling them in whole or in any part. If it is unclear whether or not you have permission to do so, assume that you do not have permission to do so. IT DEPT. will assist with any questions regarding software usage and licensing issues.

14. Interfering with a User's Authorized Services: Any activity that causes disruptions in service to other users is considered interference. In some cases, using more resources than you are entitled to can also be considered interference (e.g., using excessive storage space on the shared systems, flooding chat channels or newsgroups). More importantly, you must not monopolize computing resources for nonacademic activities such as game playing and other trivial applications locally or over an affiliated network; printing excessive copies of documents, files, images or data. You should refrain from using unwarranted or excessive amounts of storage; printing documents or files numerous times because you have not checked thoroughly for all errors and corrections; or run grossly inefficient programs when efficient alternatives are known to be available. You should be sensitive to special needs for software and services available in only one location, and cede place to those whose work requires the special items.

15. Sharing Resource Accounts and Passwords or Sharing Objectionable material on Institute :Your network login and password are for your personal use. If you share your login and password with your collogues, friends or roommates, then you are giving them access to services they are not authorized to use. They may embarrass you by sending e-mail, posting messages, or even chatting with people while posing as you. Do not share your account or password with anyone. If you suspect that someone may have obtained your password, change it immediately. If you suspect that someone has repeatedly accessed your login and password, notify IT DEPT. or send e-mail to IT DEPT. at systeadministrator@Indoreinstitute.com Conversely, using someone else's password to access services or data is also a violation of policy, regardless of how the password was obtained. Do not use anyone else's password, account, or e-mail.

Further, sharing any form of objectionable material (pornography, religious hatred mails etc.) on your PC hard-drive on SGI Network is strictly prohibited.

Disruption of System Security or Integrity: Tampering with the operation of any server or network resource is prohibited. Any such activity constitutes a threat to the normal operation of that resource and can potentially effect hundreds of users. Any attempt will be regarded as malicious in intent and will be pursued in that perspective.

Unauthorized access: Legitimate use of the Group Institutes computer systems does not extend to what one is capable of doing on that system. In some cases, there may be security loopholes through which people can gain access to a system or to data on that system, a network, or data. This is unauthorized access. If a student accidentally permits access to his or her files through the network, you do not have the right to access those files unless you have been given explicit authorization to access the material. This is similar to accidentally leaving your door room unlocked. You would not expect your neighbor to use that as an excuse for entering your room.

Do's & Don't

Forgery: You must not alter any form of electronic communication (especially via forged electronic mail and news postings). Messages, sentiments, and declarations sent as electronic mail or sent as electronic postings should meet the same standards for distribution or display as if they were tangible documents or instruments. Forgery includes using another person's identity. Forgeries intended as pranks or jokes are still violations. Attempts to alter the attribution of origin (e.g., the "from" or "addressee" lines) in electronic mail, messages, or postings, will be considered transgressions of Institute rules. You are free to publish your opinions, but they should be clearly and accurately identified as from you, or, if you are acting as the authorized agent of a group recognized by the Institute, as coming from the group you are authorized to represent.

- Always use official mail id for professional communication within & outside the organization also use of personal mail id is prohibited.

  Please check your mail accounts regularly.

- If you have received a mail containing an attachment, form an unknown sender don't open it, you need to scan the attachment through Antivirus, if you found virus with the attachment then please delete it.

- If you receive a mail containing an attachment, from a sender you know, but without any mention regarding the attachment, don't open it. It may be caring a virus, which gets automatically attached with mails. You can confirm from the sender if he has sent you this attachment and only then open it.

- Please ensure that attachments sent by you are free from virus and worms. Always use official Mail id for communication within & outside the organization also use of personal mail id is prohibited
- If you don't have official email id contact to SGI Administrative Department for new official email. Also these mail ids are for official use only.

- Use MS-Outlook for Official Email Address and if outlook is not properly configured please contact System Administrator.

CONSEQUENCES OF MISUSE: Infractions of this shared use policy will result in loss of system and network privileges and will be referred either to the Dean of Department /Principal/Director.

When IT department has reason to believe a user has violated the shared system policy, it may suspend the user's account(s) pending the outcome of an inquiry into the matter. IT Department will notify the staff or student of the alleged violation and the facts on which the alleged violation is based. The staff or student will have an opportunity to respond to the alleged violation. After gathering and considering all the facts available, and in consultation with the Dean of Department /Principal/Director, the user's privileges to the shared use systems may be withdrawn for the remainder of the Semester/Course.

If, in addition to withdrawing privileges, IT Department believes the violation is sufficiently serious to warrant more severe disciplinary action, including restitution, they may refer the matter to the Dean of Department/Principal/Director for appropriate disciplinary action.

Conclusion: The IT Department recognizes that **SGI** Information System users are extremely diverse in their needs and requirements. Providing this large range of services for research and instruction necessarily entails providing a relatively unrestricted and flexible system and network organization. To this end, we expect that our users practice considerate and responsible computing and adhere to common sense standards.

When problems arise, they will be dealt with to ensure the unimpaired operation of our systems and network, but we request that all users are considerate and prudent in their use of the resources.

The shared systems are an extremely important and ever-changing resource for the SGI. As a member you are responsible for staying informed about the policies and procedures updates.