IIM SIRMAUR
KNOWLEDGE . LEADERSHIP

INDIAN INSTITUTE OF MANAGEMENT SIRMAUR
भारतीय प्रबंध संस्थान सिरमौर

Dhaula Kuan, Distt. Sirmaur
Himachal Pradesh – 173031, India

धौला कुआँ, जिला. सिरमौर
हिमाचल प्रदेश - 173031, भारत

POLICY ON USE OF IT, COMPUTING AND NETWORK RESOURCES

SECTION – 1
(BACKGROUND AND PURPOSE)

1.1 Background

The Indian Institute of Management Sirmaur (IIMS) provides IT, computing and network facilities for use by the faculty, staff and students for academic, research and administrative purposes.

This policy provides guidelines for the appropriate use of computing and network resources. TheInstitute will take disciplinary and legal measures against any user who has been proven to have abused or disregarded this policy

1.2 Purpose

The Institute provides computing and network resources for the purposesdirectly in relation with its mission, i.e. academic, research and institute's administrative activities. The purpose of this Policy is to establish rules to ensure that usage of the IT resources complies with Institute policy, to protect the institute against damaging legal consequences and to educate the individuals who may use these resources with their responsibilities associated with such use

SECTION – 2
(OPERATIONAL PROCEDURE, AUTHORIZATION, IT INFRASTRUCTURE, RESOURCE INTEGRITY AND PRIVACY)

2.1 Operational Procedure

2.1.1 Upon request and with authorization by administration/PGP, users will be granted the privilege to use the computing and network resources.
2.1.2 Every authorized user is given an account and is allocated associated hardware/softwareresources.
2.1.3 The user ID for the faculty will be based on names, for the staff based on the designations and for students based on the batch number
2.1.4 Users are required to immediately change the default password provided by the IT department on first time login
2.1.5 The user id will be deactivated/deleted once the user ceases to be associated with IIMS
2.1.6 To defray additional operating cost, sponsored projects in the Institute are charged for some usage such as printing, at approximately cost rate, for the use of these

resources.

2.1.7 To the extent possible with its hardware, software and manpower resources, the Institutemaintains backup of user files and implements system security safeguards as well as capacity and performance enhancing measures.

2.1.8 Printing facility will be disabled once No Dues certificate issued and all other IT serviceswill be disabled on 31st July of the graduating year.

2.2 Authorization

2.2.1 Users are only allowed to access IT resources and services that they are authorized to.

2.2.2 Users must not access computing and network resources without proper authentication procedure or intentionally enable others to do so.

2.2.3 The owner of a user account can only use that user account.

2.2.4 Users are forbidden to communicate their password or otherwise give access to their accounts or any computing or network resource to any other user/third party.

2.2.5 Users are not permitted to use computing and network resources for illegal or unlawful activities.

2.2.6 Users are not permitted to use computing and network resources for commercial activities.

2.2.7 Users are not permitted to use computing and network resources for entertainment purpose.

2.2.8 Any anomaly discovered in the authentication procedure must be reported to the staff of the IT department so that the same can be investigate to take corrective action.

2.3 IT Infrastructure for the users

2.3.1 The entire IT infrastructure and facilities are maintained by the IT department of the institute

2.3.2 All students are required to bring their own laptops for accessing the services.

2.3.3 The desktops installed in the computer lab will have all the software(s) required by the students.

2.3.4 Employees of the institute will be allocated a desktop with all necessary software(s) for office work on completion of necessary joining formalities. Requirement for any additional IT resources may be dealt with on case to case basis on the merit of the case.

2.3.5 Printing facility for the employees is provided using shared printers installed in various locations within close vicinity of the users.

2.3.6 No user is allowed to carry official electronic devices out of campus without permission from the competent authority

2.3.7 Any external storage device like pen drive or hard disk connected to the PC needs to be completely scanned by the Antivirus software before using it and copying files to/from the device.

2.3.8 It is the responsibility of all users to ensure careful, safe and judicious use of the IT equipment & other assets allocated to and/or being used by them.

2.3.9 No other third-party software – free or licensed can be installed on a computer system owned or provided by the institute, without prior approval of the IT department.

2.3.10 To request installation of software on an official desktop, user needs to send a

written request

2.3.11 Any software developed & copyrighted by the institute belongs to the institute.

2.3.12 No user is allowed to install pirated software on institute's computing systems.

2.3.13 Software purchased by the institute or installed on institute computer systems must be used within the terms of its license agreement. Any unauthorized use, storage, duplication or distribution of software is illegal and subject to strict disciplinary action.

2.3.14 Any observed malfunction, error, fault or problem while operating any equipment owned by the institute must be immediately brought to the notice of the designated staff in IT department.

2.4 Resource Integrity

2.4.1 Users must not attempt to modify or remove computing/network equipment, software or peripherals that they do not own without proper authorization.

2.4.2 Users must not:

2.4.2.1 develop, use or disseminate malicious programs, computer viruses and worms

2.4.2.2 disrupt the activities of other computers or users

2.4.2.3 try accessing other's private data or restricted portions of the computing ornetworking system, damage the software or hardware components of the system,

2.4.3 The computing and network resources are shared by all users and are of finite capacity. Users must therefore not make any capacity and performance degrading usage of the resources. Such usage includes but is not limited to:

2.4.4 sending of chain-letters or excessive messages, either locally or off-campus,

2.4.5 using network protocols using an excessive amount of bandwidth,

2.4.6 printing excess copies of documents,

2.4.7 running grossly inefficient programs when efficient alternatives are known bythe user to be available,

2.4.8 unauthorized modification of system facilities, operating systems, or diskpartitions,

2.4.9 attempting to crash or tie up computing and networking resources,

2.4.10 damaging or vandalizing computing and network facilities, equipment, software or computer data.

2.4.11 Users are allowed to use the computing and network resources only for academicpurposes. Users should not engage in inappropriate or idle use of the resources nor block their access to other users.

2.5 Privacy

2.5.1 Users are forbidden to use any user account other than their own.

2.5.2 Users are prohibited to access files, emails or any form of data not belonging to them.

SECTION – 3 (Campus Network)

3 Campus Network

3.1 All the buildings including hostels have been provided with LAN/Wi-Fi.

3.2 Institute has provided all the required equipment including Wi-Fi Access Points (APs)/Routers. Using your own APs/Wi-Fi Routers is not permitted. In case of any unavoidable circumstances requiring use of your personal APs/Wi-Fi, prior permission of IT department should be taken, failing which the equipment will be seized by the IT department and the access to IT facilities & services for the concerned users will be blocked.

3.3 Users are allowed to access all the resources available on the campus network based on authentication and authorization only.

SECTION 4 (EMAIL USAGE)

4 Email Usage

Institute provides email facility to all its faculty, staff and students. These email IDs are used for communicating with other users; both internal and external. The email facility of the institute is hosted with the GMAIL with iimsirmaur.ac.in domain. The email ID of a user is UID@iimsirmaur.ac.in where the UID is the user ID provided to the user by the IT department. The following rules apply for email access:

4.1 Email ID to faculty and staff is provided after completing the joining formalities and on receipt of duly signed User Registration Form

4.2 In case of students, IT department creates the Email IDs once the Programme Office sends the details of the students to IT department. IT department then forwards all the student Email IDs to Programme Office which distributed the same to each student concerned after taking an undertaking that *the student has read and understood the IT Usage Policy of the institute and agrees to abide by the same*

4.3 Email user storage quota: 15 GB per user

4.4 The User is responsible for any data/e-mail that is transmitted using the IIMS's e-mail system. All e-mails/data sent through the mail server are the sole responsibility of the user owning the account

4.5 Sharing of passwords is prohibited.

4.6 Users are forbidden to create and transmit email containing offensive, obscene, indecent, aggressive, menacing, harassing, defamatory, intimidating, unlawful, racist and other unethical messages.

4.7 Users are forbidden to send email that does not correctly identify the sender, attempt to hide or disguise the identity of the sender or attempt to hide or disguisethe identity of the computer from which it was sent.

4.8 Users are forbidden to transmit or forward any email intended to encourage the propagation of copies of itself (e.g. chained letter).

4.9 Users are forbidden to flood the mailbox of other users with numerous or large messages with the intention to paralyze their mail system.

4.10 Users are forbidden to spread virus or worms or malicious programs through emails.

4.11 Users are forbidden to use the email facilities of the Institute for commercial activity.

4.12 Any e-mail addressed to a user, whose account has been deactivated /deleted, shall not be redirected to another e- mail address. Such e-mails may contain contents that

belong to the institute and hence no e-mails shall be redirected

4.13 Forwarding of e-mail from the e-mail id provided by IIMS to the user's personal id outside the IIMS email service is not allowed due to security reasons.

4.14 Users should ensure that e-mails are kept confidential. IIMS shall take all possible precautions on maintaining privacy. Users must ensure that information regarding their password or any other personal information is not shared with anyone

4.15 In case of threat to the security of the IIMS's email service, the email id being used to impact the service may be suspended or deactivated immediately

4.16 The security audit of the email services of the institute shall be conducted periodically through an organization approved by Deity

4.17 The email id will be deactivated/deleted once the user ceases to be associated with IIMS

4.18 Notwithstanding anything in the clauses above, the disclosure of logs/e-mails to law enforcement agencies and other organizations by the IIMS would be done only as per the IT Act 2000 and other applicable laws

4.19 Any e-mail not in use for a period of three months will automatically be suspended/deactivated.

4.20 The institute's email ID provided to any user is meant purely for official use.

SECTION 5
(INTERNET USAGE)

5 Internet Usage

The Institute provides Internet facility for use by the faculty, staff and the students. The facility is meant only for academic and research purposes and is no way meant for bandwidth intensive use such as downloading of illegal/unethical material, movies, playing games, etc. or for entertainmentpurpose. The Institute provides Internet facility only for the purposes directly in relation with its mission, i.e. academic, research and institute's administrative activities.

5.1 Internet Access Privileges

5.1.1 The use of institute's Internet facility is a privilege, not a right, and inappropriate use will result in a cancellation of those privileges

5.1.2 Users are not permitted to use the facility for illegal, unethical and unlawful activities.

5.1.3 Users are not permitted to use the facility for commercial activities.

5.1.4 Users are not permitted to use the facility for entertainment purposes.

5.2 Website/URL Blocking

The Websites classified under any of the following categories will not beaccessible:

5.2.1 Potentially Liable Sites: Sites containing content related with DrugAbuse, Hacking, Illegal or Unethical, Racism and Hate, Violence, Marijuana, Proxy Avoidance and Phishing

5.2.2 Controversial Sites: Sites containing content related with Adult Materials, Gambling, Extremist Groups, Nudity and Pornography and Weapons

5.2.3 Potentially Bandwidth Consuming Sites: Site providing Internet Radio and

TV and Internet Telephony facilities

5.2.4 Potential Security Violating Sites: Sites promoting Malware andSpyware

5.3 File Download Blocking

5.3.1 Downloading of files such as BAT, EXE, COM, SCR, PIF, CPL etc. is not permitted due to threat of spreading virus through such files.

5.3.2 Downloading of bandwidth consuming/entertainment content is not permitted hence downloading of files such as AVI, MOV, MPG/MPEG, WMV, MP3, RM etc. is not allowed.

5.4 User Access Quota

User wise download quota may be fixed if the resources are overloaded.

5.5 Website/URL Exemption

Some sites that are blocked under any specific category specified above may be unblocked based on requests by the students after evaluating them, if found acceptable.

5.6 Special Access Privilege to Students' IT Infrastructure Committee:

All the members of the students' IT Infrastructure Committee will be granted special access privileges to enable them to download multimedia content and other file types otherwise blocked. Any student genuinely needing any such content for academic purposes that is otherwise blocked can get the same through any of the members of the IT Infrastructure Committee or through IT department.

5.7 Monitoring

IIMS may deploy a system that can monitor and record all IT usage. All useractivities with respect to IT usage may be subject to logging and review, if needed.

SECTION 6
(Policy Review)

6 Periodic Reviews

6.1 Usage Compliance Reviews

To ensure compliance with this policy, periodic reviews will be conducted.These reviews will include testing the degree of compliance with usage policies.

6.2 Policy Maintenance Reviews

Periodic reviews will be conducted to ensure the appropriateness and the effectiveness of usage policy. These reviews may result in the modification, addition, or deletion of usage policy clauses to better suit users' IT needs.

SECTION 7
(Security)

7.1 Security

The User is responsible for the security of the personal account that he/she is given on IIMS network and is responsible for the following:

7.1.1 Each user is given a user account and a corresponding password initially assigned by thecomputer center. The User must protect his/her account by immediately changing his/herinitial password. The password chosen must be at least 8 characters long and must include upper and lower case letters, numbers and special characters.

7.1.2 The account given to the User is personal. In no circumstance, the User can give access to his/her account to any other individual, nor must the user disclose his/her password toothers.

7.1.3 The user must not leave a computer while he/she is logged in to the computer/network. Such unattended computer may be used by others to gain access to the User's account.

7.1.4 The User is responsible for the content that is stored in his/her account. It is the User's own responsibility to check that no unwanted file is stored in his/her account. In case any unwanted file is detected, the User must inform the staff of the IT department. User quota may be implemented on disk usage.

7.1.5 Please delete unwanted files periodically, as hard disk space is precious.

7.1.6 If the above rules are not followed, the account of the User may be terminated and no further account will be given to the User on IIMS network.

7.2 Security Incident Management Process

7.2.1 A security incident is defined as any adverse event that can impact the availability, integrity, confidentiality and authority of institute's data. Security incidents can be due to factors like malware, phishing loss of a device, compromise of an e-mail id etc.

7.2.2 It shall be within the right of the institute to deactivate or remove any feature of the IT facility/service if it is deemed as a threat that can lead to a compromise of the service.

7.2.3 Any security incident, noticed or identified by a user must immediately be brought to the notice of the IIMS authorities

If security is violated because of the User negligence in following the above rules, the User will beresponsible for the damages caused to IIMS IT resources.

SECTION 8
(PRINTING FACILITY)

8.1 Printing Facility

8.1.1 Printing facility for the employees is provided using shared printers installed in various locations within close vicinity of the users.

8.1.2 Printers are fragile and expensive equipment hence users should take good care of them.

8.1.3 Printing paper, toner and other consumables are provided by the institute
8.1.4 Printing facility will be disabled once No Dues certificate is issued

SECTION 9
(COMPUTER CENTRE USAGE)

9. Computer Centre Usage

The Computer Centre is under surveillance using CCTV cameras. In order to maintain conduciveenvironment inside the computer center, students are requested to observe the following:

9.1 Do not change cable connections between equipment
9.2 Do not disconnect peripheral equipment and do not shift equipment
9.3 Keep chairs in Order
9.4 Observe strict silence in Lab
9.5 Discussions and student meetings should not be undertaken inside the computer center
9.6 Do not keep your belongings on Computers/Computer Table
9.7 Keep waste papers etc. in the baskets provided in the center
9.8 No Food or Drink is allowed inside the Computer Centre.
9.9 Playing Computer Games in the Computer Centre is strictly PROHIBITED and will be treated as a serious matter leading to disciplinary action against the person found guilty
9.10 While leaving the computer center, please **LOGOUT**, and **SWITCH OFF** thePC

SECTION 10
(CLASSROOM EQUIPMENT USAGE)

10 Classroom Equipment Usage

Each classroom has been provided with a high tech Audio-Video (AV) System comprising ofPC. Projector, LCD Panels, Touch Monitor, and Touch based Control Panel, Amplifier, Digital Signal Processor, Video recording and streaming toolsetc. The following rules apply to the use of classroom equipment:

10.1 All the equipment installed in the classrooms are fragile and expensive equipment, hence, users should take good care of them
10.2 NEVER change cable connections between equipment as it may cause loss of some functionality, may cause electric shock and can also cause damage to these expensive equipment
10.3 Don't turn-off these equipment after each class to avoid loss of time in switching on the system. However,to save energy and also to save the Projector lamp life, please turn off the equipment when not intended to be used for a longer time

SECTION 11
(SOFTWARE PURCHASE)

11 Software Purchase

11.1 IT department will provide all the commonly used office automation software in all the desktops belonging to the institute.
11.2 All software used on all the official computer must be properly licensed.
11.3 Users must not infringe on any intellectual property right while using the Institute's computing and network resources.
11.4 Need for specialized software(s) required for academic purposes should be routed to the IT department through proper channel. The IT Infrastructure Committee of the institute will evaluate such requests received and recommend appropriate action on case to case basis to the competent authority for approval.

SECTION 12
(CESSATION OF ACCESS)

12 Cessation of Access to IT facilities

12.1 In case of faculty and staff, access to all the IT services and facilities will be disabled immediately on signing of the No Dues Certificate by the IT department.
12.2 In case of the students, printing facility will be disabled immediately on signing of the No Dues Certificate by the IT department and all other IT services will be disabled on 31st July of the graduating year.

SECTION 13
(POLICY AUDIT)

13 Audit of IT Services and Facilities

The security audit of institute's IT services shall be conducted periodically by an organization approved by Meity.

SECTION 14
(IT INFRASTRUCTURE COMMITTEE OF STUDENTs)

The IT Infrastructure Committee of Students

An IT Infrastructure Committee of the students comprising members from both the years of all the programmes is duly constituted and approved by the competent authorities of the institute. This committee acts as an interface between the student community and the IT department for reporting issues, if any, being faced by them with the existing IT facilities and services and also for bringing in improvements therein.

SECTION 15
(IT INFRASTRUCTURE COMMITTEE OF INSTITUTE)

The IT Infrastructure Committee of the Institute

A duly constituted IT Infrastructure Committee of the institute advises the IT department on the overall IT Infrastructure needs of the institute and makes necessary recommendations to the competent authority for improving these facilities on regular basis. Need for any special IT facility and service may be routed to this committee through IT department.