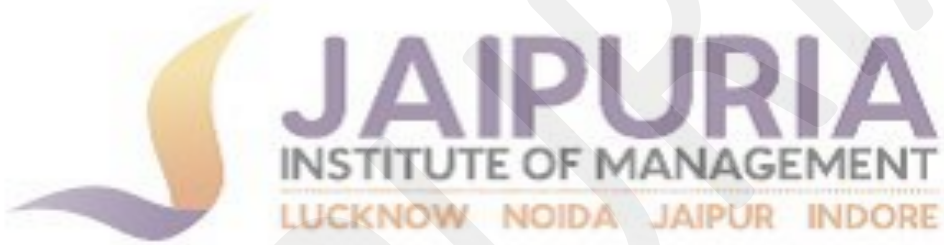
JAIPURIA INSTITUTE OF MANAGEMENT INDORE



IT Policy

VISION

To be an educational institution of choice for all stakeholders which promotes human well-being through continuous learning.

MISSION

To provide learner-centric education that focuses on developing learners as competent, ethical and socially conscious management professionals through continuous improvement in the quality of teaching-learning process and research.

ACCEPTABLE USAGE POLICY

Personal Use

The primary purpose for the Jaipuria Indore's Information systems is for Institutional use for students and faculty. Users will make limited, infrequent, or incidental use of Jaipuria Indore systems for personal use. Personal Use will be:

- Adhere to Jaipuria Indore Security Policies and Guidelines notified from time to time;
- Not interfere with Jaipuria Indore educational activity, individual's productivity, privacy or their colleagues productivity;
- Not adversely affect the Jaipuria Indore's ability to provide effective Computer Systems and
- Not adversely impact on the Jaipuria Indore's computing costs.

The email system is provided to support the Jaipuria Indore's educational activities. Personal email, (i.e. communication between individuals or parties which is not in support of the Jaipuria Indore's educational activities), whilst not prohibited, will be kept to a bare minimum and will be carried out in a manner which does not negatively affect the use of the Jaipuria Indore's systems for educational purposes.

Personal emails and other forms of communication carried out using the Institute's information systems will be clearly marked personal. This can be done by inserting the word "Personal" in the subject line of the email.

Internet Usage

Internet access will be provided to the users for carrying out education related activities in a secure manner. All the users will be uniquely identified and authenticated before being allowed to access the internet. All activities performed under a user's identification code (which shall be his/ her domain account) will be identifiable (through web content filtering application) and users will be accountable for any activities performed using their identification code.

- Connections from network to internet will be only made through proxy / web content filtering system at 1st level and shall pass through firewall at the 2nd level.
- All web browsers will be configured to use approved secure gateway http proxy. These systems must, at a minimum, prevent services except those that are explicitly allowed and have the capacity to be actively monitored and logged.
- The internet traffic content will be screened and access to web sites relevant for educational/institute's Information will only be allowed to the users.
- All access to the internet will be logged and monitored. The management retains the right to inspect any and all files stored on or transmitted over its network assets (including but not limited to, local storage media, memory and mail files) for the purpose of investigating suspected violations of its institutes policies or non-compliance with local regulations.
- Users will not attempt to probe other systems in the external world for security weaknesses, compromise other systems, possess or transfer data illegally, or send offensive or abusive messages. They will not claim to represent the institute on the internet unless authorized to do so by the management. Shall the institute observe such attempts, disciplinary actions may be initiated.

- Jaipuria Indore will ensure that practical guidance on internet and email abuse is communicated to the contract personnel from time to time.
- Periodic up-dation of content filtering rules / sites will be performed depending upon the institutional requirement and management decisions.
- Scanning any files downloaded from the Internet for viruses before loading or forwarding to other parties.

Confidentiality

- Data created by users on Jaipuria Indore information systems will be a property of Jaipuria Indore. Because of the need to protect Jaipuria Indore network, management cannot guarantee the confidentiality of individual information stored on any network device belonging to the Institute.
- Caution will be exercised over whom users disclose their or a colleague's email address to, as it can be passed on to unwanted third parties and, thereby, result in unsolicited, unpleasant or abusive email.
- Users will not provide information about, or lists of, Jaipuria Indore employees to parties outside the Institute.
- Users shall logout SAP application, if no longer required.

Property

- Employees will adhere to all intellectual property and copyright law. Users will always obtain copyright holder's permission before downloading information from internet or other public computer system.
- No employee or student related information of any kind and no confidential information regarding any third party will be sent over any public computer system unless the third party have specifically agreed to it.

- All intellectual property rights in computer data, computer files and databases created or altered during the course of employment will be property of Jaipuria Indore. On termination of employment, users will return all copies of such data, files, and databases in their possession. User will not delete copy of any such computer data, files or databases where that copy is the only, or last remaining, or most up to date copy.

Security

- Users will inform the IT Team of any communication, system problem or other circumstance that may indicate a breach of security or other risk to the integrity of the Institutes information system.
- Users will not circumvent user authentication or security of any host, network or account.

Passwords and Log-in IDs

- Every user will have a unique login ID and password to access information systems of Jaipuria Indore. Users will be responsible for setting their passwords as per the Password Management Policy and ensuring that their password is protected.
- Users will not write down their passwords but protect them by committing them to memory.
- In order to prevent unauthorised use, users will ensure that they do not divulge their password to any other person.
- Users will not disclose password protections or allow any other person access to the Institute's information systems.
- Users will not transmit ID's, passwords, internal network configurations or addresses or system names over the Internet.
- Users will not leave their computer unattended while connected to the Internet.

Desktop/Laptop/Handheld Device Security

To prevent any unauthorized access to personal computers/Handheld devices, users will always lock the Desktop/Laptop/ Handheld when not in use, and set screen savers to require password protection on resume.

Offensive Material

- Users will not use Institute's Computer Systems in any way that may be considered detrimental or offensive to others.
- Any user loading, downloading, printing, storing, or receiving (without reporting to their Manager), any material of a sexual or lewd nature via electronic means or otherwise will be subject to disciplinary.

Electronic Games, Jokes and Other Material

Electronic games, jokes, greeting cards, chain letters, non-work related videos and pictures can take up large amounts of server space and adversely impact Institute's Computing Systems. Accessing such material also increases the risk of introducing computer viruses and will thus be considered as a violation of Acceptable Usage Policy.

Prohibited Activities/Use/Communications

The following activities are prohibited for the users of Jaipuria Indore information resources. Certain authorized employees may be exempted from some of these restrictions if they are required to perform a particular activity during the course of their legitimate job responsibilities (e.g. systems administration staff may have a need to disable the network access of a host if that host is disrupting production services). The conduct of any of the activities including but not limited to listed below will be viewed by the Institute as misconduct.

- Engaging in any illegal activity (including gambling) while utilising Institute's information systems. Installation of unauthorized software's/ applications.
- Introduction of malicious programs into the network or server (e.g. viruses, worms, Trojan horses, email bombs, etc.) or use the Institute's information systems to transmit malicious programs to other parties.

- Hacking into or obtaining access to any systems or accounts that is not permitted (including systems or accounts outside of the Institute) or attempt to do the same or otherwise breach or attempt to breach any computer or network security measures.
- Transmitting (or attempt to transmit) user names, passwords or other information related to the security of the Institute's information systems to third parties.
- Using the Institute's information systems to download, transmit, distribute or process any material which may be considered to be offensive including, without limitation, material which is or may be considered to be racist or sexist, or otherwise discriminatory or to amount to harassment, victimization or bullying or otherwise to be potentially offensive, upsetting or derogatory to any group or individual or which may be considered to be pornographic, obscene or indecent (in all cases, even if one does not personally consider it to be so).
- Carrying out or assisting others in carrying out any type of port scan or security scan.
- Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
- Providing information about, or lists of, Jaipuria Indore employees to parties outside the Institute.
- Loading, downloading, sending, storing, printing or receiving without reporting, offensive, obscene, indecent or defamatory material including any sexual material such as sexually explicit images, messages or cartoonsand any material which amounts to harassment or discrimination on the grounds of race, sex or disability.
- Changing the configuration of your hardware or software without the prior approval from IT Department except for cosmetic changes such as colour, font, and resolution or display output device.
- Using the Institute's information systems for your own personal financial gain or for the financial or business advancement of any third party.
- Posting any information of any kind (including gossip, personal opinions, jokes etc) regarding the Institue to any external bulletin board on the Internet.
- Monitoring or intercepting files or electronic communications of other employees or read, delete, or copy the contents of another person's email mailbox without their consent or appropriate authority.

Password Management Policy

Access to user accounts is controlled by an authentication mechanism utilizing unique used IDs and passwords. These authentication mechanisms ensure controlled and restricted access to the information and information systems according to the institute's requirements. The purpose of this policy is to establish the rules for the creation, distribution, safeguarding, termination, and reclamation of the user authentication mechanisms.
This policy document applies to all employees, including full-time staff and off-roll staff who have access to Jaipuria Institute of Management Indore's Network and/ or information.

User Responsibility

- Each user will have a unique user identification code and password to access Institute's Computer systems, which preferably, shall be configured out of active directory.
- Users will be personally responsible and accountable for all actions performed under their user account.
- Users will be responsible for protecting their user accounts, passwords and other access codes entrusted to them.
- Users will ensure that:
  - After accessing Computer Systems the machines are logged off;
  - Machine is not in use prior to logging on to a computer system;
  - Passwords are not written down and stored anywhere around the work place; and
  - Passwords are not shared with any person for any reason (not even with administrators).
- Users will not use the same password for Jaipuria Indore accounts as for other non Jaipuria Indore accounts.
- Users will not share their passwords with anyone through any mode of communication like phone, email, questionnaires-security forms etc.
- "Remember Password" feature not to be used for any applications.
- In case an account or password is suspected to have been compromised, users will
  - Report immediately to the IT Department; and
  - Reset passwords suspected to have been compromised immediately.

Confidentiality of Password

- All User (normal users, administrators) passwords will remain confidential and not shared, posted or otherwise divulged in any manner.
- Passwords will not be stored in clear text on computer systems and will be stored in an encrypted format.
- Passwords will not be displayed on system reports.
- Display and printing of passwords will be masked, suppressed, or otherwise obscured.
- Passwords will be conveyed to users in a secure manner. Passwords will never be disclosed via telephone or through third parties or through unprotected (clear text) electronic mail messages.

Password Management

- Users will be provided with the capability to change their password on the login interface.
- All passwords will be immediately changed if they are suspected of being disclosed, or known to have been disclosed to unauthorized parties.
- Password never expired list to be reviewed periodically by the IT manager and approved by the IT head.

Backup

In order to safeguard information and computing resources from various business and environmental threats, systems and procedures need to be developed and implemented for backup of all institutional data, related application systems and operating systems software. The purpose of the Backup Management Policy is to ensure that the critical information assets of Japuria Institute of Management , Indore are backed-up and are recoverable as and when required. This would also ensure that all backups of information assets are in accordance with the approved business and technical requirements and are planned, implemented and tested in a controlled and consistent manner.

Since now major institutional activity are done through mail, so mail backup is an essential part of Back up . We at Jaipuria Indore we use Google Apps or you can say that gmail mail server for our mail so a copy of mail is always available at the gmail server due to this mail backup is not critically taken care of.

Types of Backup

a) Scheduled :-

a. Daily:- TALLY DATA Though the Auto backup feature is enabled in Tally we save the data folder of Tally on daily basis and preserve the same for one week duration

b. Weekly:- SERVER SPACE (the space provided to all employee to store their official data) data on updation basis

c. Quarterly :- To External Hard Disk :- We have issued External Hard Disk to all key departments(Admission, Placement, Training, PGDM) to store their institutional data

Quarterly we transfer the content of the same to our Hard Disk as well as we also save the data of other department to that Hard Disk and then make a copy of the same and stire one Hard disk with IT Department and the Other with Director Office/Residence

b) Unscheduled:- As and when required in view of machine condition etc.