Title	**IT Procedure manual and policy**
Version	1.0.1
Classification	Internal
Release Date	20th March 2014
Description	Acceptable usage of information assets by users
Update Date	19th, August 2020
Reviewer/ Custodian	IT Representative Noida Campus & Head IT Jaipuria Group
Approved By	Director, Jaipuria Institute of Management, Noida

Distribution List

Name
Internal Distribution Only

Version History

Version Number	Version Date
1.0	20th March 2014
1.0.1	19th, August 2020

Acceptable Usage Policy

Version: 1.01

1. Purpose

The purpose of this policy is to clearly illustrate what is considered to be acceptable and unacceptable use of Jaipuria Institute of Management Industries Limited's (hereafter Jaipuria Institute of Management or Company) information systems. The purpose of this policy is to define the boundaries of acceptable and unacceptable use of the information assets/data/ applications to which users have access.

2. Policy

2.1 Application

This policy document applies to all Jaipuria Institute of Management employees, including full-time staff and off-roll staff who have access to Jaipuria Institute of Management information resources.

- It is the responsibility of the user to know the guidelines outlined in this policy and to conduct activities accordingly.
- Each user is personally responsible for the control of his/her equipment, including the company installed software.

2.2 Monitoring

- All communications using Company facilities will be the property of Jaipuria Institute of Management and Jaipuria Institute of Management IT team reserves the right to access all communications, monitor and audit networks and systems as and when deemed necessary.
- For security and network maintenance purposes, authorised individuals within Jaipuria Institute of Management will monitor equipment, systems and network traffic at any time.
- If deemed necessary, content scans will be performed for e-mails sent/received through company systems. E-mail and internet sites that contain certain keywords such as foul language or content that may be of a sexual, pornographic or racist nature will be blocked. In the case of an employee sending inappropriate email or attempted access to blocked internet sites, disciplinary action will be taken.

- E-mails with large attachments that can impact the normal traffic flow will be blocked. Users will be advised not to send such large attachments.
- If an employee has several sent/received mails blocked, the Company will take appropriate measures to ensure such email does not enter the Jaipuria Institute of Management email system.

2.3 Personal Use

The primary purpose for the Jaipuria Institute of Management's Information systems is for Company business use. Users will make limited, infrequent, or incidental use of Jaipuria Institute of Management systems for personal use. Personal Use will:

- Adhere to Jaipuria Institute of Management Security Policies and Guidelines;
- Not interfere with Jaipuria Institute of Management Business, individual's productivity, or their colleague's productivity;
- Not adversely affect the Jaipuria Institute of Management's ability to provide effective Computer Systems; and
- Not adversely impact on the Jaipuria Institute of Management's computing costs.

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

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

2.4 Internet Usage

- Internet access will be provided to the users for carrying out business 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 the firewall at the 2nd level
- All web browsers will be configured to use an approved secure gateway HTTP proxy. These systems must, at a minimum, prevent all 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 websites relevant for business information will 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 business 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 company on the internet unless authorized to do so by the management. Shall the company observe such attempts; disciplinary actions may be initiated.
- Jaipuria Institute of Management will ensure that practical guidance on internet and email abuse is communicated to the contract personnel from time to time.
- Social Networking sites are blocked for employees for an entire time other than the allowable time period. Specific business users are granted access to social networking sites for the entire office timings (Marketing etc.).
- Periodic up-dation of content filtering rules/sites will be performed depending upon the business requirement and management decisions.
- Scanning any files downloaded from the Internet for viruses before loading or forwarding to other parties.

2.5 Archiving

Users have to archive their email database in order to manage their email quotas.

2.6 Confidentiality

- Data created by users on Jaipuria Institute of Management information systems will be a property of Jaipuria Institute of Management. Because of the need to protect the Jaipuria Institute of Management network, management cannot guarantee the confidentiality of individual information stored on any network device belonging to the Company.
- 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 an unsolicited, unpleasant or abusive email.
- Users will not provide information about or lists of, Jaipuria Institute of Management employees to parties outside the Company.
- Information that users consider sensitive or vulnerable will be classified as per the data classification rules and controls will be placed that are apt for such classification.

2.7 Property

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

2.8 Security

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

2.9 Passwords and Log-in IDs

- Every user will have a unique login ID and password to access information systems of Jaipuria Institute of Management. 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 Company'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.

2.10 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.

2.11 Offensive Material

- Users will not use Company 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.

2.12 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 Company's Computing Systems. Accessing such material also increases the risk of introducing computer viruses and will thus be considered a violation of the Acceptable Usage Policy.

2.13 Prohibited Activities/Use/Communications

The following activities are prohibited for the users of Jaipuria Institute of Management 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 Company as misconduct.

- Engaging in any illegal activity (including gambling) while utilising Company 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 Company'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 Company) 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 Company's information systems to third parties.
- Using the Company 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, victimisation 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 you do 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 Institute of Management employees to parties outside the Company.
- 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 cartoons and 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, resolution or display output device.
- Using the Company 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 Company 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.

2.14 Reporting Procedure on Discovery of Policy Violation

To comply with the Acceptable Systems Use Policy users will follow the below reporting procedure. Failure to report a Policy violation will result in disciplinary action up to and including dismissal.

Users Who	Must
receive or access Material that is offensive, obscene, indecent or defamatory, including any sexual material or any material which amounts to harassment or discrimination on the grounds of race, sex or disability	immediately inform the security Help Desk and the local Human Resources Representative.
receive or access any material, which triggers the computer virus alert software	immediately delete and inform the IT team
receive or access electronic games, jokes, greeting cards, chain letters, executables, non-work-related videos and pictures	Immediately delete such items without forwarding them on to other parties.

2.15 Disclaimer

All external emails from Jaipuria Institute of Management accounts will carry at minimum the Company details, including name, address, contact details and a disclaimer.

2.16 Email Usage

Jaipuria Institute of Management's Computer System is provided for business use, including electronic communication and the processing of information. Users should always employ good practice principles when using Company Computer Systems. These principles include:

- Treating an e-mail message as if it is a permanent hard copy document to be drafted and checked in the same way. All e-mail messages are permanent records and must be compiled with care.
- Not sending or forwarding threatening, harassing or abusive messages, or any messages that may be construed by the recipient as such, as a result of the language used, frequency of messages received or size of message, font or typeface used (eg, capitals may be perceived as "shouting" when used in an email) or otherwise.

- Ensuring that any wrongly delivered e-mail messages are immediately recalled and resent to the correct person.
- Avoiding, where possible, sending e-mail messages with large attachments because they can impair the performance of the network.
- Deleting e-mail messages on a regular basis.
- Avoiding sending unsolicited non-business E-mails to a group of users. Shall this is observed, a warning will be issued to the sender and shall this be repeated, the E-mail will be revoked.

Backup Management Policy

Version : 1.0.1

1. Purpose

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 business data, related application systems and operating systems software. The purpose of the Backup Management Policy is to ensure that the critical information assets of Jaipuria Institute of Management 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.

2. Policy

2.1. Application

This policy document applies to all information and information assets at Jaipuria Institute of Management available with Jaipuria Institute of Management employees, including full-time staff and off-roll staff, which include corporate data, business applications and system software.

2.2. Backup Types & Planning

- All company critical data (criticality of business application to be decided by business owner & IT team, whereas for IT application to be decided by IT team) will be backed up and tested for restoration to ensure availability of such information as required.
- Information will be backed up as per its classification.
- IT Department will maintain a documented Backup plan for all the information and information assets identified to be backed up. The plan will include:
  - Information to be backed up;
  - name of the system hosting the information (e.g. server name);
  - Supporting IT infrastructure details hosting the information (e.g. server hardware details);
  - The type of backup – i.e. online/offline, incremental/full, etc.;

- Backup periodicity – daily, weekly, monthly, annual based on the criticality of information; and
- Retention period of the data and offsite storage location if required.

- IT systems will be backed-up in two ways – scheduled and unscheduled. While the former will be done at a defined frequency, the latter are ad hoc in nature and will be performed as and when required.
- Full or incremental backup of data and application to be taken depending upon business co-owners and IT teams analysis/ decision.
- For full back-up, data / applications to be classified into critical or non-critical levels.

APPLICATION / DATA TYPE	PERIODICITY					
	WEEKLY	FORTNIGHTLY	MONTHLY	QUARTELY	SEMI-ANUALLY	YEARLY
CRITICAL						
NON-CRITICAL						

- For incremental back-up, data / applications to be classified into critical or non-critical levels.

APPLICATION / DATA TYPE	PERIODICITY					
	WEEKLY	FORTNIGHTLY	QUARTERLY	QUARTELY	SEMI-ANUALLY	YEARLY
CRITICAL						
NON-CRITICAL						

- The information owners will formally intimate the IT Department about any new applications and its data to be backed up. Similarly, the IT Department will be informed about discontinuing the back up of the applications systems no longer in use. IT team along with the co-owners need to validate the applications and data to be backed up once in six months.

- Retention period for unscheduled backup will be defined and the tapes will get adequately stored.
- Backup media will be regularly examined for readability of the data. The backup media will be replaced immediately after encountering an error or at predefined time intervals whichever is earlier.
- Unscheduled backups will be stored for the time period as defined by the requester.
- IT Department will be responsible for the implementation of the backup plan for production servers.
- Information custodian will be responsible for ensuring the successful backup of the information assets as per the backup plan defined.
- IT department will be responsible for amending the backup sheet as and when there is any amendment. The same shall be reviewed by the IT- Head on a periodic basis.

2.3. Backup Logging and Audit Trail

- Backup logs will be recorded for all the backups taken and will be reviewed periodically.
- A "Backup Checklist" will be maintained to include, but not limited to, the following details:
  - the application/server for which the backup has been taken;
  - start and finish times;
  - the label of the media on which the backup had been taken;
  - the Status of the Backup – Successful/ Unsuccessful/ Incomplete; and
  - Sign offs from the personnel responsible for taking the Backup and personnel approving the successful completion of the planned backup.
- Backup failures will be treated as incidents and will be reported to the IT manager for corrective action and will be logged in system/basis admin daily checklist.

2.4. Backup Storage

- Backup tapes will be "write-protected" to prevent accidental overwriting.
- All the backups shall be taken on tape drives and backup tapes shall be stored in fireproof cabinets, preferably on alternate floor / building. Critical backup tapes will be sent offsite

as per frequency specified in the backup plan. These tapes will be stored in a fire proof cabinet at the offsite location as well.

- The list of tapes going offsite and the tapes coming from the offsite location will be documented.

2.5. Backup Restoration and Testing

- Personnel requiring files to be restored from a backup will submit a request authorized by the supervisor/ function head and IT Manager to IT Department. Upon receiving authorization, data will be restored by the IT Department.
- A Backup Restoration Log will be maintained to include, but not limited to, the following details:
  - date for data recovery;
  - start and end times of recovery;
  - personnel requesting the data recovery;
  - personnel responsible for the recovery;
  - reason for data recovery; and
  - status.
- Restoration testing will be performed at least once on a quarterly basis for applications/networks wherever feasible. A tape will be selected at random by the IT Department and the full contents of the tape will be restored.
- The restored contents will be verified against the tape for an exact match. This will be verified by IT Manager.
- The entire restoration process will be documented detailing the test plan, the procedures executed and the test results.

Email Usage Policy

Version : 1.0.1

1. Purpose

Email forms a vital source of communication to carry out business processes at Jaipuria Institute of Management. The purpose of this policy is to ensure that emails are used as an efficient mode of business communication and implement control procedures so that the email services are not misused by the users. The Company should ensure that email service and operations remain secure, efficient while communicating within intranet as well as through internet.

2. Policy

2.1. Application

This policy applies to all the users of email accounts approved to be used as corporate email accounts to perform Jaipuria Institute of Management's business communication. This includes employees, fulltime and off-roll having email accounts in Jaipuria Institute of Management.

2.2. User Responsibility

- Common email ID access will be given to specific employees on approval of the HoD; if a new user needs access to these ids, employee send a request to respective head who further send a mail to IT admin and cc it to IT head and after approval from IT head, IT admin gives the access.
- Do's and Don't's for individual id's are as below:-

DO's

- Users will use Company's Email account only for the business purposes.
- Users will zip all the attachements, where possible, while sending larger sized attachments.
- Email client used by the users will be approved by the IT Department of the company. Use of any other client will be prohibited.
- Users will treat Email messages and files as confidential information.
- Users will regularly archieve important email messages or move these to word processing documents, text files, databases, and other files. Email systems are not intended for the archival storage of important information, as stored Email messages may be periodically

purged by Systems Engineers, mistakenly erased by users, and otherwise lost when system problems occur.

- Users will request permission from their supervisor before subscribing to a newsletter or group news.
- In case a user encounters profane, obscure or derogatory remarks in email, he/she will either communicate with the originator of the offensive Emails, asking him/her to stop sending such messages, or report such offensive Emails directly to the respective HR Head and/or his/her Manager.
- Users will write well-structured emails and use short, descriptive subjects. The use of Internet abbreviations and characters such as smileys is not encouraged.
- User signatures will , at minimum, include employee's name, job title and company name. Following disclaimer will be added underneath users signature:

  'This communication (including any attachments) is intended only for the person or entity to which it is addressed and may contain confidential and/or privileged material. If you are not the intended recipient, any disclosure, copying, distribution or use of the contents of this communication is prohibited. If you have received it in error, please contact the sender immediately and delete this communication without copying.
- Users will use the spell check before sending out an email.
- Users will mark emails as important only if they really are important.
- Always verify the sender's address before opening an e-mail, particularly with attachments.
- In case of receiving any suspicious mail, immediately inform the IT team.
- Ignoring mails like – 'sending this mail to 5 people will yield you benefits'.
- Ignoring jokes and other business non-requirement mails.
- Always verify the sender's address before opening an e-mail, particularly with attachments.
- Perform housekeeping - delete any unsolicited mails immediately from your mailbox.

<u>DON'Ts</u>

- Do not do unnecessary CCs and BCCs.
- Do not send mails to a mass number of users, unless relevant and necessary.

- Do not 'enable' options like delivery and read receipt on each and every mails. This adds lot of load to the system. Confidential and necessary emails can be exclusions.
- Do not forward any suspicious mail you have received to anyone else. Users will not use or access an email account assigned to another employee of the organization to either send or receive messages.
- Users will not download/ forward attachments that are from an unknown or non-reliable source to prevent computer viruses.
- Users will not create or send computer viruses through Email.
- Users will not forge or try to forge email messages.
- Users will not disguise or attempt to disguise their identity while sending email messages.
- Users will not use their personal Email accounts for sending official mail. All official Email communication will take place via official Email account.
- Users will not create their own, or forward externally provided Email messages which may be considered to be harassment or which may create a hostile work environment.
- Users will not automatically forward their emails to any address outside the company's networks.
- Do not use attachments, for greetings on Festive and other occasions, use greeting e-mails only in text form.
- Do not use your official e-mail id for registration on public internet websites for personal use.
- Users will not transmit/re-transmit chain messages.

Any unauthorized review, use, disclosure, dissemination, forwarding, printing, etc. of this email or any action taken in reliance on this e-mail is strictly prohibited and may be unlawful. Greeply Industries Limited ('Jaipuria Institute of Management') does not accept responsibility for any loss arising from unauthorized access to, or interference with the communication.

WARNING: Computer viruses can be transmitted via email. The recipient should check this email and any attachments for the presence of viruses. Jaipuria Institute of Management accepts no liability for any damage caused by any virus transmitted by this email.'

2.3. Account Creation Process

- An email account will be created for every employee joining Jaipuria Institute of Management to be used for business purposes.
- Email accounts for persons other than company employees (full-time/part-time) will be created after adequate approval from IT Manager.
- For a generation of email ID for employees at branch offices, following steps are followed: -
    - Email ID for a new joiner is requested by HR department in Branch offices through an email;
    - The request is sent for approval of the divisional HR head;
    - Upon approval from the divisional HR head, the request is sent for approval of IT head; and
    - On receipt of approval from the IT head, IT admin generates email id and communicates it to HR.
- For generation of email ID for employees at plant, following steps are followed:-
    - Email ID for a new joiner is requested by IT admin in plant through an email;
    - The request is sent for approval of the plant head;
    - Upon approval from the plant head, the request is sent for approval of IT head; and
    - On receipt of approval from the IT head, IT admin generates email id and communicates it to all stakeholders.
- Email ID for domestic employees created will be unique and will be identified with the employee name
- Exclusion
    - Format of email ID for
        1) Specific ID's for Business correspondence
    - No POP account will be created / used by fulltime or off-roll employee

2.4. Size of Mailbox and Emails

The mailbox size for each user will be restricted to a suitable size.

- The size of incoming and outgoing Emails will be restricted to 25 MB for mails received and 10 MB for mails sent within/outside Jaipuria Institute of Management.
- When the mail-box size exceeds the defined limit, users will only be able to recive the emails and shall not be able to sent the email within and outside Jaipuria Institute of Management network.
- All limits on email and mail box sizes may vary depending upon network bandwidth and business needs from time to time.

2.5. Security of Gateway PC

- A firewall will be installed on the gateway PC, which connects the Company's Intranet to the Internet and also handles the Remote Access connections.
- The firewall will restrict all services and ports other than minimum required for Email applications.
- Anti-virus software will to be loaded on gateway computer to detect and repair the files affected by viruses possibly coming through the Email attachments.

2.6. Management Rights to Review Email Content

- All messages sent by employees through the company Email account are company records and management reserves the right to examine them at any time and without prior notice for:
  - ensuring internal policy compliance;
  - supporting internal investigations for suspected criminal activity; and
  - assisting the management of information systems of the Company.
- Jaipuria Institute of Management reserves right to disclose Email messages sent or received through company email account to law enforcement officials without prior notice to the employees who may have sent or received such messages.

2.7. Maintaining Email logs

- The Systems Engineers will establish and maintain a systematic process and standard for recording, retaining, archiving and destroying Email messages and the relevant

accompanying logs (only for mails residing on the server). The e-mail logs will be reviewed on need basis in case of suspected virus/ spam incident.

2.8. Deactivation of Email Account

- The Human Resource Department will immediately notify the IT Department upon the resignation, termination or transfer of employees. The Email ID of an employee leaving the Company will be deactivated by IT Department within 24 hrs of receiving intimation from HR.
- Quaterly reconciliation of employees having email access will be carried out by IT Department with inputs from HR to ensure that email access is given to authorized employees only.
- All the emails of the employees leaving the organization will be archieved before deactivating the email account.

Password Management Policy

Version : 1.0.1

3. Purpose

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 business requirements. The purpose of this policy is to establish the rules for the creation, distribution, safeguarding, termination, and reclamation of the user authentication mechanisms.

4. Policy

4.1. Application

This policy document applies to all employees, including full-time staff and off-roll staff who have access to Jaipuria Institute of Management's Corporate Network and/ or information.

4.2. IT Admin Responsibility

4.2.1. One time use of initial password:

- An initial non-standard temporary password will be provided to the users & communicated securely to the end user by the IT Department. The system will be configured to force the users to change the initial password immediately after the first logon.
- In application systems, where this functionality of force changing the password is not available, the user will change the password manually. IT department will be responsible for making the users of such application system aware of the need for manually changing the passwords on first logon.

4.2.2. Super User Password

- All privileged user passwords for Operating Systems, Databases, Applications, Network Equipment like routers, switches etc., will be sealed in an envelope and kept in a fire proof safe. This is necessary in case the password is forgotten or the related person has left the organization without surrendering the passwords.
- These sealed envelopes will be opened with the permission of the IT head. The password will be changed immediately and kept in a new sealed envelope. Details of such activity will be logged appropriately. All privileged user passwords will be changed once in 90 days.

4.2.3. Password reset

- User will request for reset of password to the IT Helpdesk. The department will verify the identity of the user by verifying the employee number and then reset the password. The new password will be a one-time password and will be changed immediately when reset by the system administrator.

4.3. User Responsibility

- Each user will have a unique user identification code and password to access Company'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 Institute of Management accounts as for other non Jaipuria Institute of Management accounts.
- Users will not share their passwords with anyone through any mode of communication like phone, email, questionnaires-security forms etc.
- "Remember Password" feature is not 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.

4.4. Password Composition

- ERP Application
  - Account lockout after 3 unsuccessful attempts. After that user contacts the IT staff to get it reset.
  - Password length should be at least 8 character long

- Last five passwords will not be used again
- Password should expire after 90 days

- Non- ERP Application / Network Login
  - The password will be at least 8 characters long
  - Users will change password at least once in 60 days
  - Last two password will not be used again
  - User will not use user name as password
  - Three unsuccessful login attempts will lock the account and users need to contact the IT department for reset.
- Password will meet at least three conditions among below four
  - Password will contain Lower case characters
  - Password will contain Upper case characters
  - Password will contain Numerical
  - Password will contain Special characters
- Users will not use easy to guess passwords such as company name, names of pets, spouse, favourites, vendor supplied default passwords, etc.
- Password will not be a word in any language, slang, dialect, jargon, etc. or based on personal information, names of family, phone number etc.

4.5. Disabling default passwords

- Vendor Supplied User-IDs/Passwords, encryption keys, and other access codes included with vendor-supplied systems will be changed before a new system is brought on-line. Similarly, default passwords shipped with software will be disabled or changed before the software is deployed in the production environment.

4.6. 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.

4.7. 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.

BYOD Policy

Version : 1.0.1

Purpose

BYOD policies, standards, and rules of behavior for the use of personally-owned devices with in Institutional network to access resources and/or services. Access to and continued use is granted on condition that each user reads, signs, respects, and follows the IT policies concerning the use of these resources and/or services.

This policy is intended to protect the security and integrity of Institutes data and technology infrastructure. Limited exceptions to the policy may occur due to variations in devices and platforms.

Expectation of Privacy

IT Department will respect the privacy of your personal device and will only request access to the device by technicians to implement security controls or to respond to legitimate discovery requests arising out of administrative, civil, or criminal proceedings.

Acceptable Use

- The Institute defines acceptable business use as activities that directly or indirectly support the requirement of the management course or as per the institutional framework.
- The Institute defines acceptable personal use on Institute time as reasonable and limited to personal communication, assignments, project work, workshops or recreation, such as reading or watching videos, emails, social networking or as per the legitimate requirement defined by the management authorities of the institute.
- Devices may not be used at any time to:
  - Store or transmit illicit materials
  - Store or transmit proprietary information
  - Harass others
  - Engage in outside business activities
  - Use the device for any things that is potential harm to the reputation of the Institute.
- Students may use their Laptop device to access the following Institute-owned resources:
  - Email Personal or Gmail ID's as given by the institute.
  - Calendars
  - Contacts
  - Documents
  - Online PDF documents
  - Video etc. or anything as per the requirement of the course.
- Institute has a zero-tolerance policy for use of BYOD devices for bullying and harassment, or in anyways that can harm the image of the institute

Devices and Support

The following devices are supported:

- iPhone & IPads
- Blackberry devices
- Windows phones/tablets
- Windows or Mac OS based Laptops.

- Connectivity issues are supported by IT; Student/Employee should contact the device manufacturer or their carrier for an operating system or hardware-related issues.
- Devices must be presented to IT for proper job provisioning and configuration of standard apps,such as browsers, office productivity software and security tools, before they can access the network.
- Students must ensure that devices to have authorized copy of operating systems and a legitimate Antivirus software

Security

- In order to prevent unauthorized access, devices must be password protected using the features of the device and a strong password is required to access the Institute network.
- The device must lock itself with a password or PIN if it's idle for five minutes.
- Tampered/ jailbroken (iOS) devices, pirated OS are strictly forbidden from accessing the network.
- Android Smartphones and tablets are not allowed to connect to the network.
- Access to Institute data is limited based on user profiles defined by IT and automatically enforced.

Risks/Liabilities/Disclaimers

- Student/Employee to personally ensure that data is backed up in a timely manner as IT holds no responsibility for loss of Data on their own devices.
- The institute reserves the right to disconnect devices or disable services without notification.
- Lost or stolen devices must be reported to the Institute within 24 hours. Student/Employee are responsible for notifying their mobile carrier immediately upon loss of a device.
- The students/employee is expected to use his or her devices in an ethical manner at all times and adhere to the institutes acceptable use policy as outlined above.
- The Student/Employee assumes full liability for risks including, but not limited to, the partial or complete loss of Institute and personal data due to an operating system crash, errors, bugs, viruses, malware, and/or other software or hardware failures, or programming errors that render the device unusable.
- Management reserves the right to take appropriate disciplinary action up to and including termination for noncompliance with this policy.

User Acknowledgment and Agreement

I acknowledge, understand and will comply with the above referenced security policy and rules of behavior, as applicable to my BYOD usage of Jaipuria Institute of Management IT services.

Employee/Student Name:

_____

Employee/Student number:

_____

BYOD Device(s):

_____

Student/Employee Signature: _____

Date: _____

Online Video Communication Tools Policy

Version : 1.0.1

3 Policy for usage of Online Video Communication Tools

We are having a limited number of paid online conferencing/meet in the g resources and have to use them on a shared basis to meet all the requirements. We need to distribute the usage load on all the available platforms to keep all the activities running in parallel. In addition, we have limited number of IT Staff at all locations. The IT staff members will be busy in their routine work like daily Zoom licence allocation as per class schedule on Moodle, Moodle Reporting, IT support, etc. Therefore, we all should develop a habit of Self Dependency, and well verse ourselves for scheduling and executing our own meetings. IT Team will be available for any technical assistance you need.

The Policy for utilising the available platforms is as follows:

Zoom:

Zoom accounts can be of two types licensed or Basic. The details and usage of both the accounts is as follows:

Basic Account (For all Faculty Members):

These are personal accounts and are free. They are very easy to create and have a capacity of Online meetings with 100 participants and 40 minutes meeting time limit. You all can use this Basic Zoom Account for any individual online interaction with Faculty/Staff/Students or for internal team meetings. For mentoring sessions and small group interaction Zoom basic or Google Meet should be used. If the session is longer than 40 minutes, Google meet is preferable.

Licenced Account (Total 50 [Each Account is having 500 Meeting Participants + 500 Webinar Participants Capacity with no Meeting Time Limit]):

We have purchased a license for Professional Zoom Accounts. These accounts will primarily be used for Online Delivery of Classes from the Campuses, and/or for Events like Webinars, Guest Lectures, Large Student Interactions, Etc. These licensed accounts will be connected with Moodle.

Usage of the Zoom Licences, for any other activities except Online Class Delivery, a request for using the Zoom Account with all the required information like; Date, Timings, No of Participants, Nature of Event, Details of Event Organiser, Panellist, Guests should be submitted to the IT Team marking a copy to the undersigned, at-least a week before the event date.

Google Meet (For all Faculty + Staff Members [Each Account is having 250 Meeting Participants Capacity]):

Individual Google Meet Licence is available with each individual on their Official Google Email ID and should be used for Faculty/Staff Individual Official Meetings like; Team Meetings, Mentee Interactions, Area Wise Meetings, Etc. Google meet does not have any time limit on meeting. For mentoring session and small group interaction Zoom basic or Google meet should be used.

Cisco WebEx (Total 05 [Each Account is having 1000 Meeting Participants + 1000 Webinar Participants Capacity]):

These Licences are available at the HO level and can also be utilised for Events like; Webinars, Guest Sessions, etc. The request for the same with all the required information like; Date, Timings, No of Participants, Nature of Event, Details of Event Organiser, Panellist, Guests should be submitted to the IT Team marking a copy to the undersigned, at-least a week before the event date.

3.1 Action by: Faculty

1. Faculty has to share the TOPIC of the Class/Session with PMC Team on Friday of previous week. In exceptional circumstances classes can be scheduled at least a Day Prior.

3.2 Action by: PMC Team

1. Class Scheduling has to be done by Program Office as they were doing earlier.
2. Class Scheduling will be done at two levels:
    a. On Impartus (For classes being conducted Physical in campus)
    b. On Moodle (For classes being conducted Online Via Zoom)
3. Class Scheduling on Impartus is as usual as it was done earlier.
4. Class Scheduling on Moodle has to be done from the Course Page of each Course being conducted by the Faculty Member. (Training for same will be done by IT Team for PMC Staff).
5. Topic Format for Zoom Class on Moodle: **<Topic provided by the Faculty> + <Date>**

3.3 Like: **"Management Accounting 10-07-2020"**

This will bring more clarity to Faculty and Students for their scheduled class and fetching the recording from the Zoom Backend.

6. Once the PMC team does Class Scheduling, the time table for each day has to be shared with the IT Team a Day Prior for proper Licence Allocation for conduct of Online Class.

Zoom Licence Allocation:

3.4 Action by: IT Team

1. IT Team will receive Time Table for each day from PMC Team a day prior.
2. IT Team will allocate the Zoom Licence to the Faculty Accounts, which are having their classes on the day and reallocate after each slot entire day.
3. IT Team will provide any Technical Assistance as required by the Faculty/Staff.

Class Change or Swapping

3.5 Action by: Faculty & PMC Team

1. If Faculty is exchanging or swapping a class with another faculty member in case of leave, or any other issue. It will be the responsibility of the individual faculty to share the same information with the PMC team in a timely manner for smooth shift of class.

Once any information of change is received by PMC team. PMC team will share the updated Time Table to IT Team for smooth and timely allocation of Zoom Licence to faculty account.