IT Policy

The company provides the best available Infrastructure to employees in order to complete their given work in time. All the resources provided to employees are for Official purpose only.

- Organizational User IDs and e-mail accounts may only be used for organizational needs.
- It is prohibited to send or forward any email or other communication or attachments or email status, which may be considered as offensive by an individual or a group of people. This includes, but is not limited to political, religious, caste, regional, sexual or any other material.
- Use of Internet/intranet/e-mail/instant messaging may be subject to monitoring for reasons of security and network management and users may have their usage of these resources subjected to limitations by the Organization.
- Employees may not use official IT infrastructure (including but not limited to email account, office computing equipment, computers, laptops, tablet, printer, network, VPN etc) to visit Internet sites or access or download or forward in any form any material that contains obscene, hateful or other objectionable material, shall not attempt to bypass Organizational surf control technology and shall not make or post any remarks, proposals or materials on the Internet which may be deemed obscene, hateful or objectionable.
- Employees shall not solicit or send e-mails that are unrelated to the business activity of the company or which are for personal gain, shall not send or receive any material which is obscene or defamatory or which is intended to annoy, harass or intimidate another person and shall not present personal opinions as those of the company and the use of organizational e-mail facilities.
- Employee may not upload, download or otherwise transmit commercial software or any copyrighted materials belonging to the company or any third parties, may not reveal or publicize confidential information, and will not send confidential e-mails without prior approvals.
- Employees may not use office IT Infrastructure or devices to download software from the Internet or execute or accept any software programs or other code on the Internet unless it is in accordance with the Organization's policies and procedures.
- Employees will not use the resources or time of the company in any manner which violates intellectual property rights (such as third party copyrighted material) and/or laws of the land.
- Employees are prohibited from downloading content such as streaming video and MP3 music files, sharing digital photographs and similar material which may violate Intellectual Property laws. In addition, this results in wastage of precious bandwidth, for a prohibited activity.
- One Convergence reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

- Keep passwords secure and do not share accounts. System-level passwords should be changed on a periodic basis.
- All PC's, laptops, and workstations should be secured with a password-protected screensaver with the automatic activation feature set at ten minutes or less, or by logging off when the host will be unattended.
- Because information contained on portable computing or storage devices is especially vulnerable, special care should be exercised. It is the employee's responsibility to protect and ensure security of company equipment (such as laptop or other computing or storage or data device) and any company confidential information contained therein.
- Postings by employees from official e-mail address to newsgroups, forums, social networks etc should contain a disclaimer string that the opinion expressed are strictly their own and not necessarily those of One Convergence, unless posting is made in the course of business duties with appropriate approval.
- Any computing device, whether owned by the employee or One Convergence used on the office Internet/intranet/extranet/VPN must always run an approved virus-scanning software.
- Employees must use extreme caution when opening e-mail attachments received from unknown senders; these may contain viruses, e-mail bombs, or Trojan horse code.
- Any form of harassment via e-mail, telephone, paging, chatting or any other means, either through language, frequency, or size of messages is not allowed
- Unauthorized use or forging of e-mail header information is not acceptable
- Employees are required to escalate any suspicious activity or incident to the IT Head / IDC Head / HR at One Convergence immediately.

The following guidelines would help in better and safer utilization of IT resources:

- Shared files or data must be password protected to prevent unauthorized access or misuse.
- Regularly update Operating System, web browser, and other major software, using the manufacturers' update features, preferably using the auto update functionality. (Consult System Administrator for this activity). Use antivirus software, and update it on a regular basis to recognize the latest threats.
- Save attachments to the drive / disk before opening them.
- Don't write down your password. Or don't give out your password to anyone, whether you know them or not & don't select the "Remember My Password" option.
- Don't leave your laptop unattended, even for a few minutes.
- Don't install or use pirated copies of software.
- Don't install P2P file sharing programs which can increase the vulnerability of your system and also overload the office network bandwidth.
- Don't set your e-mail program to "auto-open" attachments.

- Don't run any internet servers. Running web, mail, ftp (etc) servers from your desktop leaves your data vulnerable.
- Employees using their personal laptops need to ensure that they back up the company data to the company provided machine and delete any and all materials which are of company interest.
- Employees should keep all their working notes in the drive only and have to ensure periodic back up of all work related material stored in the disk at regular intervals (employees are strongly recommended not to store any data in the disk)
- Employees have to ensure that all the system related units are switched off or suspended/hibernated while leaving for the day, exceptions being made where the system is in use (for testing etc) or if the employee is working from home, and needs access to the system.

The policy is framed as per the current requirements and needs of the company. Changes in the policy can be made anytime depending upon the need basis whose information would be shared to the employees simultaneously.