IT Policy

Revalsys Technologies provides the best of 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.
- 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 visit Internet sites or access or download in any form any material that contain 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 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 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 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. Also, download / upload of personal content is not permitted. In addition, this results in wastage of precious bandwidth, for a prohibited activity.
- Revalsys Technologies 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.

- Information contained on portable computers is especially vulnerable, special care should be exercised. It is the employee's responsibility to protect and ensure company laptop's security (or other computing or storage or data device) and any company confidential information contained therein.

- Postings by employees from a Revalsys e-mail address to newsgroups should contain a disclaimer string that the opinion expressed are strictly their own and not necessarily those of Revalsys, unless posting is made in the course of business duties.

- Internet/intranet/extranet, whether owned by the employee or Revalsys Technologies shall be continually executing 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.

- Escalate any incident or suspicious activity to IT Admin / HR immediately.

- Create a password for your files in order to protect file sharing activities.

- 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 when operating outside office.

- P2P file sharing programs cannot be used without prior approval from manager.

- Usage of personal devices (Pen drives) for official work is not permitted without prior management approval.

- Usage of official devices for personal work is not permitted.

- Employee has to ensure periodic back up of all work related material at least once in 15 days.

- Employees have to ensure that all their system related units are switched off 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. Manager needs to be informed in those cases.
- Employees need to take care of the given resources with utmost care & responsibility and any loss or damage to the given resources would demand an explanation, sometimes leading to pay for the damage.
- In case of any malfunction, employees are required to report the same to the Systems Admin Department immediately.
- Do not share/send any files through skype.
- Do not share user name and password in single communication.
- All the documents related to any department should use Revalsys template.

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 the information of which would be shared to the employees simultaneously.