CresTech™
YOUR TESTING PARTNER

W.e.f 1st September 2016

Do’s and Don’ts Policy

Do’s

1. All users must log out of all systems in which they are logged, at the end of the day. All PC equipment should also be turned off at this point, unless there is a business reason to keep the system turned on.
2. Files that are downloaded from the Internet must be scanned with virus detection software before installing or execution. All appropriate precautions should be taken to detect for a virus and, if necessary, to prevent its spread.
3. sites and downloads may be monitored and/or blocked by IT Team, if they are deemed to be harmful and/or not productive to business
4. If the working desk is left unattended even for a short period such as going for lunch, attending meeting etc. then the desktop / laptop should be locked by pressing “CTRL + ALT + DEL and lock computer”. This is to avoid unauthorized access of desktop / laptop and data safety. Immediately collect printouts from network printer, to protect the data confidentiality.
5. Choose difficult-to-guess and easy-to-remember passwords and combination of character and numbers, small and capital letters. For example, “Ihoil026” can be remembered as “It happens only in India” suffixed by last three digits of your phone number.
6. Official e-mail ID can be used only for the official purpouse.

7. Your total mailbox size is restricted to some limit by the Software itself. You should keep on deleting all unwanted mails, and chain mails, otherwise your mail box will crash without telling anybody.
8. Read and learn more about computers and latest trends. Remember in today’s world literacy is e-literacy (i.e. Computer Literacy)

Don’ts

1. Do not allow access to computer resources to un authorized person / outsiders / vendors without permission from I T department.
2. Do not Alter the configuration of Desktop application, business application or operating system. Please call IT helpdesk/IT Service provider for technical support.
3. Do not Move, Add or Change the hardware equipment to your desktop, laptop, printer etc without information to IT department.

4. Connecting accessories for e.g. speakers, head phones, PDA, web camera, modem etc should be authorized by IT department and strictly for business use only.
5. Do not install copy, distribute or use software in violation of copyright and / or software agreements or without authorization of IT department.
6. Do not attempt to access another's account, private files, or e-mail without the owner's permission.
7. Do not print non-official documents such as news from Internet, jokes received on email, manuals / magazines from web etc.
8. Don't keep simple password, which can be easily guessed by anybody such as you r spouse / children's name, vehicle number etc.
9. Don't share your password knowingly or unknowingly with any one.
10. Do not share any folder or drive of your desktop with everyone. In case you have to share drive or folder with any other user, give privileges to only authenticated users.
11. Do not store songs and video files on your hard drive unless you have permission to do so or you have copyright of the same. Remember copying and storing film or individual songs, album s and video files is illegal and employee will be responsible for all such data on his/her desktops.
12. Never open any attachment, which are having extension .SC R, .EXE, .COM or .PIF. All other attachments should be checked and only when you are sure attachment is from trusted sender it should be opened.
13. Do not send jokes, pictures, religious messages etc. on official email id.
14. Do not visit internet sites that contain obscene, hateful, pornographic or otherwise illegal material, social networking etc.
15. Do not download any commercial software or any copyrighted materials belonging to third parties through torrent/bit torrent or any other way.