**User general guidelines:**

1. You are individually responsible for protecting the data and information. Security is everyone's responsibility.
2. Recognize which data is sensitive. If you do not know or are not sure, ask.
3. Information in any form is a priceless asset, even though you cannot touch it.
4. Use the resources at your disposal only and for the benefit of the Organization.
5. Upkeep the infrastructure provided to you.
6. If you observe anything unusual, inform your supervisor.

**“Do’s”**

* 1. Do choose a password that would be hard to guess.
  2. Do log off or lock your PC before you leave your workstation
  3. Do protect equipment from theft and keep it away from food and drinks.
  4. Do delete unwanted mails to reduce mailbox size
  5. Do switch off AC, power supply and light when not required
  6. Do ensure all important data is backed up regularly.
  7. Do switch off machines before leaving the office.
  8. Do use a disclaimer in official emails.

**“Don’ts”**

* 1. Do not write down, share or disclose your password.
  2. Do not give others the opportunity to look over your shoulder if you are working on something sensitive.
  3. Do not use shareware
  4. Do not duplicate or copy software
  5. Do not install any software on your machine or alter its configuration without approval
  6. Do not use devices like CD Rom, Pen drive, mobile phone etc. to carry official or client’s data outside office premises without prior approval.
  7. Do not share mails with others
  8. Do not register company email ID’s in public domains without approval (For eg.linkedin.com , All groups updates are coming to this email ID)
  9. Do not use other’s email ID for communication
  10. Do not send non-business messages
  11. Do not download following without prior approval,
      + Software (e.g., freeware, shareware, commercial, or public domain)
      + External material from individuals or companies unknown
      + Clover Infotech or government Restricted information
  12. Do not keep unwanted documents or data in the backup folder.
  13. Do not bring your own devices in office premises without approval
  14. Do not use other/prohibited means to access internet through a personal computer at client place or in the office.

**Any deviation to the above policy will be treated with disciplinary action.**

(Note: Deviation in case of business requirement can be treated as special case and needed management’s approval to regularize the same.)

Above Do’s and Don’ts should be followed in organization as well as at client site during assignment.

**Signature : Department :**

**Name of Employee :**