**Security Guidelines to be followed in an Organization:**

**Access to Information**

Information is available on need to know basis for specific groups. The network file server is segregated to allow individual sectors for projects and units. Access to these are authorized through access privileges approved by unit Mentors or project Mentors.

**Authorization**

Only those authorized by a specific power of attorney may sign legal documents, representing the Company.

**Passwords**

Access to our network, development environment and MS-exchange is through individual’s password. For security reasons it is essential to maintain confidently of the same. if the password is forgotten , the Networking department is to be contacted to reset and allow you to use a new password.

**Unauthorized Software**

You shall not install, download, copy, and duplicate any unauthorized or unlicensed software, programs, games, attachments on to your computer system.

**Security**

Security is an important aspect of our communication and office infrastructure. We have security personnel deployed. Those of you who wish to work later or early hours are requested to produce requisition slips for working to the security personnel on demand.

If there a need to take some of the equipment infrastructure out of the office premises for any reason the associate shall obtain authorization from your mentor.

The communication security is maintained by controlling physical access to computer systems, disabling all work station floppy, disk drives, and a company-wide awareness about the need for protection of intellectual property and sensitive customer information.

For some projects the company users sophisticated data enertion devices. Your work table and store space is lockable. Please ensure they are locked when unattended. Duplicate keys are maintained with administrative department.

***In case any violation, legal actions are taken as per the cyber laws***.