



Confidentiality and Information Security Policy

A) Non-Disclosure Agreements (NDA's) with Client

- To ensure the security and confidentiality of information, a Non-Disclosure Agreement (NDA) is executed with each client and all private information is respected.

B) Non-Disclosure Agreements (NDAs) with Employees

- At the time of joining, all employees are required to sign a proprietary information and inventions agreement. Individual NDAs are also signed with every employee on joining
- Employees cannot disclose any proprietary information directly or indirectly to anyone outside the project team or company, or use, copy, publish, summarize or remove such information from the company premises
- Employees cannot use any unfair competitive practices upon termination of employment or engage in any business during employment
- Any confidential information received from third parties and clients are held in strictest confidence and employees are not allowed to disclose or use it, except as necessary to perform his/her obligations as is consistent with third parties
- Any "invention ideas" and relevant records has to be disclosed to the company and all information and records pertaining to any idea, process, trademark, service mark, invention, technology, computer program, original work of authorship, design, formula, discovery, patent, or copyright conceived or developed has to be promptly disclosed to the company

C) Project-related IP protection

- Dedicated resources made available for all projects. This prevents unauthorized usage of resources and protects all proprietary information of our clients
- We have a strong ethical framework that forbids exchange of IP between projects
- Every team dedicated to a particular client can have its own secure physical location and its own segment of the LAN.

D) Confidential Document Control

- Access to public email systems is disallowed and floppy and CD disk drives/writers are disabled on all desktops. Prior written permission of the Project Manager is required for usage of respective drives
- Random checks are made on emails that go out of official mailbox that exceeds permitted size (with or without attachments)

E) Physical Security

- Restricted access for each employee
- Presence of security guards and 24x7 surveillance system
- We have fire protection and fire extinguishers available at comfortable distance.
- The entire office premise has been designated as a non-smoking zone.
- Controlled access for Visitors to working area.

F) Data Access Security

- Security Firewalls are installed to prevent unauthorized access to the network
- Group policies in place for accessing PCs and workstations for authorized access
- Access to important files and directories is given only to specific personnel
- Monthly backups are stored at an off-site location and removable backups are kept safe with logs duly maintained. Daily backup are stored in fire-proof safe.
- By default, all ports (USB, Serial, Parallel) are disabled on PCs. Enabling of the required ports is done only on specific requests by the client
- Physical security ensures no CDs, Pen-drives, movable media goes in and out of the facility without written permission from the management

Finite010105