vr4U Global

23-B, Kavalan Street,
Thaiyar Kulam
Kanchipuram – 631501
Ph: +91-044-48055631

Data Security Policy

1. **Data Privacy:** Employees are required to sign a non-disclosure clause included in their appointment letter when they join the organization and they are made to understand that our company's privacy policy is a pledge to our customers that they need to protect their information during their stay in the company and after their tenure.

2. **Electronic Devices:** Mobile phones / tablets / cameras are not allowed inside the office premises and any electronic device or communication device ought to be handed over at the front-office.

3. **Workstation:** Workstations are not equipped with DVD R/W drives and all USB ports are locked. Any software installation is done only by the authorized person

4. **Password Management:** Password security provided for all the workstations accessed by all employees or temporary workers which should be kept with secrecy and not shared with others. Passwords are updated regularly, with a mandatory change every three months to enhance security.

5. **Internet Usage:** Established limits on employee internet usage in the workplace. Only stock photo and other knowledge sharing sites are accessible to employees.

6. **Email Usage:** Email access is provided only for the Client Managers / Process Managers who communicate with the client and the management on a regular basis to manage the workflow and assign tasks.

7. **Software Copyright and Licensing:** Only licensed software purchased by the company is installed in the workstation. Any software which needed to be downloaded pertaining to work is reviewed and downloaded only after approval from the manager.

8. **Security Incidents:** Company's network is protected using Firewall and all employees are trained and instructed on how to report incidents of malware, if any and subsequent steps are taken by the IT personnel to help mitigate damage.

9. **Data Management:** For data-backup, soft copies of everyday work are stored in the company's main drive where work-in-progress or completed files are required to be uploaded by the authorized person by end of each day. Based on the agreement we sign with our clients, copies are either maintained or deleted upon confirmation from the client, after the project is completed and delivered.

10. **Internal audits:** IT audits are conducted periodically to check everything is in place and to maintain seamless security and improvements done based on the findings.