Information Technology Policy

The Factory protects its IT system from illegal use by un-authorized personnel and maintains the integrity of the data by providing employee passwords. (It should be 8 characters long) and by using anti-virus software.

- Vamani Overseas Pvt Ltd. is using antivirus like Sequrite(Quick heal), Enterprises edition threat consol, which is updated from server on a routine basis.
- Vamani Overseas Pvt Ltd has Windows 7/8/10 to access its IT system.
- The following security measures are also in a regular Practice.

The Factory backs-up data on a regular basis.

- Vamani Overseas Pvt Ltd takes back up data in External HDD having Data Cartridge Capacity of 40-80 GB in order to ensure that all records still exist even if the main IT system is disabled in the case of virus attack, fire at the factory etc.
- Data back up in a variety of means such as Hard Disk to ensure that all the data can be recovered easily in case of any unfortunate problem.
- Scheduling of daily backup on server is done for ERP/HR Software.
- Critical and Important Data back up in Computer systems on weekly basis.
- All software, whether purchased or created, is protected by at least one full backup either in CD or in Hard Disk etc.
- All application data is protected by monthly full backup.

The following items are documented for each generated data backup.

- Data & Day of data backup.
- Type of data backup.
- Data media on which the operational data are stored.
- Name of Person Responsible for data back up.
- Backup is performed after office-hours when computer usage is low.
- Backup data is stored at a secure location.

The factory has procedures so that employees change their passwords on a periodic basis.

- All employees have access to the computer system must change their passwords at quarterly basis(12 Weeks).
- It is the Responsibility of Network administrators to notify computer users regarding password changes.
- A password is of a combination of letters and numbers, at least 6 characters long.
- Employees change their passwords more often if there is a risk that the privacy of the password has been compromised. If an employee suspects that another person may have discovered the password, a new password is issued immediately.

The factory has policies to determine which employees are authorized access to its IT system as given below.

The List of employees has authorized access to the IT system is maintained by the IT Department.

The Organization gives the user rights on the pre defined job functions by the Management for employees. Any unauthorized access/tampering and manipulating the business data will be seriously reviewed / investigated and appropriate action will be taken accordingly

Type of offence	**First Offence**	**Second Offence**	**Third Offence**	**Fourth ffence**	**Fifth Offence**
Willingly full damage of property & abuse or unauthorized access or use of IT system	**Discharge**				

The Organization has Network Administrator and other members of the senior management team are there to lead the IT disaster recovery team as per our IT contingency Plan.