Information Technology Department Policies

1. Acceptable Use Policy – AUP
Restricts use of a company's network or services for illegal activities to ensure security, and safeguard the reputation of the company.

2. Data Privacy Policy
Restricts to misuse the information's of customers, vendors, suppliers, Government sectors and employees from ERP or any manner.

3. Credentials Security Policy
Do not disclose/share your Computer or Server Credentials/Passwords with third party and to make sure that are properly maintained.

4. Disaster Recovery Policy (only for IT Employees)
To secure the critical data by responsible IT staff during downtime, and ensure business continuity in the event of downtime.

5. Bring Your Own Device - BYOD Policy
Personal mobile devices such as TAB, MOBILE, LAPTOP are not allowed within the workplace and Offices except work-related.

6. Social Media Policy
Staffs not allowed to use social media in the workplace except work-related.

7. Hardware Confirmation Policy
I hereby confirmed that, the below Hardware has been received and I acknowledge to serve the company by complying the IT policies.

- Personal Computer – PC or Laptop
- Printer or printer Connection

8. Unattended Devices Policy
If you leave your desk/table, you lust log out or lock your computer to avoid the risks access by an unauthorized user.

I myself agree to outline the consequences of breaking the rules above and any misuse /violation is subject to corrective actions mentioned below :-

Annexure #C1
Corrective actions such as :-

- Warning letters.
- Penalty.
- Legal Actions.
- Salary Deductions.
- De-promotions
- Position Transfer
- Performance revaluation
- Bad Conduct Certification
- Stamping bad mark on profile
- Charging Compensation
- Framing as bad to all

Employee Name & Signature	Software & Applications Manager	Chief Technology Officer