IT Policy

Physical Security

- Installation, set-up, maintenance and repair made on computers and/or systems without the approval of Operations Manager/CEO will be considered a breach of security.

- Users must lock their computers before leaving the desks. This is to ensure that there is no unauthorized access while they are away

- Employees shall not carry personal computer material like CD, Floppy, Pen drives etc to the work space without approval of their managers.

- Family and friends are not allowed to office premises without knowledge of their managers. Employees shall make sure of escorting them while they are in office and not allowed to access computer data.

Access Control

- Access to IT resources is primarily available to permanent employees. Temporary staff and contract workers shall get special approval. The access rights to these temporary groups shall be limited to the business need
- Connecting modem and phone to the desktops to enable dial-up networking is prohibited as it may create issues in security and settings
- Sharing confidential documents and data to competitors etc. will be considered as a serious offence and can lead into disciplinary action which includes termination of service.

Security Authentication

- Individuals shall not create system or network accounts in the computers.
- Employees must keep their user name and password confidential. Individuals will be responsible for any transactions with their password.
- Any resignation must be informed immediately to the HR Department.

Security for Virus

- Any new files /Software shall be scanned for virus before it is installed or accessed through network.
- Employees must make sure that the necessary antivirus program is installed in the machines and the updates are done on time
- Any virus attack shall be brought to the notice of Operations Manager.

Firewall Security

- Employees shall not attempt to disable any Proxy /Firewall settings installed in the system
- Hacking of network, database or individual hard disk etc are prohibited
- Accessing /Setting up additional resources (eg: Setting up FTP, dial-up etc) requires approval from System Administrator.

Internet Usage

- Internet shall not be misused as it can lead to reduction of productivity, leakage of company confidential information, degraded network speed, exposure to virus attack etc
- Internet shall be used to achieve the business goals and to improve productivity
- Non-business related documents and graphics such as pornographic or sexually explicit contents, games, unnecessary free software or shareware, audio and videos etc. from websites are prohibited. These documents, graphics and programs can pose a potential virus and security threat also.
- The company reserves the right to inspect any and all files stored in private folders of your computer in order to assure compliance with this policy.
- Employees shall schedule communications-intensive operations such as large file transfers, huge program downloads, mass e-mailings and the like, at off-peak hours as these activities substantially hinder the use of the Internet during office hours

Email Usage

- Email usages shall be limited to company business purpose.
- Sending harassing, abusive, threatening messages or attachments are strictly prohibited
- Chain mails and executable graphic files, MP3 files shall be avoided and any such mails received shall be deleted immediately
- Users shall not give official mailing address for subscribing to mailing lists, news groups etc unless it is for specific business reasons.
- Attachments and emails from unknown sources shall not be opened and deleted the same immediately, as it may carry virus
- Management has the right to access /copy individual emails if required

Telephone Usage

- Use of telephones shall be limited to company business purpose or urgent local calls.
- It is advised to use internet telephony based services for STD/ISD calls (eg: Skype ,Google talk)
- Mobile phone usage shall be strictly restricted to emergency only during business hours.

Software Usage

- It may be ensured that only approved and authorized software is used in the system
- All software including downloads shall be licensed.
- Employees shall not give company data to any outside party including clients, customers, competitors etc.

Non Disclosure Agreement

- Employees are exposed or disclosed with certain trade secrets of the Company; consisting but not necessarily limited to:

  (a) Technical information: Methods, processes, formulae, compositions, systems, techniques, inventions, source code, project ideas.

  (b) Business information: Customer lists, pricing data, sources of supply, financial data and marketing, production, or merchandising systems or plans.

- Employee should not disclose or divulge to others any trade secrets, confidential information, or any other proprietary data of the Company in violation of this agreement. If the Company may notify any future or prospective employer or third party of the existence of this agreement, and shall be entitled to full injunctive relief for any breach.
- Information regarding the company will not be used for any commercial benefits if found violating this agreement company is liable to take legal actions against the employee.

Acknowledgement

I have read the IT policy carefully and agreed to abide by the same. I also understand that violation of the above policy may lead to disciplinary action including dismissal

Name: Diana Joseph

Signature:

Diana

Place: Kakkanad
Date: 08/07/2024