User Accounts and Passwords

Where applicable, employees may be provided with user accounts, email access, or other Company systems required to perform their duties. Employees are responsible for maintaining the confidentiality of their login credentials and must not share usernames or passwords with any unauthorized person.

Passwords should contain a combination of letters, numbers, and special characters and should be changed periodically or whenever there is a concern regarding security. Employees must not leave computers or systems unattended without appropriate security measures or use another employee's login credentials without authorization.

Any suspected loss, misuse, or unauthorized access to Company systems or information must be reported immediately to the Reporting Manager or the Human Resources Department.

Internet Usage

Internet access provided by Pukhraj Additives LLP is intended primarily for official business purposes. Limited personal use may be permitted, provided it does not interfere with work responsibilities, productivity, or the Company's interests.

Employees shall not access, download, or distribute any illegal, offensive, inappropriate, or unauthorized content, install unauthorized software, or engage in activities that may compromise the security of the Company's systems or network. The Company reserves the right to monitor internet usage in accordance with applicable laws and Company policies.

Failure to comply with this policy may result in disciplinary action, including suspension of system access, termination of employment, or legal action where applicable.

Email Usage

Company email facilities are provided for official business communication and shall be used responsibly and professionally.

Employees shall:

1. Use Company email primarily for official business purposes.
2. Verify recipient details before sending confidential information.
3. Protect confidential documents by using password-protected attachments or other approved security measures, where appropriate.
4. Avoid opening suspicious emails, links, or attachments and immediately report any suspected phishing or cybersecurity incident.
5. Regularly delete unnecessary emails to maintain efficient mailbox management.

The Company reserves the right to monitor the use of its email systems in accordance with applicable laws and Company policies.

Confidential Information and Electronic Data

Employees shall protect all confidential Company information, including customer information, supplier information, product formulations, manufacturing processes, technical documents, quality records, laboratory data, pricing information, financial records, and other proprietary information.

Confidential information shall not be copied, photographed, reproduced, shared, uploaded to unauthorized websites, cloud storage, social media platforms, or Artificial Intelligence (AI) tools without prior written authorization from the Management.

Employees shall use Company computers, electronic devices, removable storage media, and other information systems responsibly and only for authorized business purposes. Any suspected data breach, information security incident, or unauthorized disclosure of Company information must be reported immediately to the Reporting Manager or the Human Resources Department

Approved By



Karina Nagpal
Managing Partner
Pukhraj Additives LLP