PDS INFOTECH PVT LTD

Email Policy

Ref No: ISMS/PDS/5.2/10.1

1. Purpose

Electronic email is used pervasively across the organization and is often a primary channel for business communication. Misuse of email can create legal, privacy, and security risks. The purpose of this policy is to ensure the proper use of PDS Infotech Pvt Ltd's ("the Company") email system, and to set out what the Company considers acceptable and unacceptable use of that system. This policy outlines the minimum requirements for use of email on the Company network.

2. Scope

This policy covers appropriate use of any email sent from a Company email address and applies to all employees, vendors, and agents operating on behalf of the Company.

3. Policy

- All use of email must be consistent with Company policies and procedures on ethical conduct, safety, compliance with applicable law, and proper business practice.
- The Company email account should be used primarily for Company business purposes. Limited, incidental personal use is permitted in accordance with the Acceptable Use Policy; use of the Company email system for non-Company commercial purposes is prohibited.
- All Company data contained within an email message or attachment must be secured in accordance with the Information Classification and Management Policy.
- Email should be retained only if it qualifies as a Company business record — that is, where a legitimate and ongoing business reason exists to preserve the information it contains.
- Email identified as a Company business record shall be retained in accordance with the Company's Record Retention Schedule.
- The Company email system must not be used to create or distribute disruptive or offensive messages, including offensive comments relating to race, caste, gender, disability, age, sexual orientation, religious belief or practice, political belief, or national origin, or content that is pornographic in nature. Employees who receive such content from a Company colleague should report the matter to their supervisor immediately.
- Users are prohibited from automatically forwarding Company email to a third-party email system. Individual messages forwarded by a user must not contain information classified as Company confidential or above.
- Non-work-related email should be saved in a folder separate from work-related email. Sending chain letters or joke emails from a Company email account is prohibited.
- Company email is provided for business purposes and is not private. The Company may access, log, and monitor messages sent, received, or stored on its email system, without prior notice, where reasonable, proportionate, and for a legitimate business or security purpose, consistent with the Digital Personal Data Protection Act, 2023. By acknowledging this policy, personnel are notified of this in advance.

4. Policy Compliance

4.1 Compliance Measurement

The Company Information Security team will verify compliance with this policy through methods including, but not limited to, periodic reviews, business tool reports, and internal and external audits, with findings reported to the manager/leadership.

4.2 Exceptions

Any exception to this policy must be approved in advance by the Information Security team.

4.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5. Roles and Responsibilities

- IT / Information Security Team: Monitors compliance, investigates reported violations, and manages exceptions in coordination with the Information Security Committee.
- Managers: Ensure their teams understand and comply with this policy.
- All Personnel: Use Company email in accordance with this policy and report suspected violations promptly.

6. Review

This policy shall be reviewed at least annually, or upon significant organizational or regulatory change, to ensure continued alignment with ISO/IEC 27001:2022 and applicable Indian law, including the Digital Personal Data Protection Act, 2023.