PDS INFOTECH PVT LTD

Email Security Policy

Ref No: ISMS/PDS/5.2/11.1

1. Purpose

The purpose of this policy is to minimize risk associated with the use of email and Internet-facing communication services, and to define controls against unauthorized access, theft of information, and malicious disruption of PDS Infotech Pvt Ltd's ("the Company") email systems.

2. Scope

- This policy applies to all users of the Company's information assets, including employees, temporary staff, vendors, business partners, and contractor personnel, regardless of geographic location.
- This policy covers all information systems environments operated by the Company, including documentation, physical and logical controls, personnel, software, and information.
- This policy addresses user responsibilities specifically; other Company Information Security policies, standards, and procedures define additional responsibilities. All users are required to read, understand, and comply with those documents. Any questions should be directed to a system administrator or the business/functional manager, who will escalate to the Information Security as needed.

3. Responsibilities

- The sponsor of this policy is the Information Security team.
- The IT/Information Security team is responsible for the maintenance and accuracy of this policy.
- Any questions regarding this policy should be directed to the IT/Information Security.

4. Policy

4.1 Information Protection

- Sensitive and confidential Company information must never be sent over the Internet, including via email, unless it has first been encrypted using an approved method.
- Unless specifically known to be in the public domain, source code must always be encrypted before being sent over the Internet.
- Credit card numbers, authentication credentials, passwords, and other parameters that could be used to gain unauthorized access to goods, services, or systems must never be sent over the Internet or via email in readable (unencrypted) form.
- Trade secrets, copyrighted material, or proprietary/confidential information must not be transmitted or received via email unless digitally signed and encrypted.
- Confidential information, including legal or contractual agreements and technical information related to Company operations or security, must not be communicated via email unless digitally signed and encrypted.

4.2 Reporting Security Problems

Each user is responsible for notifying the IT/Information Security team immediately of any evidence of a security violation involving Internet or email connectivity, including:

- Unauthorized access to network, telecommunications, or computer systems.

- Apparent transmission of a virus, worm, or other malicious software via email or networking technologies.
- Apparent tampering with any file for which the user has established restrictive access controls.

4.3 Protection from Malicious Software

- Users must not run programs obtained from external or non-trusted sources (e.g. the web) without prior approval from the IT/Information Security team and a completed virus/malware check.
- Users must not download files directly onto a network server or production machine. Downloads should be directed to an isolated environment or removable storage media, scanned, and only then moved to a working directory. Any move to a production machine requires documented approval from the machine owner.
- All email attachments must be scanned for viruses and other malicious code before being opened or stored on any Company system, regardless of source or apparent content.
- Attachments from unknown or untrusted senders must not be opened.
- Users must not execute or install any program, upgrade, or patch received via email or downloaded from the Internet unless approved by the IT/Information Security team.

4.4 Acceptable Use of Email

- Email use is limited to business needs and must comply with this policy and the Company's Acceptable Use and Email Policies. Access to electronic messages must be limited to properly authorized personnel.
- Email must comply with Company standards on decency and appropriate content. Message content must not:
    - Contain material that is offensive, defamatory, or threatening to others.
    - Contain pornographic material, ethnic or racial slurs, or content that may be construed as harassing, offensive, or insulting on the basis of race, caste, religion, national origin, colour, marital status, age, disability, or any other characteristic protected under Indian law.
- Any statement made via email that could be construed as representing the Company must carry a disclaimer such as: "These statements are solely my own opinion and do not necessarily reflect the views of my employer." This does not exempt the sender from complying with all other conduct requirements.
- Email traceable to the Company network must be drafted with the Company's reputation in mind, with the same care as any other written communication bearing the Company name.
- The email system must not be used to produce or distribute chain mail, operate a personal business, or make solicitations for personal gain or for political, religious, or outside organizational causes.
- Users must not share their password(s) with any other person, and must use only their own official Company email account.
- Impersonation is not permitted. Users must identify themselves by their real name; forging of header information (source address, destination address, timestamps) is prohibited.
- Users must not publish or distribute internal mailing lists to individuals outside the Company.
- Users must not post network or server configuration information (e.g. internal addresses, server names, software versions) to public forums, newsgroups, or mailing lists.
- Users must not send unsolicited bulk email (spam), including commercial, religious, or political bulk messages. Malicious email, including "mail bombing," is prohibited.
- Distribution list emails must not include an active link to a website unless approved by the IT/Information Security team, and must contain contact information for recipients to raise questions.

4.5 Monitoring

Company email systems and the information they contain (including messages, attachments, and access logs) are Company property. This information may be monitored, searched, reviewed, disclosed, or intercepted by the Company, with or without notice, for a legitimate purpose, including to:

- Monitor system performance.
- Ensure compliance with Company policies.

- Prevent misuse of the system.
- Troubleshoot hardware and software problems.
- Comply with legal and regulatory requests for information.
- Investigate disclosure of confidential or proprietary information, or conduct that may be illegal or adversely affect the Company.

Such monitoring shall be reasonable, proportionate, and limited to 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. The Company may also access communications that have been deleted from its systems, where technically retrievable.

4.6 Email Security Settings and Attachments

- Employees, personnel, and third-party contractors must not modify security parameters within the Company email system. Unauthorized changes constitute a violation of this policy.
- Attachments should be limited in number and compressed using approved file-compression utilities before sending.
- Attachment size is subject to limits enforced by external gateways. Non-business-related email containing large attachments (e.g. graphics, multimedia files) must not be sent via the Company email system.

5. Roles and Responsibilities

- IT / Information Security Team: Maintains this policy, investigates reported violations, manages malware protection and email security configuration.
- All Personnel: Comply with this policy and report suspected violations or security incidents immediately.

6. Review

This policy shall be reviewed at least annually, or upon significant organizational, technological, or regulatory change, to ensure continued alignment with ISO/IEC 27001:2022 and applicable Indian law.