PDS INFOTECH PVT LTD

Email Security Policy
(Ref No: - ISMS/PDS/5.2/11)

Purpose-

The purpose of the policy is to minimize risk associated with Internet and e-mail services, and defines controls against the threats of unauthorized access, theft of information, theft of services, and malicious disruption of services.

Scope-

This policy applies to all users of information assets including **PDS INFOTECH PVT LTD** employees, employees of temporary employment agencies, vendors, business partners, and contractor personnel and functional units regardless of geographic location.

This Policy covers all Information Systems environments operated by **PDS INFOTECH PVT LTD**. The term "IS environment" defines the total environment and includes, but is not limited to, all documentation, physical and logical controls, personnel, software, and information.

Although this Policy explicitly covers the responsibilities of users, it does not cover the matter exclusively. Other **PDS INFOTECH PVT LTD** Information Security policies, standards, and procedures define additional responsibilities. All users are required to read, understand and comply with the other Information Security policies, standards, and procedures. If any user does not fully understand anything in these documents, he should consult with his systems administrator, business or functional manager, or human resources department, as applicable, who will contact the Information Security Department.

The Information Security Department shall resolve any conflicts arising from this Policy.

Responsibilities-

- The sponsor of this policy is the Information Security Officer.
- The Security department is responsible for maintenance and accuracy of the policy.
- Any questions regarding this policy should be directed to the Security Department.

Policy Statement-

The new resources, services, and interconnectivity available via the Internet all introduce new opportunities and new risks. In response to the risks, this policy describes 's official practices regarding Internet and Electronic Mail (Email) security.

Information Protection-

PDS INFOTECH's sensitive and confidential information must never be sent over the Internet unless it has first been encrypted by approved methods.

Unless specifically known to be in the public domain, source code must always be encrypted before being sent over the Internet.

Credit card numbers, telephone calling card numbers, log-in passwords, and other parameters that can be used to gain access to goods or services, must not be sent over the Internet in readable form.

Reporting Securities Problems-

Each user has the responsibility to notify the information security Department immediately of any evidence of any security violation involving internet connectivity with regard to:

- Unauthorized access to network, telecommunications, or computer systems;
- Apparent transmittal of a virus or worm via networking technologies; and
- Apparent tampering with any file for which the user established restrictive discretionary access controls.

Viruses and Malicious Software Protection

Users are not allowed to run programs obtained from external sources (via the WWW or other non-trusted source) without prior permission from Information Security Department and virus protection checks.

Users should never download files directly into a network server or production machine. Downloads should be directed to a separated (isolated) environment or removable storage media. Upon successful completion of the procedures described on the previous paragraph, users might move the downloaded files to their working directories. Moves to production machine (or equivalent) can only be performed with documented approval from Machine Owner.

Confidentiality-

No sensitive information must be transmitted over the Internet and the World-Wide Web (for example through Web based E-Mail systems) without first being encrypted.

Internet Networking Services

The following Policies will apply to Internet services:

File Transfer Protocol (FTP)

Only users that have a job or business need to use FTP will be authorized to use FTP.

No inbound FTP will be allowed under any circumstances from the Internet to the firewall or internal LAN

Outbound FTP will be allowed only via proxy accounts on the firewall system.

Users will not use FTP services to any remote host machine on which they do not have accounts. This does not apply to sites that offer or advertise an anonymous FTP service.

All files that are downloaded via FTP must undergo a virus check on a machine, which is not directly connected to the Internet or the internal network.

Telnet Services

- No inbound Telnet access from the Internet will be allowed.
- All outbound Telnet access will be from a proxy account on the firewall.
- All authorized Telnet sessions will be logged.
- Users will not Telnet into ports other than the standard Telnet port.
- Telnets into ports designated for mail, FTP or WWW or other Internet services are strictly forbidden.

General E-Mail Policy

PDS INFOTECH PVT LTD provides electronic information and communications systems to facilitate the companies' business needs and interests. These systems include individual computers, the computer network, electronic mail ("Email"), voice mail, and access to the Internet (collectively, the "Systems").

E-Mail Usage

The usage of the E-Mail system is subject to the following:

- E-Mail must be used in compliance with the Corporate Security Policy and associated Supplementary Information Security Policies. All access to electronic messages must be limited to properly authorized personnel.
- Usage of E-mail system is limited to business needs or any helpful messages.

All E-Mails must be in compliance with **PDS INFOTECH PVT LTD** standards regarding decency and appropriate content. Message content restrictions include: -

- **PDS INFOTECH PVT LTD** information resources should not be used to transmit or receive statements that contain any material that is offensive, defamatory, or threatening to others.
- The Systems should not be used to communicate statements, messages, or images consisting of pornographic material, ethnic slurs, racial epithets, or anything that may be

construed as harassing, offensive, or insulting to others based on race, religion, national origin, color, marital status, citizenship status, age, disability, or physical appearance.

- Any statements or comments made via E-Mail that could in any way be construed as an action of **PDS INFOTECH PVT LTD** must bear a disclaimer such as “These statements are solely my own opinion, and do not necessarily reflect the views of my employer.” Even with this disclaimer, all practices regarding decency and appropriate conduct still apply.

Any use of E-Mail from the network is easily traceable to. Personnel must conduct these activities with the reputation of in mind. Staff must exercise the same care in drafting E-Mail, as they would for any other written communication that bears **PDS INFOTECH PVT LTD** name.

ORACLE COMMUNICATIONSE-Mail systems should not be used to produce or distribute “chain mail,” operates a business, or makes solicitations for personal gain, political or religious causes, or outside organizations. Users must not forward or otherwise propagate, to individuals or groups, chain letters, pyramid schemes or any other types of data that may unnecessarily consume system resources or otherwise interfere with the work of others.

To maintain the security of **PDS INFOTECH PVT LTD** E-Mail system, it is important to control access to the system. Users should not provide other unauthorized persons with their E-Mail ID and personal password.

Users must use only their own **PDS INFOTECH PVT LTD** official E-Mail account and must not allow anyone else access to their account. Impersonation is not permitted. Users must identify themselves by their real name; pseudonyms that are not readily attributable to actual users must not be allowed. Users must not represent themselves as another user. Each user must take precautions to prevent unauthorized use of the E-Mail account. Forging of header information in E-Mail (including source address, destination address, and timestamps) is not permitted.

Users must not publish or distribute internal mailing lists to non- staff members.

PDS INFOTECH PVT LTD Systems should not be used to transmit or receive trade secrets, copyrighted materials, or proprietary or confidential information unless it is digitally signed and encrypted.

Any information regarded as confidential including legal or contractual agreements, technical information related to **PDS INFOTECH PVT LTD** operations or security etc. must not be communicated through E-Mail unless it is digitally signed and encrypted.

Users must not post network or server configuration information about any **PDS INFOTECH PVT LTD** machines to public newsgroups or mailing lists. This includes internal machine addresses, server names, server types, software version numbers, etc.

Attachments from unknown or untrusted sources must not be opened. All E-Mail attachments, regardless of the source or content, must be scanned for viruses and other destructive programs before being opened or stored on any **PDS INFOTECH PVT LTD** computer system. Personnel must perform a virus scan on all material that is transmitted to other users via E-Mail prior to sending it.

Users must not send unsolicited bulk mail messages (also known as “junk mail” or “spam”). This practice includes, but is not limited to, bulk mailing of commercial advertising and religious or political tracts. Malicious E-Mail, including but not limited to “mail bombing,” is prohibited.

Users must not execute or install any programs, upgrades or patches that are received via E-Mail or download from the Internet unless the Information Security Department approves it.

The Systems and all information contained in the systems (including computer files, E-Mail and voice mail messages, Internet access logs, etc.) are **PDS INFOTECH PVT LTD** property. At any time, with or without notice, this information may be monitored, searched, reviewed, disclosed, or intercepted by **PDS INFOTECH PVT LTD** for any legitimate purpose, including the following:

- To monitor performance
- Ensure compliance with **PDS INFOTECH PVT LTD** policies,
- Prevent misuse of the system
- Troubleshoot hardware and software problems,
- Comply with legal and regulatory requests for information, and
- Investigate disclosure of confidential business, proprietary information, or conduct that may be illegal or adversely affect **PDS INFOTECH PVT LTD** or its associates.

PDS INFOTECH PVT LTD may also gain access to communications deleted from the Systems.

All distributed lists Emails should not include an active link to an Internet website unless approved by Information Security Department.

All distributed Lists Emails must contain contact information for the receivers in case they want to ask questions or discuss any issues regarding the Email.

Email Security Settings-

PDS INFOTECH PVT LTD employees, personnel, or third party contractors using **PDS INFOTECH PVT LTD** facilities should not modify the security parameters within **PDS INFOTECH PVT LTD** E-Mail system. Users making unauthorized changes to the E-Mail security parameters are in violation of this policy.

PDS INFOTECH PVT LTD

E-Mail Attachments

All attachments to mails must be limited and compressed using file compression utilities, before sending them.

Attachments greater than 3MB are restricted by external gateways. Non-business related E-Mail containing large file attachments, such as graphics and multimedia files, should not be sent via PDS INFOTECHE-Mail systems.

Firewall Policy-

PDS INFOTECH PVT LTD Firewalls will be configured in accordance with **PDS INFOTECH PVT LTD** Firewall Configuration Standards and Procedures document. The following high-level policies must be complied with during configuration of **PDS INFOTECH PVT LTD** Internet firewalls:

- All non-essential networking or system services must be eliminated or removed from the firewall.
- The system logs generated from the firewall must be reviewed on a continuing basis to detect any unauthorized entry attempts.
- All unauthorized access through the firewall must be reported to the security manager and network administrator.
- Proxy accounts must be used on the firewall at all times.
- Networking traffic will be subject to filtering based on current security requirements.

World Wide Web Policy-

PDS INFOTECH PVT LTD World-Wide Web presence represents a growth opportunity, but also imposes some threats to system security. Distributed computing and client- server architecture requires World-Wide Web security to be applied at various levels of **PDS INFOTECH PVT LTD** systems and network resources. Security Administration of **PDS INFOTECH PVT LTD** Web Pages Responsibility for the security administration of **PDS INFOTECH PVT LTD** World-Wide Web presence will be borne by the e-Business. In cases where **PDS INFOTECH PVT LTD** LLP’s World-Wide Web (WWW) presence is hosted by a third party, the host site must adhere to the policies defined in this document as well.