

PDS INFOTECH PVT LTD

Remote Work Policy

Ref No: ISMS/PDS/5.2/20.1

1. Purpose

This policy establishes the rules and conditions under which short-term and long-term remote work may occur, in order to maintain acceptable practices regarding the use and protection of PDS Infotech Pvt Ltd's ("the Company") information resources.

2. Scope

This policy applies to any individual connecting remotely to the information resources of the Company.

3. Policy

3.1 General Requirements

- Personnel must be approved by their manager and IT prior to remote access or remote work. Working remotely without prior permission is not permitted under any circumstance.
- Personnel are responsible for complying with all Company policies when working using Company information resources and/or on Company time. Where requirements are unclear, personnel should seek assistance from IT.
- All inventions, intellectual property, and proprietary information developed on Company time and/or using Company information resources — including reports, drawings, software code, data, and technical documentation — remain the property of the Company.
- The remote worker is responsible for ensuring that non-employees do not access Company data, whether in print or electronic form.
- Remote personnel must maintain a regular schedule, with all working hours recorded in accordance with standard Company policy. Overtime and time off must be approved in advance.
- Equipment and information must be protected according to their classification, in alignment with the Information Classification and Management Policy. Remote workers are responsible for protecting Company equipment and information from theft, damage, or loss while in transit or at the remote work location. Documents or Company equipment must never be left unattended in a public area.

3.2 Internet Connection

- Personnel must not connect to an unsecured Wi-Fi network using Company equipment or to perform Company work. Wi-Fi connections must be secured with strong encryption (WPA2 or higher).
- When connecting via Wi-Fi, personnel must use only the Company's pre-approved VPN solution.
- Users must not connect to another wireless network and the Company wireless network simultaneously.
- For long-term home office arrangements:
 - A high-speed Internet connection is required, with sufficient bandwidth to perform regular job functions. IT will determine whether the individual's network is adequately secure or whether a Company-issued wireless router is required.
 - Wireless networks must be secured with a strong password/passkey.
 - Where possible, the home network used for Company information resources should be isolated from other devices in the home.

3.3 Equipment

- Only Company-provided computing devices (e.g. desktops, laptops) may be used for remote work.
- Computing devices must be secured with Company-provided or approved active, up-to-date antivirus software; an active local firewall; full-disk encryption; and automatic screen lock.
- Personnel are responsible for regularly rebooting their device to allow software patches and updates to install.
- Personally owned devices — including USB drives, portable hard drives, mobile phones, and similar devices — must not be connected to Company equipment, including via wireless connection.
- Maintenance of Company-provided equipment must be performed or pre-approved by IT.

3.4 Printing

- Printing of non-public Company information must be pre-approved by the relevant information owner.
- Personnel must be pre-approved by IT and their manager to print at a remote location.
- All non-public information must be secured when not in use and shredded when no longer needed, in accordance with the Information Classification and Management Policy.
- Printing of Company Confidential or Client Confidential information at a remote location is not permitted.

3.5 Telephone

- Remote personnel must use the Company-provided phone or headset for Company-related calls.
- Where other people are present in the remote work location, a headset must be used to safeguard the conversation.

3.6 Office Requirements

- Remote workspaces must be secured to protect Company equipment and maintain the confidentiality of Company and customer information.
- Personnel must permit IT to inspect and/or retrieve Company-provided equipment and information, maintained at a remote location, with reasonable advance notice and at a mutually agreed time, except when there is a security emergency which requires more immediate action.

4. Roles and Responsibilities

- IT: Approves remote access requests, configures and secures remote equipment, and coordinates equipment inspection.
- Managers: Approve remote work arrangements and monitor working hours / overtime for their direct reports.
- Remote Personnel: Comply with this policy and protect Company equipment and information at the remote location.

5. 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.