PDS INFOTECH PVT LTD

Remote Work Policy (Ref No: - ISMS/PDS/5.2/20)

Purpose

The purpose of this policy is to establish the rules and conditions under which short and long-term telecommuting may occur in order to maintain acceptable practices regarding the use and protection of (PDS INFOTECH PVT LTD) **Information Resources**.

Audience

The (PDS INFOTECH PVT LTD) Remote Work Policy (Ref No: - ISMS/PDS/5.2/20) applies to any individual connecting remotely to (PDS INFOTECH PVT LTD) information resources.

Policy

General Requirements

- Personnel must be approved by their manager and IT prior to remote access or teleworking. Under no circumstance is a person permitted to work remotely without prior permission.
- Personnel are responsible for complying with (PDS INFOTECH PVT LTD) policies when working using (PDS INFOTECH PVT LTD) **Information Resources** and/or on (PDS INFOTECH PVT LTD) time. If requirements or responsibilities are unclear, please seek assistance from the Security Committee. (duplicate from AUP)
- All inventions, intellectual property, and proprietary information, including reports, drawings, blueprints, software codes, computer programs, data, writings, and technical information, developed on (PDS INFOTECH PVT LTD) time and/or using (PDS INFOTECH PVT LTD) **Information Resources** are the property of (PDS INFOTECH PVT LTD). (duplicate from AUP)
- The teleworker is responsible to ensure that non-employees do not access (PDS INFOTECH PVT LTD) data, including in print or electronic form.
- The team member will be required to maintain a regular schedule. All hours of work must be recorded according to regular (PDS INFOTECH PVT LTD) policies. Overtime and time off must have advance approval according to the regular policies of (PDS INFOTECH PVT LTD).
- Equipment and information must be protected according to their classification and in alignment with the Information Classification and Management policy. Teleworkers are responsible for protecting (PDS INFOTECH PVT LTD) equipment and information from theft, damage, or other loss while in transit or at the remote work location. At no time should documents or PDS INFOTECH PVT LTD equipment be left unattended in a public area.
- Personnel are expected to follow (PDS INFOTECH PVT LTD)'s Incidental Use policy when using (PDS INFOTECH PVT LTD) devices remotely.

Internet Connection

- Personnel must not connect to an unsecured Wi-Fi network with (PDS INFOTECH PVT LTD) equipment or to perform (PDS INFOTECH PVT LTD) work.
- Wi-Fi connections must be secured with strong encryption (WPA2). The use of WPA or WAP is not allowed.
- When connecting to a Wi-Fi network, personnel must use only the pre-approved VPN solution.
- Users must not connect to another wireless network and the (PDS INFOTECH PVT LTD) wireless network simultaneously.
- The use of split-tunnel VPN is prohibited.
- For long-term or home office networks:
    - A high-speed Internet connection is required. Personnel will provide the Internet service at their own expense. The internet connection must be of sufficient bandwidth to allow the team member to efficiently perform their regular job functions.
    - IT will determine if the person's network is secure or whether a PDS INFOTECH PVT LTD issued wireless router will be needed OR teleworkers will comply with [Teleworking Procedures] for implementing wireless networks securely.
    - Wireless networks must be secured with a strong password, consisting of 16 or more characters.
    - When possible, the home network used with (PDS INFOTECH PVT LTD) Information Resources should be isolated from other devices and computers in the home.

Equipment

- Only (PDS INFOTECH PVT LTD) provided computing devices, such as desktops and laptops, may be used for working remotely.
- Computing devices must be secured with (PDS INFOTECH PVT LTD) provided or approved:
    - Active and up-to-date antivirus software
    - Active local firewall
    - Full-disk encryption
    - Automatic screen lock
- Personnel are responsible for regularly rebooting their device in order to allow software patches and updates to be installed.
- Personally owned devices, including but not limited to USB memory, portable hard drives, mobile phones, MP3 players, iPods/iPads, and smart gadgets, are not allowed to be connected to (PDS INFOTECH PVT LTD) equipment, including wireless connections.
- Maintenance of (PDS INFOTECH PVT LTD) provided equipment must be provided or preapproved by IT.

Printing

- The printing of any non-public (PDS INFOTECH PVT LTD) information must be preapproved by the Information Owner.
- The printing of any non-public (PDS INFOTECH PVT LTD) information to a public printer is prohibited.
- Personnel must be preapproved by IT Technology and their manager for printing at a remote location. Personnel approved to print must have (or be supplied with) a shredder.
    - IT will determine if the person's network is secure or whether a PDS INFOTECH PVT LTD issued wireless router will be needed.
    - The device used to print must be directly connected to the printer used. Wireless printing must be pre-approved by Information Technology and requires the use of strong encryption.
- All non-public (PDS INFOTECH PVT LTD) information must be secured when not in use and shredded when no longer needed in accordance with (PDS INFOTECH PVT LTD)'s Information Classification and Management policy.
- The printing of Confidential information at a remote location is not permitted.

Telephone

- Remote personnel must use the (PDS INFOTECH PVT LTD) provided phone or headset for all (PDS INFOTECH PVT LTD) related calls.
- When other people are present in the remote work location, a headset must be used to safeguard the conversation.

Office Requirements

- Workspaces must be secured to protect all (PDS INFOTECH PVT LTD) equipment and maintain the confidentiality of all information related to the organization and/or its customers.
- Personnel must allow IT to inspect and/or retrieve the equipment provided to them at any time.
- The (PDS INFOTECH PVT LTD) may inspect and/or retrieve any (PDS INFOTECH PVT LTD) information maintained at home by personnel.
- The use of personal video surveillance on home entrances and exits is encouraged.