PDS INFOTECH PVT LTD

Acceptable Use Policy

Ref No: ISMS/PDS/5.2/18.1

1. Purpose

This policy defines the acceptable use of PDS Infotech Pvt Ltd's ("the Company") information resources by employees, contractors, and other personnel. It sets out the standards of conduct expected in using Company systems, networks, devices, and data, in order to protect the confidentiality, integrity, and availability of information assets and to support compliance with the Information Technology Act, 2000, the Digital Personal Data Protection Act, 2023, and applicable CERT-In directions.

2. Scope

This policy applies to all employees, contractors, consultants, interns, and third parties who use, access, or manage the Company's information resources, whether on Company premises, remotely, or via personally owned devices used for Company business.

3. Policy

3.1 General Acceptable Use

- Personnel must comply with all Company policies when using Company information resources, whether during working hours or otherwise.
- Where requirements or responsibilities are unclear, personnel should seek clarification from the Information Security Committee.
- Personnel must promptly report harmful events or policy violations involving Company assets or information to their manager or the Incident Handling Team, including but not limited to:
    - Technology incident: any event that may cause failure, interruption, or loss of availability of a Company information resource.
    - Data incident: any potential loss, theft, or compromise of Company information.
    - Unauthorized access incident: any potential unauthorized access to a Company information resource.
    - Facility security incident: any damage to, or unauthorized access of, a Company-owned, leased, or managed facility.
    - Policy violation: any potential violation of this or other Company policies, standards, or procedures.
- Personnel must not knowingly engage in activity that:
    - Harasses, threatens, impersonates, or abuses others.
    - Degrades the performance of Company information resources.
    - Deprives authorized personnel of access to a Company information resource.
    - Obtains resources beyond those formally allocated.

    - Circumvents Company security measures.
- Personnel must not download, install, or run security programs or utilities that reveal or exploit system vulnerabilities (e.g. password-cracking tools, packet sniffers, port scanners) without prior written approval from IT.
- All inventions, intellectual property, and proprietary information developed during Company time and/or using Company information resources — including reports, drawings, software code, data, and technical documentation — are the property of the Company.
- Where encryption is used, it must be managed such that designated Company personnel can access the underlying data when required for legitimate business or compliance purposes.
- Company information resources are provided to conduct Company business and must not be used for personal financial gain.
- Personnel are expected to cooperate fully with internal investigations and any lawful investigation conducted by CERT-In, law enforcement, or other statutory or regulatory authority in India.
- Personnel must respect and comply with applicable intellectual property laws, including patents, copyrights, and trademarks, for any software or material accessed using Company information resources.
- Personnel must not intentionally access, create, store, or transmit material that the Company deems offensive, indecent, or obscene.

3.2 Access Management

- Access to information is granted strictly on a need-to-know basis.
- Personnel may use only the network and host addresses issued to them by IT and must not attempt to access data or programs on Company systems for which they lack explicit authorization.
- All remote access to internal Company networks or environments must be made through an approved, Company-provided Virtual Private Network (VPN).
- Personnel must not divulge access information to anyone not specifically authorized to receive it, including IT support personnel.
- Personnel must not share personal authentication information, including:
    - Account passwords.
    - Personal Identification Numbers (PINs).'
    - Fingerprint scanning.
    - Security tokens (e.g. smartcards).
    - Multi-factor authentication credentials.
    - Digital certificates.
    - Any similar information or device used for identification and authentication.
- Access cards and/or keys no longer required must be returned to physical security personnel.
- Lost or stolen access cards, security tokens, or keys must be reported to physical security personnel as soon as possible.
- A service charge may be levied for access cards, security tokens, or keys that are lost, stolen, or not returned.

3.3 Authentication and Passwords

- All personnel are required to maintain the confidentiality of their personal authentication information.
- Any group or shared authentication information must be maintained solely among the authorized members of that group.
- All passwords, including initial or temporary passwords, must be constructed and implemented in accordance with Company password rules:
    - Must meet minimum length, complexity, and reuse-history requirements.
    - Must not be easily linked to the account owner (e.g. username, Aadhaar/PAN number, nickname, relative's name, date of birth).
    - Must not be reused from any personal or non-business account.
- Unique passwords must be used for each system, wherever technically possible.
- User account passwords must never be divulged to anyone. Company support personnel and contractors will never ask for account passwords.
- If the security of a password is in doubt, it must be changed immediately.
- Personnel must not circumvent password entry using application-remembered credentials, embedded scripts, or hard-coded passwords in client software.
- Security tokens (e.g. smartcards), where issued, must be returned on demand or upon termination of the relationship with the Company.

3.4 Clear Desk / Clear Screen

- Personnel must log off from applications or network services when no longer needed.
- Personnel must lock or log off workstations and laptops when their workspace is unattended.
- Confidential or internal information must be stored in a locked drawer or cabinet when the workstation is unattended and at the end of the workday, where physical access to the workspace cannot otherwise be secured.
- Personal items such as phones, wallets, and keys should be placed in a locked drawer or cabinet when the workstation is unattended.
- File cabinets containing confidential information must be locked when not in use or unattended.
- Physical or electronic keys used to access confidential information must not be left on an unattended or unsecured desk.
- Laptops must be secured with a locking cable or stored in a locked drawer/cabinet when the work area is unattended, unless the device is fully encrypted.
- Passwords must never be posted on, under, or near a computer or in any other physically accessible location.
- Documents containing confidential information must be removed promptly from printers and fax machines.

3.5 Data Security

- Personnel must use approved, encrypted communication methods when sending confidential information over public networks (including the Internet).
- Confidential information transmitted via India Post or a courier service must be secured in compliance with the Company's Information Classification and Management Policy.

- Only Company-authorized cloud applications may be used for sharing, storing, or transferring confidential or internal information.
- Information must be shared, handled, transferred, retained, and destroyed appropriately, based on its sensitivity classification.
- Personnel must not hold confidential conversations in public places, open offices, or over insecure communication channels.
- Confidential information must be transported only by a Company employee or an IT Management-approved courier.
- All electronic media containing confidential information must be securely disposed of; contact IT for guidance.

3.6 Email and Electronic Communication

- Auto-forwarding of electronic messages outside the Company's internal systems is prohibited.
- Electronic communications must not misrepresent the sender's identity or the Company.
- Personnel are responsible for the accounts assigned to them and for all actions taken using those accounts.
- Accounts must not be shared without prior authorization from IT, other than for calendar and related scheduling functions.
- Personnel must not use personal email accounts to send or receive Company confidential information.
- Personal use of Company-provided email must not:
    - Involve solicitation.
    - Be associated with any political party, candidate, or campaign.
    - Risk harm to the Company's reputation.
    - Forward chain emails.
    - Contain or promote anti-social or unethical behaviour.
    - Violate applicable Indian laws or regulations.
    - Result in unauthorized disclosure of Company confidential information.
    - Otherwise violate any other Company policy.
- Confidential information must only be sent using approved, secure electronic messaging solutions.
- Personnel must exercise caution when responding to, clicking links within, or opening attachments in electronic communications.
- Personnel must use discretion when disclosing confidential or internal information (e.g. employment data, internal phone numbers, location) in Out of Office or other automated responses.

3.7 Hardware and Software

- All hardware must be formally approved by IT Management before connection to Company networks.
- Software installed on Company equipment must be approved by IT Management and installed by Company IT personnel.
- All Company assets taken off-site must be physically secured at all times.

- Personnel travelling to high-risk or sanctioned jurisdictions — as advised by Ministry of External Affairs (India) travel advisories or Company Security Guidelines — must contact IT for approval before travelling with corporate assets.
- Employees must not allow family members or other non-employees to access Company information resources.

3.8 Internet Usage

- The Internet must not be used to communicate Company confidential or internal information unless confidentiality and integrity are ensured and the recipient's identity is established.
- Use of the Internet via Company networking or computing resources must be limited to business-related activities. Unapproved activities include, but are not limited to:
  - Recreational games.
  - Streaming media.
  - Personal social media use.
  - Accessing or distributing pornographic or sexually explicit material.
  - Attempting or making unauthorized entry to any network or computer accessible from the Internet.
  - Otherwise violating any other Company policy.
- Internet access from outside Company premises using a Company-owned computer must adhere to the same policies that apply within Company facilities.

3.9 Mobile Devices and Bring Your Own Device (BYOD)

- Use of a personally owned mobile device to connect to the Company network is a privilege granted only upon formal approval by IT Management.
- All personally owned laptops or workstations connecting to Company resources must run approved antivirus/anti-spyware software with an active personal firewall.
- Mobile devices used to access Company email must have a PIN or other authentication mechanism enabled.
- Confidential information may only be stored on devices encrypted in compliance with the Company's Encryption Standard.
- Company confidential information must not be stored on any personally owned mobile device.
- Theft or loss of any mobile device used to create, store, or access confidential or internal information must be reported to the Company Security Team immediately.
- All mobile devices must maintain up-to-date software and applications.
- All personnel are expected to use mobile devices in an ethical manner.
- Jailbroken or rooted devices must not be used to connect to Company information resources.
- IT Management may execute a remote wipe of a mobile device without prior warning, in accordance with the Mobile Device Acknowledgement.
- Where a suspected incident or breach is associated with a mobile device, the device may be removed from the personnel's possession as part of a formal investigation.
- Mobile device usage related to Company information resources may be monitored at the discretion of IT Management.

- Company IT support for personally owned mobile devices is limited to assistance in complying with this policy and does not extend to general device troubleshooting.
- Use of personally owned devices must comply with all other Company policies.
- The Company reserves the right to revoke personally owned device privileges where personnel fail to abide by this policy.
- Texting or emailing while driving on Company time or using Company resources is not permitted; only hands-free calling is permitted while driving.

3.10 Physical Security

- Photographic, video, audio, or other recording equipment, including devices with built-in cameras, must not be used in secure areas.
- Personnel must display their photo ID access card at all times while in the building.
- Personnel must badge in and out of access-controlled areas. Piggybacking, tailgating, door-propping, and similar circumvention of access controls are prohibited.
- Visitors accessing card-controlled areas must be accompanied by authorized personnel at all times.
- Eating or drinking is not permitted in data centres, and caution must be exercised near workstations or information-processing facilities.

3.11 Privacy and Monitoring

- Information created, sent, received, or stored on Company information resources is not private and may be accessed by Company IT personnel at any time, under the direction of executive management or Human Resources, without prior notice to the user or resource owner.
- Any such access or monitoring shall be reasonable, proportionate, and limited to a legitimate business, security, or legal purpose, consistent with the Digital Personal Data Protection Act, 2023 and its Rules. By acknowledging this policy, personnel are notified of this monitoring in advance.
- The Company may log, review, and otherwise utilize any information stored on or passing through its information resource systems.
- System administrators, IT personnel, and other authorized personnel may hold privileges beyond those granted to standard users. Personnel with such extended privileges must not access files or information beyond what is specifically required for an employment-related task.

3.12 Removable Media

- Use of removable media to store Company information must be supported by a reasonable business case.
- All removable media use must be approved by IT prior to use.
- Personally owned removable media must not be used to store Company information.
- Personnel must not connect removable media of unknown origin without prior approval from IT.
- Confidential and internal Company information must not be stored on removable media without encryption.
- All removable media must be stored in a safe and secure environment.
- Loss or theft of removable media that may have contained Company information must be reported to IT immediately.

3.13 Security Training and Awareness

- All new personnel must complete approved security awareness training prior to, or within 30 days of, being granted access to Company information resources.
- All personnel must acknowledge that they have received, read, and agree to adhere to the Company's Information Security Policies before being granted access to Company information resources.
- All personnel must complete annual security awareness training.

3.14 Social Media

- Social media communications must comply with all applicable Company policies.
- Personnel are personally responsible for content they publish online.
- Creating a public social media account intended to represent the Company, or one that could reasonably be assumed to be an official Company account, requires prior permission from the Company's Communications function.
- When discussing the Company or Company-related matters, personnel should:
    - Identify themselves by name.
    - Identify themselves as a Company representative, where relevant.
    - Make clear they are speaking for themselves and not on behalf of the Company, unless explicitly approved to do so.
- Personnel must not misrepresent their role at the Company.
- When publishing Company-relevant content online in a personal capacity, personnel should include a disclaimer, e.g.: "The opinions and content are my own and do not necessarily represent the position of the Company."
- Content posted online must not violate applicable Indian laws, including those relating to copyright, fair use, and privacy.
- Discriminatory content (including on the basis of age, sex, race, caste, colour, creed, religion, ethnicity, sexual orientation, gender, gender expression, national origin, disability, marital status, or any other characteristic protected under Indian law) affiliated with the Company will not be tolerated.
- Confidential information, internal communications, and non-public financial or operational information must not be published online in any form.
- Personal information belonging to customers must not be published online.
- Personnel approved to post, review, or approve content on Company social media accounts must follow the Company's Social Media Management Procedures.

3.15 Voicemail

- Personnel must use discretion when disclosing confidential or internal information (e.g. employment data, internal phone numbers, location) in voicemail greetings.
- Personnel must not access another user's voicemail account unless explicitly authorized.
- Personnel must not disclose confidential information in voicemail messages.

3.16 Incidental Use

- As a convenience, incidental personal use of information resources is permitted, subject to the following restrictions:
  - Incidental personal use of electronic communications, Internet access, fax machines, printers, and copiers is restricted to authorized Company personnel and does not extend to family members or other acquaintances.
  - Incidental use must not result in direct cost to the Company.
  - Incidental use must not interfere with the normal performance of an employee's duties.
  - No files or documents may be sent or received that could give rise to legal action against, or embarrassment to, the Company or its customers.
- Storage of personal email messages, files, and documents within Company information resources must be kept to a minimum.
- All information located on Company information resources is owned by the Company and may be accessed in accordance with this policy, including in response to lawful requests from regulatory or law enforcement authorities.

4. Roles and Responsibilities

- Information Security Committee: Owns this policy, resolves ambiguities, and approves exceptions.
- IT Management: Implements and enforces technical controls (access, encryption, monitoring, device management) and approves hardware/software/removable media use.
- Incident Handling Team: Receives and investigates reported incidents and policy violations.
- Managers: Ensure their teams are aware of and comply with this policy.
- All Personnel: Comply with this policy, complete required training, and report suspected violations or incidents promptly.

5. 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, including the Information Technology Act, 2000, the Digital Personal Data Protection Act, 2023, and CERT-In directions.