PDS INFOTECH PVT LTD

Media Reuse and Destruction Standard

Ref No: ISMS/PDS/5.2/16.1

1. Overview

Technology equipment often contains components that cannot simply be discarded. Proper disposal is both environmentally responsible and often required by law. Hard drives, USB drives, optical media, and other storage devices contain Company and customer data, some of which is sensitive. To protect this data, all storage media must be properly erased before disposal, reuse, or resale. Simply deleting files or formatting a device is not sufficient: data marked for deletion remains recoverable until it is overwritten. Approved tools must be used to securely erase data prior to equipment disposal or reuse.

2. Purpose

This standard defines the requirements for the secure reuse and disposal of technology equipment and storage media owned by PDS Infotech Pvt Ltd ("the Company").

3. Scope

This standard applies to any computer, technology equipment, or peripheral device that is no longer needed within the Company, including but not limited to: personal computers, servers, hard drives, laptops, mobile/handheld devices, printers, scanners, optical and floppy discs, portable storage devices, backup tapes, and printed materials. All employees and affiliates of the Company must comply with this standard.

4. Standard

4.1 Technology Equipment Disposal

- When technology assets reach the end of their useful life, they must be sent to IT Management for proper disposal.
- IT Management is responsible for securely erasing all storage media in accordance with current industry best practice, prior to disposal, reuse, or resale.
- All data, including files and licensed software, must be removed from equipment using approved disk-sanitization software or hardware, consistent with Guidelines for Media Sanitization.
- No computer or technology equipment may be sold to any individual except through the process defined in Section 4.2.
- Computer equipment must not be disposed via general waste. Where electronic recycling bins are provided on Company premises, IT Management must ensure all data is securely removed from any device before it is placed for recycling or final disposal.
- Electronic drives must be securely wiped using an approved disk-cleaning method. Where a drive cannot be reliably sanitized, it must be physically destroyed.
- "Technology equipment" includes desktop, laptop, tablet, or notebook computers; printers; copiers; monitors; servers; handheld devices; phones; disk drives or other storage devices; network switches, routers, and wireless access points; and backup tapes.
- IT Management must record, for each disposed or reused item, the date sanitization was performed and the technician responsible, whether via a physical label on the equipment or a logged entry in the asset inventory.

- Where a storage device has non-functioning memory or storage that cannot be sanitized through standard means, the memory/storage component must be removed and physically destroyed.

4.2 Employee Purchase of Disposed Equipment

- Working equipment that has reached the end of its useful life to the Company may be made available for purchase by employees, once fully sanitized in accordance with Section 4.1.
- Where demand exceeds availability, a fair allocation method will be used to determine purchase opportunity. Employees may not purchase or reserve their own previously assigned equipment directly, ensuring equal opportunity for all employees.
- Finance and IT Management will determine an appropriate sale price for each item.
- All such sales are final; no warranty or support is provided with equipment sold under this process.
- Equipment not in working order, or remaining after the allocation process, will be donated or disposed of in accordance with applicable environmental regulations, using organizations the Company has approved for this purpose.
- All equipment must be removed from the IT asset inventory system before it leaves Company premises.

5. Policy Compliance

5.1 Compliance Measurement

Compliance with this standard will be verified through methods including, but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to this standard must be approved in advance by IT.

5.3 Non-Compliance

An employee found to have violated this standard may be subject to disciplinary action, up to and including termination of employment.

6. Review

This standard 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, including the Digital Personal Data Protection Act, 2023.