# Neon Vinimay Private Limited

## ELECTRONIC STORAGE MEDIA DISPOSAL POLICY

Circular: - Ref. SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018

| | |
|---|---|
| Policy created by | Designated Officer |
| Policy reviewed by | Technology Committee |
| Policy reviewed on | 31/12/2023 |
| Policy Approved by | Board of Directors |
| Policy approved on | 04/01/2024 |

## Version – 1.2

# Purpose

The purpose of this policy is to define standards for proper data sanitization and/or disposal of electronic storage media that has (or may have) contained personal information at the Company's end and to emphasize the importance of protecting sensitive information and complying with legal and regulatory requirements during the disposal of electronic storage media.

# General/Definitions

- **Electronic Storage Media** – Any electronic device that can be used to store data. This includes but is not limited to internal and external hard drives, CDs, DVDs, Floppy Disks, USB drives, ZIP disks, magnetic tapes and SD cards.

- **Personal information** – An individual's first name and last name or first initial and last name in combination with one or more of the following data elements: social security number, driver's license number or state-identification card number, or financial account number, or credit or debit card number, with or without any required security code, access code, personally identifiable identification number or password, that would permit access to a resident's financial account.

- **Sensitive Information** – Data whose disclosure would not result in any business, financial or legal loss but involves issues of personally identifiable credibility, privacy or reputation. The security and protection of this data is dictated by a desire to maintain staff and student privacy.

- **Sanitizing Storage Media** –
  - ➢ Disposal is defined as the act of discarding media with no other sanitization considerations. Examples of Disposal include discarding paper in a recycling container, deleting electronic documents using standard file deletion methods and discarding electronic storage media in a standard trash receptacle.

  - ➢ Clearing is defined as a level of sanitization that renders media unreadable through normal means. Clearing is typically accomplished through an overwriting process that replaces actual data with 0's or random characters. Clearing prevents data from being recovered using standard disk and file recovery utilities.

  - ➢ Purging is defined as a more advanced level of sanitization that renders media unreadable even through an advanced laboratory process. In traditional thinking, Purging consists of using specialized utilities that repeatedly overwrite data; however, with advancements in electronic storage media, the definitions of Clearing and Purging are converging. For example, purging a hard drive manufactured after 2001 only requires a single overwrite. For the purpose of this Policy, Clearing and Purging will be considered the same. Degaussing is also an acceptable method of Purging electronic storage media

  - ➢ Destroying is defined as rendering media unusable. Destruction techniques include but are not limited to disintegration, incineration, pulverizing, shredding and melting. This is a common sanitization method for

single-write storage media such as a CD or DVD for which other sanitization methods would be ineffective. This is also a common practice when permanently discarding hard drives.

Data Wiping –

Identify the Media: Clearly identify the electronic storage media that needs to be wiped. Ensure that you are working with the correct device.

Backup Important Data: Before initiating the data wiping process, backup any important data if necessary. Ensure that critical information is securely stored elsewhere.

Disconnect from Network: Disconnect the electronic storage media from any network connections to prevent remote access during the wiping process.

Choose Wiping Method: Select an appropriate wiping method based on the type of storage media. Common methods include overwriting, cryptographic erasure, or using specialized software tools. Choose a method that complies with your organization's security policies.

Use Certified Software: If using software for data wiping, ensure that it is certified and recognized for secure data erasure.

Follow Software Instructions: If using a software tool, follow the step-by-step instructions provided by the software vendor. This may involve creating a bootable disk or USB drive, selecting the target storage media, and initiating the wiping process.

Verify Completion: After the wiping process is complete, use the software's verification features to ensure that all data has been successfully erased. Some tools provide a certificate or report confirming the completion of the process.

Physically Label or Tag: Physically label or tag the wiped media to indicate that it has undergone the data wiping process. This helps in tracking and inventory management.

Record Details: Maintain a record of the data wiping process, including the date, time, method used, and any relevant details. This documentation may be required for compliance purposes.

Secure Storage or Disposal: If the storage media will be reused, store it securely. If it will be disposed of, follow the organization's disposal procedures, ensuring that it is done securely and in compliance with environmental regulations.

Consider Cryptographic Erasure for SSDs: For SSDs, consider using cryptographic erasure methods that leverage the built-in encryption features of the device. This can be more effective than traditional overwriting methods.

### Organizational Scope

This policy applies to all personnel who have responsibility for the handling and proper disposal of electronic storage media at Company.

## Policy Content and Guidelines

- All electronic storage media should be sanitized (Cleared/Purged) prior to sale, donation, being moved to unsecured storage (for spare parts), or transfer of ownership. A transfer of ownership may include transitioning media to another individual or department at the Company or replacing media as part of a lease agreement.

- All electronic storage media must be destroyed when it has reached the end of its useful life and/or when other sanitizing methods are not effective (e.g. single-write media or media that is permanently write protected), provided that the destruction does not conflict with Company data retention policies or any regulatory requirements (e.g. electronic discovery).

Change in the Policy will be adopted as and when required by the company and is binding on all the Staff/Employees/and Directors of the Company.

Neon Vinimay Pvt Ltd

For NEON VINIMAY PVT. LTD.

Jatesh Jain          DIRECTOR

Designated Officer

Dated: -31/12/2023