Media Disposal Policy

Version 1 - Approved by Rishabh

Contents

1. Objective

Secure disposal of electronic and physical media adds a layer of protection to prevent critical data from being exposed to unauthorized individuals. This policy aims to mitigate the risk of unauthorized data recovery. It demonstrates to customers, Superhawk AI staff, and other partners that Superhawk AI protects their data even after it has fulfilled its purpose.

2. Scope

This policy applies to all company-issued devices and media that process, store, transmit, or provide access to Personal Identifiable Information (PII), business & operational data, or behavioral data. It specifically covers company-issued laptops and workstations, removable storage (USB drives, external HDD/SSD), and cloud-based export media that are being permanently decommissioned. Cloud-hosted data in AWS and GCP is subject to vendor-managed deletion and retention controls; for cloud exports or any locally stored copies on employee devices, this policy's disposal requirements apply. Personal devices are out of scope except where they contain company data, in which case the device owner must follow this policy before returning or repurposing the device.

3. Policy Statement

To securely dispose of company-issued laptops/workstations, the following steps can be followed:

- Encrypt the entire hard disk using a robust algorithm and a lengthy password.
- Securely delete all information by using software solutions.
- Physically destroy the device through methods such as incineration or shredding.
- It is recommended to use all three methods for extremely critical and sensitive data.
- For data with lower levels of criticality, one of these methods is sufficient.

4. Document Security Classification

Company Internal (please refer to the Data Classification policy for more details).

5. Non-Compliance

Compliance with this policy shall be verified through various methods, including, but not limited to, automated reporting, audits, and feedback to the policy owner. Any staff member found to be in violation of this policy may be subject to disciplinary action, which may include termination of employment or contractual agreement. The disciplinary action shall depend on the extent, intent, and repercussions of the specific violation.

6. Responsibilities

The Information Security Officer is responsible for approving and reviewing policy and related procedures. The IT Operations team (responsible for company asset inventory and decommissioning) must coordinate device collection, verify encryption status, perform secure

erasure using approved tools, and document disposal actions. For cloud resources in AWS and GCP, the Cloud Engineering team must confirm that vendor-managed deletion procedures were followed or securely delete any exported copies. Employees and contractors must return company-issued devices to IT upon separation and must not attempt to bypass disposal controls. Third-party disposal vendors used for physical destruction must be contracted and approved by Procurement and must provide a certificate of destruction.

7. Schedule

This document shall be reviewed at least annually and additionally after significant changes to infrastructure (e.g., adoption of new cloud providers), changes to data classification, or following any incident involving data exposure. Review responsibility lies with the Information Security Officer, with input from IT Operations, Cloud Engineering, and Legal.

End of Media Disposal Policy. For version history, please see the next page.

Version History

	Version	Log	Date
1	Current	Policy version approved by Rishabh	13 Mar, 2026
1		New policy version created	13 Mar, 2026