HARDWARE SANITIZATION & DISPOSAL POLICY

Version Number:	3.1
Version Date:	10/08/2025
Owned by:	Security, GRC
Approved by:	Nate Fitch, Sr. V.P., Chief of Staff
Confidentiality Level:	Internal

Table of Contents

1. Purpose

This policy establishes standardized, secure, and auditable procedures for the sanitization and destruction of electronic media and hardware used within Docker's environment. It ensures that residual data is irretrievably erased or destroyed prior to disposal, transfer, reuse, or decommissioning of devices to prevent data leakage, unauthorized access, and regulatory violations.

The policy enforces a tiered approach based on media type, risk level, and intended outcome (reuse vs. disposal), defining:

- Approved sanitization methods aligned with industry standards
- Mandatory documentation, logging, and verification requirements
- Physical storage requirements and vendor oversight procedures
- Dual approval processes and certificates of destruction where applicable

2. Scope

This policy applies broadly to any hardware or media used by Docker personnel—including full-time employees, contractors, vendors, and other third parties—if the device or medium has stored company-owned, managed, or processed data.

This includes, but is not limited to:

- Company-issued and leased laptops, desktops, smartphones, tablets, servers, printers, external drives, and networking devices
- Devices returned during offboarding, reassignment, or upgrade cycles
- Any system scheduled for decommissioning, donation, or transfer to a new environment

Regardless of whether the data stored is Confidential, Internal, or Public, all devices must undergo proper sanitization or destruction procedures before being removed from Docker’s operational control.

3. Roles and Responsibilities

Role	**Responsibilities**
IT Operations	Executes approved sanitization and destruction procedures; manages asset inventory updates; stores hardware securely prior to disposal or reuse.
Security Team	Defines approved sanitization methods, ensures compliance with NIST SP 800-88, and audits logs for completeness and effectiveness; investigates incidents.
People Operations (HR)	Coordinates with IT to collect hardware during offboarding and ensures devices are returned and logged for sanitization.
Data Owners	Ensure that sensitive or regulated data stored on assigned devices is properly backed up or removed prior to transfer or decommissioning.

Third-Party Vendors	Must comply with Docker's requirements, including providing valid Certificates of Destruction and maintaining a documented chain of custody.
Cloud Providers	Must provide written assurances and evidence that hardware-level data destruction is consistent with industry standards and certifications (e.g., ISO 27001, SOC 2).
All Employees and Contractors	Must return all company-owned devices when required and may not attempt to destroy or wipe data without IT or Security approval.

4. Definitions

- **Sanitization**: The irreversible process of removing or overwriting data from media to render it unrecoverable using forensic tools.
- **Destruction**: The physical act of rendering media unusable, such as shredding, incineration, or degaussing.
- **Electronic Media**: Any device or component capable of storing digital data, including hard drives, flash memory, mobile phones, and external storage devices.
- **Certificate of Destruction (CoD)**: A formal document issued by an approved vendor confirming that sanitization or destruction was completed in accordance with contractual and industry requirements.
- **Chain of Custody** - The documented, chronological record showing the seizure, custody, control, transfer, analysis, and disposition of physical media or devices, ensuring accountability and preventing tampering throughout the sanitization or destruction process.
- **Mobile Device Management (MDM)** - Enterprise software that enables centralized administration of mobile devices and laptops, including the ability to remotely wipe data, enforce security policies, and track device inventory across the organization.
- **Overwriting** - A data sanitization method that replaces existing data on storage media with non-sensitive data patterns multiple times, making the original data unrecoverable through standard or advanced recovery techniques.
- **Forensic Tools** - Specialized software or hardware designed to recover deleted, hidden, or overwritten data from storage media, used as the benchmark for verifying that sanitization methods render data truly unrecoverable.

5. Sanitization Before Transfer or Disposal

All devices and media must undergo secure data sanitization prior to being reused, transferred, donated, or destroyed. Sanitization must comply with industry standards, and all actions must be logged in Docker's Asset Inventory System, including:

- Device serial number and asset tag
- Responsible user or team
- Date of sanitization or destruction
- Method used (e.g., cryptographic wipe, degaussing)
- Confirmation of outcome (sanitized, destroyed, or pending)
- Applied label (e.g., "Sanitized – Ready for Reuse" or "Destroyed – Do Not Reuse")

6. Authorized Sanitization Methods

Method	Description
Overwriting	A software-based method that performs one or more passes of data overwriting to make previous data unrecoverable.
Degaussing	Uses magnetic fields to disrupt storage media, rendering traditional hard drives unreadable.
Cryptographic Erasure	Involves destroying encryption keys used to protect stored data, effectively rendering encrypted data irretrievable.
Physical Destruction	Mandatory for SSDs, optical media, or failed drives. Includes shredding, incineration, or industrial crushing of hardware components.

7. MDM-Based Remote Erasure (for Laptops and Mobile Devices)

Remote wipes must be executed using Docker-approved Mobile Device Management (MDM) tools, with evidence retained for at least 12 months. Control requirements include:

Platform	Tool	Controls
macOS	Jamf	Role-based wipe permissions and remote wipe logging
Windows	Intune	Wipe logs archived for at least 12 months
Linux	NinjaOne	Manual wipes require dual approval and logging in ticketing system

8. Secure Storage Prior to Sanitization

Devices awaiting wipe or pickup for destruction must be stored in a physically secured location, such as:

- A locked IT storage cabinet, server room, or secure offboarding zone
- Locations with badge-based access control and video surveillance
- Logged in a pre-sanitization queue and regularly reviewed by IT or Security

No unsanitized hardware may be left unattended in general office spaces or unsecured storage.

9. Third-Party Destruction

If destruction is performed by a vendor, the following criteria must be met:

- Vendor must have a signed Data Processing Agreement (DPA) or Master Services Agreement (MSA)
- Must provide:
  - A Certificate of Destruction (CoD)
  - A Chain of Custody document
  - Written affirmation of ISO 27001 or equivalent certification
- Vendor performance and compliance are subject to annual reviews by the Security or Compliance team
- Docker may conduct spot audits or request site documentation on demand

10. Cloud Provider Assurance

Docker may rely on cloud service providers (CSPs) for hardware-level sanitization and destruction only when the following conditions are met:

- CSP provides written confirmation (e.g., AWS Data Sanitization Whitepaper or similar)
- CSP maintains active ISO 27001, SOC 2, or FedRAMP certification
- CSP's policies and controls are reviewed during vendor onboarding or contract renewal

Documentation confirming these assurances must be retained by the Security team or Vendor Management group.

11. Enforcement and Exceptions

All Docker personnel are expected to comply with this policy in full. Failure to adhere may result in disciplinary action, up to and including termination of employment or contract. In cases involving willful misconduct, malicious activity, or violations of law, Docker may initiate legal proceedings. The organization reserves the right to monitor, audit, and inspect user activity on its systems to ensure compliance.

Any exceptions to this policy must be formally requested, documented, and approved by Docker's GRC or Legal team. Exception requests must clearly outline the business justification and associated risks, and should be submitted to Docker's Risk Submission Portal.

12. Change History

Date	Version	Responsible Party	Description of Change
10/08/2025	3.1	Nate Fitch, Sr. V.P., Chief of Staff	Revised policy approved
09/29/2025	3.0	Chad Fryer, Sr. Security Engineer, GRC	Policy annual review and update

12/04/2024	2.1	Jeff Strauss, Director of IT Operations	Revised policy approved
07/21/2024	2.0	Rachel Taylor, Director, Security, Risk & Trust	Policy annual review and update
01/4/2023	1.2	Todd Smith, VP of Information Technology	Policy Approved
01/4/2023	1.1	Rachel Taylor, Senior Manager, Information Security, Risk & Trust	Draft Submitted for review
12/19/2022	1.0	Rachel Taylor, Senior Manager, Information Security, Risk & Trust	Basic document outline