ASSET MANAGEMENT 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 a structured framework for managing physical and virtual assets throughout their lifecycle—from acquisition and provisioning through active use to secure decommissioning and disposal. It ensures all information assets are properly inventoried, classified by sensitivity, and assigned to responsible owners for ongoing oversight.

The policy defines:

- Standardized procedures for inventory management, classification, transfer, and decommissioning
- Requirements for maintaining a centralized, real-time asset inventory
- Ownership accountability to prevent orphaned systems and untracked devices
- Controls to eliminate shadow IT and ensure all systems are subject to appropriate governance
- Integration with access control, data classification, and acceptable use policies

This framework mitigates asset-related risks, enables rapid incident response, supports audits, and ensures compliance with ISO/IEC 27001, SOC 2, and contractual obligations. By maintaining comprehensive asset visibility and control, Docker protects its data, operations, and technology infrastructure while meeting regulatory and security framework requirements.

2. Scope

This policy applies to all employees, contractors, and third-parties with access to Docker assets covering all production Docker-owned, leased, or managed information assets including:

- Physical devices
- Cloud infrastructure
- T1 and T2 third-party services
- Intellectual property

3. Roles and Responsibilities

Role	Responsibilities
Security Team	Defines asset management standards, ensures that controls are applied to high-risk assets, and supports audit and compliance validation.
IT Team	Manages the asset inventory system, performs asset tagging, tracks physical and virtual asset changes, and enforces processes for acquisition, transfer, and disposal. Coordinate asset issuance and collection during employee onboarding and offboarding processes. Track asset return as part of termination workflows.
Engineering Teams	Assign and maintain accurate ownership metadata for virtual/cloud assets, including application tags and usage designations. Ensure alignment with tagging standards.
Procurement and	Maintain purchasing records and disposal documentation, reconcile

Finance	procurement data with inventory records, and track asset value for financial reporting.
Department Managers	Ensure assets assigned to their team are properly accounted for, returned when no longer needed, and reassigned or decommissioned as appropriate.
All Users	Use assigned assets responsibly, report asset loss, damage, or theft promptly, and comply with asset security requirements, including physical handling and access controls.

4. Definitions

Information Asset - Any physical or virtual resource that processes, stores, or transmits Docker data, including hardware devices, cloud infrastructure, software applications, and storage services.

Shadow IT - The use of technology solutions, applications, or services that have not been approved by IT or subjected to security review and governance controls.

Orphaned Systems - Assets that lack designated ownership or have owners who are no longer with the organization, creating security and compliance risks.

Asset Lifecycle - The complete process from initial acquisition or provisioning of an asset through active use, transfers, and ultimately secure decommissioning and disposal.

Virtual Assets - Non-physical technology resources including cloud infrastructure, virtual machines, SaaS applications, containers, and storage services.

5. Asset Inventory Requirements

5.1 Asset Identification

All information assets must be recorded in Docker’s asset inventory systems related to their type of asset.

5.2 Ownership

Every asset must have a designated owner who is responsible for its security, appropriate use, and accurate tracking. Ownership must be updated whenever the asset is transferred, reassigned, or decommissioned. Ownership data is used for access reviews and audit purposes.

5.3 Physical Assets

Physical assets are required to be tracked if they are company-owned or leased, store or access company data.

For tracked physical assets, the following information must be included:

- Serial number
- Assigned user or department
- Purchase date, location, and asset value
- MDM status, where required

5.4 Virtual Assets

Virtual assets—including cloud infrastructure, virtual machines, T1 and T2 third-party services, and storage services—must be inventoried similarly.

6. Asset Transfers and Return

- Transfers between users must be tracked with updated owner assignment.
- All assets must be returned upon employee termination or contract end.
- Asset return is documented as part of the off-boarding checklist.

7. Asset Disposal and Destruction

- Devices storing sensitive or restricted data must be securely wiped or physically destroyed.
- Decommissioned cloud resources must be deleted or locked per retention requirements.
- IT must maintain destruction logs or certificates from approved third-party providers.

8. 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.

9. 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
09/25/2025	3.0	Chad Fryer, Sr. Security Engineer, GRC	Policy annual review and update
06/17/2024	2.2	Jeff Strauss, Director of IT Operations	Revisions Approved

06/13/2024	2.1	Tim Baur, VP Engineering, Platform	Revisions Approved
04/20/2023	2.0	Karen Hajioannou, Senior Security & Compliance Engineer Rachel Taylor, Director, Security, Risk & Trust	Policy annual review and update
2/6/2023	1.3	Todd Smith, VP of IT	Draft document approved
2/6/2023	1.2	Jean-Laurent de Morlhon, SVP of Engineering	Draft document approved
1/3/2023	1.1	Rachel Taylor, Senior Manager, Security, Risk & Trust	Draft submitted for review
12/19/2022	1.0	Rachel Taylor	Basic document outline