DATA CLASSIFICATION 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 3
2. Scope 3
3. Roles and Responsibilities 3
4. Definitions 4
5. Classification Levels 5
6. Classification Requirements and Controls 5
    6.1 Assignment 5
    6.2 Labeling 6
    6.3 Enforcement 6
7. Integration with Other Policies 6
8. Enforcement and Exceptions 6
9. Change History 7
Appendix A: Classification-to-Control Matrix 8

1. Purpose

This policy establishes a standardized framework for classifying Docker's information assets based on their sensitivity, value, and associated risk. By categorizing data according to its potential impact if breached or misused, the organization ensures proportional security controls are applied throughout the data lifecycle, from creation through disposal.

The classification framework enables:

- Data labeling with defined protections, access restrictions, and handling rules for each level
- Effective enforcement of access controls and encryption practices
- Appropriate incident response based on data sensitivity
- Compliance with regulatory and contractual obligations such as SOC 2, ISO 27001, and GDPR
- Efficient data use while minimizing risk from over-exposure or under-classification

This continuous process includes periodic reclassification as business needs or legal obligations evolve. It ensures all Docker personnel understand their responsibilities in identifying and handling information appropriately according to its classification, maintaining customer trust and operational integrity.

2. Scope

This policy applies to all individuals with access to Docker-owned or Docker-managed information assets, including employees, contractors, interns, and third parties. It governs all information assets created, collected, processed, received, transmitted, or stored on behalf of Docker, regardless of the format or storage location.

Covered data formats include, but are not limited to, structured data such as databases, unstructured data such as documents and emails, information stored in cloud environments or backups, printed materials, visual captures like screenshots, and verbal communications that involve sensitive or proprietary information.

The policy is applicable across all operational environments, production, staging, development, and test, and spans both physical infrastructure and cloud-based resources managed or integrated into Docker's business operations.

3. Roles and Responsibilities

Role	**Responsibilities**
Data Owner	Assigns appropriate classification to new data assets and ensures reclassification when necessary based on use, risk, or policy triggers.
Security/GRC Team	Defines classification policy, enforces security controls by classification, and reviews compliance with classification enforcement during audits.

IT and Infrastructure Teams	Implements and enforces technical access controls (e.g., RBAC, encryption) based on classification in systems and storage platforms.
Legal Team	Ensures that data classification aligns with legal, regulatory, and contractual requirements.
Engineering and Product Teams	Integrate classification tagging and data protection into application development, especially for PII and customer-facing systems.
All Users	Understand and apply classification labels when creating, accessing, or sharing data; report suspected misclassification or misuse.

4. Definitions

Information Asset - Any data or information in any format (digital, physical, or verbal) that is created, collected, processed, transmitted, or stored by or on behalf of Docker, having business value or sensitivity requirements.

Data Owner - The individual or role accountable for determining the appropriate classification of data, authorizing access, ensuring proper handling throughout its lifecycle, and approving any reclassification decisions.

Data Lifecycle - The complete span of data existence from initial creation or collection through active use, archival, and ultimately secure destruction, during which classification and protection requirements must be continuously maintained.

PII (Personally Identifiable Information) - Any data that can be used to identify a specific individual, either alone or when combined with other information, including but not limited to names, identification numbers, location data, or online identifiers.

5. Classification Levels

Docker uses the following four-tiered classification model. All information must be classified upon creation, and labeling must reflect the most sensitive data contained within.

Level	Definition	Examples	Impacts of Unauthorized Disclosure
Restricted	Information of the highest sensitivity. Protected by law, regulation, or contract. Access must be limited to the smallest number of	Customer PII (e.g., SSNs, IDs), passwords, encryption keys, medical records, payment card	Severe legal and regulatory consequences, contractual breach, reputational damage,

	individuals with a specific business need.	information, customer authentication data, legal holds	operational disruption
Confidential	Sensitive business or technical data not publicly disclosed. Access is limited to employees or contractors with a legitimate role-based need.	Financial data, HR records, employee PII, source code, Merger and Acquisition documents, compensation data, board communications	Competitive harm, contractual violation, loss of customer or stakeholder trust
Internal Use Only	General business data intended for internal distribution. Does not contain sensitive personal or regulated content, but not appropriate for external sharing.	Organization charts, meeting notes, training guides, intranet content	Mild operational disruption or policy violation
Public	Data approved for public consumption. May be published on Docker websites, social channels, or customer documentation.	Marketing materials, blog posts, public job postings, product documentation	No harm anticipated from disclosure

6. Classification Requirements and Controls

6.1 Assignment

- All data must be classified at the time of creation, ingestion, or acquisition.
- The creator or assigned Data Owner is responsible for determining the data classification.

6.2 Labeling

Data must be labeled in accordance with its assigned classification level. Labeling mechanisms may include metadata fields, document headers/footers, system-level tagging, or file naming conventions. Accurate labeling supports consistent enforcement of retention, access control, and encryption requirements.

6.3 Enforcement

- Restricted, Confidential and Internal Use Only data must be accessed through:
  - Role-Based Access Control (RBAC) and group membership
  - Multi-Factor Authentication (MFA)
  - Endpoint protection and monitoring
- Data retention, archival, and destruction schedules must align with classification as defined in the Data Handling Policy.

7. Integration with Other Policies

This policy establishes the classification structure only. Implementation details for handling data based on its classification are governed by companion policies:

- Data Handling Policy – Defines encryption, storage, transmission, retention, and destruction practices per classification
- Access Control Policy – Details permission models and access provisioning by classification level
- Information Security Policy – Broad security and organizational controls for systems managing classified data
- Incident Response Plan – Defines procedures for reporting, investigating, and mitigating data leaks or unauthorized access incidents

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
09/19/2025	3.0	Stephen Oriowo, Sr GRC Analyst Chad Fryer, Sr. Security Engineer, GRC	Policy annual review and update
06/12/2024	2.1	Joel Benavides, Head of Legal	Legal Approval
05/20/2024	2.0	Karen Hajioannou, Senior Security & Compliance Engineer; Rachel Taylor, Director, Security, Risk & Trust	Policy annual review and update

02/6/2023	1.2	Joel Benavides, Head of Legal	Draft document approved
08/29/2022	1.1	Rachel Taylor, Senior Manager, Security, Risk & Trust	Draft Submitted for review
08/29/2022	1.0	Rachel Taylor, Senior Manager, Security, Risk & Trust	Basic document outline

See Appendix A below

Appendix A: Classification-to-Control Matrix

Classification Level	Access Control	Storage Requirements	Transmission Requirements	Logging & Monitoring	Sharing Restrictions	Minimum Retention	Portability Requirements	Examples
Restricted	Strict need-to-know, Role-based, MFA, Least privilege, data owner approval	Encrypted at rest (AES-256), centralized access logging	Encrypted in transit (TLS 1.2+, VPN, IPsec)	Mandatory logging + SIEM alerts	Internal only; external only with NDA + legal review	**Docker Data:** 7 years except for corporate records and litigation records which are not subject to deletion. **Customer Data:** Duration of agreement + 3 years Secure deletion (crypto-shred, DOD wipe); log disposal	Encrypted export, verified chain of custody	Customer PII, Payment card information, legal privileged communication, bank account numbers
Confidential	Strict need-to-know, Role-based, MFA, Least privilege, data owner approval	Encrypted at rest (AES-256), centralized access logging	Encrypted in transit (TLS 1.2+, VPN, IPsec)	Mandatory logging + SIEM alerts	Internal only; external only with NDA + legal review	**Financial Data:** 7 years **Employee Data:** Duration of employment + 3 years **Docker Email:** 6 months **Docker Messaging (Slack):** 6 months **Other Docker Data:** 3 years Secure deletion	Encrypted export, verified chain of custody	Employee records, customer lists, financial data, incident reports

						(crypto-shred, DOD wipe); log disposal		
Internal Use Only / Sensitive	RBAC, internal-only access	Default cloud encryption, access-controlled folders or S3 buckets	TLS 1.2+ preferred; unencrypted email discouraged	Logging required, alerts for sensitive access	Internal teams; external w/ approval	**Vendor Data:** Duration of agreement + 1 year **Logs:** 1 year **Other Data Types:** The information owner is responsible for retention based on business requirements. Logical delete + audit log record, Standard retention	Standard secure export	Dashboards, product specs, employee surveys
Public / Non-Sensitive	No restrictions	Public or open-source repositories allowed	Open web protocols (HTTP, FTP, etc.) allowed	Optional logging	Freely shareable	Standard delete procedures acceptable, No retention requirements	Simple export acceptable	Job postings, blog content, open-source tools