DATA HANDLING 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 consistent, secure, and privacy conscious standards for handling customer, employee, and other sensitive or regulated Docker data throughout its lifecycle, from creation through destruction. It ensures Docker complies with legal, regulatory, contractual, security, and privacy obligations while minimizing risks of data loss, unauthorized access, and reputational damage.

This policy mandates:

- Data handling practices tailored to sensitivity levels defined in Docker's Data Classification Policy
- Technical controls and procedural safeguards including access restrictions, secure transmission, encryption, retention schedules, and secure disposal
- Specific protections for data handled by third-parties or partners with contractual assurances
- Centralized governance with role-specific accountability
- Application of security and privacy principles including data minimization, purpose limitation, transparency, confidentiality, integrity, and availability

This framework ensures data is handled ethically, securely and in compliance with privacy obligations across all formats (structured databases, documents, emails, backups, printed materials) and environments (production, staging, development, corporate networks), whether managed internally or through third-party platforms.

2. Scope

This policy applies to all Docker employees, contractors, vendors, and other authorized parties who handle Docker customer data or internal Docker data as part of their role. It governs the secure handling of all data formats, both physical and digital, across the organization. This includes structured data like databases, unstructured content such as documents and emails, as well as printed materials, and verbal communication.

The policy extends to all systems, services, and environments under Docker's control, including production, staging, development, and corporate networks. It covers data throughout its entire lifecycle, regardless of location or medium,and applies to both internally managed systems and third-party platforms used by Docker.

3. Roles and Responsibilities

Roles	**Responsibilities**
Data Owner	Determines the classification, retention, and access controls for specific data types; coordinates reclassification or data lifecycle decisions.
Security Team	Defines technical control requirements, monitors access and data

	transfer risks, and responds to data security incidents.
IT / Infrastructure Team	Implements and maintains secure storage, encryption, and backup mechanisms; supports secure deletion and access enforcement.
Engineering Teams	Integrate secure data handling into applications and infrastructure; follow approved protocols for storage, transmission, and disposal.
All Employees and Contractors	Handle data in accordance with its classification; use approved tools and report any data handling violations or concerns.

4. Definitions

Data Lifecycle - The complete progression of data through distinct phases: creation or collection, active use, storage, archival, and secure destruction, during which appropriate handling controls must be continuously maintained.

Least Privilege - The security principle of granting users only the minimum access rights necessary to perform their specific job functions, with all other access denied by default.

Data Processing Agreement (DPA) - A legally binding contract between Docker and third-party service providers that defines obligations for secure handling, processing, storage, and deletion of Docker data in compliance with privacy regulations and security standards.

Data Portability - The ability to export data in a structured, commonly used, machine-readable format that enables transfer between systems or providers while maintaining data integrity and completeness.

5. Data Access

Data access must be governed by the principle of least privilege:

- Only individuals with a job-based need may access customer or internal sensitive data.
- Where access to customer data has been authorized, use of such data shall be limited to the purpose required to perform specified job functions.
- Access changes due to role updates, departures, or project transitions must be reported to IT immediately.

6. Data Handling and Transfer

- Sensitive or regulated data must only be transferred to authorized recipients using secure, encrypted protocols such as HTTPS, TLS 1.2+, or SFTP.
- Screen locks, secure file-sharing platforms, and endpoint protection must be used to prevent unauthorized viewing or interception during handling.
- Data must never be copied or moved to unapproved devices or personal cloud storage platforms.

7. Storage of Sensitive Data

Sensitive data must be stored in secure, Docker-approved platforms and infrastructure that meet the following requirements:

- Approved Environments: All sensitive data must be stored in Docker-managed or approved cloud environments such as AWS, GCP, or Azure.
- Encryption: Data at rest must be encrypted using AES-256 or stronger encryption algorithms.
- Access Controls: Systems must enforce role-based access restrictions and apply the principle of least privilege.
- Patching and Hardening: Storage systems must be regularly patched and follow Docker's hardening baselines.
- Backups: Sensitive data must be backed up securely, with backups encrypted, access-controlled, and regularly tested for integrity and recoverability.

8. Data Retention

- Retention periods must be determined based on applicable legal, regulatory, and contractual obligations.
- Data Owners are responsible for defining and reviewing retention schedules for their data assets.
- Retention timelines must be reviewed at least annually.
- Refer to *Appendix A* below for data retention requirements for each data classification.

9. Third-Party Handling

Third parties who handle Docker data must meet strict security requirements:

- Third-parties must complete a security assessment prior to onboarding and be re-evaluated periodically.
- Third-parties must sign a MSA outlining security expectations and data protection terms.
- Contracts must require third-parties to adhere to Docker's security standards and applicable policies.
- Third-party access to data must be limited to the minimum necessary for contract performance.

9.1 Cloud Service Provider Specific Requirements

Cloud providers must additionally:

- Notify Docker of any government data requests
- Confirm data deletion upon request
- Support data export in industry-standard formats
- Maintain SOC 2 Type II or any industry equivalent certifications
- Allow annual third-party security assessments

10. Data Portability and Return

10.1 Portability Requirements

Upon authorized request, Docker must provide personal data in:

- Structured, commonly used, machine-readable format
- Secure transfer method with encryption
- Complete dataset including all provided and generated data

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
09/12/2025	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 - added data labeling procedures
02/6/2023	1.2	Joel Benavides, Head of Legal	Draft document approved
01/12/2023	1.1	Rachel Taylor, Senior Manager, Security, Risk & Trust, Amn	Draft Submitted for review

		Rahman, Senior Manager, Data Engineering	
12/19/2022	1.0	Rachel Taylor, Senior Manager, Security Risk & Trust	Basic document outline

See Appendices Below

Appendix A: Data Handling 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

Appendix B: Secure Transmission Standards

Data Sensitivity	Minimum Protocols	Authentication	Additional Controls	Notes
Restricted	TLS 1.2 or TLS 1.3 HTTPS SFTP / SCP IPsec VPN	Mutual TLS or token-based (e.g., OAuth 2.0, signed JWT)	Packet inspection logging Certificate pinning (if applicable) Disable weak ciphers (e.g., RC4, 3DES)	No plaintext transmission; disable fallback to older SSL/TLS versions
Confidential	TLS 1.2 or TLS 1.3 HTTPS SFTP / SCP IPsec VPN	Mutual TLS or token-based (e.g., OAuth 2.0, signed JWT)	Packet inspection logging Certificate pinning (if applicable) Disable weak ciphers (e.g., RC4, 3DES)	No plaintext transmission; disable fallback to older SSL/TLS versions
Internal Use Only / Sensitive	TLS 1.2+ SSH (for CLI-based access) Internal APIs over HTTPS	Basic auth (internal only), token-based, API keys	IP allowlisting Rate limiting Service-to-service auth (e.g., mTLS or SPIFFE)	Transmission via email should use S/MIME or be limited to approved domains
Public / Non-Sensitive	Any (HTTP, FTP, etc.)	None required	Optional digital signatures (for integrity)	Examples include press kits, open data, OSS tools