ACCEPTABLE USE POLICY

Version Number:	4.1
Version Date:	10/09/2025
Owned by:	Security, GRC
Approved by:	Nate Fitch, Sr. V.P., Chief of Staff
Confidentiality Level:	Internal

Table of Contents

1. Purpose

This Acceptable Use Policy establishes guidelines for the appropriate, secure, and lawful use of Docker's information systems and technology assets. It defines expectations for accessing corporate devices, cloud platforms, communication systems, and collaboration tools while protecting the confidentiality, integrity, and availability of Docker's information assets.

The policy mandates:

- Use of resources for authorized business purposes only
- Compliance with legal, contractual, and regulatory obligations
- Protection of credentials and proper data handling practices
- Prohibition of unauthorized data sharing, accessing prohibited content, and shadow IT usage
- Ethical conduct that avoids reputational, legal, or cybersecurity risks

This framework supports compliance with ISO/IEC 27001, and SOC 2 Trust Services Criteria. Compliance is mandatory and monitored, with violations resulting in disciplinary action including access revocation, termination, or legal consequences based on severity.

2. Scope

This policy applies to all Docker employees, contractors, consultants, temporary staff, and third-party users who access, manage, or utilize Docker's information systems, networks, or data—whether on-site or remotely. It also applies to all devices, software, and services provided by or connected to Docker’s digital environment, including personally owned devices authorized under BYOD programs.

3. Roles and Responsibilities

Role	**Responsibilities**
Security Team	Defines acceptable use requirements and investigates AUP violations.
IT Team	Enforces technical restrictions (e.g., web filtering, device controls) and supports incident response.
Department Managers	Communicate AUP expectations and ensure team compliance.
HR/People Operations	Supports disciplinary processes for AUP violations and communicates policy during onboarding.
All Users	Follow acceptable use guidelines, use company resources ethically, and report misuse.

4. Definitions

Shadow IT - Unauthorized use of cloud services, applications, or technology solutions that bypass IT approval and security review processes.

BYOD (Bring Your Own Device) - The practice of using personally owned devices to access Docker systems and data under approved security controls.

Data Processing Agreement (DPA) - A legally binding contract between Docker and third-party services that defines how personal data will be processed, protected, and managed in compliance with privacy regulations.

EDR (Endpoint Detection and Response) - Security software that monitors and protects devices from threats and must not be disabled or tampered with.

Clear Screen Policy - The requirement to lock or log out of systems when leaving a workstation unattended to prevent unauthorized access.

5. Acceptable Use Guidelines

Users must:

- Use Docker-provided or authorized devices and services only for legitimate business activities.
- Conduct all business communications using company-approved platforms such as Docker email, Slack, and GitHub.
- Access only systems and data necessary for their job functions, following the principle of least privilege.
- Use approved channels for purchasing, data transfers, or third-party services.
- Report any observed or suspected security vulnerabilities to the security team at **security@docker.com**.
- Only use Docker-approved cloud services that have undergone privacy and security assessment.
- Ensure personal data is processed only for authorized business purposes with appropriate legal basis.
- Respect data minimization principles by accessing only the minimum Restricted or Confidential data necessary.
- Be aware of data location when using cloud services and comply with cross-border transfer restrictions.
- Honor data subject rights and direct any requests to **privacy@docker.com**.

6. Prohibited Activities

The following activities are explicitly forbidden:

- Employees are prohibited from downloading Docker Confidential Information to any non-Docker systems, including personal email, or storage accounts.
- Accessing or transmitting content that is illegal, offensive, obscene, or discriminatory.
- Using peer-to-peer (P2P) software, torrenting tools, or unapproved file-sharing applications.
- Running unauthorized software, including games, non-corporate issued VPN clients, or backup utilities is prohibited.
- Bypassing security mechanisms, including disabling EDR or removing MDM agents.
- Using Docker resources for unauthorized commercial ventures, cryptocurrency mining, or personal financial gain.
- Forwarding business emails to personal accounts without explicit, documented approval.

- Processing Restricted or Confidential data without a documented lawful basis or outside approved purposes.
- Uploading Restricted or Confidential data to unapproved cloud services or personal cloud accounts.
- Creating unauthorized copies of customer data for testing or development without proper anonymization.
- Working remotely, or taking Docker-owned equipment to restricted countries as defined in our OFAC, SDN, ITAR Compliance Policy is strictly prohibited.
- Transferring customer data outside approved geographic regions without Legal approval.
- Using cloud services that lack appropriate data processing agreements or privacy certifications.
- Circumventing privacy controls, consent mechanisms, or data retention policies.

7. Account and Authentication Responsibilities

- Users must not share their passwords or access credentials with anyone.
- Sessions must be terminated or locked when a user is away from their device.

8. Personal Devices (BYOD)

- Use of personally owned devices for business purposes is permitted in the following ways:
    - Smartphones and iOS/iPadOS/Android tablets can be used for e-mail, calendaring, Slack and paging without being a company-managed device.
    - All other devices must be company managed. Personal devices can be brought as long software and operating systems are managed by Docker IT.
    - All devices are cleared of company information and software on termination.
- Only authorized users may connect personal devices to Docker networks or systems.

9. Data Protection and Confidentiality

- Users must handle all data in accordance with Docker’s Data Handling Policy.
- Restricted and Confidential data must not be stored on unencrypted devices or shared without authorization.
- Employees must not post or transmit internal documents, code, or confidential business information outside authorized platforms.

10. Removable Media Use

- Use of USB drives, external hard disks, and similar media is prohibited unless specifically approved.
- Data classified as Restricted or Confidential must not be stored on removable devices without prior written authorization.

11. Use of Artificial Intelligence (AI) Tools

- Non-approved AI tools may not be used to process or store any data that originated from Docker as the controller or processor.
- All AI vendors must undergo security and compliance review before use.

- AI-generated content must be verified, edited, and made Docker-specific before internal or external use.

12. Monitoring and Privacy

- All use of Docker systems and data is subject to monitoring.
- Monitoring may include web activity, email traffic, file access, and device telemetry.
- Users have no expectation of privacy when using Docker-owned or managed systems.
- Data collected through monitoring may be used for security investigations, compliance audits, or legal inquiries.
- Monitoring activities are conducted in compliance with employee privacy rights and applicable laws.
- Personal data collected through monitoring is subject to retention limits and access restrictions.
- Users will be notified of monitoring activities to the extent required by local regulations.

13. 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.

14. Change History

Date	**Version**	**Responsible Party**	**Description of Change**
10/09/2025	4.1	Nate Fitch, Sr. V.P., Chief of Staff	Revised policy approved
09/23/2025	4.0	Chad Fryer, Sr. Security Engineer, GRC	Policy annual review and update
06/12/2024	3.1	Joel Benavides, Head of Legal	Legal Approval
04/20/2024	3.0	Rachel Taylor, Director, Security, Risk & Trust Karen Hajioannou, Senior Security & Compliance Engineer	Policy annual review and update
9/22/2023	2.1	Joel Benavides, Head of Legal	Legal Approval

9/12/2023	2.0	Rachel Taylor, Senior Manager, Security, Risk & Trust	Update for AI technologies
2/6/2023	1.2	Joel Benavides, Head of Legal	Legal Approval
1/3/2023	1.1	Rachel Taylor, Senior Manager, Security, Risk & Trust	Draft Submitted for review
12/19/2022	1.0	Rachel Taylor, Senior Manager, Security, Risk & Trust	Basic document outline