INFORMATION SECURITY POLICY

Version Number:	3.1
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. Roles and Responsibilities

Effective operation of Docker's ISMS depends on well-defined responsibilities that span organizational levels and technical functions. The following roles are critical to maintaining the system's integrity and ensuring policy compliance:

Role	**Responsibilities**
Executive Leadership	Sets the tone for information security across the organization, approves ISMS strategy and resource allocation, and ensures alignment with business goals.
Chief Information Security Officer (ISMS Lead)	Oversees the development, implementation, and maintenance of the ISMS. Leads risk management activities, facilitates audits, and ensures alignment with ISO and SOC 2 frameworks.
Policy Owners	Maintain and enforce domain-specific security policies such as access control, asset management, and incident response. Ensure documentation remains current and relevant.
ISMS Committee	Reviews ISMS performance annually, tracks security objectives and metrics, and supports risk treatment planning across teams.
Legal and Compliance	Supports regulatory alignment, ensures privacy and security clauses in contracts, reviews policy exceptions, and maintains audit readiness.
Security Engineering	Designs and implements security controls and tooling, supports detection and response operations, and enforces technical safeguards.
All Employees and Contractors	Are responsible for following security policies, completing mandatory training, reporting incidents, and contributing to a secure work environment.

2. Policy Inventory Register

Policy Title	Owner	Version	Last Reviewed	Review Frequency
Acceptable Use Policy	Chief Information Security Officer	4.1	Oct 2025	Annual
Access Control Policy	Chief Information Security Officer	3.1	Oct 2025	Annual
Asset Management Policy	Chief Information Security Officer	3.1	Oct 2025	Annual
Audit Log Policy	Chief Information Security Officer	3.1	Oct 2025	Annual
Backup Management Policy	Chief Information Security Officer	3.1	Oct 2025	Annual
Change Management Policy	Chief Information Security Officer	3.1	Oct 2025	Annual
Cloud Network Security Policy	Chief Information Security Officer	3.1	Oct 2025	Annual
Cryptography Policy	Chief Information Security Officer	3.1	Oct 2025	Annual
Data Classification Policy	Chief Information Security Officer	3.1	Oct 2025	Annual
Data Handling Policy	Chief Information Security Officer	3.1	Oct 2025	Annual
Hardware Sanitization Policy	Chief Information Security Officer	3.1	Oct 2025	Annual
OFAC, SDN & ITAR Compliance Policy	Head of Legal	3.1	Oct 2025	Annual
Risk Management Policy	Chief Information Security Officer	1.0	Oct 2025	Annual
Secure Software Development Life Cycle Policy	Chief Information Security Officer	3.1	Oct 2025	Annual

Security Awareness Training Policy	Chief Information Security Officer	3.1	Oct 2025	Annual
Third Party Risk Management Policy	Chief Information Security Officer	3.1	Oct 2025	Annual
Vulnerability Management Policy	Chief Information Security Officer	2.1	Oct 2025	Annual

3. 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.

4. Change History

Date	Version	Responsible Party	Description of Change
10/09/2025	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
07/22/2024	2.1	Justin Cormack, Chief Technology Officer	Policy approved
06/13/2024	2.0	Rachel Taylor, Director, Security, Risk & Trust	Policy annual review and update
02/27/2023	1.2	Todd Smith, VP of Information Technology	Draft document approved
01/12/2023	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