AUDIT LOG 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. Log Generation 4
6. Collection and Centralization 4
7. Log Review and Monitoring 5
8. Retention and Protection 5
9. Access Control and Segregation of Duties 5
10. Use in Audits and Investigations 5
11. Segregation of Duties 6
12. Enforcement and Exceptions 6
13. Change History 6

1. Purpose

This policy defines standards and requirements for the generation, collection, review, retention, and protection of audit logs across Docker's technology environment. Audit logs provide immutable records of user and system activity, enabling the organization to detect and investigate suspicious behavior, reconstruct events during security incidents, enforce accountability, and demonstrate operational control to external auditors.

The policy mandates:

- Standardized, secure, and consistent log generation across all relevant systems
- Centralized log collection and storage to ensure accessibility, integrity, and resilience
- Protection of logs from unauthorized access or tampering
- Monitoring and alerting mechanisms to identify potential threats
- Clear roles and responsibilities for log generation, management, and review

This framework supports early detection of misuse or compromise, rapid incident response, and compliance with ISO/IEC 27001, as well as SOC 2 Trust Services Criteria control objectives.

2. Scope

This policy applies to all audit and event logs generated by Docker-managed assets across both corporate and production environments. It includes systems owned, operated, or administered by Docker employees, contractors, or service providers on behalf of Docker. The policy governs audit logging at all layers of the technology stack, from infrastructure to applications, specifically covering tier 1 and tier 2 applications and systems.

3. Roles and Responsibilities

Role	**Responsibilities**
Security Team	Configure log sources, define alert rules, monitor SIEM, investigate suspicious activity.
IT Team	Ensure that infrastructure supports log forwarding, retention, and encryption standards.
Engineering Teams	Implement logging in applications and services, ensure critical events are logged.
Compliance Team	Review logging procedures during audits, verify log coverage and retention against policy.

4. Definitions

Audit Log - An immutable record of user and system activity that captures security-relevant events including who, what, when, where, and how actions were performed on Docker systems.

SIEM (Security Information and Event Management) - A centralized platform that collects, normalizes, stores, and analyzes log data from multiple sources to enable security monitoring, alerting, and incident investigation.

Immutable Format - A storage method that prevents modification or deletion of log data once written, ensuring the integrity and reliability of audit records for forensic and compliance purposes.

Chain-of-Custody - The documented process of handling and transferring log data used as evidence, maintaining its integrity and admissibility for investigations or legal proceedings.

Segregation of Duties - The security principle requiring that no single individual has the ability to generate, modify, delete, and review their own activity logs without oversight, preventing conflicts of interest and unauthorized tampering.

5. Log Generation

All in-scope systems and services must be configured to generate audit logs that capture key security-relevant events. At a minimum, logs must include:

Type of Log Event	**Description**
Access	Access and authentication activity related to critical Docker assets will be logged.
Changes	Changes to critical configurations attempted and successfully committed to critical Docker assets will be logged.
Service Interruptions	Critical Docker assets will be monitored for service interruptions and system health.
Security Tooling	Relevant alerts generated from security tooling will be logged.
Cloud Service Native Logs	Logs from Cloud Infrastructure hosting services will be logged.

6. Collection and Centralization

To ensure visibility and long-term accessibility, all logs must be:

- Forwarded to Docker’s centralized Security Information and Event Management (SIEM) platform
- Transmitted securely using encrypted protocols such as TLS 1.2 or higher

- Normalized into a consistent format to facilitate parsing, correlation, and enrichment for security analytics

Where feasible, collection should be automated to reduce gaps in coverage and support real-time monitoring.

7. Log Review and Monitoring

Logs must be actively reviewed and monitored by the Security team to detect anomalies and support continuous threat detection.

8. Retention and Protection

Audit logs are critical records and must be retained according to defined retention schedules:

- Minimum retention period: 12 months for all logs

To protect the integrity and confidentiality of logs:

- Access to logs generated must be strictly controlled and monitored

9. Access Control and Segregation of Duties

To preserve integrity and avoid conflicts of interest:

- Access to logs generated must be restricted to authorized personnel with a documented business need
- Individuals who generate logs (e.g., developers, system admins) may not review or modify logs related to their own actions unless under supervision

10. Use in Audits and Investigations

Audit logs must be made available to support:

- Internal and external security audits (e.g., ISO 27001, SOC 2, customer assessments)
- Investigations related to potential breaches, policy violations, or security incidents
- Testing and validation of internal control effectiveness

Access to logs for audit or investigation purposes must be formally requested and approved by the Security team. Chain-of-custody must be maintained for logs used as evidence in investigations.

11. Segregation of Duties

To minimize the risk of log manipulation and maintain accountability:

- No individual may simultaneously have the ability to generate, alter, delete, and review logs pertaining to their own activities without documented oversight and controls

12. 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.

13. 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
06/5/2024	2.1	Justin Cormack, Chief Technology Officer	Revisions Approved
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	Todd Smith, VP of Information Technology	Draft document approved
01/3/2023	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