BACKUP 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 ensures Docker's critical data is securely backed up and can be recovered in a timely and reliable manner following accidental deletion, system failure, cyberattack, or other business disruptions. It establishes standards for data backup, retention, restoration, testing, and validation to maintain business continuity and protect customer trust.

The policy mandates:

- Automated, verifiable backups that are securely encrypted and isolated from production environments
- Stricter backup frequency, restore time, and retention requirements for critical/sensitive systems
- Regular recovery testing to confirm readiness for outages, data corruption, or ransomware events
- Audit trails and compliance validation with escalation for any recovery or retention objective failures
- Equivalent backup capabilities from third-party vendors handling Docker data

This framework supports Docker's compliance with ISO/IEC 27001and SOC 2 Trust Services Criteria for availability, confidentiality, and processing integrity.

2. Scope

This policy applies to all systems and services that store or process data owned, managed, or controlled by Docker, whether hosted on-premises, in the cloud, or by approved third-party providers. Specifically, it includes:

- Production environments and customer-facing systems (e.g., hosted databases, managed services)
- Internal business applications containing sensitive employee, customer, or financial data
- Configuration files, deployment artifacts, and Infrastructure-as-Code (IaC) repositories
- SaaS platforms where Docker-owned data is exported or processed
- Third-party platforms where Docker data resides and backup responsibility is defined contractually

3. Roles and Responsibilities

Role	**Responsibilities**
Data Owner	Identifies critical systems and assigns data classifications that guide backup schedules and retention.
IT Operations	Configures, maintains, and monitors backup jobs, tools, and infrastructure.
Security Team	Validates encryption and isolation controls, monitors alerting, and reviews backup testing outcomes.
Compliance Team	Reviews audit logs, ensures backup processes meet regulatory expectations, and assesses vendor capabilities.

4. Definitions

Recovery Time Objective (RTO) - The maximum acceptable time between a system failure and restoration of service, measured from the point of disruption to full operational recovery.

Recovery Point Objective (RPO) - The maximum acceptable amount of data loss measured in time, representing the point to which data must be recovered after an outage.

Incremental Backup - A backup method that captures only data changes since the last backup, reducing storage requirements and backup time while requiring the full backup chain for restoration.

Full Backup - A complete copy of all data in a system at a specific point in time, providing a standalone restore point independent of other backups.

WORM (Write Once Read Many) - An immutable storage technology that prevents modification or deletion of data once written, providing protection against ransomware and ensuring backup integrity.

5. Production Backup and Frequency

Production Databases – Daily incremental and weekly full backups with 7-day retention

Backup frequency and retention must be regularly reviewed and adjusted based on business impact and compliance requirements.

6. Recovery Objectives

- Recovery Time Objective (RTO)**:** Maximum acceptable time to restore service
  - Production: 24 hours
  - Non-production: 72 hours
- Recovery Point Objective (RPO)**:** Maximum acceptable data loss measured in time
  - Production: 4 hours
  - Non-production: 24 hours

These objectives must guide backup scheduling, technology selection, and architecture design.

7. Backup Control Requirements

7.1 Backup Job Requirements

- All backups must be automated and scheduled using enterprise-grade solutions (e.g., AWS Backup, GCP Snapshots).
- Alerting mechanisms must notify responsible teams of job failures or data integrity errors in real time.

7.2 Encryption and Isolation

- All backups must be encrypted using AES-256 at rest and transmitted using TLS 1.2 or higher.

- Backup repositories must be logically isolated from production networks and accessible only by designated personnel.
- Where supported, immutable or WORM (Write Once Read Many) storage must be used for production system backups.

Backups that include personal or sensitive customer data must also comply with Docker's Data Protection and Handling Policies.

8. Backup Testing and Validation

- Frequency**:** Annual testing for all production systems and internal systems.
- Methods**:** Include full database restores, application restoration, and time-to-recover measurement.
- Documentation**:** Results must include test dates, systems tested, success/failure, and RTO achievement.

Failures or gaps discovered during testing must be remediated promptly, with escalation to Security and Compliance.

10. Monitoring and Metrics

- Alerts related to backup job failures or anomalies must be sent immediately to both IT and Security teams.
- Monthly metrics must include:
    - Backup success and failure rates
    - Incidents involving missed RTOs or failed recoveries
    - Backup coverage compared to systems in scope
    - Open issues or deviations from the policy

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
9/29/2025	3.0	Chad Fryer, Sr. Security Engineer, GRC	Policy annual review and update
7/23/2024	2.3	Tim Baur, VP of Engineering, Platform	Revisions Approved
7/23/2024	2.2	Jeff Strauss, Director of IT	Revisions Reviewed
6/5/2024 & 6/13/2024	2.1	Brett Inman, Senior Manager, Engineering, Platform and Rob Braden, Manager, Infrastructure	Policy reviewed
5/20/2024	2.0	Karen Hajioannou, Senior Security & Compliance Engineer Rachel Taylor, Director, Security Risk & Trust	Policy annual review and update
2/23/2023	1.3	Todd Smith, VP of IT	Draft document approved
2/22/2023	1.2	Jean-Laurent de Morlhon, SVP of Engineering	Draft document approved
1/3/2023	1.1	Rachel Taylor, Senior Manager, Security, Risk & Trust	Policy Reviewed by Brett Inman, Jeffrey Strauss
12/19/2022	1.0	Rachel Taylor, Senior Manager, Security, Risk & Trust	Policy Drafted