ACCESS CONTROL 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. Purpose

This policy establishes a unified framework for managing user and system access to Docker's information systems, applications, data, and infrastructure. It ensures access control based on the principles of least privilege and explicit authorization, with access denied by default and granted only when required for job duties.

The policy mandates:

- Formal, auditable provisioning through documented requests, managerial approval, and authorized implementation
- Regular access reviews and adjustments based on employment status, job responsibilities, or organizational changes
- Prompt revocation of unnecessary access and deactivation of unused accounts
- Centralized identity and access management (IAM) with automated provisioning and integrated workflows
- Comprehensive monitoring, logging, and periodic audits to detect anomalies and ensure compliance

This framework protects sensitive data, maintains system integrity, supports regulatory compliance, and prevents unauthorized access or internal misuse. It serves as the foundation for Docker's security program and is supported by detailed procedures governing identity management, password practices, and system-specific controls.

2. Scope

This policy applies to all individuals who interact with Docker-managed systems, services, or data. This includes full-time employees, part-time employees, contractors, consultants, vendors, and any third-party service providers who are granted access to Docker’s computing resources or technology environments.

It covers all access to Docker-managed environments, whether hosted on-premises or in the cloud, including internal corporate systems, development and staging environments, testing platforms, and production infrastructure. The policy governs user accounts, system identities, and integration accounts, and applies to both interactive and automated access.

3. Roles and Responsibilities

Role	**Responsibilities**
Security Team	Owns and maintains access control policies. Monitors and audits access to privileged accounts, investigates access-related anomalies, and provides oversight for the access review process.
IT Team	Implements access provisioning and deprovisioning workflows. Manages identity platforms, enforces technical safeguards (e.g., SSO, MFA), and supports system access lifecycle management.
Department Managers	Approve access requests for team members. Participate in periodic access reviews and ensure staff only have access to what

	is necessary for their role.
System and Application Owners	Define access roles and permissions for the systems they manage. Approve access requests and ensure role definitions align with job responsibilities.
HR and People Operations	Initiate access provisioning and deprovisioning based on employee onboarding, transfers, and terminations. Coordinate with IT to maintain life cycle consistency.
All Users	Are responsible for using access privileges appropriately, protecting their credentials, following acceptable use policies, and reporting any suspicious activity or access anomalies immediately.

4. Definitions

Least Privilege - The principle of granting users only the minimum access rights necessary to perform their job functions.

Privileged Access - Administrative or elevated permissions including root, superuser, system administrator access, or any access that allows system configuration or security control override.

Service Account - A non-interactive account used by applications or automated processes, requiring documented justification and enhanced monitoring.

Provisioning - The formal process of creating user accounts and granting access permissions through documented requests and approvals.

Deprovisioning - The process of disabling or removing user accounts and revoking all associated access permissions upon termination or role change.

Access Review - The periodic validation process where managers and system owners verify that user permissions remain appropriate and necessary for current job responsibilities.

5. User Access Management

5.1 Unique Accounts

All user accounts must be uniquely identifiable and assigned to a single individual. Generic or shared accounts are prohibited unless explicitly approved for specific use cases, such as service accounts, and must have documented justification.

5.2 Access to systems

Access to systems and applications within an employee's defined job scope is automatically provisioned through predefined role-based access groups. Any requests for access beyond standard job responsibilities or for privileged system access must be submitted through the official access request system with justification, approved by the user's manager or the relevant system/data owner, with all approvals documented and retained for audit purposes.

5.3 Deprovisioning access

User accounts must be deactivated or deleted within 24 business hours of termination of employment or contract.

6. Remote and Mobile Access

Remote access to Docker’s systems must occur through secure channels such as virtual private networks (VPN) or single sign-on (SSO) systems protected by multi-factor authentication (MFA).

Devices used for remote access must have endpoint protection tools installed, configured, and updated in accordance with Docker’s security standards.

7. SaaS and Cloud Access Control

Where possible access to Software-as-a-Service (SaaS) platforms and cloud infrastructure must be governed through centralized identity providers, such as Okta, using single sign-on (SSO) with role-based access controls (RBAC). Permissions within cloud environments must correspond to defined job functions and adhere to the principle of least privilege.

Provisioning and deprovisioning of SaaS and cloud access must follow the same governance and approval workflows as internal systems. All changes to access must be auditable and traceable to a documented request and approval.

8. Password and Authentication Requirements

- Users must use a password manager for secure storage of passwords
- Minimum 8 characters (user-generated) or 6 characters (machine-generated); cannot include usernames, personal information, or known breach data
- Temporary passwords delivered via 1Password/email require mandatory change on first login after identity verification
- Systems lock accounts after five consecutive failed login attempts
- Immediately change default vendor passwords, administrator credentials following terminations, and shared account passwords when group membership changes
- Prohibited: password sharing outside approved shared accounts, saving in form-filling applications, or displaying written passwords

Password rotation, secure storage, and restricted reuse are required in accordance with risk-based authentication principles. Credentials must not be shared or stored in plaintext, hardcoded in code, or saved in unsecured repositories.

9. Access Reviews and Certifications

All access to Docker-managed systems must be reviewed at least annually to ensure that permissions remain appropriate and necessary. Department managers and system owners are responsible for completing access reviews and signing off on review results.

Privileged access accounts must be reviewed quarterly. Any discrepancies identified during a review must be remediated within a defined time frame and documented. All access review actions must be retained for audit purposes.

10. 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.

11. 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
09/23/2025	3.0	Chad Fryer, Sr. Security Engineer, GRC	Policy annual review and update
06/13/2024	2.1	Jeff Strauss, Director of IT	Revisions Approved
04/20/23	2.0	Karen Hajoannou, Rachel Taylor, Director, Security, Risk & Trust	Policy annual review and update
02/6/2023	1.2	Todd Smith, VP of IT	Policy approved
01/3/2023	1.1	Rachel Taylor, Senior Manager, Security, Risk & Trust; Jeffrey Strauss, Director of IT	Draft submitted for review
12/19/2022	1.0	Rachel Taylor, Senior Manager, Security Risk & Trust	Basic document outline