SECURITY AWARENESS TRAINING 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 establishes Docker's security awareness training program to develop and maintain a security-conscious workforce capable of identifying, preventing, and responding to evolving cyber threats. Human behavior remains a critical factor in security incidents, making comprehensive awareness training essential for protecting Docker's data, systems, and reputation.

The policy mandates:

- Mandatory security awareness training for all personnel within 30 business days of onboarding
- Annual refresher training to address emerging threats and reinforce secure behaviors
- Role-specific training for positions with elevated access or data handling responsibilities
- Regular simulations and practical exercises to test and improve threat recognition
- Privacy-specific modules covering data protection obligations under GDPR, CCPA, and other regulations
- Documented completion tracking with defined escalation procedures for non-compliance

This framework ensures all Docker personnel understand their security responsibilities, recognize common attack vectors, and respond appropriately to incidents. It supports Docker's compliance with ISO/IEC 27001 Annex A.6.3 (Information Security Awareness, Education and Training), SOC 2 Trust Services Criteria, and privacy regulations requiring demonstrated workforce training. By fostering a culture of security awareness, this program reduces human-related vulnerabilities and strengthens Docker's overall security posture.

2. Scope

This policy applies to all individuals who have access to Docker-managed systems, services, and confidential information. It encompasses full-time and part-time employees, contractors, temporary personnel, and interns, regardless of geographic location.

The policy is applicable across all business units and functional teams at Docker. It governs access to corporate infrastructure, production environments, development systems, communication tools, and collaboration platforms. Whether individuals interact with information systems on-site, remotely, or through third-party platforms, their participation in security training activities is mandatory and must be completed in accordance with this policy.

3. Roles and Responsibilities

Role	**Responsibilities**
Security Team	Develops and manages the organization’s security awareness program. Designs and updates curriculum content, delivers phishing simulations, and monitors compliance. Oversees onboarding workflows to ensure new hires

	are enrolled and engaged. Tracks completion metrics, and manages reminders and escalations for overdue training to maintain program effectiveness and alignment with evolving threats.
Department Managers	Ensure their teams complete assigned training. Support enforcement actions for overdue training and encourage participation in reinforcement activities.
Engineering, IT, and High-Risk Roles	Complete any required role-based training beyond baseline awareness modules.
All Users	Complete all assigned training within the required timeframes. Acknowledge understanding of key security policies and baseline security practices.

4. Mandatory Training

Docker’s security awareness program consists of several required training activities. All users are expected to participate in the following:

- Initial Training: All new hires and authorized users must complete baseline security awareness training within 30 business days of joining Docker.
- Annual Training: All employees with a tenure date that is greater than or equal to 1 year must complete refresher training once every 12 months.
- Role-Based Training: Individuals in high-risk roles must complete supplemental training that is specific to their responsibilities and exposure to sensitive information or privileged access.
- Privacy-Specific Training: Required for all personnel upon hire and annually.

5. Curriculum Components

The training curriculum is developed to reflect Docker’s current risk landscape and regulatory obligations. Topics include, but are not limited to:

- Password and credential security
- Phishing awareness and social engineering prevention
- Data classification and appropriate handling techniques
- Review of all Information Security policies
- Privacy awareness related to regulations such as GDPR and CCPA
- Work From Home best practices
- Incident reporting procedures and escalation paths
- Data subject rights and how to respond

Training content is updated annually or more frequently if significant threats or policy changes occur.

6. Delivery Methods

Training is delivered through a blended approach that combines interactive e-learning modules, real-time simulations, and scenario-based exercises. Employees engage with short, focused lessons designed to reinforce key behaviors, followed by simulated attacks that test knowledge in a safe, controlled environment. Additional reinforcement is provided through micro-learning refreshers, periodic challenges, and explainer videos posted to internal knowledge bases or shared through team channels. Targeted follow-up is applied for individuals or teams requiring extra support, ensuring the program remains practical, engaging, and continuously aligned with emerging threats.

7. Completion Tracking and Attestation

Users formally acknowledge their understanding of security policies. Training completion is tracked through a document that is automatically updated daily.

Compliance reports are generated continuously, with Security reviewing flagged users or those nearing training deadlines. To drive timely completion, three escalating reminders are sent automatically:

1. Weekly Slack notifications to the user.
2. When training is due within 15 business days, the user’s manager is CC’d in the Slack reminder.
3. When training is due within 6 business days, a direct Slack message is sent to the manager requesting they prompt their report to complete training.

8. 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.

9. 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

09/29/2025	3.0	Chad Fryer, Sr. Security Engineer, GRC	Policy annual review and update
12/04/2024	2.2	Kathleen Swift, Chief People Officer	Policy approved
07/25/2024	2.1	Justin Cormack, Chief Technology Officer	Policy approved
07/21/2024	2.0	Rachel Taylor, Director, Security, Risk & Trust	Policy annual review and update
02/13/2023	1.2	Todd Smith, Vice President of Information Technology	Draft document approved
01/26/2023	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