OFAC, SDN, ITAR COMPLIANCE POLICY

Version Number:	3.1
Version Date:	Sep 19, 2025
Owned by:	Legal
Approved by:	Joel Benavides, Head of Legal
Confidentiality Level:	Internal

Table of Contents

1. Purpose 3
2. Scope 3
3. Roles and Responsibilities 3
4. Resources 3
5. Policy Statements 4
6. Restricted Countries 4
7. Customer Onboarding 5
8. Restricted Countries Enforcement 5
9. Enforcement and Exceptions 5
10. Change History 6

1. Purpose

The purpose of this policy is to ensure that Docker, a United States entity, fully complies with the rules and regulations administered by the United States Department of the Treasury's Office of Foreign Assets Control ("OFAC"). These regulations enforce U.S. economic and trade sanctions in alignment with national security and foreign policy objectives.

This policy establishes clear standards and procedures to prevent prohibited transactions with sanctioned countries, entities, organizations, and individuals. It also reinforces Docker's commitment to responsible business practices, safeguarding the company against legal, financial, and reputational risks.

2. Scope

This policy applies to all Docker employees, contractors, consultants, and temporary staff engaged by the company. It covers all business activities, transactions, and dealings with customers, partners, vendors, resellers, and other third parties worldwide. The policy applies to all products and services offered by Docker, and governs both direct and indirect commercial and financial transactions, whether conducted within the United States or abroad.

3. Roles and Responsibilities

Role	**Responsibilities**
Head of Legal	Owns this policy and monitors updates to OFAC regulations and ensures timely updates to policies, controls, and processes.
Security GRC Team	Supports the Legal team by handling the OFAC policy exception process.
IT Operations	Ensures GeoIP blocking to restricted countries.
All Employees and Contractors	Adhere to this policy and refrain from engaging in prohibited transactions. Report potential violations of this policy to the Legal Team.

4. Resources

- Office of Foreign Access Control ("OFAC") - Sanctions Programs and Information
- Specially Designated Nationals and Blocked Persons List (SDN) Human Readables List
- Consolidated Sanctions List (Non-SDN Lists)

- Other OFAC Sanctions Lists
- Export Administration Regulations (EAR)
- Specially Designated Nationals and Blocked Persons List (SDN)
- Third-party expert law firm as warranted.
- GeoIP Blocking Run book

5. Policy Statements

The following policy statements must be followed in relation to Docker business activities to ensure Docker maintains compliance with OFAC, SDN and ITAR policies and restrictions:

- Docker employees may not work remotely from restricted countries. Docker employees should not take Docker owned equipment (i.e. laptops) to restricted countries.
- Docker cannot do business with individuals or employees of entities included on the Specially Designated Nationals ("SDN") list, regardless of their location.
- If you are dealing with a country subject to restrictions with specific parties, a restricted party screening must be performed. A restricted party screening screens individuals and entities against lists of restricted parties to ensure compliance with sanctions regulations.
- If you are contemplating activities in countries subject to import, export, or travel restrictions, contact Docker's legal department so that a license determination can be made.
- All employees, regardless of the department they work in, may report possible OFAC violations to the Head of Legal.
- OFAC related concerns or questions should be relayed to the Head of Legal.

6. Restricted Countries

As of the date of this policy, the following countries are restricted. These countries impose both business and employee restrictions. While employees are not restricted from traveling to these regions, the employee must not bring their Docker laptop and must not access Docker systems from these regions. If you are traveling to a restricted region, please reach out to Docker Information Security via Slack or email help-security@docker.com.

Restricted Country	Is Docker Restricted from Doing Business with Customers in this Region?	Are Employees Restricted from Accessing Docker Systems from this Region?
China	Yes - restrict export to listed entities	Yes
Crimea, Donetsk and Luhansk - Regions of Ukraine	Yes	Yes
Cuba	Yes	Yes
Iran	Yes	Yes
North Korea	Yes	Yes
Syria	Partially - The licensing of Docker Desktop and Hub is permitted for Personal accounts but not for commercial accounts.	Yes
Russia	Yes	Yes

The below are countries where OFAC, SDN and ITAR checks are required for Docker customers and vendors due to sanctions currently in place (see Resources).

Other Countries Subject to OFAC Sanctions			
Balkans	Belarus	Burma (Myanmar)	Central African Republic
Congo, Dem. Rep of	Ethiopia	Hong Kong	Iraq
Lebanon	Libya	Sudan	Venezuela
Yemen	Zimbabwe		

7. Customer Onboarding

Docker utilizes the services of an expert third-party provider to perform OFAC, SDN and ITAR screening of its customers as appropriate.

8. Restricted Countries Enforcement

To comply with international trade laws and sanctions regulations, Docker restricts access to its systems and services from certain countries and regions. These restrictions are applied to ensure that Docker remains aligned with global legal requirements and industry best practices. The determination of which locations are restricted is based on authoritative geographic and regulatory data that is updated regularly to reflect changes in sanctions programs.

Docker has established processes to review and apply these updates consistently across its infrastructure, helping ensure that restrictions remain accurate, reliable, and enforceable. By maintaining these controls, Docker safeguards the integrity of its systems while upholding its legal and regulatory obligations.

9. 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.

10. Change History

Date	Version	Responsible Party	Description of Change
09/19/2025	3.1	Joel Benavides, Head of Legal	Policy approved
09/03/2025	3.0	Stephen Oriowo	Annual policy review
01/27/25	2.3	Salima Allarakhia, Sr Manager Security	Policy owner and approver changed.
12/04/2024	2.2	Joel Benavides, Head of Legal	Policy approved
12/04/2024	2.1	Kathleen Swift, Chief People Officer	Policy approved
07/21/2024	2.0	Rachel Taylor, Director, Security, Risk & Trust	Policy annual review and update
07/06/2023	1.2	Joel Benavides	Policy approved
06/12/2023	1.1	Rachel Taylor	Draft submitted for review to Alisa Avelar, VP of People, Joel Benavides, Head of Legal
05/31/2023	1.0	Rachel Taylor	Policy drafted