THIRD PARTY RISK MANAGEMENT

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 defines the governance framework for identifying, assessing, monitoring, and mitigating risks from third-party vendors, service providers, and subprocessors. It establishes a risk-based approach using a tiered model that categorizes vendors based on their access levels, data sensitivity, and potential operational impact.

The policy ensures Docker:

- Protects customer, employee, and company data (including PII and regulated data)
- Maintains service continuity and operational resilience
- Complies with privacy laws, industry standards, and contractual requirements
- Enforces appropriate security controls, incident notification requirements, and audit rights

Higher-risk vendors undergo rigorous assessment and ongoing oversight, while lower-risk vendors follow streamlined processes. This framework promotes transparency, accountability, and consistency throughout the vendor lifecycle, from onboarding and contract negotiation through performance monitoring and termination.

2. Scope

This policy applies to all software vendors that Docker engages to provide products, platforms, or systems. The scope includes software vendors who store, process, transmit, or otherwise have access to Docker’s systems, infrastructure, business data, or customer and employee personal information.

It also applies to all Docker personnel involved in vendor selection, procurement, onboarding, risk assessment, contract management, performance review, or offboarding. This includes individuals in GRC, security, legal, engineering, finance, procurement, and vendor relationship management roles.

All vendors are subject to a formal risk classification and assessment process. Depending on their access, data handling, or operational role, vendors may be required to meet specific security, privacy, and contractual controls as defined by this policy and its supporting procedures.

3. Roles and Responsibilities

Role	**Responsibilities**
GRC	Develops and maintains the corporate Third Party Risk Management (TPRM) framework, policies, and procedures. Conducts vendor due diligence including privacy and and security reviews in adherence to company policies and industry standards.

Security Team	Supports the GRC team by performing technical reviews of vendors where appropriate, providing expertise to identify potential risks and ensure security standards are met.
Legal Team	Reviews and negotiates third-party contracts, including Data Protection Addendums (DPAs), Master Service Agreements (MSAs), and Service Level Agreements (SLAs). Ensures that contractual terms reflect regulatory and internal compliance requirements, including incident notification, audit rights, and subprocessor flowdown obligations.
Procurement and Finance	Collaborate with Legal and GRC to ensure that vendors are onboarded through the appropriate review process and that renewal or payment decisions factor in compliance status and risk tier.
Business Owners	Individuals or teams who initiate vendor engagement are responsible for providing context, participating in risk evaluation, and implementing required controls. They are accountable for managing the operational relationship with the vendor.
All Docker Personnel	Must follow procurement procedures when evaluating or engaging vendors. Must not bypass risk reviews, use unsanctioned tools, or share data with vendors without proper agreements in place. Report any concerns about vendor security, compliance, or performance to Security or Legal.

4. Definitions

Third-Party Risk Management (TPRM) - A structured framework for identifying, assessing, monitoring, and mitigating risks arising from vendors, service providers, and other external entities that have access to Docker's systems, data, or infrastructure.

Subprocessor - A third-party entity engaged by Docker's vendor to perform specific processing activities on Docker's data, requiring the same security, privacy, and contractual obligations as the primary vendor through flow-down provisions.

Data Protection Addendum (DPA) - A mandatory contractual agreement between Docker and vendors that process personal data, defining privacy obligations, security measures, breach notification requirements, cross-border transfer mechanisms, and data subject rights support.

Risk Tier - A classification level assigned to vendors based on their access to sensitive data, operational criticality, and potential impact, determining the depth of due diligence, contractual requirements, and ongoing monitoring needed.

Business Owner - The Docker employee or team who initiates and maintains the operational relationship with a vendor, responsible for providing business context, participating in risk assessments, and ensuring implementation of required controls throughout the vendor lifecycle.

5. Third-Party Risk Lifecycle

5.1 Risk Assessment and Tiering

All in scope vendors must undergo an initial risk assessment prior to onboarding. The assessment evaluates the vendor's access to Docker systems and data, their potential impact on business operations, and their alignment with security, privacy and compliance requirements. Vendors are classified into one of three risk tiers based on factors such as access to confidential data, dependency for production services, financial exposure, regulatory obligations, volume and sensitivity of personal data processed, geographic locations of data processing, support for data subject rights (access, deletion, portability), international data transfer mechanisms, privacy breach history, and ability to support data retention/deletion requirements.

Tier assignments determine the level of due diligence, documentation, and oversight required. Security and privacy assessments, contractual requirements, and reassessment intervals vary by tier.

Tier	Definition	Detailed Examples	Vendor Assessment Material
Tier 1 – Critical Risk	Vendor has access to highly confidential data (e.g., customer PII), sensitive production systems, or is critical to business operations. Any failure, compromise, or misuse could cause major financial, reputational, legal, or regulatory harm.	- Cloud infrastructure (e.g., AWS, GCP, Azure) - Identity providers & access managers (e.g., Okta, Auth0) - SaaS platforms storing or processing customer PII or payment data (e.g., Salesforce, Stripe) - Core DevOps or deployment tools (e.g., GitHub, CircleCI, ArgoCD)	Comprehensive security assessment Validated SOC 2 Type II, ISO 27001, or equivalent certification Executed NDA, MSA, DPA, and SLA with defined uptime & breach notification clauses Business continuity/disaster recovery (BC/DR) evaluation

Tier 2 – Moderate Risk	Vendor has limited access to internal systems, personnel, or non-sensitive business data. Misuse or failure would cause operational disruption or minor compliance exposure, but not critical failure.	- HR & people platforms (e.g., Deel, BambooHR, Greenhouse) - Internal collaboration & productivity tools (e.g., Notion, Slack, Zoom) - Contract & legal management tools (e.g., Ironclad, DocuSign) - Marketing or sales tech storing internal contact lists (e.g., HubSpot, Marketo) - Data analytics or dashboards not linked to PII or prod - Security platforms monitoring production (e.g., Datadog, Snyk)	Comprehensive security assessment SOC 2 Type II, ISO 27001, or Standardized security questionnaire (e.g., CAIQ or SIG-Lite) Executed NDA, MSA, DPA (if HR or marketing data involved)
Tier 3 – Low Risk	Vendor offers non-critical services or open source tools with no access to production, internal systems, or Docker's data. Business impact is minimal in the event of service failure or data loss.	- Swag/merchandise providers - eLearning/training platforms - External design or video agencies - Travel or expense booking platforms - Food/catering, team events platforms - OSS libraries/frameworks (e.g., React, Lodash) - Public knowledge sources (e.g., Stack Overflow, Wikipedia) - Developer documentation (e.g., MDN, Postman Docs)	Basic procurement checklist (e.g., vendor purpose, contact info) No formal security assessment required Review at contract renewal or when service changes materially

5.2 Contractual Requirements

All third-party agreements must reflect the organization's security and compliance standards. Contracts should clearly define the scope of services, roles, responsibilities, and performance expectations, ensuring that third parties maintain standards consistent with the organization's internal requirements.

Each agreement must also include provisions that enable performance monitoring or audit rights, outline procedures for renewal and termination, and specify requirements for transition support and the secure handling, return, or disposal of organizational assets. These measures help ensure consistent governance, accountability, and risk management across all external relationships.

Cloud Hosting Provider Additional Requirements:

- Transparency about data locations and jurisdictions
- Customer control over data location selection
- Audit logging
- Security certifications

5.3 Sub-processor Governance

Transparency Requirements:

- Vendors must maintain current list of all sub-processors handling Docker's data
- Notice of sub-processor changes
- Docker retains right to object to new sub-processors
- Sub-processor list must include:
  - Entity name and location
  - Services provided
  - Data types accessed
  - Security/privacy certifications

Flow-down Requirements:

- All privacy and security obligations must flow to sub-processors
- Direct liability chain for breaches
- Docker audit rights must extend to sub-processors

5.4 Ongoing Monitoring

Vendor Tier	Reassessment Frequency	Monitoring Requirements
Tier 1 – Critical Risk	Annually	Continuous monitoring to track security posture and compliance status
Tier 2 – Moderate Risk	Every 24 months	Continuous monitoring to track security posture and compliance status
Tier 3 – Low Risk	As needed based on access changes	Minimal oversight unless scope or service changes

Monitoring includes periodic reassessment of contract terms, access levels, and security documentation, as well as incident or performance-related updates.

5.5 Vendor Termination

Upon termination of a vendor relationship, all access privileges, accounts, and credentials granted to the vendor must be revoked. Vendors must return or securely destroy all Docker data, assets, and materials in accordance with the terms of the governing contract and applicable organizational standards.

Where applicable, the vendor shall provide reasonable transition support to facilitate continuity of operations and ensure full compliance with security and contractual obligations.

6. 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.

7. 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
09/22/2025	3.0	Stephen Oriowo, Sr GRC Analyst Chad Fryer, Sr. Security Engineer, GRC	Policy annual review and update
05/20/2024	2.1	Justin Cormack	Updated document approved
5/13/2023	2.0	Rachel Taylor, Director, Security, Risk & Trust	Minor updates made - added details on reviewing financial statements for public companies based on the SEC ruling and an Artificial Intelligence (AI) questionnaire to focus on unique control sets necessary for AI which would not be captured in a SOC 2, ISO 27001 or similar attestation

1/13/2023	1.3	Todd Smith, VP of IT	Draft document approved
1/3/2023	1.2	Rachel Taylor, Sr. Manager, InfoSec, Risk & Trust	Draft Submitted for review
12/19/2022	1.1	Rachel Taylor, Sr. Manager, InfoSec, Risk & Trust	Basic document outline