INCIDENT MANAGEMENT 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 structured framework for detecting, responding to, and recovering from security incidents that may affect Docker's systems, data, or operations.

The policy defines requirements for:

- Immediate reporting and classification of security events and incidents
- Assignment of severity levels with corresponding response and resolution timelines
- Coordination of containment, eradication, and recovery activities across security, engineering, and business teams
- Documentation and logging of all incident-related actions for audit and compliance purposes
- Post-incident reviews to identify root causes and implement preventive controls
- Training and testing protocols to maintain organizational readiness

This framework ensures Docker can respond effectively to security threats, minimize impact to business operations and customers, meet regulatory notification obligations, and continuously improve security controls. It demonstrates compliance with ISO/IEC 27001 and SOC 2 Trust Services Criteria requirements for incident management capabilities.

2. Scope

This policy applies to all areas of Docker’s technology environment and organizational operations. It governs any incident that may affect the confidentiality, integrity, or availability of Docker systems, services, data, or physical assets. The policy covers all employees, contractors, and third-party service providers who interact with Docker’s infrastructure or data.

It includes both confirmed and suspected security incidents, operational disruptions, or anomalous events—regardless of origin—that may compromise systems, expose sensitive data, disrupt services, or affect compliance obligations. Incidents may involve internal systems, cloud services, third-party integrations, physical assets, or personnel behavior.

Whether the incident stems from malicious activity (such as malware or unauthorized access), human error, system failure, or environmental disruption, the response process must follow the structured lifecycle and documentation requirements outlined in this policy.

3. Roles and Responsibilities

Role	Responsibilities
Security Incident Response Team (IRT)	Leads detection, containment, eradication, and recovery efforts; performs root cause analysis and coordinates with stakeholders during the security incident lifecycle.
Security Operations Center (SOC) Analysts	Monitor alerts, triage suspicious activity, escalate verified threats to IRT, and support response actions through tooling and logging.
Engineering and IT Teams	Support investigation, containment, and remediation of system-specific or application-layer incidents; restore service availability.
Legal and Compliance Teams	Advise on regulatory and contractual reporting obligations, coordinate external disclosures (e.g., DPA notifications), and review PIR findings.
People Operations	Engage in incidents involving employee behavior or insider threats; support HR-related investigation and documentation.
Managers and Team Leads	Ensure their teams are informed of and comply with reporting obligations; participate in resolution or PIRs as needed.
All Employees and Contractors	Must report suspected or confirmed incidents immediately using official channels and cooperate fully during investigations.

4. Definitions

- **Event**: An observable occurrence in a system or network (e.g., failed login, system error, malware detection).
- **Incident**: Any event that actually or potentially compromises the confidentiality, integrity, or availability of systems, services, or data.
- **Post-Incident Review (PIR)**: A formal retrospective conducted after incident resolution to assess cause, impact, and preventive controls.

5. Incident Categories

Docker recognizes the following categories of incidents:

- Unauthorized access or attempted access to internal systems or data
- Data breach involving customer, employee, or operational information
- Malware infection, ransomware activity, or suspicious code execution

- Denial of service (DoS), distributed DoS (DDoS), or system outage
- Device loss or theft (e.g., laptop, phone, external drive)
- Insider misuse, policy violations, or negligent behavior
- Vendor or third-party security breach impacting Docker systems

Each incident is evaluated and classified based on its type, impact, and severity level.

6. Incident Lifecycle

6.1 Detection and Reporting

All employees and contractors are required to report suspected incidents as soon as they are observed. Reports may be submitted via Jira Service Desk, the #help-security-grc Slack channel, or help-security@docker.com.

In addition, Docker's monitoring tools automatically generate alerts based on predefined detection rules and anomalous patterns.

6.2 Classification and Prioritization

Incidents are classified and assigned a severity level based on impact and urgency. Response times and resolution targets are as follows:

Severity	Criteria	Response Time	Resolution Target
SEV 1	Critical – Widespread or Company-Wide Service Outage A defect or outage that causes a complete loss of core functionality for: - Many customers at once (systemic issue), or - All users within a single customer organization.	<15 min	12 hours
SEV 2	High – Team/Department-Level Impact A defect or outage that prevents a significant subset of users within one customer organization (e.g., a team, department, or site) from using key functionality. The issue has a severe business impact and no workaround exists.	<15 min	24 hours

SEV 3	Medium – Individual User Impact A problem causing partial or non-critical loss of use of functionality for an individual user or small group. Business operations continue, often with a workaround available, but productivity is reduced.	<1 business day	<5 business days
SEV 4	Low – Inquiries, Minor Issues, or Enhancements Questions, cosmetic issues, or low-impact defects with minimal business effect. Workarounds are typically available or not required.	<5 business days	<15 business days

Severity may be reclassified as new information becomes available. SLAs begin upon detection of the incident. SLAs begin upon confirmation of the incident.

6.3 Containment and Eradication

Once an incident is verified, the response team will take appropriate steps to isolate affected systems, revoke compromised credentials, block malicious IPs, or contain damage.

Root causes are remediated through patching, configuration updates, or removal of unauthorized components.

6.4 Recovery

After containment, systems are restored to operational state, e.g. ensuring malware or persistence mechanisms have been removed. Verification steps include integrity checks, restoration from trusted backups, and system testing.

6.5 Post-Incident Review (PIR)

A formal PIR is required for all P0 and P1 incidents and any incident involving regulatory notification. The PIR must document:

- Incident timeline and detection point
- Root cause analysis
- Impact and stakeholder notifications
- Lessons learned
- Opportunities for process or control improvement
- Ownership of follow-up actions and deadlines

7. External Dependencies and Vendor Coordination

For incidents involving cloud platforms, SaaS tools, or managed services, Docker will coordinate with third-party vendors using designated escalation procedures. Documentation provided by vendors must be retained and appended to the incident record.

Shared responsibility models and third-party obligations are documented and maintained within the Security team's SOP repository.

8. Logging, Auditing, and Documentation

All incident-related activity must be logged in Jira or Docker's approved incident response platform. Logs must include:

- Detection source (e.g., alert, employee report)
- Affected systems and data types
- Incident timeline and actions taken
- Notified stakeholders
- Outcome and resolution details

Incident records must be retained for at least three years and made available for audit or regulatory review.

9. Training and Testing

All employees are required to complete annual training on security incident awareness and response protocols. The training covers:

- Recognizing suspicious behavior or indicators of compromise
- How and where to report security incidents
- Response expectations and confidentiality

The Security Incident Response Team will conduct at least one tabletop exercise annually. Test results, identified gaps, and action plans must be documented and reviewed by security leadership.

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
12/04/2024	2.1	Justin Cormack, Chief Technology Officer	Revisions approval
12/04/2024	2.0	Karen Hajioannou, Senior Security & Compliance Engineer	Policy annual review and update
02/24/2023	1.2	Todd Smith	Draft document approved
02/3/2023	1.1	Rachel Taylor	Draft Submitted for review
12/19/2022	1.0	Rachel Taylor	Basic document outline