SUPPORT SERVICE LEVEL AGREEMENT FOR DOCKER HARDENED IMAGES

1. Scope of Support Services

Docker shall make commercially reasonable efforts to maintain, secure, and update its catalog of Docker Hardened Images . Docker Hardened Images are third-party container images of open source packages hardened for enhanced security and compliance ("DHIs"). This SLA shall be governed by the terms of the Docker Service Subscription Agreement as found at https://www.docker.com/legal/docker-subscription-service-agreement/ or an equivalent agreement entered into by Docker and Customer.

2. CVE Remediation and Eligibility

Docker will address Common Vulnerabilities and Exposures ("CVEs") for DHIs under the following conditions:

2.1. Eligible Fix Requirements

A CVE shall be eligible for remediation (an "Eligible Fix") only if:

(i) It is identified by Docker's standard vulnerability scanning tools;

(ii) It is independently fixable (i.e., not dependent on non-remediable issues or technical aspects outside of Docker's control);

(iii) A fix is available upstream or the image can be rebuilt to mitigate the CVE; and

(iv) It is not caused by Customer's own modifications or additions.

2.2. CVE Severity Scoring

CVE severity will be assessed according to Docker's internal severity framework, which aligns with the vulnerability assessment methodology as found at https://docs.docker.com/dhi/features/support/.

3. CVE Remediation Timeframes

Docker shall use commercially reasonable efforts to remediate Eligible Fixes within the following timeframes, measured from the date the CVE is determined by Docker to have an Eligible Fix:

Severity Level	Remediation Timeline
Critical / High	Within 7 calendar days
Medium / Low	Within 30 calendar days

4. CVE Patch Confirmation

A CVE will be considered remediated upon:

(i) Publication of a patched DHI to Docker Hub; or

(ii) The CVE no longer being reported by Docker Scout or another supported scanner; or

(iii) Issuance of a VEX (Vulnerability Exploitability eXchange) statement by Docker explaining why the CVE does not present a security risk in the current image's operational context.

5.1 Version Updates for Open Source Components

Docker shall provide updates for upstream open source packages used in DHIs according to the following schedule:

Version Type	Update Availability
Major	Within 7 business days

Minor	Within 2 business days

Docker will only adhere to the above schedule if the update does not introduce any new and unfixed vulnerabilities.

6. New Repository Requests
Customer may request that Docker include new repositories in the Docker Hardened Images Catalog ("DHI Catalog"). Docker will evaluate such requests for security and compatibility, and if accepted, will make the repository available within a reasonable time. Acceptance of requests will be at Docker's discretion.

7. Image Customization

7.1. Customer Modifications
Customer additions (e.g., packages, certificates, or configuration changes) to DHIs are not covered by this SLA. At Docker's sole discretion, Docker may:

(i) Update Software Bill of Materials ("SBOMs") to reflect customer-added components; and

(ii) Scan customer additions for CVEs and viruses (without remediation obligations).

7.2. SLA Exclusions
Docker's CVE remediation obligations do not extend to customer-added components. Docker assumes no responsibility for patching or maintaining third-party additions or custom code introduced by the Customer.

8. Support Limitations
Docker's obligations under this SLA are subject to:

(i) The continued validity of Customer's subscription to DHI and timely payment of the corresponding fees;

(ii) Customer's adherence to Docker's usage guidelines and technical documentation; and

(iii) The exclusion of issues resulting from Customer environments, configurations, or modifications not authorized by Docker.

9. Disclaimer and Limitation of Liability
This SLA defines the extent of Docker's obligations for DHI Support Services. Docker does not warrant that all vulnerabilities can be eliminated. In case of failure to meet its SLA obligations herein Docker will promptly assign resources and personnel to conduct a root-cause analysis to determine how the failure occurred, and promptly take reasonable corrective action based on that analysis. Remedies under this SLA are limited to those expressly set forth in this paragraph.

10. ELS Specific Provisions

10.1. Scope of Support Services for Applicable Extended Lifecycle Support Products
The provisions of this Section 10 apply solely to the Extended Lifecycle Support Products as identified in the applicable Order Form.

10.2. CVE Remediation and Eligibility
Docker will address Common Vulnerabilities and Exposures ("CVEs") for DHIs under the following conditions:

10.3. Eligible Fix Requirements

A CVE shall be eligible for remediation (an “Eligible Fix”) only if:

(i) It is identified by Docker’s standard vulnerability scanning tools;

(ii) It is independently fixable (i.e., not dependent on non-remediable issues or technical aspects outside of Docker’s control);

(iii) An image can be rebuilt to mitigate the CVE; and

(iv) It is not caused by Customer’s own modifications or additions.

10.4. CVE Remediation Timeframes
Docker shall use commercially reasonable efforts to remediate Eligible Fixes within the following timeframes, measured from the date the CVE is determined by Docker to have an Eligible Fix:

Severity Level	**Remediation Timeline**
Critical / High	Within 14 calendar days
Medium / Low	Within 45 calendar days