GENERAL TERMS FOR SPRING FRAMEWORK AND SPRING BOOT LONG-TERM SUPPORT SERVICES

THESE GENERAL TERMS FOR SPRING FRAMEWORK AND SPRING BOOT LONG-TERM SUPPORT SERVICES (the "**Terms**") apply to the provision of the Spring Framework And Spring Boot Long-Term Support Services identified on the Order Form (defined below) by Perforce Software, Inc., a Delaware corporation, on behalf of itself and its Affiliates (defined below) ("**Perforce**") to the customer entity identified on such Order Form (defined below) ("**Customer**"). To the extent there is any conflict between the Order Form, and this Agreement, such conflict shall be resolved pursuant to the following order of precedence: (i) an amendment to this Agreement; (ii) the Order Form; (iii) and the Agreement. Perforce and Customer are referred to in this Agreement each as a "**Party**" and together as the "**Parties**." "**Affiliate(s)**" means any natural person or entity that directly or indirectly controls or is controlled by or is under common control with a Party. For purposes of this definition, "control" means the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of a Party whether through the ownership of voting securities, by contract, or otherwise.

In exchange for the fees, and for the period of time as more specifically described on a quote that has been accepted by Customer, and/or Customer has raised a purchase order for, and for which Perforce has sent an invoice to Customer (the "**Order Form**"), the OpenLogic support services team ("**OpenLogic**"), agrees to provide the Customer with long term support ("**LTS**") for the Spring Framework, including Spring Boot (collectively, the "**Supported Framework**"). The purchase of one LTS contract entitles the Customer to receive updates for the Supported Framework for the period of time set forth on the Order (the "**Term**") subject to these Terms.

1. Each LTS contract will consist of OpenLogic's provision of the Supported Framework builds with patches for the list of core open source software packages used in the Supported Framework that are set forth on Annex A attached to these Terms (the "**LTS Proactive Core Packages**"). The LTS offered by OpenLogic only covers the proactive monitoring and the delivery of patches for the LTS Proactive Core Packages. If the Customer desires to have a patch for the Supported Framework for a package that is not included in the LTS Proactive Core Packages (each, a "**Non-LTS Proactive Core Package**"), Customer may place a request for a fix for a Non-LTS Proactive Core Package via the standard OpenLogic Support channels. If the request for a Non-LTS Proactive Core Package meets the criteria for a High Severity CVE as set forth in Section 5 of these Terms, OpenLogic will work on delivering the patch for such Non-LTS Proactive Core Package in accordance with the provisions of Section 5 of these Terms.

2. OpenLogic will make the patches for the LTS Proactive Core Packages and the Non-LTS Proactive Core Packages available to the Customer through an OpenLogic private repository in accordance with the response times described on Annex B attached to these Terms. Upon the purchase of a LTS contract, OpenLogic will provide the required credentials to the Customer to enable the Customer to access the private repository contents, and these credentials will remain valid only for the duration of the purchased LTS contract. It is the Customer's responsibility to download and to implement the patches for the LTS Proactive Core Packages or the Non-LTS Proactive Core Packages that are made available to the Customer in the OpenLogic private repository during the term of the Customer's LTS contract.

3. Customer acknowledges and agrees that Customer's access to, and use of, the updated patches for the LTS Proactive Core Packages and/or the Non-LTS Proactive Core Packages that are made available to the Customer by OpenLogic in the OpenLogic private repository during the Term is subject to the following conditions:

   a. Customer is granted the right and license to (1) use the Supported Framework patches for the LTS Proactive Core Packages and/or the Non-LTS Proactive Core Packages for its own internal use related to the testing and development of Customer's integrated offerings, and (2) redistribute the Supported Framework patches for the LTS Proactive Core Packages and/or the Non-LTS Proactive Core Packages provided by OpenLogic; and

   b. Customer shall not redistribute the OpenLogic Supported Framework patches for the LTS Proactive Core Packages and/or the Non-LTS Proactive Core Packages as a standalone offering.

4. OpenLogic will proactively monitor the Common Vulnerabilities and Exposures ("**CVEs**") database that is managed and reported by the MITRE Corporation ("**MITRE**") on its website located at www.cve.org or www.cve.mitre.org and, optionally, other reporting sources, for CVEs against the Supported Framework.

OpenLogic will provide x86_64 patches to the last minor Supported Framework release for the LTS Proactive Core Packages and Non-LTS Proactive Core Packages, at the point of the reaching end-of-life ("EOL"), when High Severity CVEs have a CVSS v3 score 7 or higher ("High Severity"), and the CVE includes documented verification of the vulnerability by an external attack vector. For High Severity CVEs disclosed prior to the EOL of the Supported Framework release that were not patched by the Supported Framework community, OpenLogic will evaluate the reasons for the Supported Framework community not fixing such High Severity CVEs, and, at OpenLogic's discretion, make commercially reasonable efforts to fix such High Severity CVEs based on the available information and CVE severity. If an LTS Proactive Core Package or Non-LTS Proactive Core Package CVE fix requires architectural changes and/or the introduction of breaking changes and/or new risks, OpenLogic may determine, in its sole discretion, not to produce a patch. In that case, OpenLogic will provide the Customer with a written explanation in the release notes document. OpenLogic fixes are not provided for older versions of the Supported Framework from the last minor release that reached community EOL.

For High Severity CVEs on LTS Proactive Core Packages or Non-LTS Proactive Core Packages with only local exploits, or without documented verification of the vulnerability, OpenLogic will research the fix for such CVEs, and will make commercially reasonable efforts to implement repairs. If viable, OpenLogic agrees to provide the Customer with patches via OpenLogic's private repositories.

5. Customer may report what the Customer believes to be a High Severity vulnerability to OpenLogic via the standard OpenLogic support channels. If the reported vulnerability has not yet been discovered or reported on the CVE websites located at www.cve.org or www.cve.mitre.org and the National Vulnerability Database (the "NVD"), the Customer will need to demonstrate the vulnerability to OpenLogic in the Customer's environment. Once the vulnerability is demonstrated, if OpenLogic considers the Customer-reported vulnerability to be of sufficient severity to require a fix or mitigation, and such vulnerability is included in the LTS Proactive Core Packages or Non-LTS Proactive Core Packages, OpenLogic will treat such vulnerability as a High Severity CVE, and OpenLogic will provide a patch for the Supported Framework as set forth in Section 5 above.

6. EXCEPT AS PROVIDED IN SECTION 5 OF THESE TERMS, PERFORCE MAKES NO OTHER REPRESENTATIONS OR WARRANTIES, AND PERFORCE, ON BEHALF OF ITSELF AND ITS AFFILIATES, INCLUDING ROGUE WAVE AND OPENLOGIC, DISCLAIMS ALL REPRESENTATIONS, WARRANTIES, AND CONDITIONS RELATING TO THE SERVICES PROVIDED UNDER THESE TERMS, OR OTHER SUBJECT MATTER OF THIS AGREEMENT, WHETHER ORAL OR WRITTEN, EXPRESS OR IMPLIED, ARISING FROM COURSE OF DEALING, COURSE OF PERFORMANCE, OR USAGE IN TRADE, OR OTHERWISE, INCLUDING, WITHOUT LIMITATION, ANY WARRANTY OF TITLE, NONINFRINGEMENT, MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE. TO THE EXTENT THAT PERFORCE IS NOT PERMITTED BY THE APPLICABLE LAW TO DISCLAIM ANY WARRANTY PROVIDED HEREIN, THE SCOPE AND DURATION OF SUCH WARRANTY SHALL BE THE MINIMUM REQUIRED UNDER SUCH LAW. EXCEPT FOR DAMAGES CAUSED BY FRAUD AND INTENTIONAL MISREPRESENTATION, IN NO EVENT SHALL EITHER PARTY'S TOTAL CUMULATIVE LIABILITY, UNDER THIS AGREEMENT, OR RELATING TO THE SUBJECT MATTER HEREOF, FOR ALL CLAIMS, COSTS, LOSSES, AND DAMAGES EXCEED THE AMOUNT PAID OR PAYABLE IN THE PRECEDING TWELVE (12) MONTH PERIOD BY CUSTOMER TO PERFORCE OR TO ROGUE WAVE, AS APPLICABLE, PURSUANT TO THESE TERMS.

7. Either party will have the right to terminate these Terms prior to the end of the Term in the event that the other party breaches the terms, conditions, and/or obligations under these Terms. Intent to terminate will be made by a written notice setting forth the details of the breach. Termination will become effective ten (10) days from the date that the notification of intent to terminate was given unless the breaching party has corrected the breach prior to the end of that ten (10)-day period. Upon termination of these Terms, OpenLogic will disable access to the Customer's OpenLogic Private repository. Termination shall be without prejudice to the rights and remedies of either party that may have accrued prior to such termination. For the avoidance of doubt, and except in the case of breach of these Terms by Perforce, Customer shall not be entitled to a refund of any prepaid fees upon termination of these Terms, and Perforce will not release Customer from its obligations to pay Perforce all fees that are due and owing under these Terms prior to its termination. These Terms, and all matters arising out of or relating to these Terms, shall be governed by the substantive laws of the State of Delaware. Neither party may assign, alienate or otherwise transfer any rights, duties, obligations or privileges under these Terms, by operation of law or otherwise, without the prior written consent of the other party,

except that either party may assign these Terms without the consent of the other party: (i) to a successor in interest in connection with a merger, acquisition or sale of all or substantially all of the assigning party's assets; (ii) to an affiliate of the assigning party; or (iii) in connection with a corporate reorganization or divestiture to separate any business unit, product(s) or assets of such party to which these Terms relate. A change in control of majority ownership of a party shall be deemed an assignment under this Section 8 for which written consent must be sought.

[The Remainder of this Page is Intentionally Left Blank]

ANNEX A

SPRING FRAMEWORK AND SPRING BOOT SUPPORTED AND EXCLUDED CORE PACKAGES

To learn which Spring Framework and Spring Boot core packages are supported, which packages are excluded from CVE patching, and which Spring ecosystem add-ons are available, see the OpenLogic LTS: Spring packages article in the Perforce Support Portal.

ANNEX B

ADDITIONAL SUPPORT DETAILS FOR SPRING FRAMEWORK AND SPRING BOOT LTS SERVICES

1. **Support Channels**. If the Customer has an issue or questions related to patches for Spring Framework, including Spring Boot, a technical support ticket can be created using the standard OpenLogic support channels provided below. The Customer agrees to provide OpenLogic with all reasonable assistance and cooperation so that OpenLogic can reproduce, identify, and verify the reported issue:

Contact Method	Details	Notes
Portal	portal.perforce.com	Requires account registration. Until portal access is approved use the email support option.
Email	support-openlogic@perforce.com	Include "*SPRING LTS*" in the email subject line.
Phone	OpenLogic: (612) 254-7315 Perforce: (612) 268 5646	The primary number is OpenLogic-specific, alternate number requires menu options to get to the OpenLogic queue.

Standard technical support response times are available on the support terms and conditions page.

2. **Patch availability**. For newly disclosed post-EOL CVEs in LTS Proactive Core Packages with CVSS v3 score 7 or higher and the CVE includes documented verification of the vulnerability by an external attack vector, OpenLogic categorizes them using two (2) levels of priority as described below. Each priority level is associated with a different level of service.

P0. A priority P0 designation encompasses CVEs for LTS Proactive Core Packages that possess documented verification of the vulnerability by an external attack vector with a CVSS v3 score equal or greater than 9.0. OpenLogic hereby commits to the following actions with respect to P0 CVEs: Provide the Customer with a patch release or workaround within fourteen (14) calendar days from the time the CVE details have been published.

P1. A priority P1 designation encompasses CVEs for LTS Proactive Core Packages that possess documented verification of the vulnerability by an external attack vector with a CVSS v3 score greater than or equal to 7.0 but less than 9.0. OpenLogic herby commits to the following actions with respect to P1 CVEs: Provide a patch release or workaround within thirty (30) calendar days from the time the CVE details have been published.

For CVEs on Non-LTS Proactive Core Packages with CVSS v3 score greater than or equal to 7.0, OpenLogic will make commercially reasonable efforts to provide a patch release or workaround as soon as possible without a specific timeframe commitment. When a patch release or workaround cannot be reasonably provided due to architectural changes or the introduction of breaking changes and risks, OpenLogic will provide the Customer with a written explanation.