GENERAL TERMS FOR ANGULARJS LONG-TERM SUPPORT SERVICES

THESE GENERAL TERMS FOR ANGULARJS LONG-TERM SUPPORT SERVICES (the "Terms") constitute a binding agreement by and between Rogue Wave Software, Inc., a Delaware corporation ("Rogue Wave"), and the entity named as "CUSTOMER" on the signature page attached hereto (the "Customer"). These Terms will be effective as of the last date entered underneath the parties' signatures (the "Effective Date").

1. In exchange for the fees, and for the duration of these Terms, both as set forth in the duly authorized quotation issued by Rogue Wave to the Customer, the OpenLogic team at Rogue Wave, a Perforce company ("OpenLogic"), agrees to provide the Customer with long term support ("LTS") for versions 1.6.10 and/or 1.8.3 of the AngularJS framework (each, a "Supported Framework," and collectively, the "Supported Frameworks"). The purchase of one LTS contract entitles the Customer to receive updates for one of the Supported Frameworks, as will be specified in the Customer's order form or quote. If LTS on both Supported Frameworks is required, the Customer must purchase two separate LTS contracts.

2. The LTS contract will consist of the provision of AngularJS framework builds and patches for the applicable Supported Framework. OpenLogic will make the framework builds and patches for the applicable Supported Frameworks available for download on OpenLogic's private repository. 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 AngularJS framework builds and patches for the applicable Supported Frameworks 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 AngularJS framework builds and patches for the applicable Supported Frameworks provided by OpenLogic is subject to the following conditions:

    a. Customer will only consume the source code builds for the applicable Supported Framework specified under the LTS contract as part of Customer's internal application build process;

    b. Customer will not redistribute the source code builds for any of the Supported Frameworks specified under the LTS contract, or any portion thereof, in any other format other than minified output of the Customer's application build process (application creation); and

    c. Unless otherwise specified in writing on the order form or quote, for each LTS contract, the Customer may install one (1) instance of the available OpenLogic AngularJS LTS framework builds or patches on systems owned by the Customer.

4. OpenLogic AngularJS LTS is being offered for a limited time. When OpenLogic ceases to provide commercial LTS contracts for the applicable Supported Framework, OpenLogic agrees to license the full source code, including all builds and patches created and/or distributed by OpenLogic, for the applicable Supported Framework via the MIT license.

5. Upon the general availability to the market of new versions of web browsers, if a web browser is updated from one major version to another, and if there is the possibility that such update will affect or break the functionality in the use of AngularJS, OpenLogic will offer AngularJS patches with corresponding fixes for the applicable Supported Framework purchased under the LTS contract, but only when new major web browser releases break the functionality of the applicable Supported Framework. The Customer may request fixes for additional browser/version combinations via OpenLogic's support channels so long as the browser is a member of the currently supported set of browsers in the AngularJS framework.

6. OpenLogic will proactively monitor the Common Vulnerabilities and Exposures database that is managed and reported by the MITRE Corporation ("MITRE") on its website located at https://www.cve.org/ and, optionally, other reporting sources, for common vulnerabilities and exposures ("CVEs") against the AngularJS Framework. OpenLogic will provide patches to the affected Supported Framework for CVEs that: (i) have a Common Vulnerability Scoring System (Version 3.1, released June 2019) ("CVSS") score of 4.0 or higher; and (ii) are remotely exploitable (via the standard http/s protocols against a website with integrated AngularJS framework directives). For all other CVEs that are not remotely exploitable, OpenLogic will work with the Customer to determine the mitigation path for such CVEs, and OpenLogic will make commercially reasonable efforts to

implement repairs in the affected Supported Frameworks. OpenLogic will then test any generated fixes and, if viable, provide the Customer with patches via OpenLogic's private repositories. For purposes of clarity, and for the avoidance of doubt, all patches, fixes, or repairs generated by OpenLogic for the Supported Frameworks under the LTS contracts are not cross-ported against other possible major/minor/patch AngularJS framework versions. Additional details about OpenLogic's technical support process, response times, and priority of the severity of reported issues for LTS contracts for the Supported Frameworks are provided on Exhibit A of these Terms.

7. Customer may report what the Customer believes to be a Medium Severity (CVSS Base Score of 4.0 – 6.9) or High Severity (CVSS Base Score of 7.0 or higher) vulnerability to OpenLogic via the standard OpenLogic support channels. If the reported vulnerability has not yet been discovered or reported on the CVE website located at https://www.cve.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 has been demonstrated, if OpenLogic considers the Customer-reported vulnerability to be of sufficient severity to require a fix, repair, patch, or mitigation, OpenLogic will treat the vulnerability as if it were a CVE and will provide LTS to the Customer for the applicable Supported Framework for such vulnerability as set forth in Section 6 above.

8. EXCEPT AS PROVIDED IN SECTION 6 OF THESE TERMS, ROGUE WAVE MAKES NO OTHER REPRESENTATIONS OR WARRANTIES, AND ROGUE WAVE, ON BEHALF OF ITSELF AND ITS AFFILIATES, 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 ROGUE WAVE 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-MONTH PERIOD BY CUSTOMER TO ROGUE WAVE PURSUANT TO THESE TERMS.

9. Either party will have the right to terminate these Terms 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 written notification of intent to terminate was given unless the breaching party has corrected the breach prior to the end of such ten (10)-day period. Upon termination of these Terms, OpenLogic will disable Customer's access to the 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 OpenLogic, Customer shall not be entitled to a refund of any prepaid fees upon termination of these Terms, and OpenLogic, will not release Customer from its obligations to pay OpenLogic all fees that are due and owing under these Terms prior to its termination. These Terms may be executed in one or more counterparts each of which will be deemed an original, but all of which when taken together will constitute one and the same instrument. The parties may transmit their signatures via scanned PDF, e-signature, or other electronic signature tools with the same effect as if the parties had provided each other with original signatures.

[The Remainder of this Page is Intentionally Left Blank]

IN WITNESS WHEREOF, the parties to these Terms have executed these Terms to be effective as of the Effective Date.

ROGUE WAVE:

ROGUE WAVE SOFTWARE, INC.

By: _____

Name: _____

Title: _____

Date: _____

CUSTOMER:

_____

Please insert the legal name of the Customer above

By: _____

Name: _____

Title: _____

Date: _____

EXHIBIT A
ADDITIONAL SUPPORT DETAILS FOR ANGULARJS SUPPORTED FRAMEWORKS

1. **Support Channels**. If the Customer has an issue or questions related to the AngularJS patches, 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 "***AngularJS 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 located at: https://www.perforce.com/software-support-agreements.

2. **Patch availability**. OpenLogic categorizes CVEs for the Supported Frameworks using three (3) levels of priority as described below. Each priority level is associated with a different level of service.

2.1. **P0.** A priority **P0** designation encompasses all CVEs that possess either a proof of concept or a publicly available exploit with a CVSS score equal to or greater than 9.0. OpenLogic hereby commits to the following actions with respect to **P0** CVEs:

2.1.1. Provide the Customer with a patch release or workaround within fourteen (14) calendar days from the time the CVE details have been published. This is a target timeframe, and when a patch release or workaround cannot reasonably be provided within this timeframe due to architectural changes or the introduction of breaking changes and risks, OpenLogic will provide the Customer with a written explanation.

2.2. **P1**. A priority **P1** designation encompasses all CVEs that possess either a proof of concept or a publicly available exploit with a CVSS 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:

2.2.1. Provide a patch release or workaround within thirty (30) calendar days from the time the CVE details have been published. This is a target timeframe, and when a patch release or workaround cannot reasonably be provided in this timeframe due to architectural changes or the introduction of breaking changes and risks, OpenLogic will provide the customer with a written explanation.

2.3. **P2**. A priority **P2** designation encompasses all CVEs that possess either a proof of concept or a publicly available exploit with a CVSS score greater than or equal to 4.0 but less than 7.0. OpenLogic hereby commits to the following actions with respect to **P2** CVEs:

2.3.1. 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 reasonably be provided due to architectural changes or the introduction of breaking changes and risks, OpenLogic will provide the Customer with a written explanation.