LICENSE AND SUPPORT AGREEMENT

This License and Support Agreement ("**Agreement**") is entered into as of the date last signed ("**Effective Date**") between Graylog, Inc., a Delaware corporation, located at 1301 Fannin St., Suite 2140, Houston, TX 77002 ("**Graylog**"), and the customer executing this Agreement ("**Customer**"). Graylog and Customer agree as follows:

1. Definitions.

1.1. "Customer Application(s)" means Customer's proprietary application(s) (i) as to which Customer deploys the Software under this Agreement and (ii) that are deployed by or on behalf of Customer in a production environment.

1.2. "Customer Content" means any data that is ingested by or on behalf of Customer into Graylog Software from Customer's internal data sources.

1.3. "Customer Network" means the hardware and software components within Customer's internal computer network at Customer's designated location or that of Customer's designated hosting provider.

1.4. "Daily Volume Limit" means the number of gigabytes of data per day as specified in the Order Form that customer may process using the Software under this Agreement.

1.5. "Documentation" means any written, electronic, or recorded work, if any, provided by Graylog to Customer, that describes the functions and features of the Software.

1.6. "Fees" means the fees described on each Order Form.

1.7. "Graylog Content" or "Third Party Content" means any Graylog or Third Party user generated configuration, including data processing rules, dashboards, alerts, and event definitions, saved searches, reports, or log collector configuration.

1.8. "Hosted Service" means a technology service hosted by or on behalf of Graylog and provided to Customer. These are services described on **Schedule C.**

1.9. "Order Form" means a document executed by Graylog and Customer pursuant to which Customer orders Software and Support Services hereunder. The initial Order Form is attached as **Schedule A** hereto.

1.10. "Service Level Schedule" means a Graylog policy that applies to the availability and uptime of a Hosted Service and which, if applicable, offers service credits as set forth therein.

1.11. "Software" means the computer software applications listed on any Order Form executed in connection with this Agreement, including any Updates thereto.

1.12. "Subscription Term" means the term for the license grant and Support Services that is specified on each Order Form.

1.13. "Support Services" means the services described on **Schedule B.**

1.14. "Updates" means subsequent releases of the Software and/or the Documentation provided hereunder, such as (a) bug or error fixes, patches, workarounds, and maintenance releases, and (b) releases that introduce new and significant features and functionality.

2. License.

2.1. Grant of License. Subject to the terms and conditions of this Agreement, Graylog hereby grants to Customer a limited, non-sublicensable, non-exclusive, non-transferable license during the applicable Subscription Term to: (a) install, or have installed, the Software within the Customer Network, and (b) use the Software in accordance with the Documentation within the Customer Network in accordance with the Software's normal and intended use and subject to applicable user license limits and the Daily Volume Limits as specified in the applicable Order Form,.

2.2. License Restrictions. Access to and use of the Software may be limited by restrictions set forth in the applicable Order Form, including, without limitation, a specific number of gigabytes or other applicable volume metrics defined therein. Licensee shall not circumvent these limitations. Unless otherwise specified in this Agreement or in another agreement between the parties, Customer may not: (a) modify, disassemble, de-compile, reverse engineer, or otherwise attempt to determine the source code or protocols from the object code of the Software, or knowingly permit or encourage any third party to do so, (b) use the Software in any manner to provide service bureau, time-sharing or other computer services to third parties, (c) use the Software in any manner to assist or take part in the development, marketing, or sale of a product potentially competitive with the Software, or (d) use the Software or allow the transfer, transmission, export, or re-export of the Software or portion thereof in violation of any export control laws or regulations administered by any government agency.

2.3. Limited Rights. Customer's rights in the Software will be limited to those expressly granted in this Section 2. Graylog reserves all rights and licenses in and to the Software not expressly granted to Customer.

3. Hosted Services.

3.1. Service Levels. When Customer purchases the Hosted Service, Graylog will make the applicable Hosted Services available to the Customer during the Term in accordance with these General Terms. The specific Service Level is defined in Schedule C (Specific Hosted Service Terms), which includes the Service Level Schedule and the associated remedies that will apply to the availability and uptime of the Hosted Service. If applicable, service credits will be available for downtime in accordance with the Service Level Schedule.

3.2. Data Protection. Schedule D sets forth Graylog's security and data protection programs for the Hosted Services.

3.3. Maintaining Protections. Notwithstanding anything to contrary in these General Terms, or any policy or terms referenced herein or any update thereto, Graylog may not, during a Term, materially diminish the security protections provided by the controls set for the Hosted Service.

3.4. Connections. Customer is responsible for obtaining and maintaining all telecommunications, broadband and computer equipment and services needed to access and use Hosted Services, and for paying all associated charges therefor.

3.5. Customer Responsibility for Data Protection. Customer is responsible for: (i) selecting and applying the security configurations and security options made available by Graylog in connection with a Hosted Service; (ii) taking additional measures outside of the Hosted

Service to the extent the Hosted Service Offering does not provide the controls that may be required or desired by Customer; and (iii) routine archiving and backing up of Customer Content. Customer agrees to notify Graylog immediately if Customer believes that an unauthorized third party may be using Customer accounts or if Customer account information is lost or stolen.

3.6. Refund Upon Termination for Graylog's Breach. If a Hosted Service is terminated by Customer for Graylog's uncured material breach in accordance with these General Terms, Graylog will refund Customer any prepaid subscription fees covering the remainder of the Term after the effective date of termination.

3.7. Customer Content. Customer owns and reserves all right, title and interest in their own Customer Content. By sending Customer Content to a Hosted Service, Customer grants Graylog and its authorized licensors or service providers providing any part of the Hosted Services a worldwide, royalty free, non-exclusive license to access and use the Customer Content for purposes of providing Customer the Hosted Service.

3.8. Return of Customer Content. Customer Content may be retrieved by Customer and removed from the Hosted Services in accordance with the then current applicable Documentation. Graylog will make the Customer Content available on the Hosted Services for thirty (30) days after termination of a subscription for Customer retrieval. After that thirty (30) day period, Graylog will have no obligation to maintain the storage of Customer Content, and Customer hereby authorizes Graylog thereafter to delete all remaining Customer Content, unless Graylog is otherwise legally prohibited from doing so. If Customer requires assistance in connection with migration of Customer Content, depending on the nature of the request, Graylog may require a mutually agreed upon fee for assistance.

3.9. Specific Hosted Services Terms. Specific security controls and certifications, data policies, service descriptions, Service Level Schedules, and other terms specific to Hosted Services ("**Specific Hosted Services Terms**") are set forth in Schedule C.

4. Support Services.

4.1. Support Services. Subject to the timely payment of the applicable Fees (as defined below), Graylog will use commercially reasonable efforts to provide Support Services during the applicable Subscription Term at the support level purchased pursuant to the Order Form and in accordance with Schedule B.

4.2. Subcontracting. Graylog reserves the right to subcontract all or part of the Support Services, provided that Graylog shall remain responsible for performance of such services by its subcontractors.

5. Fees and Payment.

5.1. License and Support Fees. Customer shall pay Graylog the applicable fees specified in each Order Form (the "**Fees**"), provided that if Customer registers for a free trial or beta version of the Software, the Software will be offered to Customer free of charge during the trial or beta period indicated at the time of registration. Unless otherwise set forth in the applicable Order Form, the Fees for the initial Subscription Term shall be due and payable upon the execution of the applicable Order Form.

5.2. Payment Terms. Except as otherwise set forth herein, all Fees are nonrefundable and payable in United States dollars. Should Customer not pay any amounts when due, Graylog may (at its discretion and in addition to other remedies it may have) suspend Customer's and its authorized users' access to the Service. Customer shall pay Graylog a late fee of one and one half percent (1.5%) per month or the highest rate allowable by law,

whichever is lower, on all past due amounts, such late fee to be compounded monthly. The Fees payable under this Agreement shall not include local, state, or federal sales, use, value-added, excise or personal property or other similar taxes or duties and any such taxes shall be assumed and paid by the Customer except those taxes based on the net income of Graylog. Customer shall not set-off or offset against Graylog's invoices amounts that Customer claims are due to it. Customer will bring any claims or causes of action it may have in a separate action and waives any rights it may have to offset, set-off, or withhold payment for Software or Support Services delivered or provided by Graylog.

6. Daily Volume Limits. From time to time, the Software will communicate to Graylog the volume of data processed by Customer through the Software beginning at 12:00 and 0 seconds AM and ending at 11:59 and 59 seconds PM. On a monthly basis, beginning the first day of each calendar month and ending on the final day of each calendar month, Graylog will provide Customer with notice of the daily volume processed by Customer through the Software. If the Customer exceeds the Daily Volume Limit 5 times or more during any month, Customer, at Graylog's request, shall negotiate in good faith with Graylog on appropriate amendments to the pricing and other relevant terms of this Agreement that are consistent with Customer's actual use of the Software. Notwithstanding the foregoing sentence, Customer acknowledges and agrees that exceeding the Daily Volume Limit constitutes a material breach of this Agreement.

7. Ownership. The license granted in Section 3 confers no ownership rights to Customer and is not a sale of any rights in the Software, the Documentation, the media on which either is recorded or printed, or in any intellectual property rights of Graylog. Graylog shall own and retain ownership of all right, title, and interest in and to (i) the Software and any copies thereof; (ii) the Documentation and any copies thereof; (iii) any ideas, suggestions, or feedback relating to the Software and Documentation ("**Feedback**"); and (iv) all intellectual property rights embodied within the foregoing (i)-(iii). Customer hereby irrevocably assigns and agrees to assign all of its right, title, and interest in and to any Feedback to Graylog.

8. Confidentiality of this Agreement.

   8.1. Confidential Information – Defined. **Confidential Information**" means non-public information that is transmitted or otherwise provided by or on behalf of a party to this Agreement (the **"Disclosing Party"**) to the other party (the **"Receiving Party"**) in connection with this Agreement and the activities hereunder, and that should reasonably be understood by the Receiving Party to be Confidential Information due to the nature of such information or the presence of legends or other markings (including, but not limited to, "Confidential" and "Restricted") to be proprietary and confidential to the Disclosing Party. Confidential Information includes, but is not limited to, the terms, conditions and pricing under this Agreement and information related to the performance of the Software. Confidential Information of Graylog includes, without limitation, the Software, all software provided with the Software, Documentation, the source code, and all algorithms, methods, techniques, and processes revealed by the source code. Confidential Information does not include information that: (a) was in the possession of, or was rightfully known by, the Receiving Party without an obligation to maintain its confidentiality prior to receipt from Disclosing Party, as evidenced by the Receiving Party's written records; (b) is or becomes generally known to the public without violation of this Agreement; (c) is obtained by the Receiving Party in good faith from a third party having the right to disclose it without an obligation of confidentiality; or (d) was developed by the Receiving Party independently of and without reference to Confidential Information, as evidenced by the written records of the Receiving Party.

   8.2. Nondisclosure Obligations. Each party to this Agreement may furnish the other party with Confidential Information. The parties agree that, during the term of this Agreement and thereafter, each Receiving Party will hold Confidential Information of the Disclosing Party in confidence and shall not (a) directly or indirectly use, copy, reproduce, distribute,

manufacture, duplicate, reveal, report, publish, disclose or cause to be disclosed, or otherwise transfer any Confidential Information of the Disclosing Party to any third party, or (b) utilize Confidential Information for any purpose, except the performance of its obligations under this Agreement or as authorized in writing by the Disclosing Party. Each Receiving Party will limit the disclosure of Disclosing Party's Confidential Information to its employees, third party contractors or consultants with a need-to-know and who have been advised of the confidential nature thereof and who are contractually obligated to maintain such confidentiality through execution of a nondisclosure agreement that is at least as protective as the terms and conditions of this Agreement. The Receiving Party shall provide copies of these agreements upon the written request of the Disclosing Party. Each Receiving Party shall be liable for any breach by any of its employees, third party contractors or consultants of the confidentiality obligations contained herein.

8.3. Required Disclosures. In the event a Receiving Party is required under applicable law, rule, regulation, court, or administrative order to disclose Confidential Information of the Disclosing Party, the Receiving Party shall use commercially reasonable efforts to: (a) give at least ten (10) days prior written notice of such disclosure to the Disclosing Party; (b) limit such disclosure to the extent practicable; and (c) make such disclosure only to the extent so required.

8.4. Terms. Neither Party will disclose the terms of this Agreement, other than to business, financial, or legal advisors, without the express written consent of the other Party. However, a Party may disclose the terms of this Agreement as required under United States law or applicable securities regulations, or in furtherance of a proposed sale, acquisition, or merger of substantially all of the Party's business interests related to this Agreement as long as such disclosure is made under a duty of confidentiality.

8.5. Customer Identification; Logo. Customer agrees that Graylog may identify Customer as a customer verbally, in print, and on its corporate web site. Customer agrees that Graylog may display Customer's name and logo (within Customer's logo usage guidelines as may have been provided to Graylog), and link to the customer web site.

9. Warranties.

9.1. Limited Support Warranty. Graylog warrants that the Support Services shall be performed in a professional and workmanlike manner. This warranty covers only problems reported to Graylog during the Subscription Term. The remedy and Graylog's entire liability for any breach of the foregoing warranty is set forth in Section 9.2 below.

9.2. Limited Software Warranty. Graylog warrants that, for a period of ninety (90) days following the Effective Date, the Software shall perform substantially in accordance with its specifications as set forth in the Documentation. Customer will notify Graylog in writing of any non-conformity with the warranty specified in this Section 9.2, which notice shall include a detailed description of the non-conformity such that Graylog can reproduce the non-conformity. Upon receipt of such written notice, Graylog shall, at its expense, promptly repair, replace, or modify the affected Software so that it is compliant. If Graylog determines that it is not commercially feasible to repair, replace or modify the affected Software so that it is compliant, Graylog may terminate the license to use the non-confirming Software and refund to Customer the portion of prepaid Fees that relate to the remaining portion of the then-current Subscription Term. THIS SECTION 9.2 SETS FORTH CUSTOMER'S SOLE AND EXCLUSIVE REMEDY FOR ANY BREACH OF THE WARRANTY SET FORTH IN THIS SECTION 9.2. The limited warranty in Section 9.2 is void and shall not apply: (a) if the Software is not used in accordance with the Documentation or this Agreement; (b) the non-conformity results from accident, abuse, misuse, or misapplication of the Software; (c) if the Software has been customized,

modified, enhanced, or altered (other than by Graylog); or (d) if Customer is not using the most recent Updates to the Software.

9.3. Hosted Services Warranty. Graylog warrants that during the applicable Term: (i) Graylog will not materially decrease the overall functionality of the Hosted Services; and (ii) the Hosted Services will perform materially in accordance with the applicable Documentation. Graylog's sole and exclusive liability, and Customers sole and exclusive remedy for any breach of these warranties, will be Customer's right to terminate the Hosted Services, and Graylog will refund to Customer any prepaid but unused Fees for the remainder of the Term.

9.4. Disclaimer of Warranties. EXCEPT FOR THE EXPRESS WARRANTIES SET FORTH IN THIS SECTION 9, GRAYLOG MAKES NO WARRANTIES, EXPRESS OR IMPLIED, WITH RESPECT TO THE SUPPORT SERVICES, HOSTED SERVICES, THE SOFTWARE OR THE DOCUMENTATION OR ANY OTHER SERVICES SUPPLIED BY GRAYLOG, ITS RESELLERS, OR ITS AGENTS, AND GRAYLOG HEREBY EXPRESSLY DISCLAIMS ANY IMPLIED WARRANTIES, INCLUDING WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INTERFERENCE, ACCURACY OF DATA, AND NON-INFRINGEMENT.

10. Customer Indemnity. Customer will indemnify Graylog and, at its option, defend any action brought against Graylog to the extent that it is based upon a third party claim arising out of any Customer Application, or which result from Graylog's compliance with Customer's designs, specifications, or instructions, and will pay any costs, damages and reasonable attorneys' fees attributable to such claim that are awarded against Graylog.

11. Graylog Indemnity

11.1. Infringement Indemnification. Subject to the terms of this Section 11, Graylog shall indemnify and defend Customer against any claim brought against Customer by third parties alleging the use of the Software or Documentation (a) infringes a United States patent, copyright or trademark registered as of the date Graylog provides Customer with the Software, or (b) misappropriates any third party trade secret (collectively, an "**Infringement Claim**"); provided, however, that (i) Customer gives Graylog prompt notification in writing of any such Infringement Claim and reasonable assistance, at Graylog's expense, in the defense of such Infringement Claim; and (ii) Graylog has the sole authority to defend or settle such Infringement Claims so long as any such settlement shall not include a financial obligation on, or an admission of liability by, Customer.

11.2. Indemnification Limitations. Graylog shall have no obligation for any Infringement Claim arising out of or relating to: (a) any modification created by or at the direction of Customer; (b) use of the Software other than in accordance with the Documentation and/or the terms of this Agreement; (c) use of a release of the Software no longer supported by Graylog; (d) use of the Software without Customer's implementation of all applicable Updates; (e) any third-party software; or (f) use of the Software in combination with any other hardware, software or other materials where, absent such combination, the Software would not be the subject of the Infringement Claim.

11.3. Effect of Infringement Claim. If an Infringement Claim is or, in Graylog's reasonable belief, is likely to be asserted, (a) Graylog may require Customer to discontinue use of the Software immediately and Customer shall comply with such requirement; and (b) Graylog will, at its sole option, either (i) procure for Customer the right to use and exercise its rights with respect to the Software or Documentation or affected part thereof as provided in this Agreement; (ii) replace the Software or Documentation or affected part thereof with other non-infringing products or (iii) modify the Software or Documentation or affected part

thereof to make it not infringing while retaining substantially similar functionality; or (c) if the remedies set forth in clause (b) are not commercially feasible, as determined by Graylog in its sole discretion, terminate this Agreement, in whole or in part, and the licenses granted pursuant to it, and refund to Customer the portion of prepaid Fees that relate to the remaining portion of the then-current Subscription Term.

11.4. Exclusive Remedy. THE PROVISIONS OF THIS SECTION 11 STATES THE SOLE, EXCLUSIVE, AND ENTIRE LIABILITY OF GRAYLOG TO CUSTOMER, AND IS CUSTOMER'S SOLE REMEDY WITH RESPECT TO, ANY CLAIM OF INFRINGEMENT OR MISAPPROPRIATION OR ALLEGED INFRINGEMENT OR MISAPPROPRIATION OF ANY THIRD-PARTY PATENT, COPYRIGHT, TRADMARK, TRADE SECRET OR OTHER INTELLECTUAL PROPERTY RIGHT.

12. Limitation of Liability.

12.1. Disclaimer of Consequential Damages. IN NO EVENT WILL EITHER PARTY BE LIABLE TO THE OTHER PARTY FOR ANY SPECIAL, INDIRECT, INCIDENTAL OR CONSEQUENTIAL DAMAGES (INCLUDING LOSS OF USE, DATA, BUSINESS OR PROFITS) ARISING OUT OF OR IN CONNECTION WITH THIS AGREEMENT, OR THE USE OR PERFORMANCE OF THE SOFTWARE OR SERVICES, WHETHER SUCH LIABILITY ARISES FROM ANY CLAIM BASED UPON CONTRACT, WARRANTY, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY OR OTHERWISE, AND WHETHER OR NOT SUCH PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE. GRAYLOG SHALL HAVE NO LIABILITY FOR CUSTOMER'S PROVISION OF ITS OWN SERVICES TO ITS CUSTOMERS.

12.2. Aggregate Liability. IN NO EVENT WILL EITHER PARTY'S CUMULATIVE LIABILITY TO THE OTHER PARTY, FROM ALL CAUSES OF ACTION AND ALL THEORIES OF LIABILITY, EXCEED THE AGGREGATE AMOUNT PAID OR OWED TO GRAYLOG BY CUSTOMER DURING THE ONE (1) YEAR PRECEDING THE DATE ON WHICH THE CAUSE OF ACTION ACCRUED. THE FOREGOING LIMITATIONS WILL APPLY NOTWITHSTANDING THE FAILURE OF ESSENTIAL PURPOSE OF ANY LIMITED REMEDY HEREIN.

FOR THE AVOIDANCE OF DOUBT, THE FOREGOING LIMITATION WILL NOT LIMIT CUSTOMER OBLIGATIONS UNDER THE "FEES AND PAYMENT" SECTION ABOVE AND WILL NOT BE DEEMED TO LIMIT CUSTOMER RIGHTS TO ANY SERVICE LEVEL CREDITS UNDER ANY APPLICABLE SERVICE LEVEL SCHEDULE. FURTHERMORE, THE CAP ABOVE WILL NOT BE DEEMED TO LIMIT GRAYLOG'S RIGHT TO RECOVER AMOUNTS FOR CUSTOMERS USE OF THE SOFTWARE IN EXCESS OF THE CAPACITY PURCHASED OR USE OUTSIDE OF INTERNAL BUSINESS PURPOSES.

13. Term and Termination.

13.1. Term. This Agreement will begin on the Effective Date and will remain in effect through the end of each Subscription Term that is set forth in an Order Form, unless this Agreement is earlier terminated in accordance with this Section 13.

13.2. Termination for Breach. Each party will have the right to terminate this Agreement or any Software license granted hereunder if the other party breaches any material term of this Agreement and fails to cure such breach within thirty (30) days (five (5) days in the case of non-payment) after written notice thereof.

13.3. Termination for Insolvency: Graylog may terminate this Agreement if Customer ceases to conduct business in the normal course, becomes insolvent, enters into a suspension of payments, moratorium, reorganization or bankruptcy, makes a general assignment for the

benefit of creditors, admits in writing its inability to pay debts as they mature, suffers or permits the appointment of a receiver for its business or assets, or avails itself of or becomes subject to any other judicial or administrative proceeding that relates to insolvency or protection of creditors' rights.

13.4. Effect of Termination. Upon any termination of this Agreement, all amounts due and owing by Customer to Graylog under this Agreement and all Order Forms will be immediately payable and all Support Services and Software licenses granted pursuant to this Agreement shall immediately terminate. At such time, Customer will promptly return the Software to Graylog or destroy the Software and all copies and portions thereof, in all forms and types of media, and, at Graylog's request, provide Graylog with an officer's written certification, certifying to Customer's compliance with the foregoing.

13.5. Survival. The rights and obligations of the Parties contained in Sections 5 (as to amounts owed as of termination), 7, 8, 9.4, 10, 11, 12, 13.4, 13.5 and 14 will survive the termination of this Agreement.

14. General.

14.1. Purchasing through Authorized Reseller. If Customer purchases through a Graylog authorized reseller, these General Terms will govern those Offerings. Customer payment obligations for the Purchased Offerings will be with the authorized reseller, not Graylog. Customer will have no direct Fee payment obligations to Graylog for those Offerings.

Any terms agreed to between Customer and the authorized reseller that are in addition to these General Terms are solely between Customer and the authorized reseller. No agreement between Customer and an authorized reseller is binding on Graylog or will have any force or effect with respect to the rights in, or the operation, use or provision of, the Software, Support Services or Hosted Services.

14.2. Governing Law and Jurisdiction. This Agreement will be governed by and construed in accordance with the laws of the State of Texas without regard to its conflicts of laws provisions. Any legal action or proceeding arising under this Agreement will be brought exclusively in the federal or state courts applicable to Harris County, Texas and the Parties hereby consent to personal jurisdiction and venue therein.

14.3. Open Source Software. In order to use the Software, Customer may need to install on its Customer Network certain other software or components that are available in the public domain (the "**Open Source Software**"). Graylog has no proprietary interest in or to such Open Source Software and the Open Source Software is not licensed under this Agreement. Customer's rights in the Open Source Software are governed by and subject to the terms and conditions set forth in their applicable license(s).

14.4. Audit Rights. Graylog may, at its expense, audit Customer's records and its installation and use of the Software to evaluate compliance with this Agreement. Any such audit shall be conducted during regular business hours at Customer's facilities after five (5) days prior written notice, shall be limited to records relevant to installation and use of the Software, compliance with the terms of this Agreement and calculation of fees hereunder and shall not unreasonably interfere with Customer's business. Audits shall be conducted no more than once annually. If an audit reveals that Customer has underpaid applicable fees to Graylog, Customer shall be invoiced for such underpaid fees, which shall be due and payable within fifteen (15) days of receipt of such invoice. If the underpayment of fees exceeds five percent (5%), Customer shall reimburse Graylog for all reasonable costs incurred to conduct the audit.

14.5. Relationship of Parties. The Parties to this Agreement are independent contractors and this Agreement will not establish any relationship of partnership, joint venture, employment, franchise, or agency between the Parties. Neither Party will have the power to bind the other or incur obligations on the other's behalf without the other's prior written consent.

14.6. Equitable Relief. The Parties agree that a material breach of the license or confidentiality provisions of this Agreement would cause irreparable injury to Graylog for which monetary damages would not be an adequate remedy, and therefore Graylog shall be entitled to equitable relief in addition to any other remedies it may have hereunder or at law.

14.7. Force Majeure. Neither Party shall be deemed to have breached any provision of this Agreement as a result of any delay, failure in performance, or interruption of service resulting directly or indirectly from acts of God, network failures, acts of civil or military authorities, civil disturbances, wars, terrorism, energy crises, fires, transportation contingencies, interruptions in third-party telecommunications or Internet equipment or service, other catastrophes, or any other occurrences which are beyond such Party's control.

14.8. Government Use. The use, duplication, reproduction, release, modification, disclosure, or transfer ("use") of the Software and the Documentation, no matter how received by the United States Government, is restricted in accordance with the terms and conditions contained in this Agreement. All other use is prohibited. Further, the Software and the Documentation was developed at Graylog's private expense and is commercial in nature. By using, receiving, or downloading the Software and the Documentation, the Government user agrees to the terms and conditions contained in this license agreement including the terms and conditions contained in this paragraph.

14.9. Export Control. Customer acknowledges that the Software and all related technical information, documents and materials are subject to export controls under applicable laws, including, without limitation, the U.S. Export Administration Regulations, and Customer shall comply with all applicable export control laws, rules, and regulations.

14.10. Assignment. Customer may not assign this Agreement, in whole or in part, without Graylog's prior written consent. Graylog may assign this Agreement in its discretion. Any purported assignment in violation of this section shall be null and void. This Agreement shall be binding on all permitted assignees.

14.11. Severability. The invalidity or unenforceability of any provision of this Agreement shall not affect the validity or enforceability of any other provision of this Agreement.

14.12. Waiver. The failure of either Party to enforce at any time the provisions of this Agreement, or the failure to require at any time performance by the other Party of any of the provisions of this Agreement, shall in no way be construed to be a present or future waiver of such provisions, nor in any way affect the ability of either Party to enforce each and every such provision thereafter. The express waiver by either Party of any provision, condition or requirement of this Agreement shall not constitute a waiver of any future obligation to comply with such provision, condition, or requirement.

14.13. Entire Agreement. This Agreement, including any and all exhibits attached hereto, is the entire agreement of the Parties and supersedes any prior representations, agreements, negotiations, or understandings between them, whether written or oral, with respect to the subject matter hereof. No waiver, alteration, or modification of any of the provisions of this Agreement shall be binding unless in writing and signed by duly authorized representatives of the Parties hereto. In the event of a conflict between any applicable Order Form and this Agreement, the Order Form shall control. This Agreement (including each Order Form)

supersedes any conflicting or additional terms and conditions set forth on any purchase order, work order, or similar commercial document which may be issued by Customer.

14.14. Notices. All notices required or permitted under this Agreement will be in writing and delivered by email, confirmed facsimile transmission, by courier or overnight delivery service, or by certified mail, and in each instance will be deemed given upon receipt. All communications will be sent to the addresses set forth below or to such other address as may be specified by either Party to the other in accordance with this section. Either Party may change its address for notices under this Agreement by giving written notice to the other Party by the means specified in this section.

14.15. Counterparts. This Agreement may be signed in counterparts, each of which shall be deemed an original and which shall together constitute one and the same Agreement. The exchange of copies of this Agreement in electronic format (e.g. in "pdf" format) shall constitute effective execution and delivery of this Agreement as to the parties and may be used in lieu of the original Agreement for all purposes.

The Parties hereby execute this License and Support Agreement as of the Effective Date.

GRAYLOG, INC.:	**CUSTOMER**:
By:	By:
Print Name:	Print Name:
Title:	Title:
Date:	Date:
Address for Notices 1301 Fannin St., Suite 2140, Houston, TX 77019	Address for Notices: _____ _____

Schedule A

Initial Order Form

This Order Form incorporates by reference and is governed by the terms and conditions of the License and Support Agreement between the signatories hereto dated _____, 20__ ("**Agreement**"). This Order Form is effective as of _____, 20__ ("**Order Effective Date**").

Graylog and Customer agree to this Order Form, as follows:

1. Subscription Term

Subscription Term: [___] years
Subscription Term Start Date: [_____]

Unless cancelled by one party by giving written notice of cancellation to the other party no less than ninety (90) days prior to the end of the then-current Subscription Term, the Subscription Term shall automatically extend for an additional year. Graylog's then-current list prices shall apply to any renewal period.

2. **Software or Hosted Service**:

Software or Hosted Service	Daily Volume Limit

3. Support Services

SUPPORT INFORMATION:

Support Level (check one):

[ ] Graylog Enterprise Support

4. Fees

[$_____], which includes the license to use the Software and Support Services during the Subscription Term. The Fees for the initial Subscription Term are due and payable on the Order Effective Date.

Additional Terms: None

The Parties hereby execute this Order Form as of the date last written below.

Graylog, Inc.:	Customer:
By:	By:
Print Name:	Print Name:
Title:	Title:
Date:	Date:

Schedule B

Description of Support Services

1. **Description of Support Services**. Upon payment of the fees set forth in the Order Form and during the term for which Customer is subscribed for Support Services (and current on all fees), Graylog shall perform the Support Services set forth below.

   Following is a description of the Support Services. The level of Support Services to which customer is subscribed set forth in the Order Form:

   Enterprise: Support Hours: 3:00 AM to 8:00 PM Eastern, Monday through Friday
   Unlimited number of support inquiries
   6 Support Services contacts within Customer's organization

2. **Methods of Support**.

   a. Jumpstart. Graylog will provide a one-hour offsite Jumpstart support session to Customer as soon as reasonably practical after the Effective Date, regardless of the Subscription Level. Graylog may, at its discretion, offer onsite support, which may incur additional fees.

   b. Training. Formal training is not included in the Jumpstart session. Additional training is available and may incur additional fees.

   c. General. Graylog may provide telephone assistance to Customer at telephone numbers designated by Graylog.

   d. Preparing for Call. Customer should have the following information and materials ready when calling for support: (a) customer number, (b) product version, and (c) direct access to the network device (if possible) with the error.

   e. Remote Support. Graylog may provide remote assistance to Customer via a Customer or Graylog provided remote collaboration tool.

   f. Support Contact. The Customer's primary point of contact for Support Services under this Agreement is:

   Contact name: _____
   Email: _____
   Phone: _____

   g. First Level Support/Single Point of Contact. All communications relating to the Support Services shall be supervised, coordinated, and undertaken by no more than 1 designated contact person, in accordance with Customer's Subscription Level, for each separate support inquiry who shall act as a single point of contact between Customer and Graylog.

3. **Maintenance Services**.

   a. Description. Upon payment of the fees set forth in the Order Form and during the term for which Customer is subscribed for Support Services (and current on all fees), Graylog shall provide Customer with Updates generally released to customers during the applicable Subscription Term. Such Updates shall be provided to Customer at no additional charge.

b. Limitations. Except for Updates, Customer shall not be entitled to any other software as part of Support Services. Graylog shall offer Support Services on the current version and immediately prior released version of the Software in accordance with Graylog's lifecycle and/or end-of-life policy unless Customer and Graylog otherwise enter into a mutually agreeable written agreement for additional Support Services. If Customer notifies Graylog of a problem and Graylog determines that the problem is due to Customer's incorrect or improper use of the Software or failure to comply with the terms of this Agreement (as opposed to a defect in the Software), Graylog may enter into a mutually agreed work order for Graylog to correct the problem, under which Customer would pay Graylog its then current time and materials rate for all services provided and all expenses associated with performance of those services, whether or not the problem is corrected. Graylog shall have no responsibility for loss of or damage to Customer's data, regardless of the cause of any such loss or damage. Customer shall take all necessary steps to back up its data. Standard maintenance and support do not include any on-site services. On-site services may be available for an additional fee. Customer acknowledges and agrees that Updates may require additional training of Customer's personnel.

Schedule C

Specific Hosted Services Terms

1. **Description of Hosted Services**. Graylog Cloud delivers the capabilities of Graylog Enterprise as a cloud-based service. Using Graylog Cloud, Customer gains the functionality of the Graylog Enterprise platform using a cloud service that is delivered and managed by Graylog.

2. **Security.** Graylog maintains administrative, physical, and technical safeguards to protect the security of Customer Content on Graylog Cloud as set forth in the Graylog Cloud Security Addendum in Schedule D.

   Graylog's security safeguards include, without limitation, employee (and contractor, as applicable) security training, background testing and confidentiality obligations. Graylog's security controls adhere to generally accepted industry standards, are subject to audit by third-parties (as described in the Cloud Security Addendum) and are designed to (a) ensure the security and integrity of Customer Content; (b) detect and protect against threats or hazards to the security or integrity of Customer Content; and (c) prevent unauthorized access to Customer Content.

3. **Maintenance.** In order to operate in an efficient and secure manner, the Graylog Cloud Service requires routine maintenance and upgrades. These are Graylog's policies regarding offline periods so that maintenance may be performed.

   3.1. **Routine Maintenance**. Routine Maintenance is performed during the hours of Monday 1 AM through Saturday 1 AM UTC. Routine Maintenance encompasses service changes initiated by Graylog or Customer. For Graylog initiated changes, maintenance is performed at most once per month and Customers will receive notice of Routine Maintenance by email to their registered email address at least 48 hours in advance of scheduled downtime. Customer can accept the assigned maintenance time or request an alternate time within the Routine Maintenance window. Customer will also receive email notice when such maintenance is starting and when complete. For Customer initiated changes, the maintenance can be performed more than once per month and during a time of Customer's choosing within the Routine Maintenance window. Customer will receive email notice when such maintenance is starting and when complete.

   3.2. **Emergency Maintenance**. In circumstances that require immediate attention, Graylog will perform Emergency Maintenance. This service-affecting maintenance is by its very nature not scheduled. Graylog will make commercially reasonable efforts to notify Customers by email to their registered email address should Emergency Maintenance become necessary.

4. **Service Level Commitment**. The Graylog Cloud Services will be available 100% of the time, as measured by Graylog over each calendar quarter of the Subscription Term, and subject to the exclusions set forth. A Graylog Cloud Service is considered available if the Customer is able to login to its Graylog Cloud Service account and initiate a search using Graylog Software.

   4.1. **Service Level Credit**. If Graylog fails to achieve the above Service Level Commitment for the Graylog Cloud Service over a calendar quarter measurement period, Customer may claim a credit for such Graylog Cloud Service as provided below which will result in an extension to the Customer's term.

AVAILABILITY PER CALENDAR QUARTER	CREDIT
100	NO CREDIT
Less than 99.9%	8 Hours
Less than 99.0%	1.5 Days
Less than 95.0%	3 Days

4.2. **Exclusions**. A Customer will not be entitled to a service credit if it is in breach of its Agreement with Graylog, including payment obligations. The Service Level Commitment does not apply to any downtime, suspension, or termination of the applicable Graylog Cloud Service (or any Graylog Content or Graylog Software operating in connection with the Graylog Cloud Service) that results from:

4.2.1. Account suspension or termination due to Customer's breach of the Agreement.

4.2.2. Routine scheduled maintenance as described above.

4.2.3. Graylog's reasonable control, including force majeure events such as acts of God, acts of government, flood, fire, earthquake, civil unrest, acts of terror, Customer Content, Third Party Content or Internet Service Provider failures or delays.

4.2.4. A Customer's equipment, software or other technology, or third-party equipment, software, or technology (other than those which are under Graylog's control).

4.2.5. Failures resulting from software or technology for which Graylog is not responsible under the Agreement.

4.2.6. Customer's ability or inability to operate the Graylog Forwarder software is addressed by Graylog's support services. For purposes of the Service Level Commitment, the Graylog Forwarder software is excluded from the calculation of the availability of the Graylog Cloud Services.

4.3. **Free Trial or POC**. No Service Level Commitment is provided for free, proof-of-concept or unpaid trial services.

4.4. **Service Credit Claims**. To receive a service credit, a Customer must file a claim for such credit within five (5) days following the end of the calendar quarter in which the Service Level Commitment was not met for an applicable Graylog Cloud Service, by contacting Graylog at accounting@graylog.com with a complete description of the downtime, how the Customer was adversely affected, and for how long. Graylog reserves the right to deny the service credit if the Customer does not qualify. The service credit remedy set forth in this Service Level Schedule is the Customer's sole and exclusive remedy for the unavailability of any applicable Graylog Cloud Service.

5. **Data Usage Policy for Graylog Cloud.** For Subscriptions based on Daily Volume Limit, Customer can exceed the purchased daily index volume a maximum of five times in a calendar month, up to a maximum of two times the volume of their contracted Daily Volume Limit in aggregate over the calendar month. Without limiting Graylog's foregoing rights, with respect to Hosted Services, Graylog may work with Customer to reduce usage so that it conforms to the applicable usage limit, and Graylog will in good faith discuss options to right size Customer's subscription as appropriate. For the avoidance of doubt, notwithstanding anything to the contrary herein, Graylog will have the right to directly invoice Customer for overages, regardless of whether Customer purchased the Hosted Service from an authorized reseller.

Schedule D

Graylog Cloud Security Addendum

This Graylog Cloud Security Addendum (CSA) sets forth the administrative, technical, and physical safeguards Graylog takes to protect Customer Content in Graylog Cloud. Graylog may update this CSA from time to time to reflect changes in Graylog's security posture, provided such changes do not materially diminish the level of security herein provided.

This CSA is made a part of Customer Terms of Service with Graylog. In the event of any conflict between the terms of the Agreement and this CSA, this CSA will control. This CSA applies to Graylog Cloud environments initially provisioned on or after the Effective Date, including without limitation Trial or Beta Services.

1. Purpose

    1.1. This CSA describes the minimum information security standards that Graylog maintains to protect Customer Content. Requirements in this CSA are in addition to any requirements in the Agreement.

    1.2. The CSA is reasonably designed to protect the confidentiality, integrity, and availability of Customer Content against anticipated or actual threats or hazards; unauthorized or unlawful access, use, disclosure, alteration, or destruction; and accidental loss, destruction, or damage in accordance with laws applicable to the provision of the Service.

2. Graylog Security Program

    2.1. Scope and Content. Graylog Security Program: (a) complies with industry recognized information security standards; (b) includes administrative, technical, and physical safeguards reasonably designed to protect the confidentiality, integrity, and availability of Customer Content; and (c) is appropriate to the nature, size, and complexity of Graylog's business operations.

    2.2. Security Policies, Standards and Procedures. Graylog maintains security policies, standards, and procedures (collectively, Security Policies) designed to safeguard the processing of Customer Content by employees and contractors in accordance with this CSA.

    2.3. Security Program Office. Graylog's Chief Technology Officer leads Graylog's Security Program and develops, reviews, and approves Graylog's Security Policies.

    2.4. Security Program Updates. Graylog reviews, updates, and approves Security Policies once annually to maintain their continuing relevance and accuracy. Employees receive information and education about Graylog's Security Policies during onboarding and annually thereafter.

    2.5. Security Training and Awareness. New employees are required to complete security training as part of the new hire process and receive annual and targeted training (as needed and appropriate to their role) thereafter to help maintain compliance with Graylog's Security Policies, as well as other corporate policies, such as the Graylog Code of Conduct. This includes requiring Graylog employees to annually re-acknowledge the Code of Conduct and other Graylog policies as appropriate. Graylog conducts periodic security awareness campaigns to educate personnel about their responsibilities and provide guidance to create and maintain a secure workplace.

3. Risk Management

3.1. Graylog has a security risk assessment program and management process to identify potential threats to the organization.

3.2. Graylog management rates and reviews identified, material risks to determine if existing controls, policies, and procedures are adequate. Risk mitigation plans are implemented as needed to address material gaps considering the nature of Graylog's business and the information it stores.

4. Change Management

4.1. Graylog deploys changes to the Services during maintenance windows, details of which are posted to the Graylog website or communicated to customers as set forth in the Specific Hosted Services Terms.

4.2. Graylog follows documented change management policies and procedures for requesting, testing, and approving application, infrastructure, and product related changes.

4.3. Changes undergo appropriate levels of review and testing, including security and code reviews, regression testing and user acceptance prior to approval for implementation.

4.4. Software development and testing environments are maintained and logically separated from the production environment.

5. Incident Response and Breach Notification

5.1. Graylog has an incident response plan and team to assess, respond, contain, and remediate (as appropriate) identified security issues, regardless of their nature (e.g., physical, cyber, product). Graylog reviews and updates the plan once annually to reflect emerging risks and "lessons learned."

5.2. Graylog notifies Customers without undue delay after becoming aware of a Data Breach. As used herein, Data Breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Customer Content under the applicable Agreement, including Personal Data as defined under the General Data Protection Regulation (EU) 2016/679 (GDPR), while being transmitted, stored, or otherwise processed by Graylog.

5.3. In the event of a Data Breach involving Personal Data under the GDPR, if customer reasonably determines notification is required by law, Graylog will provide reasonable assistance to the extent required for the Customer to comply with applicable data breach notification laws, including assistance in notifying the relevant supervisory authority and providing a description of the Data Breach.

6. Governance and Audit

6.1. Graylog conducts internal control assessments on an ongoing basis to validate that controls are designed and operating effectively. Issues identified from assessments are documented, tracked, and remediated as appropriate.

6.2. Third party assessments are performed to validate ongoing governance of control operations and effectiveness. Issues identified are documented, tracked, and remediated as appropriate.

7. Access and User Management

7.1. Graylog implements reasonable controls to manage user authentication for employees or contractors with access to Customer Content, including without limitation, assigning each employee or contractor with unique and/or time limited user authorization credentials for access to any system on which Customer Content is accessed and prohibiting employees or contractors from sharing their user authorization credentials.

7.2. Graylog allocates system privileges and permissions to users or groups on a “least privilege” principle and reviews user access lists and permissions on a quarterly basis, at minimum.

7.3. New users must be pre-approved before Graylog grants access to Graylog corporate and cloud networks and systems. Pre-approval is also required before changing existing user access rights.

7.4. Graylog promptly disables application, platform, and network access for terminated users upon notification of termination.

8. Password Management and Authentication Controls

8.1. Authorized users must identify and authenticate to the network, applications and platforms using their user ID and password. Graylog’s enterprise password management system requires minimum password parameters.

8.2. SSH key authentication and enterprise password management applications are utilized to manage access to the production environment.

8.3. Two-factor authentication (2FA) is required for remote access and privileged account access for Customer Content production systems.

9. Encryption and Key Management

9.1. Graylog uses industry-standard encryption techniques to encrypt Customer Content in transit. The Graylog System is configured by default to encrypt user data files using transport layer security (TLS) encryption for web communication sessions.

9.2. Graylog relies on policy controls to help ensure sensitive information is not transmitted over the Internet or other public communications unless it is encrypted in transit.

9.3. Graylog uses encryption key management processes to help ensure the secure generation, storage, distribution, and destruction of encryption keys.

10. Threat and Vulnerability Management

10.1. Graylog continuously monitors for vulnerabilities that are acknowledged by vendors, reported by researchers, or discovered internally through vulnerability scans, Red Team activities or personnel identification.

10.2. Graylog documents vulnerabilities and ranks them based on severity level as determined by the likelihood and impact ratings assigned by TVM. Graylog assigns appropriate team(s) to conduct remediation and track progress to resolution as needed.

10.3. For systems containing Customer Content, an external vendor conducts security penetration tests on the corporate and cloud environments at least annually to detect network and

application security vulnerabilities. Critical findings from these tests are evaluated, documented and assigned to the appropriate teams for remediation.

11. Logging and Monitoring

11.1. Graylog continuously monitors application, infrastructure, network, data storage space and system performance.

11.2. Graylog reviews key reports daily and follows up on events as necessary.

12. Secure Development

12.1. Graylog's Software Development Life Cycle (SDLC) methodology governs the acquisition, development, implementation, configuration, maintenance, modification, and management of software components.

12.2. For major product releases, Graylog uses a risk-based approach when applying its standard SDLC methodology, which may include such things as performing security architecture reviews, open source security scans, dynamic application security testing, network vulnerability scans and external penetration testing in the development environment. Graylog performs security code review for critical features if needed; and performs code review for all features in the development environment. Graylog scans packaged software to ensure it is free from trojans, viruses, malware, and other malicious threats.

12.3. Graylog utilizes a code versioning control system to maintain the integrity and security of application source code. Access privileges to the source code repository are reviewed periodically and limited to authorized employees.

12.4. The SDLC methodology does not apply to free Graylog Content or to Third Party Content, including any made available on Graylog Marketplace.

13. Network Security

13.1. Graylog uses industry standard technologies to prevent unauthorized access or compromise of Graylog's network, servers, or applications, which include such things as logical and physical controls to segment data, systems, and networks according to risk. Graylog monitors demarcation points used to restrict access such as firewalls and security group enforcement points.

13.2. Remote users must authenticate with two-factor authentication prior to accessing Graylog networks containing Customer Content.

14. Vendor Security

14.1. Graylog assesses risks associated with new vendors prior to onboarding and thereafter manages them through its risk management program.

14.2. Confidential Information is shared only with those who are subject to appropriate confidentiality terms with Graylog.

14.3. Graylog uses a risk-based approach to verify on-going vendor compliance with Graylog's Security Policies.

15. Physical Security

15.1. Graylog grants physical access to Graylog based on role. Graylog removes physical access when access is no longer required, including upon termination.

15.2. Personnel must carry, and visitors must wear, identity badges when in Graylog facilities. Visitors must always be accompanied. Graylog logs visitor access to Graylog facilities.

16. Disaster Recovery Plan

16.1. Graylog has a Business Continuity / Disaster Recovery Plan to manage significant disruptions to Graylog Cloud operations and infrastructure. Graylog management updates and approves the Plan annually.

16.2. Graylog personnel perform annual disaster recovery tests. Test results are documented and corrective actions are noted.

16.3. Data backup, replication and recovery systems/technologies are deployed to support resilience and protection of Customer Content.

16.4. Backup systems are configured to encrypt backup media.

17. Asset Management and Disposal

17.1. Graylog maintains and regularly updates an inventory of Cloud infrastructure assets.

17.2. Documented, standard build procedures are utilized for installation and maintenance of production servers.

17.3. Documented data disposal policies are in place to guide personnel on the procedure for disposal of Customer Content.

17.4. Upon expiration or termination of the Agreement, Graylog will return or delete Customer Content in accordance with the terms of the Agreement. If deletion is required, Customer Content will be securely deleted, except that Customer Content stored electronically in Graylog's backup or email systems may be deleted over time in accordance with Graylog's records management practices.

17.5. Graylog retains Customer Content stored in its cloud computing services for at least thirty (30) days after the expiration or termination of this Agreement.

18. Human Resources Security

18.1. Graylog personnel sign confidentiality agreements and acknowledge Graylog's Acceptable Use Policy during the new employee onboarding process.

18.2. Graylog conducts background verification checks for potential Graylog personnel with access to Customer Content in accordance with relevant laws and regulations. The background checks are commensurate to an individual's job duties.

19. CSA Proof of Compliance

19.1. Security Audits. At least once a year, Graylog Cloud undergoes a security audit by an independent third party that attests to the effectiveness of the controls Graylog has in place to safeguard the systems and operations where Customer Content is processed, stored, or transmitted (e.g., System and Organizational Control (SOC 2), Type 2) audit in accordance with the Attestation Standards under Section 101 of the codification standards (AT 101). Upon request, Graylog will supply Customer with a summary copy of Graylog's annual audit reports, which will be deemed Confidential Information under the Agreement.