HOSTED SERVICE TERMS

These Hosted Service Terms ("**Hosted Service Terms**") are entered into as of the date last signed ("**Effective Date**") between Graylog, Inc., a Delaware corporation, located at 1301 Fannin St., Suite 2000, Houston, TX 77002 ("**Graylog**"), and the customer executing the General Terms ("**Customer**").

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. **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 therefore.

3. **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.

4. **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.

5. **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.

6. **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.

7. **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. 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.

   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.

8. **Maintenance.** In order to operate in an efficient and secure manner, the Graylog Cloud Service requires routine maintenance and upgrades.

8.1. **Off-line Maintenance**. Off-line maintenance encompasses service changes initiated by Graylog or Customer that has the potential to impact the Hosted Service Level Commitment. For Graylog initiated changes, maintenance is performed at most once per month and Customers will receive notice of Off-line 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. For Customer initiated changes, the maintenance can be performed more than once per month. Customer will receive email notice when off-line maintenance is starting and when complete. Off-line maintenance is performed during the hours of Monday 1 AM through Saturday 1 AM UTC or at a time agreed to with the Customer in advance.

8.2. **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.

9. **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.

9.1. **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

9.2. **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:

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

9.2.2. Off-line scheduled maintenance as described above.

9.2.3. 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.

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

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

9.2.6. 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.

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

9.4. **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.

10. **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.

11. **Definitions.**

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

11.2. "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.

11.3. "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 these Terms.

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

11.5. "Graylog Cloud" – please see "Hosted Service"

11.6. "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.

11.7. "Hosted Service" means a technology service hosted by or on behalf of Graylog and provided to Customer and governed by "Hosted Service Terms"

11.8. "Hosted Service Terms" means separate specific terms regarding Hosted Service in addition to these General Terms set forth here: www.graylog.org/legal/

11.9. "Software" means the computer software applications listed on any Order Form executed in connection with these Terms, including any Updates thereto.

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

11.11. "Support Services" means the services described in Support Terms.

11.12. "Support Terms" means separate Support Terms regarding support and maintenance services as part of your purchase set forth here: www.graylog.org/legal/

11.13. "Terms" means collectively all Graylog provided Terms which include General Terms, Support Terms, Hosted Service Terms, and all other agreed upon terms as further outlined in the Order Form.

11.14. "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.

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.