SMARSH SERVICES AGREEMENT

This Smarsh Services Agreement (the "Agreement") constitutes a binding agreement between Smarsh Inc. ("Smarsh") and the company signing this Agreement ("Client"). This Agreement includes all exhibits, appendices, or other addenda that reference this Agreement, and incorporates any applicable Service Specific Terms, Service Level Agreements, or Documentation by reference.

This Customer Agreement, including all exhibits, attachments, and incorporated documents, expressly includes and is subject to the GOVERNMENT RIDER TO SUPPLIER END USER LICENSE AGREEMENT AND TERMS OF SERVICE ("Rider"), which is attached hereto as Exhibit A and incorporated herein by reference. In the event of any conflict between the terms of this Agreement and the Rider, the Rider shall govern for all transactions with Public Sector Customers.

1. Services. Smarsh will provide the services ("Services") according to (i) the terms of the Agreement, (ii) with respect to any software ("On-Prem Software") or software-as- a-service ("SaaS Service") provided by Smarsh, the applicable Service Specific Terms for such SaaS Service, and (iii) with respect to any support services, the applicable Service Level Agreement or support package documentation provided by Smarsh to Client. Service Documentation can be found at https://central.smarsh.com under Production Documentation ("Documentation").

1.1. Orders. Client may purchase new Services provided under this Agreement. The Service Term for any additional services purchased after or during the Client's existing Service Term will co-term to, sync with, and renew based upon Client's then current Services Term for the Services to which Client has subscribed (the "Recurring Services").

1.2. Access & Use. Subject to the terms of the Agreement and as applicable to the Service, Client may license, access and use the applicable Service during the Service Term. Smarsh reserves the right to temporarily suspend Client's access to a Service (i.e., disable login credentials) or any User's access to the SaaS Service if (i) Smarsh reasonably believes that (a) Client is in material breach of the Agreement, or (b) a User is in breach of the Agreement, (ii) with respect to a SaaS Service, a User or Client's use of a SaaS Service is likely (in Smarsh's reasonable opinion) to negatively affect the availability, security, or performance of Smarsh's systems or such SaaS Service; or (iii) Smarsh in good faith suspects that an unauthorized third party has gained access to the Service using credentials issued to the Client by Smarsh. With respect to Documentation or a Service that requires a license, Smarsh grants Client a revocable, non-exclusive, worldwide license to use the Documentation or such Service for the duration of the applicable Service Term.

1.3. Restrictions. The Client will not (and will not knowingly permit any third party, including its Users, to): (a) use the Service to develop a similar or competing product or service; (b) reverse engineer, decompile, disassemble, or seek to access the source code, algorithms, or non-public APIs to the Service or any related features; (c) modify or create derivative works of the Service or any element of the Service; (d) copy, rent, lease, distribute, assign (except as authorized under this Agreement), or otherwise transfer rights to the SaaS Service or any part thereof, for the benefit of a third party, or remove any proprietary notices or labels from the SaaS Service or any part thereof; (e) use the Service to perform or publish

benchmarks or performance information about the Service; (f) provide access to or sublicense the Service to a third party except as authorized under the Agreement, (g) transmit, or allow any Third Party Service to transmit on Client's behalf to Smarsh any data that is subject to PCI (e.g., Payment Card Industry Security Standards) data protection requirements, (h) use the SaaS Service in a manner that (i) violates applicable laws, rules, or regulations, or (ii) negatively affects the availability, security, or performance of the SaaS Service, or (i) use the Services (i) in excess of the scope of its licensing, (ii) contrary to the particular SaaS Service's Service Specific Terms, or (iii) to circumvent another service offered by Smarsh, such as subscribing to email archiving for the purpose of archiving email marketing data. The Client will not, directly or indirectly, in whole or in part, use or knowingly permit the use of any security testing tools in order to probe, scan or attempt to penetrate or ascertain the security of the Services.

1.4. Updates. Smarsh may, in its sole discretion, update or modify the SaaS Service by making available updates or modifications which may add new or eliminate existing features or functions to the SaaS Service, so long as such update or modification, does not materially degrade the SaaS Service. For clarity, elimination of an existing material feature or function shall be replaced with a feature or function with similar effect unless Smarsh provides reasonable advance notice of said elimination and said elimination (i) is in furtherance of accepted industry practice, or (ii) is made pursuant to applicable law.

1.5. Upgrades. Smarsh may upgrade the SaaS Services used by Client to new versions of such SaaS Service, or install patches, service packs, security updates or the like to the SaaS Services. For upgrades substantially impacting the functionality of the SaaS Services (i.e., those which may require the Client to retrain its Users or update a connection), Smarsh will provide Client with written notice prior to upgrade. Certain upgrades may introduce new functionality modules which will be made available to Client on an optional basis for an additional fee and Client will be given prior notice of any additional fees that may apply for such new modules, and an option to accept or reject use of such new modules.

1.6. Replacements. Smarsh may, upon reasonable advance notice to the Client, sunset, end of life, deprecate, retire, or replace any Service or feature thereof upon reasonable advance written notice to Client, provided that Smarsh makes a substantially similar Service or feature available to Client for the remainder of Client's then current Service Term at no additional charge. If Smarsh is unable or determines in good faith that is economically infeasible to provide a substantially similar Service or feature, then Smarsh will issue Client a credit for the unused portion of any pre-paid Fees that are attributable to the discontinued Service or feature. Refunds will not apply to any modifications to Services or features that are made by Smarsh to comply with applicable law or address a material security risk.

2. Support & User Groups. Smarsh Central, located at https://central.smarsh.com is where Client can access support resources for the Services as well as engage with other end users in online forums regarding the Services.

2.1. Smarsh Central. Support FAQ's and other support resources are available on Smarsh Central. Client may initiate support requests by submitting support tickets on Smarsh Central. Changes to Smarsh's support policies will be made available on Smarsh Central, provided, however, that any such changes shall not materially degrade the support services.

2.2. Groups. Smarsh Central also provides online forums and related features to Users of the Services (as defined below) for discussion, feedback, and general Q&A purposes (such forums and related features are collectively called “Groups”). Smarsh grants Client and its Users a revocable, non- exclusive, non-transferable license to access and use Groups within Smarsh Central in connection with Client's use of the Services. Client or Users may post comments or content to Groups ("Groups Content"). Client hereby grants Smarsh a worldwide, exclusive, royalty-free, irrevocable license to access, use, reproduce, make derivatives of, and incorporate Groups Content into Smarsh products or services for commercial use. Client acknowledges that Groups Content is not confidential and is subject to the terms of use for Groups. Smarsh may delete Groups Content without prior notice. Client is responsible for all Groups Content posted by its Users. Smarsh disclaims all liability arising from Groups Content and use of Groups, including exposure to content that is potentially offensive, indecent, inaccurate, objectionable, or otherwise inappropriate. Smarsh may suspend or discontinue Groups at any time. Smarsh provides Groups without charge and Groups is not part of the Services.

3. Third Party Data Sources & Client Data. To capture or archive data, the Services are dependent on receiving data from Third Party Data Sources or Client’s own systems.

3.1. Third Party Data Sources. The Services may receive Client Data from third party data sources on behalf of the Client, such as Microsoft, telecommunication companies (such as Verizon or AT&T), social media networks (e.g. Facebook), or other business content management providers or customer relationship management software (e.g. Salesforce), including but not limited to those third parties’ APIs or platforms (“Third Party Data Sources”).

3.1.1. The Client understands that Third Party Data Sources are not offered, controlled, or provided by Smarsh, and thus, Smarsh is not responsible for any outages, lost data, service interruptions, or failures caused by, or that are the result of, any action or failure to act by a Third Party Data Source. Smarsh does not control and is not responsible or liable for how a Third Party Data Source transmits, accesses, processes, stores, uses, or provides data to Smarsh. Smarsh expressly disclaims all liability related to or arising from any Third Party Data Sources, including the Client’s use thereof, or liability related to or arising from any updates, modifications, outages, delivery failures, corruption of data, loss of data, discontinuance of services, or termination of the Client’s account by the Third Party Data Source.

3.1.2. Client is solely responsible for ensuring that Client complies with all Third Party Data Source terms and conditions. Client acknowledges that certain Third-Party Data Sources do not represent that they are suitable for sensitive communications and do not encrypt messages sent over such Third Party Data Source networks, including social media providers, telecommunication carriers and certain messaging platforms. Client agrees that if Client transmits sensitive health, financial, or personal information via these unsecured Third Party Data Source networks, Client assumes all risk associated with such transmission and is responsible for any damages or losses incurred with respect to transmitting such sensitive data over such networks and to Smarsh.

3.2. As used in this Agreement, the term “Client Data” means: (a) the data that the SaaS Services capture or archive from Client’s systems or from Client’s Third Party Data Sources (as defined below), (b) Client’s historical data provided by or on behalf of Client that is ingested into the SaaS Services, and (c) all

content, data, and information, that is submitted, posted, uploaded, captured, or otherwise transmitted to a SaaS Service by or on behalf of the Client from Client's Systems or Third Party Data Sources. Client hereby grants Smarsh a limited, non-exclusive license to access and use Client Data as necessary to provide support and improve the Services on behalf of the Client, or as otherwise authorized hereunder or by Client in writing to Smarsh. Telemetry data generated by the Client's use and operation of the SaaS Services is usage data and is not Client Data ("Usage Data"). Smarsh shall only use Usage Data to provide, improve, or support the Services.

4. Client Obligations.

4.1. Because Smarsh does not have access to Client's systems, nor does Smarsh control or have access to Client's Third Party Data Sources, Client is solely responsible for monitoring the data within the Services, Client's systems, and Third Party Data Sources to ensure that all such data is being captured accurately by the Service. Client will promptly notify Smarsh of any inconsistencies or inaccuracies in the capturing of Client Data, as well as of any delivery failures or outages of Client's systems or Client's Third Party Data Sources, that could affect the transmission or capture of Client Data by the Services.

4.2. It is Client's responsibility to protect and encrypt (i) all data sent to the Services from Client's systems and Client's Third Party Data Sources, and (ii) historical data sent to Smarsh by Client or on behalf of Client for ingestion into the Services. Smarsh will have no responsibility or liability for any data that Client, or any third party on behalf of Client, transmits to Smarsh in an unencrypted format. Smarsh is not responsible or liable for any update, upgrade, patch, maintenance or other change to Client's systems or Third Party Data Source that affects the transmission or capture of Client Data to the Services. Client is solely responsible for ensuring that the Services are configured to capture data from authorized end-user accounts, devices, web domains, as applicable.

4.3. Client is solely responsible for all Client Data. Client represents and warrants that (a) Client Data will not (i) infringe any third party right, including third party rights in patent, trademark, copyright, or trade secret, or (ii) violate the rights of any third parties, including any right that may exist under contract or tort theories. Client will comply with all applicable local, state, national, or foreign laws, rules, regulations, or treaties in connection with Client's use of the Services, including those related to data privacy, data protection, communications, SPAM, or the transmission, recording, or storage of technical data, personal data, or sensitive information.

4.4. Client is responsible for creating an account within the Services and ensuring that (a) Client's account registration information is complete and accurate; and (b) Client's account credentials remain confidential. Client will notify Smarsh immediately of any unauthorized use of Client's account or account credentials, or any other known or suspected breach of the security of Client's account. Client is responsible for the activity that occurs within Client's account and for the actions or omissions of Client's employees, contractors or agents, whether such person is or was acting within the scope of their employment, engagement, or agency relationship.

4.5. Client may provide Representatives with access to the Services or where Client is required to review Representative communications, Client may use the Services to meet such requirement. A

"Representative" means any entity (a) that Client controls or that is under common control with Client; or (b) on behalf of which Client has a regulatory requirement to archive or review communications data. Representatives' use of the Services is subject to the terms of this Agreement. Client is responsible for the actions or omissions of each Representative whether such person is or was acting within the scope of their employment, engagement, or agency relationship.

4.6. Client may designate user roles with different levels of access for use or support of the Services. An "Authorized User" is the administrative user with the highest level of access and is responsible for managing the Services for Client. Only Authorized Users may appoint other Authorized Users, request or agree to changes to the Services, add or remove users, make billing inquiries, contact support, or take other, similar actions. A "User" is any individual who is granted login credentials to the Services. Users may not share account login credentials with any other third party.

4.7. Privacy Jurisdictions. Reasonably prior to the Services ingesting Client Data, the Client shall inform Smarsh in writing if Client Data is subject to any data protection rules and regulations, including Regulation (EU) 2016/679 of the European Parliament of the Council of 27 April 2016 ("Privacy Rules"). If Client plans to capture and archive any Client Data subject to any Privacy Rules not currently contemplated by this Agreement, Client shall promptly notify Smarsh and the parties will work in good faith to update the Agreement, including the applicable Data Protection Addendum (or other similar document) to address such new privacy jurisdictions.

5. Termination.

5.1. Termination for Breach. Either party may terminate this Agreement if the other party materially breaches its obligations under this Agreement and such breach remains uncured for a period of thirty (30) days following the non-breaching party's receipt of written notice thereof. Smarsh reserves the right to temporarily disable or suspend Client's access to the Services in the event of a breach of this Agreement until such breach is cured, and will not be liable for any damages resulting from such suspension.

5.2. Smarsh may terminate the Services if Client materially breaches its obligations pertaining to the Services or this Agreement and such breach remains uncured for a period of thirty (30) days following Client's receipt of written notice thereof.

5.3. Effect of Termination. Upon any termination or expiration of the Agreement: (a) all rights and licenses to the Services granted to Client by Smarsh will immediately terminate; (b) Client will pay any Fees due and payable up to the date of termination, except in the case of Smarsh's termination for Client's breach, and in such case, Client will pay the Fees owing for the remainder of the then-current Term; and (c) upon request, each party will return to the other or delete the Confidential Information of the other party (except Client Data, the return and deletion of which is handled separately as detailed below).

5.4. Client Data Transition. Upon the termination of this Agreement, Client will cease to have access to the SaaS Services (and the Client Data stored within the SaaS Services). Client may request that Smarsh perform professional services to export or migrate the Client Data remaining in the SaaS Services subject to the execution of (i) a statement of work covering such export or migration services between the Client

and Smarsh and the applicable fees, and (ii) as applicable, an order form covering any fees for maintaining Client's data and access to the SaaS Services during the duration of the professional services. Any export or migration services will be performed at Smarsh's then current rates for professional services. Unless agreed otherwise in writing by the parties or prohibited by applicable law, if Client has not made plans to retrieve its data Smarsh shall delete all Client Data 6 months following termination of the Agreement.

6. Confidentiality.

6.1. "Confidential Information" means (a) the non-public information of either party, including but not limited to information relating to either party's product plans, present or future developments, customers, designs, costs, prices, finances, marketing plans, business opportunities, software, software manuals, personnel, research, development, or know-how; (b) any information designated by either party as "confidential" or "proprietary" or which, under the circumstances, would reasonably be deemed to be confidential; and (c) the terms of this Agreement. "Confidential Information" does not include information that: (i) is in, or enters, the public domain without breach of this Agreement; (ii) the receiving party lawfully receives from a third party without restriction on disclosure and without breach of a nondisclosure obligation; (iii) the receiving party knew prior to receiving such information from the disclosing party, as evidenced the receiving party's records; or (iv) the receiving party develops independently without reference to the Confidential Information.

6.2. Obligations with Respect to Confidential Information. Each party agrees: (a) that it will not disclose to any third party, or use for the benefit of any third party, any Confidential Information disclosed to it by the other party except as expressly permitted by this Agreement; and (b) that it will use reasonable measures to maintain the confidentiality of Confidential Information of the other party in its possession or control but no less than the measures it uses to protect its own confidential information. Either party may disclose Confidential Information of the other party: (i) pursuant to the order or requirement of a court, administrative or regulatory agency, or other governmental body, provided that the receiving party, if feasible and legally permitted to do so, gives reasonable notice to the disclosing party to allow the disclosing party to contest such order or requirement; or (ii) to the parties' agents, representatives, subcontractors or service providers who have a need to know such information provided that such party shall be under obligations of confidentiality at least as restrictive as those contained in this Agreement (its "Agents"). A party shall remain fully liable under this Agreement for any breach of this Section by its Agents. Each party will promptly notify the other party in writing upon becoming aware of any unauthorized use or disclosure of the other party's Confidential Information.

6.3. Remedies. Each party acknowledges and agrees that a breach of the obligations of this Section by the other party may result in irreparable injury to the disclosing party for which there may be no adequate remedy at law, and the disclosing party will be entitled to seek equitable relief, including injunction and specific performance, in the event of any breach or threatened breach or intended breach by the recipient of Confidential Information.

6.4. Feedback. Feedback is not Confidential Information. Nothing in the Agreement will restrict Smarsh's right to make use of Feedback in any way Smarsh sees fit and is not required to compensate or credit Client or the individual who provided such Feedback. "Feedback" is any suggestion or idea for

improving or otherwise modifying Smarsh's products or services. If Feedback contains Client's Confidential Information, Smarsh may only use that portion of the Feedback that is not Client's Confidential Information.

The Confidentiality section shall survive the termination of this Agreement.

7. Intellectual Property. As between Smarsh and Client, all right, title and interest in and to the Services, the information technology infrastructure including the software, hardware, databases, electronic systems, networks, and all applications, APIs or Client-Side Software (as defined in the Service Specific Terms) required to deliver the Services, or made available or accessible to Client by Smarsh, including all documentation regarding the use or operation of the Services (collectively "Intellectual Property") are the sole and exclusive property of Smarsh. Except as expressly stated herein, nothing in this Agreement will serve to transfer to Client any right in or to the Intellectual Property. Smarsh retains all right, title and interest in and to Intellectual Property. As between Smarsh and Client, Client Data is the sole and exclusive property of Client and other than the limited license to Client Data granted hereunder, nothing in this Agreement will serve to transfer to Smarsh any intellectual property rights in Client Data.

The Intellectual Property section shall survive the termination of this Agreement.

8. Representations and Warranties; Warranty Disclaimer.

8.1. Performance Warranty. Smarsh represents and warrants that it will use commercially reasonable efforts to provide the Services in accordance with generally accepted industry standards.

8.2. Authority. Each party represents and warrants that it has the right and authority to enter into this Agreement and that the performance of its obligations under this Agreement will not breach, or conflict with, any other agreement to which itis a party.

8.3. Compliance with Laws. Each party represents and warrants that it will comply in all material respects with the laws and regulations applicable to the operation of their business.

8.4. Warranty Disclaimer; No Guarantee. EXCEPT AS SET FORTH ABOVE, SMARSH MAKES NO REPRESENTATION OR WARRANTY OF ANY KIND IN CONNECTION WITH THE SERVICES, PROFESSIONAL SERVICES OR SOFTWARE, INCLUDING, WITHOUT LIMITATION, ANY INFORMATION OR MATERIALS PROVIDED OR MADE AVAILABLE BY SMARSH. SMARSH HEREBY DISCLAIMS ANY AND ALL OTHER REPRESENTATIONS AND WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. SMARSH DOES NOT REPRESENT OR WARRANT THAT THE SERVICES OR SOFTWARE WILL BE AVAILABLE OR ERROR-FREE. SMARSH WILL NOT BE LIABLE FOR DELAYS, INTERRUPTIONS, SERVICE FAILURES OR OTHER PROBLEMS INHERENT IN THE USE OF THE INTERNET, ELECTRONIC COMMUNICATIONS, OR OTHER SYSTEMS OUTSIDE THE REASONABLE CONTROL OF SMARSH. SMARSH DOES NOT GUARANTEE THAT USE OF THE SERVICES BY CLIENT OR THE ADVICE, CONSULTING OR PROFESSIONAL SERVICES PROVIDED TO CLIENT WILL ENSURE CLIENT'S LEGAL COMPLIANCE WITH ANY FEDERAL, STATE, OR INTERNATIONAL STATUTE, LAW, RULE, REGULATION, OR DIRECTIVE. THE SOFTWARE IS NOT DESIGNED OR INTENDED FOR

USE IN HAZARDOUS ENVIRONMENTS REQUIRING FAIL-SAFE PERFORMANCE, INCLUDING BUT NOT LIMITED TO ANY APPLICATION IN WHICH THE FAILURE OF THE SOFTWARE COULD LEAD DIRECTLY TO DEATH, PERSONAL INJURY, OR SEVERE PHYSICAL OR PROPERTY DAMAGE. THIS SECTION SHALL SURVIVE THE TERMINATION OF THIS AGREEMENT.

9. Indemnification.

9.1. Client Indemnification. Client will defend and indemnify Smarsh, its officers, directors, employees, and agents, from and against all third party claims, losses, damages, liabilities, demands, and expenses (including fines, penalties, and reasonable attorneys' fees), arising from or related to (i) Client Data and Client's use of Client Data, (ii) Smarsh's use of Client Data in accordance with this Agreement, and (iii) Client's use of the Services in violation of this Agreement or applicable laws, rules, and regulations. Smarsh will (a) provide Client with prompt written notice upon becoming aware of any such claim; except that Client will not be relieved of its obligation for indemnification if Smarsh fails to provide such notice unless Client is actually prejudiced in defending a claim due to Smarsh's failure to provide notice in accordance with this Section ; (b) allow Client sole and exclusive control over the defense and settlement of any such claim; and (c) if requested by Client, and at Client's expense, reasonably cooperate with the defense of such claim.

9.2. Smarsh Indemnification. Smarsh will defend and indemnify Client, its officers, directors, employees, and agents, from and against all third party claims, losses, damages, liabilities and expenses (including fines, penalties, and reasonable attorneys' fees) arising from a claim that Client's use of the Services in accordance with this Agreement infringes upon any United States patent, trademark or copyright. Client will (a) provide Smarsh with prompt written notice upon becoming aware of any such claim; except that Smarsh will not be relieved of its obligation for indemnification if Client fails to provide such notice unless Smarsh is actually prejudiced in defending a claim due to Client's failure to provide notice in accordance with this Section ; (b) allow Smarsh sole and exclusive control over the defense and settlement of any such claim; and (c) if requested by Smarsh, and at Smarsh's expense, reasonably cooperate with the defense of such claim. Notwithstanding the foregoing, Smarsh will not be liable for any claim that relates to or arises from: (i) custom functionality provided to Client based on Client's specific requirements; (ii) any modification of the Services by Client or any third party not authorized in writing by Smarsh; (iii) the combination of the Services with any technology or other services, software, or technology not provided or authorized in writing by Smarsh; or (iv) Client's failure to use updated or modified versions of the Services made available by Smarsh.

9.3. Sole Remedy. The indemnification obligations contained in this Section are Client's sole remedy, and Smarsh's sole obligation, with respect to claims of infringement under the Agreement. If the Services are subject to, or Smarsh reasonably believes that the Services may become subject to, a claim of infringement under Section 11.2, Smarsh may, in its sole discretion, either (a) procure for Client the right to continue to use the Services; (b) modify the Services such that they are non-infringing; or (c) if in the reasonable opinion of Smarsh, neither (a) nor (b) is commercially feasible, then Smarsh may, upon thirty (30) days' prior written notice to Client, terminate the applicable Service.

The Indemnification section shall survive the termination of this Agreement.

10. Remedies and Limitation of Liability.

10.1. Remedies.

10.1.1. Performance. In the event of a breach of any performance warranty under this Section, Smarsh will use commercially reasonable efforts to provide Client with an error correction or work-around that corrects the reported non-conformity. The foregoing remedy is Client's sole and exclusive remedy for a breach of this Section. In the event that Smarsh is unable to provide an error correction or work-around that corrects the reported non-conformity, Client may terminate the applicable Service and be entitled to a pro-rata refund of any pre- paid Fees for the duration of time between the termination date of such Service and the end of the applicable Service Term.

10.1.2. Service Levels. In the event of a breach of the applicable Service Level Agreement, Smarsh will provide Client with the credit stated in the Service Level Agreement. The foregoing remedy is Client's sole and exclusive remedy for a breach of the applicable Service Level Agreement.

10.2. Limitation of Liability.

10.2.1. IN NO EVENT WILL EITHER PARTY BE LIABLE TO THE OTHER, OR TO ANY THIRD PARTY, FOR ANY SPECIAL, INDIRECT, INCIDENTAL, PUNITIVE, EXEMPLARY OR CONSEQUENTIAL DAMAGES ARISING FROM OR IN CONNECTION WITH THE SERVICES, WHETHER BASED ON BREACH OF CONTRACT, BREACH OF WARRANTY, TORT (INCLUDING NEGLIGENCE), OR OTHERWISE, REGARDLESS OF WHETHER SUCH DAMAGES WERE FORESEEABLE OR WHETHER THE PARTY HAD BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SMARSH WILL NOT BE LIABLE FOR ANY DAMAGES, WHETHER CONSEQUENTIAL OR OTHERWISE, ARISING FROM OR RELATED TO CLIENT'S NON-COMPLIANCE WITH ANY FEDERAL, STATE, OR FOREIGN LAWS RULES, REGULATIONS, OR DIRECTIVES.

10.2.2. EXCEPT WITH RESPECT TO SECTION 11 - INDEMNIFICATION, SMARSH'S AGGREGATE LIABILITY FOR ALL DAMAGES ARISING FROM OR RELATING TO THIS AGREEMENT, NOTWITHSTANDING THE FORM IN WHICH ANY ACTION IS BROUGHT (E.G., CONTRACT, TORT, OR OTHERWISE), WILL NOT EXCEED THE TOTAL FEES ACTUALLY RECEIVED BY SMARSH FROM CLIENT FOR THE APPLICABLE SERVICES IN THE TWELVE (12) MONTH PERIOD IMMEDIATELY PRECEDING THE DATE OF THE INCIDENT FROM WHICH THE DAMAGES AROSE.

10.2.3. THE LIMITATION OF LIABILITY SET FORTH ABOVE IS CUMULATIVE; ALL PAYMENTS MADE FOR ALL CLAIMS AND DAMAGES WILL BE AGGREGATED TO DETERMINE IF THE LIMIT HAS BEEN REACHED.

The Remedies & Limitation of Liability section shall survive the termination of this Agreement.

11. General Terms.

11.1. Data Security and Privacy. Smarsh shall implement and maintain commercially reasonable and appropriate technical and organizational measures to protect Client Data, including any Personal Information contained within the Client Data, as set forth in Smarsh's Information Security Addendum

attached to this Agreement. If Client intends to transmit any Personal Information or Personal Data to Smarsh, the transfer and processing of such Personal Information will be subject to Smarsh's Data Processing Addendum, a copy of which can be requested from privacy@smarsh.com.

11.2. Export Restrictions. Client will comply with the applicable export laws and regulations of the United States and other applicable jurisdictions when using the Services. Client will not transfer the Software, or any other software or documentation provided by Smarsh (a) to any person on a government promulgated export restriction list; or (b) to any U.S.-embargoed countries. Without limiting the foregoing: (a) Client represents that it and its Authorized Users and any other users of the Services are not named on any United States government list of persons or entities prohibited from receiving exports; (b) Client represents that Client will not use the Software or Services in a manner which is prohibited under United States Government export regulations; (c) Client will comply with all United States anti-boycott laws and regulations; (d) Client will not provide the Software or Service to any third party, or permit any user to access or use the Software or Service, in violation of any United States export embargo, prohibition or restriction; and (e) Client will not, and will not permit any user or third party to, directly or indirectly, export, re-export or release the Software or Services to any jurisdiction or country to which, or any party to whom, the export, re-export or release is prohibited by applicable law, regulation or rule.

11.3. Assignment. Neither party may assign this Agreement, in whole or in part, without the other party's prior written consent, except that either party may assign this Agreement without the other's consent in the case of a merger, reorganization, acquisition, consolidation, or sale of all, or substantially all, of its assets ("Change of Control"). Any attempt to assign this Agreement other than as permitted herein will be null and void. This Agreement will inure to the benefit of, and bind, the parties' respective successors and permitted assigns.

11.4. Force Majeure. A failure of party to perform, or an omission by a party in its performance of, any obligation of this Agreement will not be a breach of this Agreement, nor will it create any liability, if such failure or omission arises from any cause or causes beyond the reasonable control of the parties, including, but not limited to the following (each a "Force Majeure Event"): (a) acts or omissions of any governmental entity; (b) any rules, regulations or orders issued by any governmental authority or any officer, department, agency or instrumentality thereof; (c) fire, storm, flood, earthquake, accident, war, rebellion, insurrection, riot, third party strikes, third party lockouts and pandemics; or (d) utility or telecommunication failures; so long as such party the provides prompt notice of the Force Majeure Event, uses reasonable efforts to mitigate the impact of the Force Majeure Event, and uses reasonable efforts to resume performance after any such Force Majeure Event. A Force Majeure Event will not relieve Client's obligation to pay Fees under this Agreement. This section shall survive the termination of this Agreement.

11.5. Governing Law. This Agreement will be governed by and construed in accordance with the laws of the State of Delaware, without regard to conflict/choice of law principles. This Section shall survive the termination of this Agreement.

11.6. Relationship of the Parties. The parties are independent contractors as to each other, and neither party will have power or authority to assume or create any obligation or responsibility on behalf of the other. This Agreement will not be construed to create or imply any partnership, agency, or joint venture.

11.7. Legal Notices. Any legal notice under this Agreement will be in writing and delivered by personal delivery, express courier, certified or registered mail, postage prepaid and return receipt requested, or by email. Notices will be deemed to be effective upon personal delivery, one (1) day after deposit with express courier, five (5) business days after deposit in the mail, or when receipt is acknowledged in the case of email to Smarsh. Notices will be sent to Client at the address specified by Client. Notices will be sent to Smarsh at the following address: Smarsh Inc., Attention: Legal, 851 SW 6th Ave, Suite 800, Portland, OR 97204, or in the case of email, to legal@smarsh.com.

11.8. Publicity. Smarsh may disclose that Client is a customer of Smarsh, provided, however, that Client may revoke, limit, or withdraw its consent at any time by providing Smarsh with written notice to marketing@smarsh.com.

11.9. Severability; Waiver. If for any reason a court of competent jurisdiction finds any provision or portion of this Agreement to be unenforceable, that provision of the Agreement will be enforced to the maximum extent permissible so as to reflect the intent of the parties, and the remainder of this Agreement will continue in full force and effect. Failure of either party to insist on strict performance of any provision herein will not be deemed a waiver of any rights or remedies that either party will have and will not be deemed a waiver of any subsequent default of the terms and conditions thereof.

11.10. Entire Agreement; Electronic Signatures. This Agreement is the entire agreement between the parties with respect to its subject matter, and supersedes any prior or contemporaneous agreements, negotiations, and communications, whether written or oral, regarding such subject matter. Smarsh expressly rejects all terms contained in Client's purchase order documents and such terms form no part of this Agreement. The parties agree that electronic signatures, whether digital or encrypted, or Client's click-through acceptance of this Agreement, give rise to a valid and enforceable agreement. This Agreement shall become effective as between the Client and Smarsh upon Client's click-through acceptance of this Agreement.

11.11. Amendments. This Agreement may be amended in accordance with this Section. The Parties may amend this Agreement by a writing signed by both parties. For the avoidance of doubt, electronic communications on their own will not amend this Agreement. Smarsh may amend this Agreement (or any Service Specific Terms) by providing Client with written notice of any update to the Agreement (including a general description of the changes), and such update(s) shall be deemed to be effective between the Parties fifteen (15) days after the date of such notice, unless Client objects to such changes in writing within the fifteen-day period.

11.12. Letter of Undertaking. Upon Client's written request and only to the extent that Smarsh is providing an "electronic record keeping system" as described in SEC Rule 17a-4(f)(or similar SEC Rule such as 18a-6), Smarsh agrees to provide the Client with an undertaking that (i) Smarsh's archive software (as applicable) used by Client is an "electronic recordkeeping system," and (ii) that Smarsh will facilitate within its ability, and not impede or prevent, the examination, access, download, or transfer of the Client's records by a representative or designee of the Securities and Exchange Commission as permitted under the law, or a trustee appointed under the Securities Investor Protection Act of 1970 ("17a-4 Letter"). In

the event that Client requires a 17a- 4 Letter, Client represents and warrants to Smarsh that (i) Client (or a Client Affiliate) is subject to the rules of the Securities and Exchange Commission governing the maintenance and preservation of the records (e.g., Client Data) maintained by the SaaS Service, (ii) Client has "independent access" to, and the ability to download, Client Data using the SaaS Service, and (iii) Client consents to Smash fulfilling its obligations with respect to the provision of the Services under this Agreement and to Smarsh providing the required undertakings as set forth in SEC Rule 17a-4(f), including those required by 17a-4(f)(3)(v)(A), 17a-4(i)(1)(ii)(A, or any successor provisions. In the event that Client wishes for Smarsh to act as a "designated-third party" under SEC Rule 17a-4(f)(3)(v)(A), Client must provide Smarsh with advance written notice and the ability to consent to such role, and such consent may require Client to agree to certain reasonable conditions in order for Smarsh to act in such capacity.

11.13. Audits.

11.13.1. Annual Due Diligence & Security Audits. Smarsh uses external auditors to verify the adequacy of Smarsh's Security Program ("Security Audits"), Smarsh agrees to conduct Security Audits on an annual basis using independent third party auditors according to ISO 27001 or SSAE 18 standards (or any equivalent standard). Client agrees that Smarsh may satisfy Client's audit requests (which shall in no event be more than once every 12 months) by making available (to the extent applicable and available for the applicable SaaS Service) to Client, Smarsh's most recent (i) standard information gathering questionnaire, (ii) ISO 27001 report (or other similar third party audit report), (iii) annual independent SSAE 18 report (to the extent available), and (iv) an executive summary of Smarsh's most recent annual penetration test for the applicable SaaS Services ("Standard Audit Documentation") to demonstrate its compliance with the terms of this Agreement. Smarsh will use commercially reasonable efforts to respond to such requests for due diligence within 30 days of receiving such request, with, at a minimum, Smarsh's Standard Audit Documentation, and in the case of additional requests for information, a proposed timeframe for response (based on the nature and scope of the requests). Upon written notice, Smarsh reserves the right to charge and Client agrees to pay for any requests that require more than one (1) hour to complete.

11.13.2. Additional Audits & Due Diligence Questionnaires. If Client requires Smarsh to (i) respond to Client's or a third party's due diligence questionnaires, or (ii) answer questionnaires that are outside the scope of Section 13.12.1 (determined at Smarsh's reasonable discretion) in addition to the Standard Audit Documentation, such requirement will be referred to as a Non-Standard Audit. In the event Client elects to audit Smarsh using a Non-Standard Audit, Smarsh, at Client's sole expense, will respond to such additional requests for information under the Non-Standard Audit, including additional security questionnaires, subject to Smarsh's standard hourly rate (currently $300/hr) which may be modified by Smarsh from time to time. Prior to answering such additional questionnaire(s) or due diligence, Smarsh will provide Client with an estimate of the cost associated with responding to such questions, and may request a deposit, before beginning such work. Smarsh will use commercially reasonable efforts to respond to such requests for a Non- Standard Audit within 30 days of receiving such request, with, at a minimum, Smarsh's Standard Audit Documentation, and a proposed timeframe for response (based on the nature and scope of the requests).

11.13.3. Regulatory Requests for Information. If Client receives a request for information about Smarsh's provision of Services from a regulator or regulatory authority with jurisdiction over the Client, Smarsh

agrees to provide reasonable cooperation and assistance to Client to address any such requests in a reasonable and timely manner, including by making available to the regulator Smarsh's Standard Audit Documentation. For the sake of clarity, a request for information under this section by the Client to answer questions from a regulatory authority about Smarsh's provision of services to Client will not be considered Client's annual Security Audit.

This Audits section shall survive the termination of this Agreement.

11.14. Drafting. The Parties have participated jointly in the negotiation and drafting of this Agreement. In the event of an ambiguity or question of intent or interpretation arises, this Agreement shall be construed as if drafted jointly by the Parties and no presumption or burden of proof shall arise favoring or disfavoring any Party by virtue of the authorship of any of the provisions of this Agreement.

11.15. Conflict. In the event of a conflict between the terms of this Agreement and the applicable Data Processing Addendum, the conflict shall be resolved in the following order of precedence with each taking precedence over those listed subsequently, unless specifically set forth otherwise in the applicable agreement or document:

1. The Data Processing Addendum (with respect to the processing of Personal Data);
2. The Agreement

Any additional, conflicting, or different terms or conditions proposed by Client in any Client issued document are hereby rejected by Smarsh and excluded herefrom.

SERVICE SPECIFIC TERMS EXHIBIT

The Service Specific Terms contained herein shall apply to Client during the applicable Service Term if Client uses, or purchases, the applicable Service.

Service Specific Terms for Services not purchased nor used by Client shall not apply unless or until that time when Client or a Client Affiliate uses or purchases such Services.

The applicable Service Specific Terms are incorporated into this Agreement by reference.

These Service Specific Terms shall govern Client's use of the applicable Services. Client's use of the applicable Service shall be deemed to be acceptance of the applicable Service Specific Terms.

The Client agrees to comply with the applicable Service Specific Terms for the duration of the Agreement or applicable Service Term for such Service.

SERVICE SPECIFIC TERMS

Specific Terms – Capture Mobile Service

SERVICE SPECIFIC TERMS - CAPTURE MOBILE

1) MOBILE CARRIER CAPTURE SERVICES.

A. Subject to any applicable Mobile Carrier (defined below) specific requirements, the Capture Mobile Services provided by Smarsh (or one of its affiliates) to Client enables Client to capture electronic communications, and other content types from (such service as "Mobile Carrier Capture Services") certain mobile telecommunication carriers ("Mobile Carriers") located within the United States when using Client's corporate devices registered with such Mobile Carrier, such as Verizon or AT&T.

B. CLIENT OBLIGATIONS. Client is responsible for configuring any applicable third-party platforms or systems to enable the transmission of Client Data to the Mobile Carrier Capture Services, including any specific requirements of any Mobile Carrier.

2) Additional Terms. In the event that Client leverages the Capture Mobile Service and uses certain Mobile Carriers (such as Verizon, AT&T), Smarsh is required by such Mobile Carriers to pass along such carriers' additional terms of service to the Client set forth below ("Carrier Pass Through Terms of Use"). Those Carrier Pass Through Terms of Use shall be by and between the Client and the applicable Mobile Carrier and only apply to Client's capture and use of such electronic communications and content types from the applicable Mobile Carrier. Client agrees to comply with the Carrier Pass Through Terms of Use of those Mobile Carriers used by Client in connection with these Service Specific Terms.

3) Temporary Data Retention. The Capture Mobile Services are designed to retain Client Data for a temporary retention period of ("Temporary Retention Period") up to 30 days, as configured by the Client.

4) Data Deletion. The Capture Mobile Services are designed to delete Client Data after the expiration of the Temporary Retention Period.

5) Service Environment. Unless agreed otherwise by the Parties in writing, the Capture Mobile Services are deployed in a service environment or data center located in the United States. Client Data will be stored and maintained by the Capture Mobile Services within the United States.

6) Capture Mobile Service Documentation. Smarsh will make available to the Client the Capture Mobile Service Documentation in Smarsh's support portal - http://central.smarsh.com ("Documentation"), including any performance constraints or service guidelines, as amended from time to time, or directly upon written request.

7) UNIQUE PHONE NUMBERS[1].

a) Phone Numbers. The Capture Mobile Services may require Client to use a unique phone number in connection with the Capture Mobile Services in order to send and receive messages and other data using the applicable mobile device application on a Client user's device (generally "Mobile App," and

[1] For clarity, the Mobile Device App may not require a unique Phoner Number and may use Client's corporate device mobile carrier line.

included as part of the “Capture Mobile Services”). Upon written request, Smarsh can provide Client with unique phone numbers which will be allocated to the applicable client device user’s account (“Smarsh Numbers”). Provision of Smarsh Numbers is subject to applicable numbering rules and regulatory practices, which may change or be amended from time to time, as well as additional fees associated with such lines. Smarsh reserves the right to change the terms related to Smarsh Numbers accordingly, including without limitation to impose or amend local residency requirements and/or to require the provision of further user information for continued access to defined Smarsh Numbers.

b) Smarsh Number Restrictions. The Mobile Apps and Smarsh Numbers do not support any type of emergency calling, nor does it support activation of SMS. Client cannot use Smarsh Numbers to receive messages for the purpose of identity verification, such as activation via SMS or activation calls, and the like.

c) Compliance. Client may purchase and allocate Smarsh Numbers to User accounts subject to compliance with the allocation requirements displayed upon subscription to receive a Smarsh Number. Client, and not Smarsh, is responsible for compliance with any requirements related to the residence and/or the location of Client’s Users.

8) Notice & Consent. Client is only authorized to use the Capture Mobile Services to capture electronic communications (both incoming and outgoing) from mobile devices or corporate mobile accounts linked to Client’s current employees and independent contractors (each a “Client Individual”). Prior to capturing electronic communications of the Client Individual, Client shall (i) provide each Client Individual with clear and conspicuous notice of Client’s policies regarding Client’s receipt, transmission, capture, use and storage of such Client Individual’s, and generally Client’s employees and independent contractor’s electronic communications, (ii) obtain such Client Individual’s consent for such capture of their electronic communications, and (iii) ensure that such Client Individual has been made aware of, and understands that, they have no reasonable expectation of privacy with respect to their electronic communications connected to such devices and accounts. To the extent required by applicable law, Client is responsible for ensuring that all Client Individuals using mobile devices or mobile account lines subject to the Capture Mobile Services inform any third parties that such Client Individual’s electronic communications are being captured and retained by Client. Client shall process all Personal Data or Personal Information in accordance with all applicable data protection and privacy laws.

9) DISCLAIMER; LIMITATION OF LIABILITY

a. THE CAPTURE MOBILE SERVICES ARE NOT DESIGNED TO BE USED FOR LONG-TERM STORAGE OR AS A DATA ARCHIVE SERVICE. THE CAPTURE MOBILE SERVICE IS NOT DESIGNED TO PERFORM AS AN ARCHIVE OF RECORD ON BEHALF OF THE CLIENT OR TO MEET CLIENT’S RECORD RETENTION REQUIREMENTS. WITH RESPECT TO THE CAPTURE MOBILE SERVICES ONLY, SMARSH EXPRESSLY DISCLAIMS ANY RESPONSIBILITY OR OBLIGATION IMPOSED ON THIRD- PARTY RECORD HOLDERS (AS A SERVICE PROVIDER TO THE APPLICABLE REGULATED ENTITY) BY STATUTE OR BY RULE, REGULATION OR OPINION OF ANY GOVERNMENTAL AGENCY, REGULATORY ORGANIZATION OR SIMILAR INSTITUTION, INCLUDING WITHOUT LIMITATION, THE U.S. SECURITIES AND EXCHANGE COMMISSION, THE FINANCIAL INDUSTRY REGULATORY AUTHORITY, OR ANY SECURITIES EXCHANGE.

b. GENERAL. NOTWITHSTANDING ANYTHING TO THE CONTRARY IN THE AGREEMENT, CLIENT EXPRESSLY ACKNOWLEDGES AND AGREES THAT USE OF THE CAPTURE MOBILE SERVICES AND THE INTERNET GENERALLY IS AT CLIENT'S OWN RISK AND, EXCEPT AS SPECIFICALLY PROVIDED FOR HEREIN, THAT THE CAPTURE MOBILE SERVICES ARE PROVIDED "AS IS" AND "AS AVAILABLE" WITHOUT ANY WARRANTIES OR CONDITIONS WHATSOEVER, EXPRESS OR IMPLIED. SMARSH WILL USE COMMERCIALLY REASONABLE EFFORTS TO MAKE ACCESS TO THE CAPTURE MOBILE SERVICES AVAILABLE TO CLIENT THROUGH THE REQUIRED ACCESS PROTOCOLS BUT MAKES NO WARRANTY OR GUARANTEE THAT CLIENT WILL BE ABLE TO ACCESS THE SERVICE OR ANY PART THEREOF AT ANY PARTICULAR TIME OR ANY PARTICULAR LOCATION.

c. ADDITIONAL LIMITATIONS. WITHOUT LIMITING THE GENERALITY OF THE TERMS SET FORTH HEREIN, SMARSH AND ITS AFFILIATES, AGENTS, CONTENT PROVIDERS, SERVICE PROVIDERS, AND LICENSORS:

(I) HEREBY DISCLAIM ALL EXPRESS AND IMPLIED WARRANTIES AS TO THE ACCURACY, COMPLETENESS, NONINFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OF THE SERVICE GENERALLY, AND ANY CONTENT OR SERVICES CONTAINED THEREIN, AS WELL AS ALL EXPRESS AND IMPLIED WARRANTIES THAT THE OPERATION OF THE CAPTURE MOBILE SERVICES GENERALLY AND ANY CONTENT OR SERVICES CONTAINED THEREIN WILL BE UNINTERRUPTED OR ERROR-FREE;

(II) SHALL IN NO EVENT BE LIABLE TO CLIENT OR ANYONE ELSE FOR ANY INACCURACY, ERROR OR OMISSION, OR LOSS, INJURY OR DAMAGE CAUSED IN WHOLE OR IN PART BY FAILURES, DELAYS OR INTERRUPTIONS IN THE CAPTURE MOBILE SERVICES, OR INSTALLATION AND COMPUTER, MOBILE PHONE OR TABLET DISRUPTIONS RELATED TO THE SERVICES, AND ANY CONTENT OR SERVICES CONTAINED THEREIN. SMARSH SHALL IN NO EVENT BE LIABLE TO CLIENT OR ANYONE ELSE FOR ANY CONSEQUENTIAL, INCIDENTAL, OR SPECIAL DAMAGES ARISING OUT OF, RESULTING FROM, OR RELATING IN ANY MANNER TO THE USE OR INABILITY TO USE THE CAPTURE MOBILE SERVICES, AND ANY CONTENT OR SERVICES CONTAINED THEREIN.

(III) SHALL IN NO EVENT BE LIABLE TO REIMBURSE MESSAGE CREDITS, REIMBURSE PAYMENTS OR HAVE ANY OTHER LIABILITY FOR MESSAGES THAT WHERE SENT BUT NOT DELIVERED, NOT RECEIVED OR NOT ACCURATELY DISPLAYED, HEARD OR REPRESENTED ON ANY SUCH COMMUNICATION DEVICE DUE TO THE FAILURE OF SUCH THIRD PARTIES DUE TO THE FACT THAT DELIVERY METHODS OF ELECTRONIC COMMUNICATIONS TO VARIOUS COMMUNICATION DEVICES IS SUBJECT TO A COMBINATION OF NETWORK PROVIDERS' AND SERVICE PROVIDERS' TERMS AND CONDITIONS AND NETWORK STATUS OVER WHICH SMARSH HAS NO CONTROL

(IV) HEREBY DISCLAIMS ANY LIABILITY OF ANY KIND FOR COSTS OR DAMAGES ARISING OUT OF PRIVATE OR GOVERNMENTAL LEGAL ACTIONS RELATED TO CLIENT'S USE OF ANY OF THE CAPTURE MOBILE SERVICES IN ANY COUNTRY.

d. HIGH RISK ACTIVITIES. THE CAPTURE MOBILE SERVICES ARE NOT FAULT-TOLERANT AND ARE NOT DESIGNED, MANUFACTURED OR INTENDED FOR USE OR RESALE AS ONLINE CONTROL EQUIPMENT IN HAZARDOUS ENVIRONMENTS REQUIRING FAIL-SAFE PERFORMANCE, INCLUDING BUT NOT LIMITED TO USE IN THE OPERATION OF NUCLEAR FACILITIES, AIRCRAFT NAVIGATION OR COMMUNICATION SYSTEMS, AIR TRAFFIC CONTROL, DIRECT LIFE SUPPORT MACHINES, OR WEAPONS SYSTEMS, IN WHICH THE FAILURE OF SERVICE COULD LEAD DIRECTLY TO DEATH, PERSONAL INJURY, OR SEVERE PHYSICAL OR ENVIRONMENTAL DAMAGE ("HIGH RISK ACTIVITIES"). IN ADDITION TO THE OTHER DISCLAIMERS AND LIMITATIONS CONTAINED WITHIN THESE TERMS, SMARSH AND ITS AFFILIATES, AGENTS, CONTENT PROVIDERS, SERVICE PROVIDERS AND LICENSORS SPECIFICALLY DISCLAIM ANY EXPRESS OR IMPLIED WARRANTY OF FITNESS FOR HIGH RISK ACTIVITIES INCLUDING EMERGENCY NOTIFICATION SERVICES.

SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF WARRANTIES OR INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATIONS OR EXCLUSIONS MAY NOT APPLY TO CLIENT. IN SUCH JURISDICTIONS, SMARSH'S LIABILITY (AND THE LIABILITY OF ITS AFFILIATES, AGENTS, CONTENT PROVIDERS AND SERVICE PROVIDERS) SHALL BE LIMITED TO THE GREATEST EXTENT PERMITTED BY APPLICABLE LAW.

10) SUB-PROCESSORS. The Capture Mobile Services may rely on the Sub-Processors set forth in the Sub- Processor Exhibit attached hereto.

11) SERVICE LEVELS. The Capture Mobile Services, and the relevant support services, will be provided in accordance with to the Service Level Agreement attached to this Agreement. For the sake of clarity, in the event of a breach of these SLAs with respect to Capture Mobile Services, Smarsh will provide Client with the credit stated in the SLAs. The foregoing remedy is Client's sole and exclusive remedy for a breach of the applicable SLAS.

CAPTURE MOBILE SERVICES

SUB-PROCESSOR EXHIBIT

Sub-Processor(s). With respect to the Capture Mobile Services, the following entities are sub- processors:

Name	Country	Subject matter and nature of the processing	Duration of the processing
Amazon Web Services (AWS)	USA	Infrastructure as a Service	
Cyxtera	Waltham, MA	Infrastructure as a Service	
Digital Realty	Clifton, NJ	Infrastructure as a Service	

CARRIER PASS THROUGH TERMS OF USE

AT&T MOBILE TERMS.

This agreement is between you as our subscriber ("You") and the affiliate of AT&T Mobility National Accounts, LLC providing wireless service to You ("AT&T"), and it sets forth the terms and conditions ("Terms and Conditions") under which You agree to use and AT&T agrees to provide access to Archived Messages through the Archived Messages Service (as such terms are defined below). By using the Archived Messages Service, You accept these Terms and Conditions, which AT&T may modify from time to time.

1. DEFINITIONS.

1.1. Archived Messages means a Participating Employee's Messages that AT&T has made available to SMARSH for retrieval through use of SMARSH's Archived Messages Service.

1.2. Archived Messages Service means SMARSH's service that provides You access to Archived Messages.

1.3. Customer Liable MDNs means a Mobile Directory Number (MDN) for AT&T wireless service that is established under Your corporate account and corporate name and for which You are financially responsible to AT&T for an AT&T service.

1.4. Employee Liable MDN means a MDN for AT&T wireless service that is established in the name of an individual employee of Your company or other authorized individual and for which such individual is financially responsible to AT&T for AT&T services.

1.5. Messages means messages sent or received by any Participating Employee via short message service (SMS), multimedia message service (MMS) and/or AT&T Business Messaging Service.

1.6. Participating Employee means Your employee or other authorized user of a mobile device with a Customer Liable MDN whose Customer Liable MDN(s) is subscribed to the Archived Messages Service.

2. ARCHIVED MESSAGES SERVICE.

2.1. You authorize AT&T to make the Messages available to Smarsh for use solely in connection with SMARSH's Archived Messages Services.

2.2. You will only access, use, copy, store or disclose Archived Messages in accordance with these Terms and Conditions. You will not access, use, copy, store or disclose Archived Messages for any other purpose.

2.3. SMARSH. You will enter into an agreement with SMARSH Inc. ("SMARSH") for the Archived Messages Service, and You will pay all of SMARSH's charges for such Archived Messages Service in accordance with that agreement and these Terms and Conditions.

2.4. Customer Liable MDNs Only. You will enroll only Customer Liable MDNs in the Archived Messages Service. You may not enroll any Employee Liable MDNs in the Archived Messages Service.

2.5. Notice and Consent. Prior to enrolling any individual's device in the Archived Messages Service and accessing, using, storing, copying or disclosing any Participating Employee's Archived Messages, You will provide advance disclosure to each such individual containing clear and conspicuous notice of the terms and conditions of the Archived Messages Service, including how You and SMARSH will access, use, copy, retain, protect or disclose such individual's Archived Messages, as well as the duration and purpose of such access, use, copying or retention. You will also obtain all lawfully required consents for those uses of such individual's Messages. You agree to maintain the currency of such consent at all times.

2.6. Transferring a Mobile Device or Customer Liable MDN to Another Employee. Prior to transferring a mobile device or Customer Liable MDN that is enrolled in the Archived Messages Service to another person, you will disenroll or notify SMARSH to disenroll the then-current Participating Employee and the Customer Liable MDN on that mobile device from the Archived Messages Service.

2.7. Acknowledgement and Agreement. You acknowledge that AT&T will make the Archived Messages available to SMARSH for use in connection with the Archived Messages Service and that AT&T will have no further control for the Archived Messages after they are provided to SMARSH. You further agree that AT&T will have no responsibility or liability to You with respect to the Archived Messages after they are provided to SMARSH.

2.8. Limitations and Restrictions. You may access a Participating Employee's Archived Messages only with that Participating Employee's express knowledge and consent. You must maintain records of each Participating Employee's express, informed consent for You to collect and use his or her Archived Messages. If a Participating Employee revokes such consent at any time, then you must immediately cease initiating requests for that individual's Archived Messages.

2.9. Customer Business Records. You agree to maintain full, complete and accurate records related to Your performance under these Terms and Conditions, and You agree to preserve such records for five (5) years from the date of preparation; provided, however, that You agree to retain for at least five (5) years following Your latest access to Archived Messages Service records that are sufficient to demonstrate each Participating Employee's consent to Your access to and use of his or her Archived Messages. Such records shall be available for inspection and copying by AT&T during Your normal business hours, upon five (5) days' notice, but not more than once per quarter, unless otherwise required by applicable law, rule or regulation. If You fail to comply with the obligations set forth in this Section, or if AT&T's review of such records reveals that You are in violation of any of these Terms and Conditions, then, in addition to its other remedies under these Terms and Conditions, Your account agreement with AT&T or at law or in equity, AT&T may terminate your access to the Archived Messages.

2.10. Compliance with Laws, Policies and Practices. You agree to comply with all applicable laws, rules and regulations, including all applicable consumer protection, marketing, data security, export and privacy laws and Federal Trade Commission privacy initiatives. You are solely responsible for making any disclosures required by law, rule, regulation, or otherwise regarding the nature, accuracy, effectiveness, or limitations of the Archived Messages Service.

2.11. Indemnification. You agree to indemnify and hold AT&T, its officers, directors, employees and agents harmless from and against any claim, damage or loss that is related to or arising out of Your failure to comply with any of these Terms and Conditions, including reasonable attorney's fees.

VERIZON MOBILE TERMS

This agreement is between Verizon Wireless ("VZW" or "We") and you as a VZW subscriber ("You" or "Your") and it sets forth the terms and conditions under which You agree to use, and We agree to provide access to, Archived Messages through the Archived Messages Service (as such terms are defined below). By using the Archived Messages Service, You accept these Terms and Conditions, which may be modified from time to time.

1. Definitions.

1.1 Archived Messages means the Participating Employee's Messages available for retrieval by Smarsh Inc. ("Smarsh") from VZW.

1.2 Archived Messages Service means Smarsh's service that provides Archived Messages to You.

1.3 Customer Liable VZW MDN means a VZW Mobile Directory Number ("MDN") that is established under Your corporate account and corporate name for which You are financially responsible for the payment to VZW for VZW service.

1.4 Employee Liable VZW MDN means a VZW MDN that is established in the name of an individual employee of Your company and such individual employee is financially responsible for the payment to VZW for VZW services.

1.5 Messages means messages sent or received by the Participating Employee via the short message service (SMS) or the multimedia message service (MMS).

1.6 Participating Employee means Your employee who has opted into the Archived Messages Service via Your Corporate Liable VZW MDN.

2. Archived Messages Service.

2.1 You will only access, use, copy, store or disclose Archived Messages in accordance with these Terms and Conditions. You will not access, use, copy, store or disclose Archived Messages for any other purpose.

2.2 Smarsh Agreement. You will enter into an agreement with Smarsh for the Archived Messages Service and You will pay all of Smarsh's charges for such Archived Messages Service in accordance with such agreement.

2.3 Customer Liable VZW MDNs Only. You will enroll only Customer Liable VZW MDNs in the Archived Messages Service. You will not enroll any Employee Liable VZW MDNs in the Archived Messages Service.

2.4 Notice and Consent.

2.4.1. For Public Sector Only. Prior to enrolling any employee in the Archived Messages Service and accessing, using, storing, copying or disclosing any Participating Employee's Archived Messages, You, as a Public Sector employer, will provide advance disclosure to each employee containing clear and conspicuous notice of how You and Smarsh (and its affiliate(s)) will access, use, copy, retain, protect or disclose such employee's Archived Messages, as well as the duration and purpose of such access, use, copying or retention. Prior to enrolling any employee in the Archived Messages Service, and after providing the above-described disclosure, You will obtain the employee's consent, in writing or electronically, to the archiving of the employee's Archived Messages, including a consent for a carrier, including VZW, to share the Archived Messages with You and SMARSH and You will not access, use, store, copy or disclose any employee's Archived Messages until such consent has been obtained. The disclosure and consent must advise the employee that he/she/they are not permitted to allow anyone else to use their assigned device. In addition, VZW will send a free to end user text message to the device or MDN, pre-approved by You, with notice that You require archiving of text/SMS messages on Customer provided or funded devices, and that continued use of the device is deemed as the device or MDN user's consent to deliver Messages to You and/or SMARSH for archiving through the Archived Messages Service ("Consent Notice"). Successful delivery of the Consent Notice is a pre-requisite to VZW enabling Archived Messages through the Archived Messages Service. You will also include a similar notice and consent process in Your organization's device acceptable use policy.

2.4.2. For Non-Public Sector Only. Prior to enrolling any employee in the Archived Messages Service and accessing, using, storing, copying or disclosing any Participating Employee's Archived Messages, You, as a Non-Public Sector employer, will provide advance disclosure to each employee containing clear and conspicuous notice of how You and Smarsh (and its affiliate(s)) will access, use, copy, retain, protect or disclose such employee's Archived Messages, as well as the duration and purpose of such access, use, copying or retention. Prior to enrolling any employee in the Archived Messages Service, VZW will send a free to end user text message, pre-approved by You, to each employee containing a notice to opt-in to the Archived Messages Service, and You will not access, use, store, copy or disclose any employee's Archived Messages until such consent has been obtained.

2.5 Revocation of Consent. You will ensure that each Participating Employee may immediately revoke consent through mechanisms that are readily available to the Participating Employee. You will immediately notify Smarsh Inc. of any such revocation of consent so that Smarsh can notify VZW of such revocation. If consent is revoked, then You will not access, retrieve, use, store, copy or disclose such employee's Archived Messages dated after the revocation date. You may access, use, store, copy or disclose such employee's Archived Messages retrieved by You prior to such revocation date.

2.6 Transferring Mobile Device or Customer Liable VZW MDN to Another Employee. Prior to transferring a mobile device or Customer Liable VZW MDN enrolled in the Archived Messages Service to another employee, You will disenroll or notify SMARSH to disenroll from the Archived Messages Service the Participating Employee and the Customer Liable VZW MDN on that mobile device.

2.7 Periodic Reminders. You will provide periodic reminders to each Participating Employee of its enrollment in the Archived Messages Service.

2.8 Acknowledgement. You acknowledge that VZW will make available to Smarsh the Archived Messages for use in connection with the Archived Messages Service and VZW will have no further control or responsibility for the Archived Messages once they are provided to Smarsh.

2.9 Limitations and Restrictions. You may access the Participating Employee's Archived Messages only with that Participating Employee's express knowledge and consent. You must maintain records of each Participating Employee's express, informed consent for You to collect such Participating Employee's Archived Messages. If a Participating Employee revokes such consent at any time, then You must immediately cease initiating requests for that employee's Archived Messages.

3. Customer Business Records. You will maintain full, complete and accurate records related to Your performance under these Terms and Conditions, and shall preserve such records for five (5) years from the date of preparation; provided, however, that You will retain, for at least five (5) years following the latest access to Archived Messages, records sufficient to demonstrate each Participating Employee's consent to access and use its Archived Messages. Such records shall be available for inspection and copying by VZW during Your normal business hours, upon five (5) days' notice, but not more than once per quarter, unless otherwise required by applicable law, rule or regulation. If You refuse to comply with the obligations set forth in this Section or if VZW's review of such records reveals that You are in violation of any of these Terms and Conditions, then, in addition to its other remedies under these Terms and Conditions, Your account agreement with VZW, or at law or in equity, VZW may terminate Your access to the Archived Messages.

4. Compliance with Laws, Policies and Practices. You will comply with all applicable laws, rules and regulations, including all applicable consumer protection, marketing, data security, export and privacy laws and Federal Trade Commission privacy initiatives. You are solely responsible for making any disclosures required by law, rule, regulation, or otherwise regarding the nature, accuracy, effectiveness, or limitations of the Archived Messages Service.

5. Responsibility and Indemnification.

5.1 Responsibility. You assume all responsibility and risk for the Notice and Consent of Participating Employees and the Periodic Reminders as set forth above.

5.2 Indemnification.

5.2.1 You will defend, indemnify and hold harmless VZW, its Affiliates, and their respective directors, officers, employees, contractors, agents, shareholders, any successors and assigns and their respective heirs and legal representatives (collectively, the "VZW Indemnitees"), from and against any and all Claims and Losses, reasonable attorney's fees and defense costs arising out of, relating to or resulting from Your acts or omissions or Your failure to comply with the terms of Section 2.1 (c) Notice and Consent and 2.1(e) Periodic Reminders. For any Claims that are the subject of your indemnification obligations herein, VZW will have sole control of the defense, unless VZW tenders such defense thereof to You, and will provide You with reasonable information throughout the course of such defense. (i) "Claims" means any third party claims, demands, actions, disputes, controversies or requests for equitable or injunctive relief by a

Participating Employee that You have not complied with Your notice and/or consent requirements and (ii) "Losses" means any damages or settlement amounts payable to a Participating Employee as a result of the final adjudication or settlement of a Claim, including, without limitation, judgments, arbitration awards, payments of interest, fines, assessments, penalties and deficiencies, and any other losses, obligations, liabilities, costs or expenses suffered or incurred as a result of a Claim.

5.2.2 Your indemnification obligations are subject to the following: (a) You will cooperate reasonably with VZW in connection with any Claim; (b) You will not consent to the entry of any judgment or enter into any settlement of Claim without VZW's prior written consent, which will not be unreasonably withheld; and (c) You are obligated to VZW for its reasonable attorney's fees and expenses incurred in the enforcement of the indemnification hereunder.

6. Billing and Payment. The billing and payment terms set forth in your account agreement with VZW apply to all of Smarsh Inc.'s charges set forth on the VZW bill and You will pay VZW for all of Smarsh Inc.'s charges set forth on the VZW bill in accordance with that agreement

Updated November 2025

INFORMATION SECURITY ADDENDUM

1. Security Program

i. Smarsh has implemented and will maintain appropriate technical, physical, and administrative measures reasonably designed to prevent accidental or unlawful destruction, loss, alteration, or unauthorized disclosure of, or access to confidential information ("Information Security Program").

ii. Smarsh's Information Security Program oversees all areas of security applicable to Smarsh and information security, including physical access to Smarsh's data centers that store data ingested by the applicable service ("Client Data"), system and data access, transmission of Client Data, as well as general supervision and enforcement. Smarsh's Information Security Program generally aligns with the security standards published by International Organization for Standardization (ISO).

iii. Smarsh undergoes annual independent third-party SSAE 18 SOC 2 Type II (or its equivalent or successor) assessments of its Information Security Program. After each such assessment, Smarsh assesses the criticality of any issues presented in such report or assessment, and remediates, or implements compensating controls for, any issues identified in such assessment in a timely manner based on level of criticality and risk.

1.2 Personnel Security

Smarsh performs criminal background checks on all Smarsh employees prior to commencement of employment. Smarsh requires each employee to maintain the confidentiality of Confidential Information, including written confidentiality agreements and annual security and data privacy awareness training. Smarsh also requires additional role-based security training for employees with access to Client Data or the application that processes and stores Client Data.

1.3 Third Party Risk Management

Smarsh screens and enters into written confidentiality agreements with its vendors to maintain the security of Confidential Information. Smarsh conducts an initial risk assessment of each vendor, including an initial risk review and verification before engaging such vendor. Thereafter, Smarsh conducts an annual risk review of such vendor.

1.4 Smarsh's Access Security

i. Facilities Access. Smarsh employs physical security procedures which require that only authorized individuals have access to corporate facilities. Such procedures include the use of CCTV, cardkey access, processes to log and monitor visitors, and use of receptionists or security guards.

ii. Systems Access. Smarsh follows the principle of "least privilege" when granting access to Smarsh internal systems ("Smarsh Systems"). Smarsh uses complex password requirements across all Smarsh Systems to minimize password-related access control risks. Smarsh, when reasonably possible and feasible, utilizes multi-factor authentication for access and administration of Smarsh's Systems. Smarsh's

information security policies prohibit Smarsh employees from sharing, writing down, or storing passwords in an unencrypted manner on any Smarsh System (including desktops).

1.5 Application Security – Software as a Service

i. Applications. Smarsh provides various software as a service solution that, as configured by Client, capture, ingest, store, and archive Client Data from various third-party service providers of Client (each, a "SaaS Application").

ii. Software Code Review and Design. Smarsh uses a "security by design" approach that follows generally accepted industry standards for a secure software development life cycle. Smarsh performs both static and dynamic web application security code analysis on all code prior to deployment in a production environment. Smarsh uses a formal change management process that includes the tracking and approval for all software product updates and changes. Any such changes are internally reviewed and tested within a staging environment before such changes are finalized and deployed to production environments.

iii. Monitoring & Application Scanning. Smarsh, in accordance with generally accepted industry standards, monitors the SaaS Applications and the Smarsh networks, servers, and service environments hosting the SaaS Applications for potential security vulnerabilities consistent with Smarsh's vulnerability management program. Smarsh will promptly assess discovered security vulnerabilities talking into account the risk posed and prioritize them for remediation activities.

iv. Anti-Malware Testing. Smarsh, using industry-standard measures, on a regular basis, tests and scans the SaaS Applications for (a) 'back door,' 'time bomb,' 'Trojan Horse,' 'worm,' 'drop dead device,' 'virus', 'spyware' or 'malware;' or (b) any computer code or software routine that disables, damages, erases, disrupts or impairs the normal operation of the SaaS Applications or any component thereof.

v. Physical and Software Security. Smarsh's information security policy requires all network devices and servers that host or process Client Data to be secured to address reasonable threats through industry standard technical measures. Smarsh physically or logically separates quality assurance and test environments from production environments. Smarsh uses industry- standard firewalls, intrusion detection, and malware detection on its networks and hosted systems and requires the use of VPN for access to its secured environments.

vi. Client Data. Smash will not use Client Data for testing purposes or access Client Data, except as authorized by Client, or as required by the applicable services. Smarsh will not use any data derived from Client Data for any purpose except to provide the Services.

vii. Smarsh Physical Data Center Security. Smarsh ensures that physical security controls are implemented to prevent unauthorized individuals from accessing Smarsh data centers. Smarsh uses data center security measures that align with industry standard practices for physical security and, at a minimum, require that Smarsh data centers use: floor-to-ceiling walls, multi- factor authentication for data center access, 24/7 security monitoring, alarmed exits, and onsite security personnel.

viii. Cloud Environment Data Center Security. Smarsh may use infrastructure-as-a-service providers ("Cloud Providers") to provide the services (as applicable). Before utilizing a Cloud Provider, Smarsh evaluates the Cloud Provider's security controls and processes to ensure that such security program meets the applicable obligations contained in Smarsh's own Information Security Program. On a regular basis thereafter, Smarsh reviews each Cloud Provider's security controls as audited by Cloud Provider's third-party security audits and certifications to ensure that such Cloud Provider maintains its Security Program at a level consistent with Smarsh's Information Security Program. Such controls include the use, at a minimum, physical access controls, multi-factor authentication for data center access, 24/7 security monitoring, alarmed exits, and onsite security personnel.

ix. Penetration Testing. Smarsh performs annual penetration testing on the SaaS Applications using independent, third-party resources. Upon written request (and not more than once every 12 months), Smarsh will provide a summary penetration testing report to Client.

x. Performance. Smarsh uses industry-standard technology and tools to monitor the uptime status of its SaaS Applications and to send alerts when any warning conditions need to be reviewed.

xi. Data Management. Client Data is stored in a logically separated environment.

xii. Encryption. Smarsh encrypts Client Data in transit and at rest using encryption techniques that comply with security industry standards published by NIST.

1.6 Business Continuity/Disaster Recovery. Smarsh maintains a Business Continuity and Disaster Recovery Plan ("BCP") and shall activate the BCP in the event of a disaster, as defined in the BCP. Upon written request, Smarsh will make an executive summary of the BCP available to Client. Smarsh tests the BCP on a regular basis, and at least annually.

1.7 Incident Response.

i. Security Incident. Smarsh's Information Security Program includes incident response policies and procedures in the event that there is any actual, or reasonably suspected, unauthorized access to Smarsh facilities, Smarsh Systems, or the SaaS Applications ("Security Incident"), including processes to ensure that (i) the Security Incident is contained and remediated in a timely fashion; (ii) if required, timely notice is provided to any affected parties (iii) the Security Incident is appropriately tracked; (iv) all related server logs are retained for at least ninety (90) days following the Security Incident; (v) all related Security Incident reports are retained for at least three (3) years; and (vi) all related Security Incident logs are appropriately protected to ensure the integrity of such log. Smarsh will promptly implement such procedures upon becoming aware of a Security Incident.

ii. Client Data Incident. Upon becoming aware of any actual or reasonably suspected unauthorized third-party access to, or disclosure of, Client Data ("Client Data Incident"), Smarsh will: (i) investigate, and take reasonable measures to remediate, the cause of such Client Data Incident, and (ii) promptly, after discovery, provide written notice to the Incident Response Contact set forth in the Incident Contact Sheet.

2. Security Documentation; Audit Rights; Security Assessments

i. Security Documentation. Upon written request, not more than once every 12 months, and subject to the confidentiality obligations set forth in the Agreement, Smarsh will make available to Client, at no cost to Client, a copy of Smarsh's most recent (i) annual independent SSAE 18 SOC 2 Type II report, (ii) executive summary of Smarsh's annual penetration test, and (iii) Smarsh's standard information gathering questionnaire (collectively, "Security Packet") to demonstrate Smarsh's compliance with the Information Security Program.

ii. Security Assessments of Cloud Providers. Client recognizes that Smarsh utilizes Cloud Providers to process Client Data or provide the Services. Client agrees that Smarsh does not have access to, or control over, the physical infrastructure or facilities used by such Cloud Providers or the manner in which such Cloud Providers allow third parties to audit such Cloud Provider's security controls and processes. If Client wishes to conduct an audit of any related Cloud Provider applicable to the Services, Client may elect to do so in the manner set forth in this Section 3. Upon Client's written request (and no more than once every 12 months), and subject to the confidentiality obligations set forth in this Agreement, Smarsh agrees to use commercially reasonable efforts to provide Client with sufficient information to obtain such security documentation on its own.

SUPPORT AND SERVICE LEVEL AGREEMENT

1. SUPPORT

Smarsh offers a broad range of technical support services as set forth below.

2. SERVICE INCIDENTS AND SUPPORT REQUESTS

Except with respect to Severity Level 1 issues, Smarsh recommends reporting issues regarding availability or performance of the Services by creating a case at Smarsh Central. All Severity Level 1 issues must be reported via phone. Support requests must include a detailed description of the error or request, including the operating conditions that gave rise to the error. The individual requesting support will receive notification via email to confirm receipt of a Support request, along with a case number for reference. Smarsh standard phone support is available Monday through Friday between the hours of 8 am and 8 pm Eastern (excluding United States Federal or Smarsh- observed Holidays). If Client purchases a premium support package, standard phone support hours may be expanded. Off-hours phone support is available 24 hours per day, 365 days per year for Severity Level 1 issues. Smarsh may limit the right to submit support requests to a maximum of 10 Users, unless specified otherwise in the Agreement.

Severity	Description
1	Issue impacts multiple users: Service is down, or major functionality is unavailable or materially impacted by performance issues, and no workaround is available.
2	Issue impacts multiple users: important features are unavailable or degraded, or multiple users are degraded, and no workaround is available. Or The issue impacts a single user, major functionality is unavailable or materially impacted by performance issues, and no workaround is available.
3	Issue impacts multiple or single users: important features are unavailable, but a workaround is available, Or intermittent disruption of Services.
4	A minor feature is unavailable, Or there is a minor performance impact.

Initial Response

After Client creates a case, Smarsh will use commercially reasonable efforts to respond to Client within the target response time indicated below for the corresponding severity level and support package. For all packages, Smarsh will respond to routine service requests (e.g. requests for information, password

resets, reports of potential defects, feature requests, and troubleshooting guidance) within one business day.

Target Initial Response Time	
Severity	**Basic**
1	60 minutes
2	2 hours
3	4 hours
4	1 Business Day

Resolution Process

Smarsh will address and resolve issues with the Services reported by Client that are within the control of Smarsh based on the resolution process indicated below for the corresponding severity level. If Client purchases a premium support package, Smarsh will provide notification of a target resolution or workaround plan, updates, and escalation based on the process for the corresponding severity level specified below, unless specified otherwise in the Agreement.

Severity	Resolution Process
1	Smarsh will investigate the issue and will work continuously until the error is fixed or a temporary workaround is implemented.
2	Smarsh will investigate the issue and will work continuously until the error is fixed or a temporary workaround is implemented.
3	Smarsh will work during normal business hours to investigate the issue and implement a fix or workaround.
4	Smarsh will work to provide a fix in the next maintenance release.

Escalation Process

Client may escalate an active support case if (i) Client is not satisfied with the resolution method implemented by Smarsh, (ii) there has been a significant change in the business impact to Client after the issue was reported, or (iii) Smarsh fails to respond in a timely manner during the resolution process. Instructions for initiating the escalation process are available at Smarsh Central.

3.3. Service Levels

This section applies only to those SaaS Services set forth specifically herein. It does not apply to products that are deployed on-premises.

i. Definitions

"Availability" means that Client can access the platform and is measured using the formula in section 2.2 below.

"Downtime" means service interruptions that occur outside applicable maintenance windows specified in section 2.4 below, including Planned Maintenance, Emergency Maintenance, and Outages.

"Emergency Maintenance" means maintenance required to: (i) maintain Availability on a go-forward basis, or (ii) execute a critical security change.

"Outages" means unplanned service interruptions that temporarily prevent access to major functions of the applicable platform.

"Planned Maintenance" means: (i) maintenance that occurs during applicable maintenance windows specified in section 2.4 below, or (ii) maintenance that occurs outside applicable maintenance windows for which Smarsh has provided advance notice in accordance with section 2.4 below.

ii. Uptime Commitment

The Availability for the production instance of those SaaS Services (set forth below during each calendar month (the "Uptime Commitment") is as specified below. The Uptime Commitments specified below do not apply to user acceptance testing environments or other non-production environments.

Product	Uptime Commitment
Capture Mobile	99.9%

Availability is measured using the following industry-standard formula:

4. Service Credits

If Smarsh does not meet its Uptime Commitment in any calendar month, Smarsh will issue Client a credit for a portion of Client's platform Fees for the affected Service in accordance with the table below. Client must request credits within thirty (30) days from the end of the month in which Smarsh did not meet its Uptime Commitment. Smarsh will use its diagnostic monitoring tools to verify its failure to meet its Uptime Commitment before Smarsh issues a credit. Smarsh will apply applicable credits to Client's next invoice.

Uptime	Service Credit
98.0% - 99.89%	5% of monthly platform Fee (or 0.5% of annual platform Fee)
95.0% - 97.9%	10% of monthly platform Fee (or 1% of annual platform Fee).

Below 95.0%	20% of monthly platform Fee (or 1.75% of annual platform Fee)

5. Maintenance Windows

Smarsh provides maintenance notifications and reminders, and Client may subscribe to such notifications and reminders, through the Status Page at https://status.smarsh.com/.

Capture Platform and Capture Mobile. To the extent reasonably possible, Smarsh will refrain from performing maintenance that causes interference with or disruption to Client's access to Cloud Capture Mobile during normal business hours for the region in which Client's Cloud Capture Mobile instance is deployed. Smarsh will perform planned maintenance during the maintenance windows specified below. To the extent feasible, Smarsh will provide at least three (3) days' advance notice of any maintenance it will perform outside its maintenance windows and that may cause interference with or disruption to Client's access to Cloud Capture Mobile. Smarsh may perform Emergency Maintenance without providing advance notice to Client.

Capture Mobile maintenance windows:

- Mon-Fri: 12 AM - 5AM and 8 PM - 11:59 PM
- Weekends: any time

The times specified above are local to the region in which Client's Cloud Capture Mobile instance is deployed.

EXHIBIT A

GOVERNMENT RIDER TO SUPPLIER USER LICENSE AGREEMENT AND TERMS OF SERVICE

1. This Government Rider ("Rider") and attached commercial supplier agreement (e.g. terms of sale or lease, Terms of Service, End User License Agreement, or another similar legal instrument or agreement) as defined in 48 C.F.R. 502.101 ("CSA"), regardless of the media or delivery mechanism used to deliver the CSA, establish the terms and conditions enabling Verizon to provide software and/or services to Government agencies ("Government"). Section 22 applies to licensees under a state or local agency Master Contract, if applicable.
2. Applicability. The CSA is a part of a contract between the Supplier and the Government for the acquisition of the supply or service that necessitates a license or other similar legal instrument (including all contracts, task orders, and delivery orders under FAR Part 12).
3. End user. The CSA shall bind the ordering activity as end user but shall not operate to bind a Government employee or person acting on behalf of the Government in his or her personal capacity.
4. Law and disputes. The CSA is governed by Federal law and any language in the CSA on the following subjects that is different from that prescribed by applicable Federal law is hereby deleted:
    a) Any language purporting to subject the Government to the laws of a U.S. state, U.S. territory, district, or municipality, or a foreign nation, except where Federal law expressly provides for the application of such laws.
    b) Any language requiring dispute resolution in a specific forum or venue.
    c) Any language prescribing a different time period for bringing an action in relation to a dispute.
5. Continued performance. Subject to FAR 52.212-4(f) Excusable delays, Supplier shall not unilaterally revoke, terminate or suspend any rights granted to the Government except as allowed herein. If Supplier believes the ordering activity to be in breach of the agreement, it shall pursue its rights under the Contract Disputes Act or other applicable Federal statute while continuing performance as set forth in the prime contract Disputes clause.
6. Arbitration; equitable or injunctive relief. In the event of a claim or dispute arising under or relating to the CSA, (A) binding arbitration shall not be used unless specifically authorized by agency guidance, and (B) equitable or injunctive relief, including the award of attorney fees, costs or interest, may be awarded against the Government only when explicitly provided by statute.
7. Updating terms. After award, the contractor may unilaterally revise CSA terms if they are not material. A material change is defined as: (1) terms that change the Government's rights or obligations; (2) terms that increase Government prices; (3) terms that decrease overall level of service; or (4) terms that limit any other Government right addressed elsewhere in the prime contract. For revisions that will materially change the terms of the contract, the revised CSA must be incorporated into the contract using a bilateral modification. Any CSA terms revised unilaterally subsequent to award that are inconsistent with any material term or provision shall not be enforceable against the Government, and the Government shall not be deemed to have consented to them.
8. No automatic renewals. If any license or service tied to periodic payment is provided in the CSA (e.g., annual software maintenance or annual lease term), such license or service shall not renew automatically upon expiration of its current term without prior express consent by an authorized Government representative.

9. Indemnification. Any clause of the CSA requiring the Supplier to defend or indemnify the end user is hereby amended to provide that the U.S. Department of Justice has the sole right to represent the United States in any such action, in accordance with 28 U.S.C. § 516.

10. Audits. Any clause of the CSA permitting the commercial supplier or licensor to audit a Government end user's compliance with this agreement is hereby amended as follows: (A) discrepancies found in an audit may result in a charge to the ordering activity. Any resulting invoice must comply with the proper invoicing requirements specified in the underlying Government contract or order; (B) this charge, if disputed by the ordering activity, will be resolved in accordance with the prime contract's Disputes clause; no payment obligation shall arise on the part of the ordering activity until the conclusion of the dispute process; (C) any audit requested by the contractor will be performed at the Supplier's expense, without reimbursement by the Government or Verizon.

11. Taxes or surcharges. Any taxes or surcharges which Supplier seeks to pass along to the Government as end user will be governed by the terms of the underlying Government contract or order and, in any event, must be submitted to the Contracting Officer for a determination of applicability prior to invoicing unless specifically agreed to otherwise in the Government contract.

12. Non-assignment. The CSA may not be assigned, nor may any rights or obligations thereunder be delegated, without the Government's prior approval, except as expressly permitted under subparagraph (b) of GSAR 552.212-4.

13. Confidential information. If the CSA includes a confidentiality clause, such clause is hereby amended to state that neither the agreement nor the contract price list, as applicable, shall be deemed "confidential information." Issues regarding release of "unit pricing" will be resolved consistent with the Freedom of Information Act (FOIA). Notwithstanding anything herein to the contrary, the Government may retain any confidential information as required by law, regulation or its internal document retention procedures for legal, regulatory or compliance purposes; provided, however, that all such retained confidential information will continue to be subject to the confidentiality obligations of this agreement.

14. Unilateral Termination. Subject to FAR 52.212-4(f) Excusable delays (JUN 2010), unilateral termination by Supplier does not apply to a Government order. All clauses in the CSA referencing such rights are deleted.

15. Waiver of Jury Trial. All clauses referencing waiver of Jury Trial are subject to FAR Clause 52.233-1, Disputes (JUL. 2002), and all clauses governing waiver of jury trial in the CSA are deleted.

16. Customer Indemnities. All CSA clauses requiring Customer Indemnities (as applicable to the Government) are deleted.

17. Future Fees or Penalties. All CSA clauses that violate the Anti-Deficiency Act (31 U.S.C. §1341, 41 U.S.C. § 11), which prohibits the Government from paying any fees or penalties beyond the Contract amount, unless specifically authorized by existing statutes, such as the Prompt Payment Act, or Equal Access To Justice Act 31 U.S.C. § 3901, 5 U.S.C. § 504 are deleted.

18. Third Party Terms. Should the Government require any modification to the CSA outside of this Rider, the supplier and/or third party manufacturer will be brought into the negotiation.

19. Limitation of Liability: Verizon, Supplier and Ordering Activity shall not be liable for any indirect, incidental, special, or consequential damages, or any loss of profits, revenue, data, or data use. Further, Verizon, Supplier and Ordering Activity shall not be liable for punitive damages except to the extent this limitation is prohibited by applicable law. This clause shall not impair the U.S.

Government's right to recover for fraud or crimes arising out of or related to this Government Contract under any federal fraud statute, including the False Claims Act, 31 U.S.C. §§ 3729-3733.

20. Advertisements and Endorsements. Unless specifically authorized by an Ordering Activity in writing, such use of the name or logo of any Government entity is prohibited.

21. Public Access to Information. Supplier agrees that this Rider and the CSA contain no confidential or proprietary information and acknowledges they will be available to the public.

22. Harmonization with State & Local Contracts. To the extent the CSA is part of a Master Contract with any state or local government entity ("Master Contract"), the foregoing provisions are modified as follows:

    d) Acceptance. Date of acceptance shall be governed by the Master Contract, and if silent as to such matters, the date of acceptances shall be the date of first use by an authorized end-user.

    e) Choice of Law. Section 4 hereof shall be governed by the choice of law provisions of the Master Contract.

    f) Contracting Officer. References to the term "Contracting Officer" shall mean the procurement officer or other person designated as the state entity's administrative or contracting authority under the Master Contract.

    g) Laws and Regulations. All references to Federal laws and regulations in this Rider shall be interpreted as incorporating their state and local equivalents in lieu of such Federal references.

23. If any language, provision, or clause of the CSA conflicts or is inconsistent with this Rider, the language, provisions or clause of this Rider shall prevail to the extent of such inconsistency.

24. If the CSA is invoked through an "I agree" click box or other comparable mechanism (e.g., "click-wrap" or "browse-wrap" agreements), execution does not bind the Government or any Government authorized end user to such clause.