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.

2. **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.

3. **Security Documentation; Audit Rights; Security Assessments**

i. **Security Documentation.** Upon written request, 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. **Audit Rights** Upon Client's written request (and no 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, Smarsh's Security Packet to demonstrate its compliance with the Information Security Program. After reviewing the Security Packet, if Client identifies areas of concern that have not been covered and are areas that Client is lawfully able to audit under applicable **laws, rules, or regulations**, then Client may submit to Smarsh additional reasonable requests for information regarding those areas of concern that are necessary to confirm Smarsh's compliance with its Security Program. If Client has additional requests for information outside the scope of this Section 2, Smarsh, at Client's sole expense, will respond to such additional requests for information about Smarsh's Security Program, including additional security questionnaires, subject to Smarsh's standard hourly rate of $300/hr. Prior to completing such additional security questionnaire(s), Smarsh will provide Client with an estimate of the cost associated with responding to such questionnaire, and may request a deposit, before beginning such work.

iii. **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 2. Upon Client's written request (and no more than once every month), and subject to the confidentiality obligations set forth in this Agreement, Smarsh agrees to use commercially reasonable efforts to obtain the applicable sub-processor's or cloud provider's internal or independent security audit reports or SIG on behalf of the Client, and Smarsh shall provide such security documentation to the Client to the extent permitted and feasible. If Smarsh cannot provide such security documentation to the Client, Smarsh agrees to use commercially reasonable efforts to provide Client with sufficient information to obtain such security documentation on its own.

smarsh
Capture. Reveal. Respond.

Incident Response Contact Sheet

In the event of a Security Incident or Client Data Incident, Smarsh will notify the following contact:

Main Contact:

Name:

Title:

Contact Information:

Email:

Phone:

Backup Contact:

Name:

Title:

Contact Information:

Email:

Phone: