Information Security Addendum

Overview

Smarsh will implement and maintain a written information security program that maintains administrative, technical, and physical safeguards, designed to:

- ensure the security and confidentiality of all Client Confidential Information that is processed, stored, or controlled by Smarsh;
- protect against anticipated threats or hazards to the security or integrity of such Confidential Information;
- prevent unauthorized access to or loss, acquisition, disclosure, or use of such Confidential Information; and
- ensure the secure disposal of such Confidential Information in compliance with applicable National Institute of Standards and Technology (NIST) standards.

Smarsh will use reasonable efforts to ensure its written information security program and administrative, technical, and physical safeguards align with accepted industry practices [such as applicable security standards published by International Organization for Standardization (ISO) or NIST], and comply with applicable data protection and privacy laws, as well as the terms and conditions of the Agreement, including those contained in this Information Security Addendum. Detailed information about Smarsh's information security program is contained in the security documentation available by secure login at https://central.smarsh.com.

Smarsh will designate a security manager to oversee its information security program and ensure its compliance with this Information Security Addendum.

1. Personnel Security

1.1. Screening. Smarsh will perform criminal background checks on all Smarsh employees prior to commencement of employment. Smarsh shall not allow any employee to perform services for Client or to access Client Data if such background checks reveal such individual was convicted of a crime involving any type of theft, fraud, bribery, other dishonest acts or the violation of any securities law.

1.2. Training. Smarsh will provide annual security awareness training to all Smarsh employees and contractors and will require Subcontractors to provide such training for their employees. Smarsh will provide additional role-based security training for Smarsh employees and contractors with access to Client Data or the applications that process and store Client Data.

1.3. Revocation. Smarsh will revoke physical and logical access for each Smarsh employee within 24 hours of such employee's termination of employment.

2. Facilities & Systems Security

2.1. Facilities Access. Smarsh will employ physical security procedures to ensure that only authorized individuals and guests have access to corporate facilities. Such procedures will include the use of CCTV, cardkey access, processes to log and monitor visitors, and use of receptionists or security guards. Smarsh will maintain surveillance records for at least ninety (90) days.

2.2. Systems Access. Smarsh will follow the principle of "least privilege" when granting access to Smarsh systems. Smarsh will enforce complex password requirements across all Smarsh systems to minimize password-related access control risks. Smarsh will utilize multi-factor authentication when feasible. Smarsh's information security policies will prohibit Smarsh employees from sharing, writing down, emailing, IM'ing or storing passwords unencrypted on any Smarsh system (including desktops).

3. Product Security

3.1. Smarsh will leverage a "security by design" approach and will utilize a software development life cycle that follows best practices defined by NIST and the OWASP Software Assurance Maturity Model (SAMM).

3.2. Smarsh will proactively ensure the security of its applications and environment by leveraging a "security by design" approach. Smarsh will, in accordance with industry accepted benchmarks such as those published by the Center for Internet Security (or equivalent), security-harden all network devices and servers that will host or process Client Data and code or web applications that are under Smarsh control. Smarsh will perform both static and dynamic automated web application security code analysis on all code prior to deployment in a production environment and correct security flaws discovered by source code analyses prior to deployment. Smarsh will, in accordance with generally accepted industry standards, monitor the Services and Smarsh networks, servers, and applications for potential security vulnerabilities. Smarsh will promptly respond to any identified vulnerabilities and assess criticality to resolve, or implement compensating controls for, such identified vulnerabilities within a reasonable amount of time, taking into account the risks posed by each such vulnerability.

3.3. Smarsh will employ then-current industry-standard measures to test the Services 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 Services or any component thereof.

3.4. Smarsh QA and test networks and environments will be physically or logically separated from production networks and environments and will not be globally accessible to anyone on the internet. Administrative passwords across QA and test environments will be different than those used in production environments.

3.5. Smarsh will enforce a formal change management process which will include tracking and approving all product changes. Any such changes will be internally reviewed and tested within a staging environment before such changes are finalized and deployed.

3.6. Smarsh will not use Client Data for testing purposes.

4. Data Center Security

4.1. Data Center Access. Smarsh will employ physical security procedures and controls to ensure that only authorized individuals have access to Smarsh data centers.

4.2. Physical Security. Smarsh will employ data center security measures that align with the AICPA trust principles for physical security and will, at a minimum, secure Smarsh data centers using: floor-to-ceiling walls, multi-factor authentication for data center access, 24/7 security monitoring, alarmed exits, and onsite security personnel.

4.3. Data Center Locations. Smarsh primary and disaster recovery data centers will be located in geographically diverse locations to enhance security, availability, and resiliency.

5. Secure Configuration

Smarsh will use the Center for Internet Security (CIS) benchmarks for its secure baseline configurations. Smarsh will use secure configuration management tools to alert of changes to baseline configurations.

6. Data Management

6.1. Segregation. Client Data will be logically segregated from the data of other Smarsh clients.

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

6.3. Back-ups. Smarsh leverages data replication across multiple geographically dispersed data centers as well as a local backup data center.

6.4. Media Destruction. Smarsh will ensure removal of all data from any media taken out of service and destroy or securely erase such media to make it unreadable, undecipherable, and unrecoverable by any means in compliance with applicable NIST standards.

6.5. Removable media. Smarsh will not allow its employees to store Client Data on any portable removable media (such as USB mass storage, external hard drives, and CD/DVDs); provided, however, that if storage on removable media is required to support the services (such as for client-requested data exports) provided under the Agreement, portable removable media must be encrypted as described above in Section 4.2.

7. Vulnerability Management

7.1. Smarsh will deploy vulnerability scanning mechanisms in its information systems and on hosted applications and will configure such mechanisms to conduct regular scans on Smarsh operating systems and infrastructure, web applications, and databases. Smarsh will analyze and assess all scan reports.

7.2. Smarsh will undergo annual penetration testing and will conduct quarterly security audits to identify potential vulnerabilities in the infrastructure used to provide the Services. Smarsh will implement a software/firmware patching program and will apply updates to all infrastructure components in a timely manner in accordance with the NIST 800-53 vulnerability remediation guidelines for critical or high-risk vulnerabilities.

8. Application Performance and Security

Smarsh will use industry-standard technology and tools to monitor the uptime status of its hosted applications and send alerts when any warning conditions need to be reviewed. Smarsh will use industry-standard firewalls, IDS/IPS technology, and malware detection on its networks and hosted applications and will harden its device configurations. Smarsh will require the use of VPN for access to its secure networks.

9. Business Resiliency and Incident Response

9.1. Incident Response. Smarsh's information security program will include written incident response policies and procedures to define roles and responsibilities in the event that there is any actual, or reasonably suspected, unauthorized access to Smarsh facilities or Smarsh systems ("**Security Incident**"). Such policies and procedures will include processes to ensure that (i) server logs are maintained; (ii) all

Security Incidents (defined below) are appropriately logged; (iii) all such server logs are retained for at least ninety (90) days; (iv) all such Security Incident logs are retained for at least three (3) years; and (v) all such logs are appropriately protected to ensure the integrity of such log. Smarsh will immediately implement such procedures immediately upon becoming aware of a Security Incident.

9.2. 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) immediately investigate, and take reasonable measures to remediate, the cause of such Client Data Incident, and (ii) promptly, but no later than forty-eight (48) hours after discovery, notify Client of such Client Data Incident. The notification will include, to the extent known, details of the incident, including the time, date, and nature of the incident and contact information for a member of Smarsh's information security team who can answer additional questions.

9.3. Business Continuity/Disaster Recovery. Smarsh will maintain a Business Continuity and Disaster Recovery Plan ("BCP") for the Services and implement the Plan in the event of a disaster, as defined in the BCP. The BCP will include disaster avoidance procedures which are designed to safeguard Client Data and Smarsh's data processing capabilities in the event of a disaster as defined in the BCP. Smarsh will make an executive summary of the BCP available in its Security Packet. Smarsh will test the BCP on at least an annual basis.

10. Annual Security Reviews

10.1. Smarsh will undergo an annual independent third-party SSAE 16 SOC 2 Type II (or its equivalent or successor) assessment of its information security program and its administrative, technical, and physical safeguards for all facilities used to deliver the Services. Such assessment will include, at a minimum, a network-level vulnerability assessment based on recognized industry practices.

10.2. Smarsh will assess criticality and remediate, or implement compensating controls for, all issues identified in such assessment in a timely manner based on level of criticality and risk.

10.3. Smarsh will include an executive summary of the results of such assessment in the Security Packet available to Client via login at https://central.smarsh.com.

11. Vendor and Third-Party Security

11.1. Risk Assessments. Smarsh will conduct an initial risk review and verification before engaging third-party vendors or subcontracting any of the Services. Thereafter, Smarsh will conduct annual risk reviews of such third-party vendors and subcontractors.

11.2. Subcontractors. A list of Smarsh subcontractors is available at https://www.smarsh.com/legal/subprocessors. Smarsh will provide prior notice to Client and allow time for Client to object before Smarsh engages any new subcontractors who will have access to or process Client Data. If Smarsh uses subcontractors to perform any of the Services, Smarsh will (a) enter into a written agreement with each such subcontractor that imposes obligations on the subcontractor (i) that are at least as restrictive as those imposed on or required of Smarsh under the applicable provisions of the Agreement and (ii) that prohibit the subcontractor from accessing or using Client Data except to the extent necessary to perform the subcontracted services; (b) only disclose Client Data to such subcontractor to the extent necessary for the subcontractor to perform the subcontracted services, (c) not be relieved of any of its obligations under this Agreement; and (d) remain liable and responsible for the performance or non-performance of such subcontractor.

12. Client Security Assessments

12.1. Security Documentation. To facilitate Client's risk-based assessment of Smarsh's information security program and administrative, technical, and physical safeguards applicable to Client's Confidential Information, Smarsh will make its Security Packet available to Client via https://central.smarsh.com. The Security Packet includes, among other documentation, Smarsh's completed industry-standard information gathering questionnaire ("SIG") and Smarsh's annual independent SSAE 16 SOC 2 Type II report. Smarsh will update the Security Packet on a regular basis. If Client requests that Smarsh complete Client's security or other questionnaire(s) in lieu of, or in addition to, the Security Packet, Client must execute an order form and pay a professional services fee based on the size and scope of such questionnaire(s).

12.2. On-site Assessments. Where sufficient to allow Client to complete its risk-based assessment of Smarsh's information security program and administrative, technical, and physical safeguards applicable to Client's Confidential Information, Client shall refer to Smarsh's Security Packet. If Client desires to complete an on-site assessment, Client may conduct no more than one on-site assessment in a 12-month period, all such requests must be received by Smarsh at least 30 days prior to the requested assessment date, all such on-site assessments must be conducted during Smarsh's normal business hours, and Client shall bear all costs associated with such on-site assessment. Smarsh will scope the work required to facilitate such assessment and provide Client with a quote for the professional services fees associated with such on-site assessment. If Client desires to proceed with such on-site assessment, Client must execute an order form or statement of work for such on-site assessment and provide Smarsh with its proposed list of

attendees. Smarsh will invoice Client for such on-site assessment, and Client shall pay the associated fees within 30-days of the invoice date.

13. Export Controls

Smarsh will comply with the export laws and regulations of the United States and other applicable jurisdictions when providing the Services. Smarsh will neither conduct business with nor allow access to its information systems by (a) any person on a government promulgated export restriction list; (b) any U.S.-embargoed countries; or (c) any organization or company on the U.S. Commerce Department's "Denied Parties List."