REPORT ON SMARTSHEET INC.'S CLOUD BASED PLATFORM RELEVANT TO SECURITY, AVAILABILITY AND CONFIDENTIALITY FOR THE PERIOD SEPTEMBER 1, 2018 TO AUGUST 31, 2019

SOC 3® - SOC for Service Organizations: Trust Services Criteria for General Use Report

COALFIRE CONTROLS

TABLE OF CONTENTS

SECTION 1

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To: Smartsheet Inc. ("Smartsheet")

Scope

We have examined Smartsheet's accompanying assertion titled "Assertion of Smartsheet Inc. Management" (assertion) that the controls within Smartsheet's Cloud Based Platform (system) were effective throughout the period September 1, 2018 to August 31, 2019, to provide reasonable assurance that Smartsheet's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability and confidentiality (applicable trust services criteria) set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Service Organization's Responsibilities

Smartsheet is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Smartsheet's service commitments and system requirements were achieved. Smartsheet has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Smartsheet is responsible for selecting, and identifying in its assertion, the applicable trust service criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements.
- Assessing the risks that controls were not effective to achieve Smartsheet's service commitments and system requirements based on the applicable trust services criteria.
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Smartsheet's service commitments and system requirements based on the applicable trust services criteria.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within Smartsheet's Cloud Based Platform were effective throughout the period September 1, 2018 to August 31, 2019, to provide reasonable assurance that Smartsheet's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Coalfire Controls LLC

Westminster, Colorado
December 16, 2019

SECTION 2

ASSERTION OF SMARTSHEET INC. MANAGEMENT

Assertion of Smartsheet Inc. Management

We are responsible for designing, implementing, operating and maintaining effective controls within Smartsheet Inc.'s ("Smartsheet") Cloud Based Platform (system) throughout the period September 1, 2018 to August 31, 2019, to provide reasonable assurance that Smartsheet's service commitments and system requirements relevant to security, availability and confidentiality were achieved. Our description of the boundaries of the system is presented in attachment A and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period September 1, 2018 to August 31, 2019, to provide reasonable assurance that Smartsheet's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability and confidentiality (applicable trust services criteria) set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*). Smartsheet's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in attachment B.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period September 1, 2018 to August 31, 2019 to provide reasonable assurance that Smartsheet's service commitments and system requirements were achieved based on the applicable trust services criteria.

Smartsheet Inc.

ATTACHMENT A

SMARTSHEET INC.'S DESCRIPTION OF THE BOUNDARIES OF ITS CLOUD BASED PLATFORM

TYPE OF SERVICES PROVIDED

Smartsheet Inc. (“Smartsheet”) is a software-as-a-service (SaaS) company formed in 2006 and headquartered in Bellevue, Washington, which offers a Cloud Based Platform for work execution, enabling teams and organizations to plan, capture, track, automate, and report on work at scale, helping to result in more efficient processes and better business. Smartsheet’s Cloud Based Platform is used by thousands of businesses and millions of users in countries throughout the world. Customers range from small and medium-sized businesses, Fortune 500 companies, and academic institutions, as well as local and federal government agencies.

Smartsheet’s Cloud Based Platform provides a number of solutions for customers that strive to eliminate obstacles to capturing information, including a spreadsheet interface, as well as customizable forms. The reporting and automation capabilities help reduce time spent on administration and repetitive work and allows teams to apply business logic to automate repetitive actions using a list of conditions. Business users, with little or no training, can configure and modify the platform to customize workflows to suit their needs. In January and May of 2019, Smartsheet acquired 10,000 ft and Slope, respectively, enabling organizations to improve capacity and resource management, and enhancing the ability for users to collaborate and manage creative work. The user interface and functionality allows users to realize the benefits of the platform without changing the behaviors developed using lightweight productivity tools. Customers access the platform online via app.smartsheet.com, via the mobile applications for Android and iOS, or through integrations with leading web services

The boundaries of the system are the specific aspects of Smartsheet’s infrastructure, software, people, procedures, and data necessary to provide its services and that directly support the services provided to customers. Any infrastructure, software, people, procedures and data that indirectly support the services provided to customers are not included within the boundaries of the system.

The components that directly support the services provided to customers are as follows:

INFRASTRUCTURE

The Smartsheet Cloud Based Platform is hosted on either dedicated infrastructure managed by third-party hosting provider Equinix or cloud services provider Amazon Web Services (AWS). Smartsheet leverages its providers’ ability to deliver sufficient capacity and availability for its customers’ current and future needs, and to maximize performance and reliability.

SOFTWARE

The main Smartsheet Cloud Based Platform is built on a Linux based platform, utilizing modern acid-compliant relational database management system (RDBMS) backends and a proprietary data access framework. Application processing is built on Java, JavaScript, and other proven open source tools, including Apache Tomcat, HTTP, and Poor Obfuscation Implementation (POI), among others. All software used in the Smartsheet Cloud Based Platform is vetted by Company security and operations teams to ensure compliance and reliability objectives are addressed.

PEOPLE

Smartsheet maintains multiple discipline-aligned teams to promote secure development practices while minimizing total time to market for approved features. Smartsheet Quality Assurance personnel perform both automated and manual testing of all product releases. The Infrastructure and Operations teams are responsible for product delivery and providing design input as needed. These roles ensure adequate capacity, and approval and implementation of scaling plans. The Architecture Security Team is involved in

all stages of application development, testing, and delivery to act as the primary stewards of customer trust and data integrity.

PROCEDURES

Smartsheet has documented policies and procedures to support the operations and controls over its physical and logical environments. Specific examples of the relevant policies and procedures include the following:

- Policy management and communication
- System security administration
- Server security configuration
- Network operations
- Enterprise change management
- Incident/problem management
- Physical security administration
- Data retention and off-site storage

DATA

Smartsheet processes customer data in one of two categorizations. Customer relationship data is data that is provided by customers in order to facilitate the business relationship (e.g., billing addresses, email addresses, application preferences, etc.). Customer Relationship Data is available to personnel at Smartsheet on a need-to-know basis and is governed by corporate IT controls. Protected customer data is any data that is uploaded or submitted to the Cloud Based Platform by the customer and/or collected by the customer through use of forms or similar features. Ownership of Protected Customer Data is dictated directly by the customer, and any designated system administrators for that customer. Any access to Protected Customer Data by Smartsheet personnel is governed by one of two mechanisms:

- The primary means of access is for the customer to explicitly share Protected Customer Data with Smartsheet personnel as they would any other collaborator within the Cloud Based Platform. This interaction is then governed by the same controls that would apply to any Smartsheet customer. There is no additional access available to Smartsheet personnel by nature of that sharing action.
- The secondary means of access is extremely rare and limited to Company core team operations specialists who have been specifically trained and approved. Direct access may be granted in order to investigate potential abuse of the Cloud Based Platform or to respond to lawful requests for Protected Customer Data such as a subpoena. This secondary means is outlined to customers in the agreements that govern their use.

ATTACHMENT B

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Commitments are declarations made by management to customers regarding the performance of Smartsheet's Cloud Based Platform. Commitments are communicated on Smartsheet's online User Agreement.

System requirements are specifications regarding how Smartsheet's Cloud Based Platform should function to meet Smartsheet's principal commitments to user entities. System requirements are specified in the Smartsheet's policies and procedures, which are available to all employees.

Smartsheet's commitments include the following:

- Smartsheet shall maintain a comprehensive written information security program, including policies, standards, procedures, and related documents that establish criteria, means, methods, and measures governing the processing and security of customer content.
- If Smartsheet becomes aware of confirmed unauthorized or unlawful access to any customer content processed by Smartsheet Information Systems, Smartsheet will promptly notify the customer of the security incident, and take reasonable steps to mitigate the effects and to minimize any damage resulting from the security incident.
- Smartsheet shall implement appropriate physical, organizational, and technical controls designed to ensure the security, integrity, and confidentiality of customer content accessed, collected, used, stored, or transmitted to, or by Smartsheet.
- Smartsheet shall implement appropriate physical, organizational, and technical controls designed to protect customer content from known or reasonably anticipated threats or hazards to its security, integrity, accidental loss, alteration, disclosure, and other unlawful forms of processing.
- Smartsheet will maintain and enforce appropriate information security, confidentiality, and acceptable use policies for employees, subcontractors, agents, and suppliers that meet the standards set forth in its security practices, including methods to detect and log policy violations.
- Smartsheet will maintain a disaster recovery program designed to recover the subscription service availability following a disaster.

Smartsheet's system requirements include the following:

- Employee provisioning and deprovisioning standards
- Logical access controls such as use of user IDs and passwords to access systems
- Access reviews
- Intrusion detection and prevention standards
- Incident handling standards
- Vendor management
- System monitoring
- Backup and recovery standards
- Data classification
- Data handling standards
- Risk assessment standards
- Change management controls
- Monitoring controls