chronicle

System and Organization Controls (SOC) 3 Report on the Chronicle Services System Relevant to Security, Availability, and Confidentiality For the Period 1 February 2019 to 30 April 2019

Chronicle, LLC
1600 Amphitheatre Parkway
Mountain view, CA 94043

Management's Report of its Assertion on the Effectiveness of its Controls Over the Chronicle Services System based on the Trust Services Criteria for Security, Availability, and Confidentiality

We, as management of, Chronicle LLC ("Chronicle" or " the Company") are responsible for:

- Identifying the Chronicle Services System (System) and describing the boundaries of the System, which are presented in Attachment A
- Identifying principal service commitments and system requirements
- Identifying the risks that would threaten the achievement of its principal service commitments and system requirements that are the objectives of our system, which are presented in Attachment B
- Identifying, designing, implementing, operating, and monitoring effective controls over the Chronicle Services System to mitigate risks that threaten the achievement of the principal service commitments and system requirements
- Selecting the trust services categories that are the basis of our assertion

We assert that the controls over the system were effective throughout the period 1 February 2019 to 30 April 2019, to provide reasonable assurance that the principal service commitments and system requirements were achieved based on the criteria relevant to security, availability, and confidentiality set forth in the AICPA's TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy.*

Very truly yours,

Chronicle LLC

20 June 2019

Ernst & Young LLP
303 Almaden Boulevard
San Jose, CA 95110

Tel: +1 408 947 5500
Fax: +1 408 947 5717
ey.com

Building a better working world

Report of Independent Accountants

To the Management of Chronicle LLC:

Scope

We have examined management's assertion, contained within the accompanying "Management's Report of its Assertions on the Effectiveness of its Controls over the Chronicle Services System based on the Trust Services Principles and Criteria for Security, Availability and Confidentiality" (Assertion), that Chronicle's controls over the Chronicle Services System (System) were effective throughout the period 1 February 2019 through 30 April 2019, to provide reasonable assurance that its principal service commitments and system requirements were achieved based on the criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in the AICPA's TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy.*

Management Responsibilities

Chronicle's management is responsible for its assertion, selecting the trust services categories and associated criteria on which its assertion is based, and having a reasonable basis for its assertion. It is also responsible for:

- Identifying the Chronicle Services System (System) and describing the boundaries of the System
- Identifying principal service commitments and system requirements and the risks that would threaten the achievement of its principal service commitments and service requirements that are the objectives of its system
- Identifying, designing, implementing, operating, and monitoring effective controls over the System to mitigate risks that threaten the achievement of the principal service commitments and system requirements

Our Responsibilities

Our responsibility is to express an opinion on the Assertion, based on our examination. 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. An examination involves performing procedures to obtain evidence about management's assertion, which includes: (1) obtaining an understanding of Chronicle's relevant security, availability, and confidentiality policies, processes and controls, (2) testing and

Building a better working world

evaluating the operating effectiveness of the controls, and (3) performing such other procedures as we considered necessary in the circumstances. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risk of material misstatement, whether due to fraud or error. We believe that the evidence obtained during our examination is sufficient to provide a reasonable basis for our opinion.

Our examination was not conducted for the purpose of evaluating Chronicle's cybersecurity risk management program. Accordingly, we do not express an opinion or any other form of assurance on its cybersecurity risk management program.

Inherent limitations

Because of their nature and inherent limitations, controls may not prevent, or detect and correct, all misstatements that may be considered relevant. Furthermore, the projection of any evaluations of effectiveness to future periods, or conclusions about the suitability of the design of the controls to achieve Chronicle's principal service commitments and system requirements, is subject to the risk that controls may become inadequate because of changes in conditions, that the degree of compliance with such controls may deteriorate, or that changes made to the system or controls, or the failure to make needed changes to the system or controls, may alter the validity of such evaluations. Examples of inherent limitations of internal controls related to security include (a) vulnerabilities in information technology components as a result of design by their manufacturer or developer; (b) breakdown of internal control at a vendor or business partner; and (c) persistent attackers with the resources to use advanced technical means and sophisticated social engineering techniques specifically targeting the entity.

Opinion

In our opinion, Chronicle's controls over the system were effective throughout the period 1 February 2019 through 30 April 2019, to provide reasonable assurance that its principal service commitments and system requirements were achieved based on the applicable trust services criteria.

Ernst & Young LLP

20 June 2019
San Jose, CA

Attachment A – Chronicle Services System

Chronicle Services Overview

Chronicle LLC ("Chronicle") is developing enterprise, cloud-native services to enable security analysts to rapidly and cost-effectively investigate and hunt cybersecurity threats more efficiently. Chronicle's product offering ("Backstory" or the "Chronicle Services") allows enterprise customers to better analyze their own security telemetry through enhanced, curated analytics and investigative visualizations enabling enterprises to more rapidly detect, prevent and block harm to their systems, networks and data.

Google, as a sub-service provider for Chronicle, is a global technology service provider focused on improving the ways people connect with information. Google provides Cloud services, infrastructure, and applications to support the Chronicle Services.

As an Alphabet, Inc. ("Alphabet") company and an affiliate of Google, LLC ("Google"), Chronicle leverages Google's technology platform, control framework, and governance structure throughout the organization. References to "Google" collectively includes Chronicle's and Google's operations.

Infrastructure

Chronicle Services run in a multi-tenant, distributed environment to support high availability through the use of redundant architecture. Rather than segregating user entity data to one machine or set of machines, data from all user entities is distributed amongst a shared infrastructure. For Chronicle Services, this is achieved through a Google distributed file system designed to store extremely large amounts of data across many servers. Customer data is then stored in large distributed databases, built on top of this file system.

Data Centers and Redundancy

Google maintains consistent policies and standards across all data centers for physical security to help protect production and corporate servers, network devices and network connections within Google data centers.

Redundant architecture exists such that data is replicated in real-time to at least two (2) geographically dispersed data centers. The data centers are connected through multiple encrypted network links and interfaces. This provides high availability by dynamically load balancing across those sites. Chronicle uses a dashboard that provides details such as resource footprint, central processing unit capacity, and random-access memory availability to monitor resource availability across their data centers and to validate that data has been replicated to more than one location.

Authentication and Access

Strong authentication and access controls are implemented to restrict access to Chronicle's production systems, internal support tools, and customer data. Machine-level access restriction relies on a certificate based distributed authentication service, which helps to positively identify the resource access requester. This service also offers transport encryption to enhance data confidentiality in transit. Data traffic is encrypted between Chronicle and the Google production facilities that Chronicle uses

Google and Chronicle adhere to Google's formal processes to grant and revoke employee access to Google and Chronicle resources. Credentials are provisioned through Google's Lightweight Directory Access Protocol ("LDAP"), Kerberos, and a proprietary system which utilizes Secure Shell ("SSH") and Transport Layer Security ("TLS") certificates - mechanisms designed to ensure only authorized users are granted access rights to systems and data in a secure and flexible manner.

Internal access to customer data is restricted through the use of unique user account IDs. Access to sensitive systems and applications requires two-factor authentication in the form of unique user account IDs, strong passwords, security keys and/or certificates. Periodic reviews of access lists are implemented to help ensure access to customer data is appropriate and authorized. Access to production machines, network devices and support tools is managed via an access group management system. Membership in these groups must be approved by respective group administrators. User group memberships are reviewed on a semi-annual basis under the direction of the group administrators.

Change Management

Change Management policies, including security code reviews and emergency fixes, are in place, and procedures for tracking, testing approving, and validating changes are documented. Changes are developed utilizing the code versioning tool to manage source code, documentation, release labeling and other functions. Chronicle and Google require all code changes to be reviewed and approved by a separate technical resource, other than the developer, to evaluate the quality and accuracy of changes. Further, all application and configuration changes are tested prior to migration to production environment. Following successful pass of tests, multiple binaries are then grouped into a release and deployed to production.

Data

Chronicle provides controls at each level of data storage, access, and transfer. Chronicle and Google have established training programs for privacy and information security to support data confidentiality. All employees are required to complete these training programs annually. All product feature launches that include new collection, processing, or sharing of user data are required to go through an internal design review process. Chronicle and Google have also established incident response processes to report and handle events related to confidentiality.

Chronicle and Google establish agreements, including non-disclosure agreements, for ensuring adherence to laws and preserving confidentiality of information and data exchange with external parties.

Network Architecture and Management

The Chronicle Services system architecture utilizes a fully redundant network infrastructure managed by Google. Google has implemented perimeter devices to protect the Google network from external attacks. Network monitoring mechanisms are in place to detect and disconnect access to the Google network from unauthorized devices.

People

Chronicle has implemented a process-based service quality environment designed to consistently deliver Backstory to customers over time. The fundamentals underlying the services provided are the adoption of standardized, repeatable processes; the hiring and development of highly skilled resources; and leading industry practices. Chronicle and Google have established internal compliance teams utilizing scalable processes to efficiently manage core infrastructure and product-related security, availability, and confidentiality controls.

Formal organizational structures describing Chronicle and Google's corporate organization exist and are available to employees on the Alphabet-wide intranet. The intranet provides drill-down functionality for identifying employees in the functional operations team. Chronicle also adhere to Google's documented policies, procedures, and job descriptions for applicable operational areas including data center operations, security administration, system and hardware change management, hiring, training, performance appraisals, terminations and incident escalation. These policies and procedures have been designed to segregate duties and enforce responsibilities based on job functionality. Policies and procedures are reviewed and updated as necessary.

Attachment B – Principal Service Commitments and System Requirements

Service Commitments

Commitments are declarations made by management to customers regarding the performance of Backstory. Commitments to customers are communicated via Backstory's Terms of Service, including a Service Level Agreement, and Data Processing Addendum.

System Requirements

Chronicle has established internal policies and processes to support the delivery of the Chronicle Services to customers. These internal policies leverage and supplement Google's policy suite and are developed in consideration of legal and regulatory obligations, to define Chronicle and Google's organizational approach and system requirements. The delivery of Chronicle Services depends upon the appropriate functioning of system requirements.

The following processes and system requirements function to meet Chronicle's commitments to customers with respect to the terms governing the processing and security of customer data:

- Access Security: Google maintains, and Chronicle adheres to, Google's data access and logical security policies, designed to prevent unauthorized persons and/or systems from gaining access to systems used to process personal data. Access to systems is restricted based on the principle of least privilege.
- Change Management: Standard change management procedures are required to be applied during the design, development, deployment, and maintenance of all Google applications, systems, and services on which Chronicle operates or which it otherwise leverages.
- Incident Management: Google and Chronicle monitor a variety of communication channels for security incidents, and Google and Chronicle's security personnel will react promptly to known incidents affecting the Chronicle Services.
- Data Management: Google and Chronicle comply with applicable obligations with respect to the processing of customer personal data. Google and Chronicle process data in accordance with customer instructions and comply with applicable regulations.
- Data Security: Google and Chronicle implement and maintain technical and organizational measures to protect customer data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access.
- Third Party Risk Management: Google conducts routine inspections of subprocessors to evaluate control conformance. Google defines and enforces the security and privacy obligations with which sub-processors must comply.