Report on the Elastic Cloud Service Relevant to Security, Availability, Confidentiality, and Privacy Throughout the Period November 1, 2022 to October 31, 2023

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

Table of Contents

Section 1

Section 2

Attachment A

Attachment B

Section 1

Independent Service Auditor’s Report

Independent Service Auditor’s Report

To: Elasticsearch N.V. (“Elastic”)

Scope

We have examined Elastic’s accompanying assertion titled “Assertion of Elastic Management” (assertion) that the controls within the Elastic Cloud Service (system) were effective throughout the period November 1, 2022 to October 31, 2023, to provide reasonable assurance that Elastic’s service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, confidentiality, and privacy (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*).

The description of the boundaries of the system indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Elastic, to achieve Elastic’s service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system presents the complementary user entity controls assumed in the design of Elastic’s controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Elastic uses subservice organizations to provide data center colocation services. The description of the boundaries of the system indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Elastic, to achieve Elastic’s service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system presents the types of complementary subservice organization controls assumed in the design of Elastic’s controls. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

Service Organization’s Responsibilities

Elastic 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 Elastic’s service commitments and system requirements were achieved. Elastic has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Elastic 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 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.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

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 Elastic'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 Elastic'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 the Elastic Cloud Service were effective throughout the period November 1, 2022 to October 31, 2023, to provide reasonable assurance that Elastic's service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls and complementary user entity controls assumed in the design of Elastic's controls operated effectively throughout that period is fairly stated, in all material respects.

Coalfire Controls LLC

Greenwood Village, Colorado
January 29, 2024

Section 2

Assertion of Elastic Management

Assertion of Elasticsearch N.V. (“Elastic”) Management

We are responsible for designing, implementing, operating and maintaining effective controls within the Elastic Cloud Service (system) throughout the period November 1, 2022 to October 31, 2023, to provide reasonable assurance that Elastic’s service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, confidentiality, and privacy (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*). Our description of the boundaries of the system is presented in attachment A and identifies the aspects of the system covered by our assertion.

The description of the boundaries of the system indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Elastic, to achieve Elastic’s service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system presents the complementary user entity controls assumed in the design of Elastic’s controls.

Elastic uses subservice organizations for data center colocation services. The description of the boundaries of the system indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Elastic, to achieve Elastic’s service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system presents the types of complementary subservice organization controls assumed in the design of Elastic’s controls. The description of the boundaries of the system does not disclose the actual controls at the subservice organizations.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period November 1, 2022 to October 31, 2023, to provide reasonable assurance that Elastic’s service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls and complementary user entity controls assumed in the design of Elastic’s controls operated effectively throughout that period. Elastic’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 November 1, 2022 to October 31, 2023, to provide reasonable assurance that Elastic’s service commitments and system requirements were achieved based on the applicable trust services criteria.

Elasticsearch N.V.

Attachment A

Elastic’s Description of the Boundaries of Its Elastic Cloud Service

Type of Services Provided

Elastic ("Elastic" or "the Company") is a search company founded in 2012 which, for the purposes of this report, includes Elasticsearch N.V. and its affiliates. Search refers to rapidly obtaining relevant information and insights from large amounts of data.

Elastic offers a number of products and solutions, including Elastic Cloud, which is a set of software products that ingest and store data from any source and in any format and performs search, analysis, and visualization.

Elastic Cloud is a family of software-as-a-service (SaaS) products that includes the Elasticsearch Service (ESS), Elasticsearch Service Private (ESSP), Elastic Workplace Search, Elastic App Search Service, Elastic Security, and Elastic Observability. Elastic Cloud is a service in which Elastic hosts and manages Elastic Stack components, including Elasticsearch and Kibana, on infrastructure from multiple public cloud providers, including Amazon Web Services (AWS), Google Cloud Platform (GCP), and Microsoft Azure known as the Hosting Providers. Elastic Cloud and its related software solutions (i.e., Elastic Enterprise Search, logging, metrics, application performance monitoring, business analytics, and security analytics) can also be deployed on-premises, in public or private clouds, or in hybrid environments to satisfy various user and customer needs.

Elastic Cloud offerings include advanced Elastic Stack features, such as security, alerting, monitoring, reporting, machine learning, and graphing capabilities. Elastic Cloud deployments allow customers to launch with use-case-configured templates, including hot-warm architecture, CPU-optimized workloads, I/O optimized workloads, and memory optimized workloads. Elastic Cloud includes enhanced security features, including default encryption at rest, Security Assertion Markup Language (SAML) and native authentication for hosted deployments.

Elastic Cloud is comprised of the following components:

Elastic Cloud Component	Component Description
ESS	ESS is a distributed, real-time search and analytics engine and datastore for all types of data, including textual, numerical, geospatial, structured, and unstructured data.
ESSP	ESSP is an ESS subscription tier that offers an isolated ESS environment hosted in a dedicated virtual private cloud (VPC), running on an exclusive set of hosts.
Elastic Enterprise Search	Elastic Enterprise Search provides powerful tools to deliver search experiences quickly and scale them seamlessly: • Workplace Search is a tool to unify an organization's content platforms (Google Drive, Slack, Salesforce, and many others) into a personalized, natural search experience. • App Search is a toolbox for developers to leverage the power of Elasticsearch to add search to mobile and SaaS applications, complete with a web crawler, refined set of application programming interfaces (APIs), intuitive dashboards, and tunable relevance controls. • Site Search enables the addition of powerful search capabilities to a website, including the search box if needed.

Elastic Cloud Component	Component Description
Elastic Observability	Elastic Observability, built on the Elastic Stack, enables unified analysis across logs, metrics, application performance, and uptime monitoring information. Using Elastic Agent and pre-built integration connectors for data collection, organizations can surface outliers with machine learning and out-of-the-box detection rules supporting both DevOps and SecOps teams.
Elastic Security	Elastic Security enables threat prevention, detection, and response through a single user interface: • Elastic Security Information and Event Management (SIEM) provides conventional log aggregation and correlation that support threat detection and response and advanced security features such as risk assessment with machine learning, integrated case management, and security orchestration, automation and response (SOAR.) • Elastic Agent offers versatility with a small footprint that works almost anywhere, including hybrid environments. It can prevent threats, forward data, and support multiple use cases to enrich security information and protection. • Limitless XDR modernizes security operations, unifying SIEM and endpoint security, enabling analytics across years of data, automating key processes, and bringing native endpoint protection to every host.

The boundaries of the system in this section details Elastic Cloud. Any other Elastic services are not within the scope of this report.

The Boundaries of the System Used to Provide the Services

The boundaries of Elastic Cloud are the specific aspects of the Company’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 Elastic Cloud.

The components that directly support the services provided to customers are described in the subsections below.

Infrastructure

In order to help bring Elastic Cloud components online with speed and efficiency, Elastic Cloud runs on top of public cloud environments, including AWS, Microsoft Azure, and GCP.

The primary infrastructure used to provide Elastic Cloud includes the following:

Infrastructure		
Production Tool	Hosted Location	Business Function
Web, application, database, and search servers	Cloud infrastructure managed by Hosting Providers.	These tools are a set of managed services deployed in hosting providers’ data centers across the globe (including North America, Asia, Australia, Europe, the Middle East, and Africa [EMEA]).

Infrastructure		
Production Tool	**Hosted Location**	**Business Function**
Background processing and business analytics	Cloud infrastructure managed by Hosting Providers.	These tools perform background processing, analytics, and other offline workloads that do not interact with confidential customer content; handled by cloud instances provided by Hosting Providers.
Backup recovery and testing	Cloud infrastructure managed by Hosting Providers.	Cloud instances are used by Elasticsearch for off-site backup validation and recovery.
Security infrastructure	Cloud infrastructure managed by Hosting Providers.	In accordance with the shared responsibility model, the cloud provider handles all perimeter security, including basic distributed denial of service (DDoS) protection, services security, and perimeter firewall protection.

Services Provided by Subservice Organizations and Vendors

Elastic Cloud uses the following subservice organizations and vendors to provide services to customers:

Subservice Organizations	
Subservice Organization	**Purpose**
AWS	Infrastructure-as-a-service (IaaS) hosting Elastic Cloud components provided by AWS. Data centers are in the following locations: • North America • South America • Asia • Australia • EMEA
GCP	IaaS hosting Elastic Cloud components provided by GCP. Data centers are in the following locations: • North America • South America • Asia • Australia • EMEA
Microsoft Azure	IaaS hosting Elastic Cloud components provided by Microsoft Azure. Data centers are in the following locations: • North America • South America • Asia • Australia • EMEA

Software

Software consists of the programs and technical components that support Elastic Cloud (operating systems, middleware, and utilities). The list of software and ancillary components used to build, support, secure, maintain, and monitor Elastic Cloud include the following applications, as shown in the table below:

Software	
Component	**Overview**
Operating system	Linux is the operating system used for Elastic Cloud.
Monitoring solutions	There are multiple monitoring systems in use for Elastic Cloud, including: • SIEM centralized log correlation analysis and alert system • Performance and capacity monitoring system • Vulnerability scanning • Application monitoring • File integrity monitoring
Databases	All in-scope databases are Amazon Relational Database Service (Amazon RDS) databases. Elasticsearch can be considered a logical data store for customer content and exists wherever the customer deploys a cluster.
Network	Elastic Cloud’s network infrastructure utilizes a common set of network components: • Elastic load balancers (ELBs) • Firewalls and security groups • Proxies • Virtual private cloud (VPC) segmenting • Infrastructure deployment automation • Virtual private network (VPN) • Configuration management
Identity and Access	Elastic Cloud’s Identity and Access infrastructure utilizes a common set of components: • Authentication systems • Administrative consoles
Code Management	Elastic Cloud’s Code Management infrastructure utilizes a common set of components: • Code repository • Code deployment pipeline • Infrastructure as Code (IaC)

People

The Company develops, manages, and secures Elastic Cloud via separate departments. The responsibilities of these departments are defined in the following table:

People	
Group/Role Name	**Function**
Executive Management	Provides general oversight and strategic planning of operations.

People	
Group/Role Name	**Function**
Engineering	Responsible for design, implementation, and ongoing maintenance of Elastic Cloud. Engineering consists of five (5) separate teams: • Design team: develops brand identity and design language; responsible for user interface (UI) and user experience (UX) design and product design; designs websites and emails. • Development team: responsible for the architectural design, implementation, and ongoing maintenance of Elastic Cloud software, products, and services. • Cloud Operations and Security team: responsible for design and support for Elastic Cloud production infrastructure; maintains the security and availability of the infrastructure comprising Elastic Cloud product offerings, including vulnerability management and monitoring. • Product Management team: responsible for working with Engineering to define and implement product vision. • Platform team: responsible for creating tools and services for the Company; manages code repositories, develops configuration management libraries, and maintains a continuous integration system.
Support	Responsible for supporting customers at every level of their Elastic Cloud adoption and providing free trial support, implementation support, and ongoing support.
Information Security	Provides standards, guidance, assistance, and oversight to ensure that security requirements are maintained across the organization and holistically manages information risk. Information Security is also responsible for security monitoring and incident response activities.
Information Technology (IT)	Responsible for help desk operations, integration and data management, and application customizations to support business operations.

Procedures

Formal information security policies and procedures exist that describe logical access, computer security, change control, and data management standards. All teams are expected to adhere to the Elastic information security policies, standards, and procedures that define how services should be delivered. These are local on the Company's intranet and can be accessed by any Elastic team member.

Policy update requests can be made by any workforce member at any time and are subject to the Information Security Officer's approval. The Information Security Officer reviews all policies annually to ensure that they are accurate and up to date.

Elastic has the following security policies, standards, and procedures in place, which are owned by the Information Security Officer:

- Logical Access Management
- Change Management
- Risk Management
- Incident Management
- Data Classification
- Asset Management

- Record Retention
- Supplier Management
- Vulnerability Management
- Workstation and Server Management
- Security Logging and Monitoring
- System Hardening Standards
- Anti-Malware Technology
- Security Awareness and General Privacy Awareness Training
- Business Continuity and Disaster Recovery
- Encryption Key Management
- Privacy Policy

Data

Customers upload electronic data to Elastic Cloud for processing. This data is referred to as customer content. Customer content has been classified as restricted information under Elastic's data classification policy and is subject to the strictest access and sharing restrictions. Encrypted connections are made to the service organization using client VPN hardware that connects system users via Secure Shell (SSH) to secure servers that operate following TLS standards and protocols.

Complementary User Entity Controls (CUECs)

Elastic's controls related to Elastic Cloud cover only a portion of overall internal control for each customer deployment of Elastic Cloud. It is not feasible for the service commitments, system requirements, and applicable criteria related to the system to be achieved solely by Elastic. Therefore, each user entity's internal control should be evaluated in conjunction with Elastic's controls taking into account the related CUECs identified for the specific criterion. In order for user entities to rely on the controls reported herein, each user entity must evaluate its own internal control to determine whether the identified CUECs have been implemented and are operating effectively.

The CUECs presented should not be regarded as a comprehensive list of all controls that should be employed by user entities. Management of user entities is responsible for the following:

Criteria	Complementary User Entity Controls
CC2.1	• User entities have policies and procedures to report any material changes to their overall control environment that may adversely affect services being performed by Elastic according to contractually specified time frames. • Controls to provide reasonable assurance that Elastic is notified of changes in: – User entity vendor security requirements – The authorized users list
CC2.3	• It is the responsibility of the user entity to have policies and procedures to: – Inform their employees and users that their information or data is being used and stored by Elastic. – Determine how to file inquiries, complaints, and disputes to be passed onto Elastic.

Criteria	Complementary User Entity Controls
CC6.1	• User entities grant access to Elastic's system to authorized and trained personnel. • User entities are responsible for securely configuring their Elastic Cloud environment. User entities can reference Elastic's public website for any additional details needed for the customer to secure its deployment: https://www.elastic.co/guide/en/cloud/current/index.html. • Controls to provide reasonable assurance that policies and procedures are deployed over user IDs and passwords that are used to access services provided by the Company.
CC6.4 CC6.5 CC7.2 A1.2	• User entities deploy physical security and environmental controls for all devices and access points residing at their operational facilities, including remote employees or at-home agents for which the user entity allows connectivity.
CC7.3 CC7.4 CC7.5	• User entities are responsible for immediately notifying Elastic of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.
C1.2	• User entities have processes and procedures to remove confidential information when it needs to be purged or removed from the system.
P2.1 P3.2	• User entities are responsible for informing data subjects (a) about the choices available to them with respect to the collection, use, and disclosure of personal information and (b) that implicit or explicit consent is required to collect, use, and disclose personal information. • User entities obtain and document implicit or explicit consent from data subjects at or before the time personal information is collected or soon thereafter.
P4.3	• User entities have controls in place to communicate personal information that needs to be purged or removed and follow Elastic's procedures for removal.
P6.1	• User entities have policies and procedures in place to notify data subjects of disclosures of personal information to third parties and obtain these disclosures from Elastic.
P5.1 P5.2 P6.7 P7.1	• User entities have policies and procedures in place for: – Identifying and authenticating data subjects requesting access to their personal information – Stating the reasons for denial of access to data subjects' personal information – Correcting, amending, or appending data subjects' personal information and communicating those changes to third parties – Providing an accounting of personal information held to data subjects – Collecting and maintaining accurate, complete, up-to-date, and relevant personal information

Subservice Organizations and Complementary Subservice Organization Controls (CSOCs)

The Company uses AWS, Microsoft Azure, and GCP (subservice organizations or Hosting Providers) as subservice organizations for data center colocation services. Elastic's controls related to Elastic Cloud cover only a portion of the overall internal control for each user entity of Elastic Cloud.

Although the subservice organizations have been carved out for the purposes of this report, certain service commitments, system requirements, and applicable criteria are intended to be met by controls at the subservice organizations. CSOCs are expected to be in place at Elastic's Hosting Providers related to physical security and environmental protection, as well as backup, recovery, and redundancy controls related to availability. The Hosting Providers' physical security controls should mitigate the risk of unauthorized access to the hosting facilities. The Hosting Providers' environmental security controls should mitigate the risk of fires, power loss, climate, and temperature variabilities.

Elastic management receives and reviews the audit or attestation reports of the Hosting Providers annually. In addition, through its operational activities, Elastic management monitors the services performed by the Hosting Providers to determine whether operations and controls expected to be implemented at the subservice organizations are functioning effectively. Management also communicates with the Hosting Providers to monitor compliance with the service agreement, stay informed of changes planned at the hosting facility, and relay any issues or concerns to the Hosting Providers' management.

It is not feasible for the service commitments, system requirements, and applicable criteria related to Elastic Cloud to be achieved solely by Elastic. Therefore, each user entity's internal control must be evaluated in conjunction with Elastic's controls taking into account the related CSOCs expected to be implemented at the Hosting Providers as described below:

Criteria	Complementary Subservice Organization Controls
CC6.4	• The Hosting Providers are responsible for restricting data center access to authorized personnel. • The Hosting Providers are responsible for the 24/7 monitoring of data centers by closed circuit cameras and security personnel.
CC6.5 CC6.7	• The Hosting Providers are responsible for securely decommissioning and physically destroying physical production assets in their control.
CC7.2 A1.2	• The Hosting Providers are responsible for the installation of fire suppression and detection and environmental monitoring systems at the data centers. • The Hosting Providers are responsible for protecting data centers against a disruption in power supply to the processing environment by an uninterruptible power supply (UPS). • The Hosting Providers are responsible for overseeing the regular maintenance of environmental protections at data centers.

Specific Criteria Not Relevant to the System

The below Trust Services Criteria are not relevant to Elastic Cloud:

TSC Reference	Criteria	Reasoning
C1.2	The entity disposes of confidential information to meet the entity's objectives related to confidentiality.	Elastic Cloud, per its policies and procedures, does not perform any destruction action on behalf of a customer. The customer must delete their cluster and data.

TSC Reference	Criteria	Reasoning
P2.1	The entity communicates choices available regarding the collection, use, retention, disclosure, and disposal of personal information to the data subjects and the consequences, if any, of each choice. Explicit consent for the collection, use, retention, disclosure, and disposal of personal information is obtained from data subjects or other authorized persons, if required. Such consent is obtained only for the intended purpose of the information to meet the entity's objectives related to privacy. The entity's basis for determining implicit consent for the collection, use, retention, disclosure, and disposal of personal information is documented.	Elastic is provided personal information from data controllers, and it is not Elastic's responsibility as part of the service offering to communicate the choices available regarding the collection, use, retention, disclosure, and disposal of personal information to the data subjects and the consequences of each. It is also not Elastic's responsibility as part of the service offering to obtain explicit consent for the collection, use, retention, disclosure, and disposal of personal information. That is the responsibility of the data controller.
P3.2	For information requiring explicit consent, the entity communicates the need for such consent, as well as the consequences of a failure to provide consent for the request for personal information, and obtains the consent prior to the collection of the information to meet the entity's objectives related to privacy.	Elastic is provided personal information by data controllers, and it is the data controllers' responsibility to obtain explicit consent from data subjects prior to the collection of personal information.
P4.3	The entity securely disposes of personal information to meet the entity's objectives related to privacy.	Elastic is provided personal information by data controllers, and it is the responsibility of data controllers to securely delete and dispose of personal information that resides in their service environments.
P5.1	The entity grants identified and authenticated data subjects the ability to access their stored personal information for review and, upon request, provides physical or electronic copies of that information to data subjects to meet the entity's objectives related to privacy. If access is denied, data subjects are informed of the denial and reason for such denial, as required, to meet the entity's objectives related to privacy.	Elastic is provided personal information from data controllers, and it is not Elastic's responsibility as part of the service offering to identify and authenticate data subjects for accessing their personal information or to determine when access should be denied. That is the responsibility of the data controller.
P5.2	The entity corrects, amends, or appends personal information based on information provided by data subjects and communicates such information to third parties, as committed or required, to meet the entity's objectives related to privacy. If a request for correction is denied, data subjects are informed of the denial and reason for such denial to meet the entity's objectives related to privacy.	Elastic is provided personal information by data controllers, and it is the data controller's responsibility to correct, amend, or append personal information and communicate necessary changes to Elastic. If a request for correction is denied, it is the responsibility of the data controller to inform the requesting data subject of the denial and reason for such denial.

TSC Reference	Criteria	Reasoning
P6.7	The entity provides data subjects with an accounting of the personal information held and disclosure of the data subjects' personal information, upon the data subjects' request, to meet the entity's objectives related to privacy.	Elastic does not collect personal information from data subjects. Elastic's customers collect personal information from data subjects and load it into Elastic Cloud. Therefore, privacy criteria related to the accounting of personal information is not applicable to Elastic, as it is the responsibility of the data controllers.
P7.1	The entity collects and maintains accurate, up-to-date, complete, and relevant personal information to meet the entity's objectives related to privacy.	Elastic is provided personal information from data controllers, and it is not Elastic's responsibility as part of the service offering to determine the quality of that information. Therefore, privacy criteria related to quality is not applicable to Elastic.

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 Elastic Cloud. Commitments are communicated in the General Privacy Notice, Customer Data Processing Addendum, and on the Cloud Security homepage. Details of the standard agreements and full commitments made by management to customers can be found on the Elastic website or in standard form agreements, which are included as embedded uniform resource locator (URL) links to the website on the customer order form.

The Company's commitments include the following for Elastic Cloud Standard (monthly standard subscription) or Elastic Cloud Premium negotiated and non-negotiated (an annual subscription to the premium services or an annual subscription to the premium services with a local copy):

- Elastic maintains a comprehensive information security program that includes appropriate technical and organizational measures designed to protect customer data against unauthorized access, use, disclosure, modification, or deletion.
- Elastic will provide 24/7 operations and availability monitoring.
- Elastic takes significant measures to ensure that customer data cannot be read, copied, modified, or deleted during electronic transmission, transport, or storage through unauthorized means.
- Elastic will retain data only as permitted by law and while the data continues to have a legitimate business purpose.
- Elastic shall ensure that any person who is authorized by Elastic to process customer personal data shall be under an appropriate obligation of confidentiality.

Subscription Level	Hours of Operation	Target Response (by Severity)		
		Level 1	Level 2	Level 3
Enterprise	24/7/365	One (1) hour	Four (4) hours	One (1) business day
Platinum	24/7/365	One (1) hour	Four (4) hours	One (1) business day
Gold	Business hours (8 a.m. to 6 p.m.) in the time zone applicable to the location based on the sales order	Four (4) business hours	One (1) business day	Two (2) business days

Severity Level Definitions

A **Level 1** issue is a major production error within the software that severely impacts the customer's use of the software for production purposes, such as the loss of production data or production systems not functioning when no work-around exists. Elastic will use continuous efforts during the normal business hours of operation stated above for the applicable subscription level to provide a resolution for any Level 1 errors as soon as is commercially reasonable.

A **Level 2** issue is an error within the software where the customer's system is functioning for production purposes, but in a reduced capacity, such as a problem that is causing significant impact to portions of the customer's business operations and productivity or where the software is exposed to potential loss or interruption of service. Elastic will use continuous efforts during the normal business hours of operation stated above for the applicable subscription level to provide a resolution for any Level 2 errors.

A **Level 3** issue is a medium- to low-impact error that involves partial and non-critical loss of functionality for production purposes or development purposes, such as a problem that impairs some operations but allows the customer's operations to continue to function. Errors for which there is limited or no loss of functionality or impact to the customer's operation and for which there is an easy work-around qualify as Level 3.

Principal System Requirements

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