Report on Elastic's App Search and Site Search System Relevant to Security, Availability, Confidentiality, and Privacy Throughout the Period November 1, 2021 to October 31, 2022

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

Table of Contents

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 Elastic's App Search and Site Search System (system) were effective throughout the period November 1, 2021 to October 31, 2022, 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 certain 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 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 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.

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

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 Elastic's App Search and Site Search System were effective throughout the period November 1, 2021 to October 31, 2022, 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

Westminster, Colorado
February 9, 2023

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 Elastic’s App Search and Site Search System (system) throughout the period November 1, 2021 to October 31, 2022, to provide reasonable assurance that Elastic’s service commitments and system requirements relevant to security, availability, confidentiality, and privacy 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.

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, 2021 to October 31, 2022, 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*) 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, 2021 to October 31, 2022, 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 App Search and Site Search System

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. Swiftype, the creator of App Search and Site Search, was founded in January 2012 to provide a secure and intelligent cloud-based search service. In November 2017, Swiftype merged with Elastic.

The App Search and Site Search System is built on Elastic’s free and open distributed search engine, Elasticsearch Service (ESS), which provides hosted and self-managed search solutions. Companies can deploy search experiences that connect employees and customers to relevant information through modern and accessible user interfaces.

The App Search and Site Search System consists of the following:

App Search

App Search is a toolbox used by developers to create search experiences. It contains a suite of documented application programming interfaces (APIs) with supporting clients and open-source user interface (UI) frameworks, crafted to enable the development of highly relevant searches backed by Elastic Stack.

App Search has dashboard UI tools that permit users to fully administer, tune, test, and analyze their search engine. The App Search engine supports up to 15 different languages and allows customers to implement search within their desktops, mobile applications, games, information technology (IT) infrastructure, or websites, with access to features such as typo tolerance, bigram matching, stemming, synonym, and phrase matching.

Site Search

The Site Search solution allows website owners to create and manage a user-facing search experience tailored to their specific needs. It offers autocomplete, advanced analytics insights, fully customizable interfaces, and a suite of relevance tuning and access controls.

The Site Search Crawler is an automatic web crawler that can index a website’s documents with no involvement from the end user. Site Search is built to bring search capabilities to a variety of websites, from knowledge bases to customer support portals, online stores, publications, and blogs.

The boundaries of the system in this section details the App Search and Site Search System hosted on International Business Machines (IBM) Softlayer and Amazon Web Services (AWS). 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 the App Search and Site Search System 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 the App Search and Site Search System.

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

Infrastructure

The primary infrastructure used to provide the App Search and Site Search System includes the following:

Infrastructure		
Production Tool	**Hosted Location**	**Business Function**
Web servers, application servers, database servers, and search servers	Bare-metal infrastructure and cloud instances managed by IBM SoftLayer.	Most of Elastic's production infrastructure is based on IBM SoftLayer managed servers and cloud instances located in multiple data centers in Dallas, Texas.
Background processing and business analytics	Cloud instances provided by IBM SoftLayer.	Some background processing, analytics, and other offline workloads that do not interact with confidential customer content are handled by cloud instances provided by IBM SoftLayer.
Content delivery acceleration servers	Bare-metal infrastructure managed by IBM SoftLayer.	A set of managed servers deployed in IBM SoftLayer data centers across the globe (including North America, Asia, Australia, and Europe) is used to provide content delivery acceleration.
Backup recovery and testing	Cloud instances provided by AWS.	On-demand Amazon Elastic Compute Cloud (Amazon EC2) cloud instances are used by Elastic for off-site backup validation and recovery.

Software

The primary software used to provide the App Search and Site Search System includes the following:

Software	
Software	**Purpose**
CentOS 7	Primary Linux distribution used across the infrastructure.
OpenSSH	Secure Shell Protocol (SSH) access service on all servers.
Pritunl	Virtual private network (VPN) access service for external access to the infrastructure.
Chef	Configuration management system controlling all servers within the infrastructure.
Nagios	Monitoring service for infrastructure and internal service monitoring.
Elasticsearch	Search servers used to index customer documents.
MySQL	Primary data storage system
Mongo DB	Legacy data storage system
Nginx	HTTP(S) web server
Haproxy	HTTP(S) load balancer

Software	
Software	**Purpose**
Filebeat, Scribe	Data processing pipeline for logs.
Kibana/Grafana	Metrics dashboard applications
Jenkins	Continuous integration system
Docker	Linux Container management system
HashiCorp Vault	Secrets management and data encryption service
Elastic Auditbeat	System-level audit data collection
KernelCare	Provides live patching of the systems' Linux kernels without requiring reboots.

People

There are multiple groups at Elastic that provide support for the above services in each of the following functional areas:

People	
Group/Role Name	**Function**
Executive Management	Provides general oversight and strategic planning of operations.
Engineering	Responsible for the design, implementation, and ongoing maintenance of Elastic software and services. Engineering consists of three (3) separate teams: • Design team: develops brand identity and design language; responsible for UI and user experience (UX) design, product design, and website design. • Development team: responsible for the architectural design, implementation, and ongoing maintenance of Elastic software, products, and services. • Site Reliability team: responsible for design and support for Elastic production infrastructure; maintains the security and availability of the infrastructure comprising Elastic product offerings, including vulnerability management and monitoring.
Support	Responsible for supporting customers at every level of their Elastic adoption and providing free trial support, implementation support, and ongoing support.
Elastic Site Reliability Team	Validates all patches have been installed and, if applicable, that reboots have been completed.
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.
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 internal website 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
- Password Requirements
- Security Awareness and General Privacy Awareness Training
- Business Continuity and Disaster Recovery
- Encryption Key Management
- Privacy Policy

Data

Customer content is managed, processed, and stored in accordance with the relevant data protection and other regulations, with specific requirements formally established in customer contracts. Best practices such as data encryption in transit and at rest and RBAC are utilized to protect confidential customer content.

Elastic stores and processes all information provided by its customers without inspection; all such information is maintained as confidential and private to that customer. All personally identifiable information (PII) data stored is available only to members of the customer organization. Each customer organization has designated administrators who authorize access to information stored in their Elastic account.

Application data consists of customer documents that are indexed by Elastic and returned to the customers via HTTPS API, App Search Dashboard, or the Elastic Enterprise Search Interface.

Complementary User Entity Controls (CUECs)

Elastic's controls related to the App Search and Site Search System cover only a portion of overall internal control for each user entity of the App Search and Site Search System. 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.
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.
CC7.4	• 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.

Criteria	Complementary User Entity Controls
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 IBM SoftLayer and AWS as subservice organizations for data center colocation services. Elastic's controls related to the App Search and Site Search System cover only a portion of the overall internal control for each user entity of the App Search and Site Search System.

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 IBM SoftLayer and AWS related to physical security and environmental protection, as well as backup, recovery, and redundancy controls related to availability. IBM SoftLayer's and AWS' physical security controls should mitigate the risk of unauthorized access to their facilities. IBM SoftLayer's and AWS' 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 IBM SoftLayer and AWS annually. In addition, through its operational activities, Elastic management monitors the services performed by IBM SoftLayer and AWS to determine whether operations and controls expected to be implemented at the subservice organizations are functioning effectively. Management also communicates with the subservice organizations to monitor compliance with the service agreements, stay informed of changes planned at the hosting facilities, and relay any issues or concerns to IBM SoftLayer and AWS management.

It is not feasible for the service commitments, system requirements, and applicable criteria related to the App Search and Site Search System 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 subservice organizations as described below.

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

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

TSC Reference	Criteria	Reasoning
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.
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 the App Search and Site Search System. 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 the App Search and Site Search System. Commitments are communicated in written master customer agreements, the privacy policy, the support policy, and subscription agreements, where applicable. 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 principal service commitments and system requirements include the following:

- Elastic will utilize reasonable and appropriate security measures to safeguard information against unauthorized access, use, modification, destruction, or disclosure.
- Elastic agrees that it (and its contractors) will not collect, access, use, store, disclose, transfer, or otherwise process any personal data except (i) for the purposes of the terms of service, including without limitation, to implement and deliver Elastic Cloud and its features and associated services, provide customer support, and help customers prevent or address service or technical problems; (ii) as expressly permitted by customers in the terms of service or otherwise; or (iii) as compelled by law.
- Elastic will retain data only as permitted by law and while the data continues to have a legitimate business purpose.
- Elastic will keep in trust and confidence all customer confidential information using commercially reasonable care.
- Elastic will not use customer confidential information other than as necessary to carry out Elastic's duties or disclose any such customer confidential information to third parties (other than affiliates) without the customer's prior written consent.

The scope of the support services provided to customers includes general assistance and support regarding the use of Elastic Site Search Pro and Elastic Site Search Premium subscription levels. Elastic will provide support services to customers in accordance with this support services policy.

Elastic offers three (3) different levels of support services which are described below. As of the date of this report, details can be found at https://www.elastic.co/support/welcome/swiftype, as well as in the following table:

Subscription Level	Hours of Operation	Target Response (by Severity)		
		Level 1	Level 2	Level 3
Premium	8 a.m. to 6 p.m. PST	4 business hours	1 business day	2 business days
Pro	8 a.m. to 6 p.m. PST	N/A	N/A	3 business days
Standard	8 a.m. to 6 p.m. PST	N/A	N/A	3 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 the App Search and Site Search System 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. The Company’s system requirements are documented within Elastic’s information security policies.