Elastic


SOC 3® - SOC for Service Organizations: Trust Services Criteria for General Use Report
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section/Attachment</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Section 1: Independent Service Auditor’s Report</td>
<td>3</td>
</tr>
<tr>
<td>Section 2: Assertion of Elastic Management</td>
<td>7</td>
</tr>
<tr>
<td>Attachment A: Elastic’s Description of the Boundaries of its Elasticsearch Software Services App Search and Site Search System</td>
<td>9</td>
</tr>
<tr>
<td>Attachment B: Principal Service Commitments and System Requirements</td>
<td>21</td>
</tr>
</tbody>
</table>
Section 1

Independent Service Auditor’s Report
INDEPENDENT SERVICE AUDITOR’S REPORT

To: Elastic

Scope

We have examined Elastic’s accompanying assertion titled “Assertion of Elastic Management” (assertion) that the controls within the Elasticsearch Software Services App Search and Site Search System (system) were effective throughout the period January 1, 2019 to September 30, 2019, 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).

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 Elastic’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 Elastic’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 Elastic’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 Elasticsearch Software Services App Search and Site Search System were effective throughout the period January 1, 2019 to September 30, 2019, to provide reasonable assurance that Elastic’s service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Restricted Use

Certain 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. Users of this report should have sufficient knowledge and understanding of complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization’s service commitments and system requirements. Elastic uses
Amazon Web Services (AWS) and IBM SoftLayer as data center colocation providers. Users of this report should obtain the relevant SOC 2 or SOC 3 reports.

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. Users of this report should have sufficient knowledge and understanding of complementary user entity controls and how those controls interact with the controls at the service organization to achieve the service organization’s service commitments and system requirements.

Coalfire Controls LLC
Westminster, Colorado
December 30, 2019
Section 2

Assertion of Elastic Management
Assertion of Elastic Management

We are responsible for designing, implementing, operating and maintaining effective controls within Elastic’s Elasticsearch Software Services App Search and Site Search System (system) throughout the period January 1, 2019 to September 30, 2019, 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.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period January 1, 2019 to September 30, 2019, 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). 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 January 1, 2019 to September 30, 2019, to provide reasonable assurance that Elastic’s service commitments and system requirements were achieved based on the applicable trust services criteria.

Elastic
Attachment A

Elastic’s Description of the Boundaries of its Elasticsearch Software Services App Search and Site Search System
Type of Services Provided

Elastic ("the Company") is a search company founded in 2012 that for the purposes of this report, includes Elasticsearch B.V. and its affiliates. Search refers to rapidly obtaining relevant information and insights from large amounts of data. Swiftype, the makers 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 joined forces with Elastic.

App Search and Site Search are built on Elastic’s open source distributed search engine, Elasticsearch, which provides hosted and self-managed search solutions. Companies can deploy search experiences that connect both employees and customers to relevant information through modern and accessible user interfaces.

Swiftype, now part of Elastic, is an international company with offices in the Netherlands, United States, Canada, Germany, Korea, India, Japan, China, and other countries. Through their global network of personnel and high-performance network systems, Elastic provides search services to tens of thousands of customers.

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

**App Search**

App Search is a toolbox for developers looking 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 the Elastic Stack.

App Search has dashboard UI tools that grant users the ability to fully administer, tune, test, and analyze their search engine.

The App Search engine supports up to 15 different languages. Whether a team is implementing search within their desktop or mobile applications, games, IT infrastructure, or websites, they have 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, blogs, and more.

The boundaries of the system in this section of the report details the App Search and Site Search System. Any other Elastic services are not included within the scope of this report.

The Components of the System Used to Provide the Services

The boundaries of the 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 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:

<table>
<thead>
<tr>
<th>Primary Infrastructure</th>
<th>Type</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web servers, application servers, database servers, and search servers</td>
<td>Bare-metal infrastructure and cloud instances managed by SoftLayer/IBM.</td>
<td>Most of Elastic’s production infrastructure is based on SoftLayer managed servers and cloud instances located in multiple datacenters.</td>
</tr>
<tr>
<td>Background processing, business analytics, etc.</td>
<td>Cloud instances provided by SoftLayer/IBM.</td>
<td>Some background processing, analytics, and other offline workloads that do not interact with confidential customer data are handled by cloud instances provided by SoftLayer.</td>
</tr>
</tbody>
</table>
Primary Infrastructure

<table>
<thead>
<tr>
<th>Hardware</th>
<th>Type</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content delivery acceleration</td>
<td>Bare-metal infrastructure managed by SoftLayer/IBM.</td>
<td>A set of managed servers deployed in SoftLayer data centers across the globe (including North America, Asia, Australia, and Europe) is used to provide content delivery acceleration.</td>
</tr>
<tr>
<td>servers</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Backup recovery and testing</td>
<td>Cloud instances provided by Amazon Web Services (AWS).</td>
<td>On-demand Elastic Compute Cloud (EC2) cloud instances are used by Elastic for off-site backup validation and recovery.</td>
</tr>
</tbody>
</table>

Software

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

<table>
<thead>
<tr>
<th>Primary Software</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software</td>
<td></td>
</tr>
<tr>
<td>CentOS 6/7</td>
<td>Primary Linux distribution used across the infrastructure</td>
</tr>
<tr>
<td>Iptables</td>
<td>Software firewall used on all servers</td>
</tr>
<tr>
<td>Fail2ban</td>
<td>Automated account lock-out service for Secure Shell (SSH)</td>
</tr>
<tr>
<td>OpenSSH</td>
<td>SSH access service on all servers</td>
</tr>
<tr>
<td>Pritunl</td>
<td>Virtual private network (VPN) access service for external access to the infrastructure</td>
</tr>
<tr>
<td>Chef</td>
<td>Configuration management system controlling all servers within the infrastructure</td>
</tr>
</tbody>
</table>
## Primary Software

<table>
<thead>
<tr>
<th>Software</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nagios</td>
<td>Monitoring service for infrastructure and internal service monitoring</td>
</tr>
<tr>
<td>Elasticsearch</td>
<td>Search servers used to index customer documents</td>
</tr>
<tr>
<td>MySQL</td>
<td>Primary data storage system</td>
</tr>
<tr>
<td>Mongo DB</td>
<td>Legacy data storage system</td>
</tr>
<tr>
<td>Redis</td>
<td>Ephemeral data structure storage system</td>
</tr>
<tr>
<td>Kestrel</td>
<td>Distributed queue broker</td>
</tr>
<tr>
<td>Nginx</td>
<td>HTTP(S) web server</td>
</tr>
<tr>
<td>Haproxy</td>
<td>HTTP(S) load balancer</td>
</tr>
<tr>
<td>Filebeat, Scribe</td>
<td>Data processing pipeline for logs</td>
</tr>
<tr>
<td>Graphite</td>
<td>Metrics storage for monitoring applications</td>
</tr>
<tr>
<td>Kibana/Grafana</td>
<td>Metrics dashboard applications</td>
</tr>
<tr>
<td>Cloudera Hadoop Distribution</td>
<td>Data processing and business analytics software</td>
</tr>
<tr>
<td>Jenkins</td>
<td>Continuous integration system</td>
</tr>
<tr>
<td>Docker</td>
<td>Linux Container management system</td>
</tr>
<tr>
<td>Hashicorp Vault</td>
<td>Secrets management and data encryption service</td>
</tr>
<tr>
<td>Elastic Auditbeat</td>
<td>System-level audit data collection</td>
</tr>
</tbody>
</table>
People

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

<table>
<thead>
<tr>
<th>Team</th>
<th>Responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive management</td>
<td>Provides general oversight and strategic planning of operations.</td>
</tr>
</tbody>
</table>
| Engineering Department      | Responsible for the design, implementation and ongoing maintenance of Elastic software and services. It consists of three separate teams:  
  - Design team: develops Elastic brand identity and design language; responsible for UI and user experience (UX) design and product design; designs website, emails, etc.  
  - 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, monitoring, etc. |
| Support                     | Responsible for supporting customers at every level of their Elastic adoption and providing free trial support, implementation support, ongoing support. |

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 and procedures that define how services should be delivered.
Policy update requests can be made by any workforce member at any time, which are subject to the Information Security Officer’s approval. Furthermore, all policies are reviewed annually by both the Information Security Officer and Legal to ensure that they are accurate and up to date.

Elastic has the following security procedures and policies 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

**Physical Security**

Elastic does not physically house any systems used by its systems in Elastic facilities. The Company works with SoftLayer/IBM and AWS to ensure the restriction of physical access to systems used as part of the Elastic platform. SoftLayer/IBM, and AWS control access to the physical buildings and facilities that house these systems and applications.

**Logical Access**

Elastic uses role-based security architecture and requires users of the system to be identified and authenticated prior to the use of any system resources. Resources are protected using native system security and add-on software products that identify and authenticate users and validate access requests against the users’ authorized roles in access
control lists. In situations in which incompatible responsibilities cannot be segregated, Elastic implements monitoring of one or more of the responsibilities using automation.

The termination process is in place to ensure that all accounts for a terminated employee are deleted on the last day of employment. The process is based on a detailed checklist that includes all systems comprising the Elastic production infrastructure.

**Computer Operations – Backups**

Customer data is backed up and monitored by operations personnel for completion and exceptions. In the event of an exception, operations personnel perform troubleshooting to identify the root cause and then rerun the backup job immediately (if possible).

**Computer Operations – Availability**

Incident response policies and procedures are in place to guide personnel in reporting and responding to availability incidents. Procedures exist to identify, report, and act upon system security breaches and other incidents.

Elastic monitors the capacity utilization of physical and computing infrastructure both internally and for customers to ensure that service delivery matches service level agreements. The Company evaluates the need for additional infrastructure capacity in response to growth of existing customers or the addition of new customers.

Elastic has implemented a vulnerability management process to ensure that infrastructure systems and application-level dependencies are patched in accordance with vendor-recommended operating system patches. The Elastic Site Reliability team, with the help of automated systems, validates that all patches have been installed and, if applicable, that reboots have been completed.

**Change Control**

Elastic maintains documented systems development life cycle (SDLC) policies and procedures to guide personnel in documenting and implementing application and infrastructure changes. Change control procedures include change request and initiation processes, documentation requirements, development practices, quality assurance testing requirements, and required approval procedures.

A ticketing system is utilized to document the change control procedures for changes in the application and the implementation of new changes. Automated testing results are documented and maintained with the associated change request.
Version control software is utilized to maintain source code versions and migrate source code through the development process to the production environment. The version control software maintains a history of code changes to support rollback capabilities and tracks changes to developers.

Elastic has implemented a patch management process for monitoring third-party dependencies for vulnerabilities and ensuring that all relevant patches are installed on production systems.

Data Communications

Firewall systems are in place to filter unauthorized inbound network traffic from the Internet and deny any type of incoming network connection that is not explicitly authorized.

Redundancy is built into the system infrastructure supporting the data center services to help ensure that there is no single point of failure, including firewalls, routers, and servers. If a primary system fails, the redundant hardware is configured to take its place.

Data

Customer data 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 like data encryption in transit and at rest and RBAC are utilized to protect confidential customer data.

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. Each user entity must evaluate its own internal control to determine whether the identified Complementary User Entity Controls (CUECs) have been implemented and are operating effectively.
The user entity controls 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:

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Complementary User Entity Controls (CUECs)</th>
</tr>
</thead>
</table>
| 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, disputes which would get passed onto Elastic. |
| CC6.1    | • User entities grant access to Elastic’s system to authorized and trained personnel.  
  • 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. |
| CC6.6    | • 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. |
| 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. |
| 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. |
### Subservice Organizations and Complementary Subservice Organization Controls (CSOCs)

The Company uses SoftLayer/IBM 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.

Certain service commitments, system requirements, and applicable criteria are intended to be met by controls at the subservice organization. Complementary Subservice Organization Controls (CSOCs) are expected to be in place at SoftLayer/IBM and AWS related to physical security and environmental protection, as well as backup, recovery, and redundancy controls related to availability. SoftLayer/IBM and AWS physical security controls mitigate the risk of fires, power loss, climate, and temperature variabilities.

Elastic management receives and reviews the audit or attestation reports of SoftLayer/IBM and AWS annually. In addition, through its operational activities, management of Elastic monitors the services performed by SoftLayer/IBM and AWS to determine whether operations and controls expected to be implemented at the subservice organizations are functioning effectively. Management also has communication with the subservice organizations to monitor compliance with the service agreement, stay abreast of changes planned at the hosting facility, and relay any issues or concerns to SoftLayer/IBM 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, accounting for the related CSOCs expected to be implemented at the subservice organizations as described below.

---

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Complementary User Entity Controls (CUECs)</th>
</tr>
</thead>
<tbody>
<tr>
<td>P5.1</td>
<td>• User entities have policies and procedures in place to:</td>
</tr>
<tr>
<td>P5.2</td>
<td>- identify and authenticate data subjects requesting access to their personal information.</td>
</tr>
<tr>
<td>P6.7</td>
<td>- stating the reasons for denial of access to their personal information.</td>
</tr>
<tr>
<td>P7.1</td>
<td>- correcting, amending or appending their personal information and communicating those changes to third parties.</td>
</tr>
<tr>
<td></td>
<td>- providing an accounting of personal information held to data subjects.</td>
</tr>
<tr>
<td></td>
<td>- collecting and maintaining accurate, complete, up to date and relevant personal information.</td>
</tr>
<tr>
<td>Criteria</td>
<td>Complementary Subservice Organization Controls (CSOCs)</td>
</tr>
<tr>
<td>----------</td>
<td>-------------------------------------------------------</td>
</tr>
</tbody>
</table>
| CC6.4    | • SoftLayer/IBM and AWS are responsible for restricting data center access to authorized personnel.  
          • SoftLayer/IBM and AWS are responsible for the 24/7 monitoring of data centers by closed circuit cameras and security personnel. |
| A1.2     | • SoftLayer/IBM and AWS are responsible for the installation of fire suppression and detection, and environmental monitoring systems at the data centers.  
          • SoftLayer/IBM and AWS are responsible for protecting data centers against a disruption in power supply to the processing environment by an uninterruptible power supply (UPS).  
          • SoftLayer/IBM and AWS are responsible for overseeing the regular maintenance of environmental protections at data centers. |
Attachment B

Principal Service Commitments and System Requirements
Principal Service Commitments and System Requirements

Principal Service Commitments

Commitments are declarations made by management to customers regarding the performance of Elastic services. Commitments are communicated in written terms of service agreements or 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 standard form agreements, which are included as embedded URL links to the website on the customer order form.

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

The Company’s principal service commitments and system requirements include the following:

- Elastic will utilize reasonable and appropriate physical, technical, and administrative procedures to safeguard the information collected and processed by Elastic.
- 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 Elasticsearch Service on 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.
- Data will be deleted from Elastic Cloud no earlier than 14 days after a termination notice has been sent to customers.
- 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 confidential information of the customer using commercially reasonable care.
- Elastic will not use confidential information other than as necessary to carry out Elastic’s duties or disclose any such confidential information to third parties other than affiliates without the customer’s prior written consent.
**Elasticsearch Service on Elastic Site Search Pro and Elastic Site Search Premium Subscription Levels**

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

Elastic offers three 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:

<table>
<thead>
<tr>
<th>Subscription Level</th>
<th>Hours of Operation</th>
<th>Target Response (by Severity)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Level 1</td>
</tr>
<tr>
<td>Premium</td>
<td>8 a.m. to -6 p.m. PST</td>
<td>4 business hours</td>
</tr>
<tr>
<td>Pro</td>
<td>8 a.m. - to 6 p.m. PST</td>
<td>-</td>
</tr>
<tr>
<td>Standard</td>
<td>8 a.m. - to 6 p.m. PST</td>
<td>-</td>
</tr>
</tbody>
</table>

**Severity Level Definitions**

Level 1, Urgent: Production is down and customer business has stopped. Customers should be helped immediately.

Level 2, High: Production is affected, but still functioning. Personnel are not sure if it is severe. Help should be sent as quickly as possible.

Level 3, Normal: Production seems fine, but personnel have questions. This is usually the default.

**Principal System Requirements**

System requirements are specifications regarding how the App Search and Site Search System should function to meet the Company’s commitments to user entities. Requirements are specified in the Company’s policies and procedures, which are available to all employees. The Company’s system requirements are documented within the information security policies. Policies include (but are not limited to) the following:

- 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
• Third-Party Risk Management
• Privacy Statement
• Backup and Recovery Management