Elastic


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

Section 1: Independent Service Auditor’s Report 3

Section 2: Assertion of Elastic Management 7

Attachment A: Elastic’s Description of the Boundaries of its Elasticsearch Service System and App Search 9

Attachment B: Principal Service Commitments and System Requirements 20
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 Service System and App 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 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 Service System and App Search 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), Google Cloud Platform (GCP), Microsoft Azure, 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 the Elasticsearch Service System and App Search (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 Service System and App Search
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.

Elastic offers the Elastic Stack (previously known as the Elasticsearch, Logstash, Kibana [ELK] Stack), a set of software products that ingest and store data from any source and in any format and perform search, analysis, and visualization. The Elastic Stack is designed for direct use by developers to power a variety of use cases. Software solutions built on the Elastic Stack are also offered that address a wide variety of use cases. The Elastic Stack and its related software solutions (i.e., App Search, Site Search, Enterprise Search, logging, metrics, application performance monitoring, business analytics, and security analytics) can be deployed on-premises, in public or private clouds, or in hybrid environments to satisfy various user and customer needs.

Elastic Cloud is a family of software-as-a-service (SaaS) products that includes the Elasticsearch Service (ESS), Elastic Site Search Service, and Elastic App Search Service. ESS is a service where 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), Microsoft Azure, and IBM SoftLayer. ESS offerings include advanced Elastic Stack features such as security, alerting, monitoring, reporting, machine learning, and graphing capabilities. ESS 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. ESS also includes enhanced security features, including default encryption at rest and Security Assertion Markup Language (SAML) and native authentication for hosted deployments.

ESS on Elastic Cloud

ESS is comprised of the following Elastic Stack components:

<table>
<thead>
<tr>
<th>Elastic Stack Component</th>
<th>Component Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Elasticsearch Service</td>
<td>Elasticsearch Service (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.</td>
</tr>
<tr>
<td>Elastic Stack Component</td>
<td>Component Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Elasticsearch Service Private</td>
<td>Elasticsearch Service Private (ESSP) is an Elasticsearch Service subscription tier that offer an isolated Elasticsearch Service environment that resides in a</td>
</tr>
<tr>
<td></td>
<td>dedicated virtual private cloud (VPC), running on an exclusive set of hosts.</td>
</tr>
<tr>
<td>Kibana</td>
<td>Kibana is the user interface for the Elastic Stack. It is the visualization layer for data stored in Elasticsearch. It is also the management and configuration</td>
</tr>
<tr>
<td></td>
<td>interface for all parts of the Elastic Stack.</td>
</tr>
<tr>
<td>App Search</td>
<td>App Search is a toolbox for developers looking to create search experiences. It contains a suite of application programming interfaces (APIs) with supporting</td>
</tr>
<tr>
<td></td>
<td>clients and open source user interface (UI) frameworks, crafted to enable the development of highly relevant searches backed by the Elastic Stack.</td>
</tr>
</tbody>
</table>

The boundaries of the system in this section of the report details ESS and App Search. 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 described in the subsections below.

Infrastructure

In order to help bring Elasticsearch and Kibana deployments online with speed and efficiency, Elastic provides the ESS offering. This offering runs on top of public cloud environments, including AWS, Microsoft Azure, IBM Softlayer and Google Cloud Platform (GCP).
The primary infrastructure used to provide ESS and App Search includes the following:

<table>
<thead>
<tr>
<th><strong>Hardware</strong></th>
<th><strong>Type</strong></th>
<th><strong>Purpose</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Web, application, database, and search servers</td>
<td>Cloud infrastructure managed by hosting providers</td>
<td>A set of managed services deployed in hosting provider’s data centers across the globe (including North America, Asia, Australia, and Europe).</td>
</tr>
<tr>
<td>Background processing, business analytics, etc.</td>
<td>Cloud infrastructure provided by hosting providers</td>
<td>Some background processing, analytics, and other offline workloads that do not interact with confidential customer data, handled by cloud instances provided by hosting providers.</td>
</tr>
<tr>
<td>Backup recovery and testing</td>
<td>Cloud infrastructure provided by hosting providers</td>
<td>Cloud instances are used by Elasticsearch for off-site backup validation and recovery.</td>
</tr>
<tr>
<td>Security infrastructure</td>
<td>Cloud infrastructure provided by hosting providers</td>
<td>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.</td>
</tr>
</tbody>
</table>

**Services Provided by Subservice Organizations and Vendors**

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

<table>
<thead>
<tr>
<th><strong>Subservice Organization</strong></th>
<th><strong>Purpose</strong></th>
</tr>
</thead>
</table>
| AWS | Infrastructure-as-a-service (IaaS) hosting ESS and App Search provided by AWS. Data centers are in the following locations:  
  - North America  
  - South America  
  - Asia  
  - Australia  
  - Europe |
Subservice Organization | Purpose
--- | ---
GCP | Infrastructure-as-a-service (IaaS) hosting ESS and App Search provided by GCP. Data centers are in the following locations:
- North America
- Asia
- Australia
- Europe

Microsoft Azure | IaaS hosting ESS and App Search provided by Azure. Data centers are in the following locations:
- North America
- Europe
- Asia

IBM SoftLayer | IaaS hosting ESS and App Search provided by IBM.

Software

The following table details the key software used to provide the ESS environment:

<table>
<thead>
<tr>
<th>Component</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating system</td>
<td>The operating system is used to run ESS and App Search.</td>
</tr>
<tr>
<td>Monitoring solutions</td>
<td>There are multiple monitoring systems in use for ESS and App Search, including:</td>
</tr>
<tr>
<td></td>
<td>- Security incident event monitoring (SIEM) centralized log correlation analysis and alert system</td>
</tr>
<tr>
<td></td>
<td>- Performance and capacity monitoring system</td>
</tr>
<tr>
<td></td>
<td>- Vulnerability management</td>
</tr>
<tr>
<td></td>
<td>- Application monitoring</td>
</tr>
<tr>
<td>Databases</td>
<td>All in-scope databases are AWS Relational Database Service (RDS) databases.</td>
</tr>
<tr>
<td>Component</td>
<td>Purpose</td>
</tr>
<tr>
<td>--------------------</td>
<td>--------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Network</td>
<td>The ESS and App Search network infrastructure utilizes a common set of network components:</td>
</tr>
<tr>
<td></td>
<td>• Elastic Load Balancers (ELBs)</td>
</tr>
<tr>
<td></td>
<td>• Firewalls and security groups</td>
</tr>
<tr>
<td></td>
<td>• Proxies</td>
</tr>
<tr>
<td></td>
<td>• Virtual Private Cloud (VPC) segmenting</td>
</tr>
<tr>
<td></td>
<td>• Infrastructure deployment automation</td>
</tr>
<tr>
<td></td>
<td>• Virtual private network (VPN)</td>
</tr>
<tr>
<td></td>
<td>• Configuration management</td>
</tr>
<tr>
<td>Identity and Access</td>
<td>• Authentication systems</td>
</tr>
<tr>
<td></td>
<td>• Administrative consoles</td>
</tr>
<tr>
<td>Code Management</td>
<td>• Code repository</td>
</tr>
<tr>
<td></td>
<td>• Code deployment pipeline</td>
</tr>
<tr>
<td></td>
<td>• Infrastructure as Code (IaC)</td>
</tr>
</tbody>
</table>

**People**

There are multiple groups at Elastic involved in the governance, management, operation, security, and use of the system, to include the following:

<table>
<thead>
<tr>
<th>Component</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive management</td>
<td>Provides general oversight and strategic planning of operations.</td>
</tr>
<tr>
<td>Component</td>
<td>Purpose</td>
</tr>
<tr>
<td>-----------</td>
<td>---------</td>
</tr>
</tbody>
</table>
| Engineering department | Responsible for design, implementation, and ongoing maintenance of Elasticsearch software and services. It consists of five separate teams:  
  - Design Team: develops brand identity and design language; responsible for UI and user experience (UX) design and product design; designs websites, emails, etc.  
  - Development Team: responsible for the architectural design, implementation, and ongoing maintenance of Elasticsearch and App Search software, products, and services.  
  - Cloud Operations and Security team: responsible for design and support for Elasticsearch production infrastructure; maintains the security and availability of the infrastructure comprising Elasticsearch and App Search product offerings, including vulnerability management and monitoring.  
  - Product Management: responsible for working with engineering to define and implement product vision.  
  - Infrastructure: responsible for creating tools and services for the Company; managing code repositories, developing configuration management libraries, and maintaining a continuous integration system. |
| Support | Responsible for supporting customers at every level of their Elasticsearch or App Search 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 manage 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 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

Data

Customers upload electronic data to ESS and App Search for processing. This data is referenced to as Cluster Data. Cluster Data has been classified as “restricted” under Elastic’s data classification policy, which receives the highest level of protection.
Complementary User Entity Controls (CUECs)

Elastic's controls related to ESS and App Search cover only a portion of overall internal control for each user entity of ESS and App Search. 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 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:

<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.  
• User entities are responsible for securely configuring their ESS and/or App Search environment. 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. |
Criteria | Complementary User Entity Controls (CUECs)
--- | ---
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.
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.
P5.1 | • User entities have policies and procedures in place to:
   - identify and authenticate data subjects requesting access to their personal information.
   - stating the reasons for denial of access to their personal information.
   - correcting, amending or appending their 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 GCP, IBM SoftLayer, Azure, and AWS (“the Hosting Providers”) as subservice organizations for data center colocation services. Elastic’s controls related to ESS and App Search cover only a portion of the overall internal control for each user entity of ESS and App Search.

Certain service commitments, system requirements, and applicable criteria are intended to be met by controls at the subservice organizations. Complementary Subservice Organization Controls (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 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, management of Elastic 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 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 the Hosting Providers’ management.

It is not feasible for the service commitments, system requirements, and applicable criteria related to ESS 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 Subservice Organization Controls (CSOCS)</th>
</tr>
</thead>
</table>
| 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. |
| A1.2 CC7.2 | • 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. |
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 ESS. Commitments are communicated in written master customer agreements, privacy policy, support policy 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.

Elasticsearch Service

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 will utilize reasonable and appropriate physical, technical, and administrative procedures to safeguard the information collected and processed.
- 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 ESS 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 later 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.
### Subscription Level

<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>Enterprise</td>
<td>24/7/365</td>
<td>1 hour</td>
</tr>
<tr>
<td>Platinum</td>
<td>24/7/365</td>
<td>1 hour</td>
</tr>
<tr>
<td>Gold</td>
<td>Business hours (8 a.m. to 6 p.m.) in the time zone applicable to the location based on the sales order</td>
<td>4 business hours</td>
</tr>
</tbody>
</table>

#### 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 ESS 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