algolia

REPORT ON ALGOLIA, INC.’S SEARCH SOLUTION SYSTEM RELEVANT TO SECURITY, AVAILABILITY, AND CONFIDENTIALITY THROUGHOUT THE PERIOD JANUARY 1, 2020 TO DECEMBER 31, 2020

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

COALFIRE®
CONTROLS

TABLE OF CONTENTS

SECTION 1

SECTION 2

ATTACHMENT A

ATTACHMENT B

SECTION 1

INDEPENDENT SERVICE AUDITOR’S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To: Algolia, Inc. ("Algolia")

SCOPE

We have examined Algolia's accompanying assertion titled "Assertion of Algolia, Inc. Management" (assertion) that the controls within the Search Solution System (system) were effective throughout the period January 1, 2020 to December 31, 2020, to provide reasonable assurance that Algolia's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (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 Algolia, to achieve Algolia'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 Algolia'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.

Algolia 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 Algolia, to achieve Algolia'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 Algolia'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

Algolia 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 Algolia's service commitments and system requirements were achieved. Algolia has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Algolia 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 Algolia'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 Algolia's service commitments and system requirements based on the applicable trust services criteria.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

INHERENT LIMITATIONS

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

OPINION

In our opinion, management's assertion that the controls within the Search Solution System were effective throughout the period January 1, 2020 to December 31, 2020, to provide reasonable assurance that Algolia'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 Algolia's controls operated effectively throughout that period is fairly stated, in all material respects.

Coalfire Controls LLC

Westminster, Colorado
March 10, 2021

SECTION 2

ASSERTION OF ALGOLIA, INC. MANAGEMENT

Assertion of Algolia, Inc. (“Algolia”) Management

We are responsible for designing, implementing, operating and maintaining effective controls within the Search Solution System (system) throughout the period January 1, 2020 to December 31, 2020, to provide reasonable assurance that Algolia’s service commitments and system requirements relevant to security, availability, and confidentiality 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 Algolia, to achieve Algolia’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 Algolia’s controls.

Algolia 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 Algolia, to achieve Algolia’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 Algolia’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 January 1, 2020 to December 31, 2020, to provide reasonable assurance that Algolia’s service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (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 Algolia’s controls operated effectively throughout that period. Algolia’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, 2020 to December 31, 2020, to provide reasonable assurance that Algolia's service commitments and system requirements were achieved based on the applicable trust services criteria.

Algolia, Inc.

ATTACHMENT A

ALGOLIA, INC.’S DESCRIPTION OF THE BOUNDARIES OF ITS SEARCH SOLUTION SYSTEM

TYPE OF SERVICES PROVIDED

Since 2014, Algolia, Inc. (“Algolia” or “the Company”) has provided its Search Solution System to businesses of all sizes around the world. Algolia provides user entities (customers) a hosted and internally developed search solution to provide an end-to-end search experience for their applications and services.

The scope of Algolia’s Search Solution System includes all the products as listed below, the teams supporting the development and maintenance of these products, and the physical locations of Paris, France and San Francisco, CA.

The scope of services includes the following components of the Search Solution System:

ALGOLIA SEARCH

Algolia Search Application Programming Interface (API) is the internally developed proprietary core of Algolia’s services. Algolia Search API is a schema-less JavaScript Object Notation (JSON)-based search engine optimized for user-facing searches. Algolia Search API is operated in clusters where servers cooperate together using distributed consensus protocol to ensure consistency of the data and availability of the service. Algolia Search API provides up to 99.999% availability which is achieved by its distributed nature.

In order to mitigate the impact of network latency, Algolia Search API provides an option of enriching the primary cluster by an arbitrary number of Distributed Search Network (DSN) servers that serve as read replicas. The users are then geo-routed to the closest server having the customer data. Besides lowering network latency, this solution also improves the availability of the whole system by making it more resilient to region scale outages.

Internally, Algolia Search API uses encrypted binary communication protocol between the servers. Externally, Algolia exposes public Hypertext Transfer Protocol (HTTP) and HTTP Secure (HTTPS) interfaces for the Algolia Search API.

ALGOLIA DASHBOARD

Algolia Dashboard is a web management interface that uses the Algolia Search API and provides a user-friendly interface for using and configuring the Algolia Search API. The dashboard also provides user-management functionality.

The Algolia Dashboard is available using HTTPS with HTTP Strict Transport Security, preloaded in most modern browsers to eliminate the possibility of downgrade attacks that strip away the Transport Layer Security (TLS) of HTTPS connections.

ALGOLIA ANALYTICS & INSIGHT

Algolia Analytics & Insight API is a JSON-based API that provides access to analytics data generated from the queries. The queries performed through the Algolia Search API are collected, analyzed, and made available through Algolia Analytics & Insight APIs allowing the customer to analyze the user experience, trends, and impacts of changes.

ALGOLIA MONITORING

Algolia Monitoring API is an abstraction API for Algolia’s multiple monitoring systems that collects data about the usage and operations of the Algolia Search API. Algolia Analytics & Insight APIs allows customers to get the data that is available in the Algolia Dashboard and is used for the Algolia status page.

ALGOLIA PERSONALIZATION

Algolia Personalization help make users a personalized experience more compelling and relevant with Algolia.

ALGOLIA SHOPIFY

Algolia Shopify creates personalized e-commerce site search and discovery experiences that shoppers love.

ALGOLIA CRAWLER (ALGOLIA SITE SEARCH)

Algolia Crawler is a customized site search and discovery tool which automatically extracts and enriches a website's content to deliver it through a rewarding experience. It is a content discovery platform that enables businesses to build, manage and deliver customer centric, content-based experiences on every channel.

The boundaries of the system in this section of the report details the Algolia Search Solution System. Any other Algolia services are not within the scope of this report.

THE BOUNDARIES OF THE SYSTEM USED TO PROVIDE THE SERVICES

The boundaries of the Search Solution System are the specific aspects of Algolia’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 Search Solution System.

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

INFRASTRUCTURE

Algolia operates its services on a physical and virtual infrastructure placed in third party datacenters and colocation services of third-party server providers. The data centers hosting the services are located in US West (California), US Central (Dallas area), US East (Virginia), Canada (Montreal area), South America (São Paulo), Europe (France, Netherlands and Germany), Russia (Moscow), South Africa, India, Singapore, Hong Kong, Japan (Tokyo and Osaka), Australia (Sydney), and the United Arab Emirates (Dubai). Portions of the provided services are hosted by various cloud providers, including OVH, Amazon Web Services (AWS) and Google Cloud Platform.

In order to increase the overall security of the system, Algolia has designed its network environment as a Zero-Trust Network with traditional network concepts of external untrusted and internal trusted networks, but without a demilitarized zone (DMZ) network. In Algolia’s environment, all the networks are external untrusted and each of the two servers need to be authorized to communicate together internally. Algolia’s environment spans multiple data centers, multiple service providers, and multiple network autonomous systems while maintaining the security, resiliency, and availability of the service.

Algolia also operates the related network equipment (located in-house) that supports the infrastructure located at colocation provider facilities.

SOFTWARE

The environment of Algolia is based on Linux operating systems (OSs) and heavily utilizes open-source software. Algolia’s environment is composed of multiple systems offering the services to its customers which work in tandem with internal systems supporting the operations of the infrastructure.

Internal Systems

Infrastructure Monitoring

Every system in the Algolia environment is monitored, including infrastructure metrics such as central processing units (CPU), memory, and network utilization. This data is then transparently collected and analyzed. Additional alerts are evaluated on top of this data to provide Algolia with pro-active alerting that might impact the service before the actual degradation happens.

Backups and Disaster Recovery

Algolia has developed internal backup mechanisms that mirror the application data multiple times per day from the production servers to backup locations over an encrypted tunnel. Once the mirror is finished, a local processing of the data is performed, and consistency of the data is verified before further processing. Then an encrypted backup is generated and distributed to the recovery storage closest to the source cluster in order to provide the fastest possible recovery times.

All the databases are backed up once per day using the appropriate database backup mechanisms to ensure consistency of the backups.

Algolia also maintains a Disaster Recovery (DR) plan for its systems in case of a complete outage. The DR plan is tested on at least an annual basis. System failures that do not impact the availability of the Algolia service are continuously tested to ensure all the fallback and recovery mechanisms work as expected.

Logging

Algolia collects and maintains detailed logs from both the infrastructure and application level. These logs are centrally collected, analyzed, and respective alerts are evaluated. The collection of the logs is automatic. Additional application specific collections are configured either by the Configuration Management tool or implicitly by producing the logs to Syslog.

Patch Management

All Algolia servers and the running software are regularly patched. If the particular software allows it, automatic updates are enabled, and security updates are installed automatically without intervention.

Integrity Monitoring

Algolia uses a Host-Based Intrusion Detection System (HIDS) to ensure file integrity and protection of the systems from intrusion. The HIDS performs integrity tests of important files of the system and reports any changes. The HIDS uses its known signatures to regularly scan the systems for rootkits and other malware. HIDS alerts are centrally collected and analyzed.

PEOPLE

The development and operations of the systems are the responsibility of the Research & Development organization unit of Algolia, which is led by the Chief Technology Officer (CTO) and Vice President (VP) of Engineering.

Engineering teams working on particular systems are given the necessary infrastructure and tools they need for system development, testing, and operations. These teams operate their systems on their own and are responsible for the availability and operations of the system.

The engineering team led by the Director of Infrastructure works on the automation, maintenance, operations, and security of all systems in Algolia. This engineering team also includes Algolia’s Security Team who is responsible for developing and designing the secure practices of Algolia systems, performing internal training, and developing new systems to improve the overall security of Algolia.

The Product team leads the development of Algolia's services based on the feedback from customers, market needs, and future visions of Algolia.

The Sr Director of Infrastructure, CTO, VP of Engineering, and Head of Legal ensure Algolia's continuous compliance with all developed policies and legal requirements.

Human Resources (HR) of Algolia contributes to the security of Algolia's systems by performing background checks on new employees, adding new employees to Active Directory, and revoking assigned rights during the termination process.

PROCEDURES

Algolia utilizes automation for all its systems to help achieve security, recovery from failures, administration, and provide an overview of its assets. In order to ease the adoption of internal policies and guide employees through the correct processes, Algolia encompasses as much as possible into internal applications, configuration management, and internal systems.

Algolia has developed policies covering the needs of operations and nature of services provided. These policies are available to all employees of the Company, business partners, and customers. Each policy is versioned, and changes are logged.

The default system and server security configurations of all Algolia systems are anchored in the configuration management system based on the Chef configuration management tool that reconfigures the system to a desired state using predefined and dynamic templates. The configuration management system also provides the functionality of service discovery allowing Algolia to operate its systems in a Zero-Trust architecture.

The Change Management policy governs how changes are made to production. Most of the changes are performed by changing code or configurations in system-related Git code repositories. These changes are tested in testing environments, approved by an engineering peer, and then deployed to production. Algolia employs multiple methods of production software deployment depending on the criticality of the system including cold restart, hot reload, blue-green deployment, canary deployment, gradual deployment based on service type, and regional deployment.

The automatic monitoring system has the ability to trigger critical alerts and notify the 24/7 on-call team in order to resolve immediate issues and restore service. The most critical applications, like Algolia Search API, has the ability to trigger alerts directly without the monitoring system if the monitoring system is unavailable.

Algolia has developed a policy specifying the requirements for its data centers. Verification of these requirements is performed through the monitoring of subservice organizations.

Algolia has developed a series of policies, procedures, and technical measures to deal with large scale technical issues that could impact the availability of Algolia's services or a pandemic issue that could impact a significant portion of Algolia's employees operating the service.

DATA

Algolia's business does not sell customer data and Algolia has developed an environment that protects the data and confidentiality of its customers.

Data Classification

Algolia has developed a Data Classification Policy for both customers and its own data. Due to the implicit sensitivity of customer data, this data is classified as "confidential".

Algolia Search

Algolia Search API works with semi-structured JSON formatted objects received via Representational State Transfer (REST) API. Algolia Search API is available via HTTP for legacy systems and HTTPS for modern systems, with TLS configuration and certificates from public certification authorities. Algolia Search API follows HTTP standards and is usable as-is or through integration libraries that Algolia provides as an open-source software.

Algolia Search API features an authentication scheme which allows customers to generate and manage access keys with different levels of permissions. This authentication scheme contains security parameters that allow customers to generate access keys using communication with the service as well as locally (offline) without any contact with the service.

Upon reception, the data is formatted into proprietary file format, distributed, and stored on Algolia servers composing the solution. All modifications of the data are performed via Algolia Search API and every interaction with the data is logged. These audit logs are used for auditing and accounting purposes. Once generated, the audit logs are processed in Algolia’s log processing system, where necessary information is extracted and the logs are stored for further analysis, incident response, and modification/improving of the service.

Algolia Dashboard

The Algolia Dashboard is a web application primarily built on top of the Algolia Search API that provides additional user management and authentication for management. The Algolia Dashboard stores information about authorized users which were added by the customer.

Algolia Analytics & Insight

Algolia Analytics and Insight does not handle customer data records. Analytics API produces data generated from the usage and audit logs of the Algolia Search API. This allows customers to get visibility into search requests being performed by their systems or their users.

Algolia Monitoring

Algolia Monitoring API does not handle customer data. Monitoring API produces data collected from Algolia about the state of the service and makes that information available to customers.

Logging

All systems produce application and operations logs which are collected, processed, and stored in Algolia’s systems. These logs are purged from the system following its retention requirements.

Data Retention

When data is being requested for deletion via Algolia Search API, it is made unavailable as soon as the system converges and marks the data as ready for garbage collection (data purge). During the next garbage collection, the data is purged from the system by removing the data from its data storage, and thus making it unavailable. At this point, the data is no longer accessible to the customer or Algolia, cannot be restored, and will not be listed by any of the tools or APIs.

After the backup retention period expires, the data is also purged from the backup systems. All Algolia systems are designed to automatically remove data marked for deletion in a timeframe specified by the internal Data Retention and Disposal Policy.

Algolia has established processes to allow customers to request data to be deleted from all systems.

COMPLEMENTARY USER ENTITY CONTROLS (CUECS)

Algolia's controls related to the Algolia Search Solution System cover only a portion of overall internal control for each user entity of the Algolia Search Solution System. It is not feasible for service commitments, system requirements, and applicable criteria related to the system to be achieved solely by Algolia. Therefore, each user entity's internal control should be evaluated in conjunction with Algolia's controls considering the related CUECs identified for the specific criterion. 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 (CUECs)
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 Algolia according to contractually specified time frames. • Controls to provide reasonable assurance that Algolia 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 Algolia. ○ Determine how to file inquiries, complaints, and disputes to be passed on to Algolia.
CC6.1 CC6.4 CC7.2 A1.2	• User entities grant access to the Algolia Search Solution 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.

SUBSERVICE ORGANIZATIONS AND COMPLEMENTARY SUBSERVICE ORGANIZATION CONTROLS (CSOCS)

Algolia uses multiple data center colocation providers as subservice organizations for data center colocation services. Algolia's controls related to the Algolia Search Solution System cover only a portion of the overall internal control for each user entity of the Algolia Search Solution System. The description does not extend to the services provided by the subservice organizations that provide colocation services for IT infrastructure.

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 all subservice organizations related to physical security and environmental protection, as well as backup, recovery, and redundancy controls related to availability. The subservice organizations' physical security controls mitigate the risk of fires, power loss, climate, and temperature variabilities.

Algolia monitors these controls by obtaining and reviewing subservice organization SOC 2 and/or SOC 1 reports on an annual basis when they are available. Due to the wide variety of subservice organizations that are used by Algolia, not all of the organizations used for data center and data center colocation services have a readily available SOC 2 or SOC 1 report to inspect. Algolia accepts valid ISO 27001 and PCI DSS reports to determine adequate physical security controls. If none of the accepted reports are available, Algolia performs its own evaluation of the subservice organizations using evaluation questionnaires and walkthroughs of these sites on an annual basis to ensure the controls are compliant with Algolia's requirements, are in place, and are operating effectively.

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

Criteria	Complementary Subservice Organization Controls (CSOCs)
CC6.4	• Co-location service providers are responsible for restricting data center access to authorized personnel. • Co-location service providers are responsible for the 24x7 monitoring of data centers by closed circuit cameras and security personnel.
CC6.5	• Co-location service providers are responsible for securely decommissioning and physically destroying production assets in its control.
CC7.2 A1.2	• Co-location service providers are responsible for the installation of fire suppression and detection, and environmental monitoring systems at the data centers. • Co-location service providers are responsible for protecting data centers against a disruption in power supply to the processing environment by an uninterruptible power supply (UPS). • Co-location service providers are responsible for overseeing the regular maintenance of environmental protections at data centers.

Data Center Service Providers

The datacenters that are in scope for purposes of this report are listed in the table below.

Subservice Organization	Monitoring Control Performed
Leaseweb	Obtain and review a SOC 1 and an ISO27001
Amazon Web Services (AWS)	Obtain and review a SOC 2 and/or an ISO27001
Google Cloud Platform	Obtain and review a SOC 2 and/or an ISO27001
IPTP	Obtain and review a SOC 1, and/or a SOC 2, and/or an ISO27001
Equinix	Obtain and review a SOC 1, and/or a SOC 2, and/or an ISO27001
Packet	Obtain and review a SOC 1 and/or a SOC 2, and/or an ISO27001, and/or an Algolia Walk-through

Subservice Organization	Monitoring Control Performed
Internap	Obtain and review a PCI DSS and/or a SOC 2
MaxiHost	Obtain and review an ISO27001, and/or Algolia Walk-through
Anexia	Obtain and review an ISO27001 and ISO9001
OVH	Obtain and review an ISO27001, and/or Algolia Walkthrough
Hetzner	Obtain and review an ISO27001
Zone Networks	Obtain and review an ISO27001
WAN Security	Obtain and review an ISO27001
E2E Networks	Obtain and review an ISO27001
Web Werks	Obtain and review PCI-DSS, and/or Algolia Walk-through with Questionnaires
Microsoft Azure	Obtain and review a SOC 2

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 Algolia Search Solution System. Commitments are communicated in Master Subscription agreements, service-level agreements (SLAs), and online in the Company's Terms of Service and Privacy Policy.

System requirements are specifications regarding how the Algolia Search Solution System should function to meet Algolia's principal commitments to user entities. System requirements are specified in Algolia's policies and procedures, which are available to all employees.

Algolia's principal service commitments and system requirements include the following:

Trust Services Category	Service Commitments	System Requirements
Security	• Algolia will maintain administrative, physical, and technical safeguards for the security and integrity of the Algolia Search Solution System consistent with industry standard practices.	• Logical access standards • Employee provisioning and deprovisioning standards • Access review standards • Intrusion detection and prevention standards • Risk and vulnerability management standards • Configuration management standards • Incident handling standards • Change management standards • Vendor management standards • Hardening standards • Anti-malware standards
Availability	• Algolia will maintain a production system uptime of 99.99%.	• System monitoring • Backup and recovery standards
Confidentiality	• Algolia will maintain all customer data as confidential and will not disclose information to any unauthorized parties. • Algolia will safeguard all confidential information with the same degree of care it would its own information and will not use confidential information other than to provide the Search Solution System.	• Data classification • Retention and destruction standards • Internal confidentiality standards • Information sharing standards