System and Organization Controls (SOC) 2 Type II
Report on Management's Description of its

Hybrid And Remote Work Platform

And the Suitability of Design of Controls Relevant to the
Controls Placed in Operation and Test of Operating Effectiveness Relevant to
Security, Availability, Confidentiality, Processing Integrity, and Privacy

For the Period
December 1, 2021 to November 30, 2022

Together with
Independent Service Auditors' Report

Table of Contents

I. Independent Service Auditors' Report

Independent Service Auditors' Report

To the Management of Art Tech Shock Ltd. , Inc. (Artishok)

Scope

We have examined Artishok's accompanying description of its Work Platform titled "Description of Artishok's Work Platform" throughout the period December 1, 2021 to November 30, 2022(description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA,*Description Criteria*), and the suitability of the design and operating effectiveness of controls stated in the

description throughout the period December 1, 2021 to November 30, 2022, to provide reasonable assurance that Artishok 's service commitments and requirements were achieved based on the trust services criteria relevant to Security, Availability, Confidentiality, Processing Integrity, and Privacy (applicable trus services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability,Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Artishok uses subservice organizations to provide application maintenance and support services.The description indicates that complementary subservice organization controls that are suitably designedand operating effectively are necessary, along with controls at Artishok, to achieve Artishok's service commitments and system requirements based on the applicable trust services criteria. The description presents Artishok's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Artishok'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.

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

Service Organization's Responsibilities

Artishok 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 Artishok's service commitments and system requirements were achieved. Artishok has provided the accompanying assertion titled "Assertion of Artishok Management" (assertion) about the descriptionand the suitability of design and operating effectiveness of controls stated. Artishok is also responsiblefor preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selectingthe applicable trust services criteria and stating the related controls in the description; and identifying therisks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditors' Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness of controls stated in the description based on our examination. 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, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of the description of a service organization's system and the suitability of the design and operating effectiveness of controls involves the following:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria
- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria
- Evaluating the overall presentation of the description

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

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs.

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 are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitabilityof the design and operating 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.

Description of Tests of Controls

The specific controls we tested, and the nature, timing, and results of those tests are listed in section IV.

Opinion

In our opinion, in all material respects,

a. the description presents Artishok's Work Platform that was designed andimplemented throughout the period December 1, 2021 to November 30, 2022, in accordance with the description criteria.
b. the controls stated in the description were suitably designed throughout the period December 1, 2021 to November 30, 2022, to provide reasonable assurance that Artishok's servicecommitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period and if the subservice organization and user entitiesapplied complementary controls assumed in the design of Artishok's controls throughout thatperiod.
c. the controls stated in the description operated effectively throughout the period December 1, 2021 to November 30, 2022, to provide reasonable assurance that Artishok'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 Artishok's controls operated effectively throughout that period.

Restricted Use

This report, including the description of test of controls and results thereof in section IV, is intended solely for the information and use of Artishok user entities of Artishok's Work Platform duringsome or all of the period December 1, 2021 to November 30, 2022, business partners of Artishok subject to risks arising from interactions with the Work Platform, practitioners providingservices to such userentities and business partners, prospective user entities and business partners,and regulators who have sufficient
knowledge and understanding of the following:

- The nature of the service provided by the service organization
- How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties
- Internal control and its limitations
- Complementary user entity controls and complementary subservice organization controls andhow those controls interact with the controls at the service organization to achieve the serviceorganization's service commitments and system requirements
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services
- The applicable trust services criteria
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks

This report isnot intended to be, and should not be, used by anyone other than these specified parties.

San Jose, California

Nov 24, 2022

II. Assertion of Artishok Management

Assertion of Artishok **Management**

We have prepared the accompanying description of Artishok, Inc.'s (Artishok) Work Operation Platform titled "Description of Artishok's Work Operation Platform" throughout the period December 1, 2021 to November 30, 2022, (description) based on the criteria for a description of a service organization's system in DCsection 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (AICPA, Description Criteria). The description is intended to provide report users with information about the platform that may be useful when assessing the risks arising from interactions with Artishok's system, particularly information about system controls that Artishok has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, Confidentiality, Processing Integrity, 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).

Artishok uses subservice organizations to provide application maintenance and support services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Artishok, to achieve Artishok's service commitments and system requirements based on the applicable trust services criteria. The description presents Artishok's controls, the applicable trust services criteria, and the types of complementary sub service organization controls assumed in the design of Artishok's controls. The description does not disclose the actual controls at the subservice organizations.
The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Artishok, to achieve Artishok's service commitments and system requirements based on the applicable trust services criteria. The description presents Artishok's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Artishok's controls.

We confirm, to the best of our knowledge and belief, that

a. the description presents Artishok's Work Platform that was designed andimplemented throughout the period Dec 1, 2021 to Nov 30, 2022, in accordance with the descriptioncriteria.

b. the controls stated in the description were suitably designed throughout the period Dec 1, 2021 to Nov 30, 2022, to provide reasonable assurance that Artishok's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organization and user entities applied the complementary controls assumed in the design of Artishok's controls throughout that period.

c. the controls stated in the description operated effectively throughout the period Dec 1, 2021 to Nov 30, 2022, to provide reasonable assurance that Artishok'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 Artishok's controlsoperated effectively throughout that period.

Signed by Artishok Management

Nov 25, 2022

III. Description of Artishok's Work Platform

Description of Artishok's Work Platform

Background and System Overview

Artishok, Inc. provides a platform for managing hybrid and remote organization as a software-as-a-service (SaaS) to its customers across North America. The company was founded in 2019 to provide its services to cloud-native SaaS companies, with headquarters located in Tel Aviv, Israel.

Artishok Inc.'s core application, Artishok (the application or platform), is a single-tenant-architected software application suite that is an operating system for managing hybrid and remote organizations. Artishok streamlines the following tasks and processes:

- Integrate with HRIS to get employee data
- Manage workspace and workforce assets
- Manage meetings rooms and desks
- Visitor management system
- Mailroom and delivery management solution
- Communication center for news and events
- Nudge hub for promoting in-person interaction

Principal Service Commitments and System Requirements

Artishok designs its processes and procedures to meet its objectives for its compliance audit readiness services. Those objectives are based on the service commitments that Artishok makes to user entities, the laws and regulations that govern the provision of services, and the financial, operational, and compliance requirements that Artishok has established for the services. The services of Artishok are subject to the security

requirements of SOC 2, as well as state privacy security laws and regulations in the jurisdictions in which Artishok operates.

Security commitments to user entities are documented and communicated in SLAs and other customer agreements, as well as in the description of the service offering provided online. Per Artishok's Master Services Agreement (MSA), the uptime requirement for availability is 99.9%
. Security commitments are standardized and include, but are not limited to, the following:

- Customer data is always encrypted at rest and in transit.
- The platform is housed in state-of-the-art cloud environments that undergo an annual SOC 2 Type 2 examination.
- The platform is continuously monitored and tested for any security vulnerabilities.
- The platform security enables segregation of responsibilities and application functional access.
- Artishok provides access to customer data on the principle of least privilege. All employee access to the platform is audited to assure access levels are never-out-of-date.
- Artishok employees authorized to work with customers and their data are trained to handle data properly and never expose the data via insecure practices.
- Artishok is built on a single-tenant database architecture.

Artishok establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Artishok's system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the service.

Infrastructure

Artishok runs in the Amazon Web Services (AWS) Cloud, utilizing the container technology EKS to serve its application programming interface (API) alongside AWS Relational Database Services (RDS) for its permanent storage. The web and internal site-admin applications are served from Netlify's Content Delivery Network (CDN).

Each platform instance (Production, Quality Assurance (QA), Development (DEV)) is contained within a separate AWS account. The account provides granular access control to all aspects of the infrastructure via roles which are assumed from Artihsok's parent organization AWS account. Access from external locations is controlled through configuration and strict Virtual Private Cloud (VPC) rules. Access to internal components of the platform is only possible via multi-factor authentication (MFA)-controlled access utilizing Secure Shell (SSH) protocol to a "jump" server, then internal communication from within the network. Access is granted on an account level basis based on the employee's role at Artishok. Only a select few have access to the production account.

Data is persisted in both AWS RDS (MySQL) and S3. Both utilize Advanced Encryption Standard (AES) 256 encryption for all data stored at rest. Each customer instance in production establishes a database that is allocated for use solely for that customer alongside a namespace within the application's S3 storage bucket. Customer data is never co-mingled in Artishok.

There is a short-lived caching layer using AWS ElastiCache (Redis) for performance benefits. All data is name-spaced to its tenant.

User entities access their instance using standard web browsers utilizing Transport Layer Security (TLS) 1.2 or above for encrypted communications.

For intrusion detection, AWS GuardDuty is in place. For vulnerability scanning, Intruder.io automatically scans the system. For web application firewall services (WAF), DDoS prevention, OWASP rules, networking acceleration, caching, and the Domain Name System (DNS) service, CloudFlare has been implemented.

Software

Artishok uses Jenkins to build and deploy its Back-End software via Docker Images that run on EKS, and Netlify to build and deploy its Front-End software. EKS enables software deployments via images. Images are secure, fully contained versions of the platform service. Artishok has several services that provide scalable system operations. Image operating environments are based on a secure version of Amazon Linux 2 distribution. Artishok's services are primarily developed using ReactJS and NodeJS technologies. Netlify provides a platform-as-a-service (PaaS) to host and deliver static content from a global CDN.

User entities access the application using standard web browsers. The client application is a ReactJS application and is downloaded from a global CDN.

In addition, Artishok uses the following software and tools to assist with security operations:

Cloudflare

Artishok uses Cloudflare to provide DNS services and to protect all public web sites from Distributed Denial of Service. Artishok requires SSL on all public-facing web services and uses Cloudflare to create and manage those SSL certificates. Artishok also leverages the caching and optimization tools offered by Cloudflare.

Datadog

Artishok uses Datadog to track server telemetry, Application Performance Monitoring (APM), server logging, Real- User Monitoring (RUM), and client-side error tracking.

Clickup

Clickup is a project management tool that Artishok uses to track engineering efforts. All sprint management, planning, and reporting is handled by Clickup. Engineers use Clickup to guide their individual tasks throughout the Software Development Lifecycle.

Bitbucket

Bitbucket is a software development platform that ata uses to track changes in the code for all applications. Engineers conduct code reviews on all pull requests before they are merged into the main branch for deployment.

AWS Work Mail

Artishok work email accounts are provisioned to personnel using AWS Workmail upononboarding. Google Workspace is used as Artishok's identity service provider.

Terraform

Artishok used Hashicorp's Terraform technology to define and provision its infrastructure and configurations at AWS. This allows Artishok to control all aspects of its AWS services and allows for the team to follow its Software Development Lifecycle (SDLC) on code changes.

AWS SSO

Artishok uses AWS SSO as the primary platform to manage identity and logical access in providing single-sign-on (SSO) and multi-factor authentication (MFA).

People

Artishok has a staff of approximately 29 employees and contractors organized in the following functional areas:

Executive Management (CEO, CTO, CRO, and CISO):
Team members responsible for overseeing the operations of the company.

Engineering:
Team members that develop, innovate and support the technology.

Product Development:
Team members that support Artishok product management, development and development operations.

Customer Success:
Team members that work with customers to assure they are able to successfully use Artishok to accomplish their goals.

Sales and Marketing:
Team members that support sales and marketing activities.

Operations:
Team members that support back office operations.

Processes and Procedures

The Executive Management Team has developed and communicated processes that control and restrict access to Artishok instances that contain customer data. Review of these processes and controls are conducted by the CEO, CTO, and CISO and all changes are approved by the CEO prior to implementation.

These processes are documented in the Artishok Information Security Policy document and include the following key security life cycle areas:

- Data classification (data at rest, in motion, and output)
- Categorization of information
- Assessment of the business impact resulting from proposed security approaches
- Selection, documentation, and implementation of security controls
- Performance of annual management self-assessments to assess security controls
- Authorization, changes to, and termination of information system access
- Monitoring security controls
- Management of access and roles
- Maintenance and support of the security system and necessary back-up and offline storage
- Incident response
- Maintenance of restricted access to system configurations, super user functionality, master passwords, powerful utilities, and security devices (for example, firewalls)

Data

Data, as defined by Artishok, constitutes the following:

- Company data
- reports
- System files
- Error logs

Output reports are available in electronic PDF, comma-delimited value file exports, or electronically from the various websites. The availability of these reports is limited by user role. Reports delivered externally will only be sent using secure websites over connections secured by trusted security certificates.

Third-Party Access

operations. These service providers do not have day-to-day access to Artishok data. Some of these providers do have system administration level privileges to the services, but these privileges are only used to access Artishok services when explicitly authorized by Artishok development operations for the purpose of resolving system issues. All of the third-party service providers covered in the scope of the SOC 2 report have SOC 2 Type 2 reports, and Artishok reviews these reports annually.

RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT PROCESS, INFORMATION AND COMMUNICATION SYSTEMS, AND MONITORING OF CONTROLS

Control Environment

Management Philosophy

Artishok's control environment reflects the senior management's commitment to the security of data and information. The Security Committee, which reports to the board annually and meets quarterly, is responsible for overseeing the security activities of Artishok under the direction of the board. The committee is responsible for setting overall security policies and procedures for the organization. Artishok places a strong emphasis on security through the development and communication of policies and procedures, as well as the allocation of resources and personnel to implement these policies.

In designing its controls, Artishok has taken into consideration the relevance of controls to meet the relevanttrust services criteria.

Security Management

Artishok's CEO and CTO are responsible for maintaining and enforcing the company's information security policies, and they are required to annually sign and acknowledge their review of these policies. The CTO also reviews and approves the information security policy annually. The Security Committee monitors known incidents and patches, as well as results from recent vulnerability assessments, and makes any necessary changes to the policies and procedures. These changes may include reclassification of data, reassessment of risk, updates to incident response plans, and verification of responsibilities for authorizing and monitoring access. Any changes are reviewed and communicated during meetings or through system alerts. Information security personnel at Artishok are selected based on their ability to fulfill the duties and responsibilities of their positions, as well as their education, past experience, positive performance history, and knowledge of relevant cybersecurity controls and processes. Annual security training and awareness programs ensure that management communicates the latest security policies and provides written job descriptions for security management.

Security Policies

Artishok has defined a set of information security standards and policies that are under the direction andownership of the CTO and implemented through the Security Committee. The standards and policiesaddress the management and implementation of security controls, ranging from the physical security offacilities and equipment to the logical security at the data element layer. The information security policiesand standards are designed to provide information to employees, contractors, and vendors that arealigned to their job or functional responsibilities, while also contemplating segregation of functions thatmay otherwise create a segregation of duties conflict.

Security policies are published on the Company’s SaaS platform Artishok, included in onboarding packages,and reiterated through annual training that all employees are required to take and acknowledge. The CTOand CEO review and approve policies on an annual basis.

The following security policies and related processes are in place for Artishok:

- Acceptable Use

- Asset Management
- Data Backup
- Business Continuity
- Code of Conduct
- Data Classification
- Data Deletion
- Data Protection
- Disaster Recovery
- Encryption
- Incident Response
- Information Security
- Password
- Physical Security
- Responsible Disclosure
- Risk Assessment
- Software Development Lifecycle
- System Access Control
- Vendor Management
- Vulnerability Management

All employees are required to review and accept the code of conduct and Acceptable Use Agreement at the time of employment. Confidentiality, computer security, general expectation of business behavior, performance and financial dealings are addressed. Employees must avoid any appearance of impropriety or conflict of interest. It is a policy that no employee shall engage in any outside activity that interferes with his or her job, competes with Artishok's activities or involves any use of Artishok's facilities.

Personnel Security

Background checks are performed for all new hires as a condition of employment, who are also required to review and acknowledge their receipt of relevant security policies. The new positions are supported by

job descriptions. Once employed, employees are subject to Artishok procedures for accessing systems.
Employees who violate Artishok's information security policy are subject to related disciplinary action.
Employees are instructed to report potential security incidents to the help desk.

Artishok's service agreements instruct user entities to notify Artishok if they become aware of apossiblesecurity breach or any security-related incident involving Artishok or interaction with anyArtishokemployee orthird party.

Physical Security and Environmental Controls

A Physical Security Policy has been developed to adequately describe the preventative and detective measures in place to provide physical and environmental safeguards.

All visitors to Artishok's location are required to sign-in at the front reception desk, wear a visible visitor badge and be escorted by a Artishok employee.

All Artishok centralized data storages are housed in data centers that undergo annual SOC 2 Type 2 examinations.

Change Management

Artishok has a formal change management process in place that requires the identification and recording of significant changes, assessment of risk and potential impact of these changes, approval of proposed changes, and testing of changes to customer-facing instances. Proposed changes are classified, recorded, and approved, and can be classified as a release, maintenance patch, or hotfix. Releases are driven by feature requests recorded in a backlog and can take three to four months to complete. Maintenance patches are planned changes that address accumulated defects and are planned as needed for a two-week release. Hotfixes are used to address critical system or security issues identified in Artishok. All changes are approved by the CTO and QA before being applied to customer-facing instances. Changes are also tested in separate development/QA and deployment instances before being migrated to production. Developers do not have the ability to migrate changes into production environments. The Artishok Software Development Lifecycle (SDLC) process includes several steps that incorporate security and quality review, including security code review, daily security vulnerability testing, and external third-party security tests of new releases.

Patch Management

Artishok runs on the AWS EKS service. This service's operating system has periodic releases that address issues, add functionality and resolve security issues. AWS notifies Artishok of new releases and once a quarter, the Artishok Site Reliability Engineering (SRE) team begins the test and apply process.

This process starts with the application of the patch to the QA environment. The patch is tested and once passed by the QA team, the patch is scheduled to be applied to production and all other instances of Artishok.

This process is accelerated in the event of a zero-day or high severity security issue. High severity security issues are tested in QA. Provided the patch passes QA, it is then applied to all other Artishok instances.

Firewalls and Perimeter Security

All Artishok instances are deployed in the AWS Cloud which provides firewall and perimeter security. Only the ports and protocols necessary to run the platform are enabled. Only the Artishok SRE team has access to theVPC settings. VPC settings are reviewed daily via the Artishok Autopilot Platform to assure all settings continue to meet the platform requirements. Artishok also runs a yearly penetration test on the production instances which among other things report on anychanges to perimeter security.

AWS provides multiple redundant layers to the network and firewall and provides native intrusion and prevention services via GuardDuty.

Data Backup and Recovery

Artishok has multiple redundant backup strategies in place for the production instances. These include the database having a live "hot" replica in a different Availability Zone (AZ) ready to be promoted tothe primary instance if the live AZ were to fail. Encrypted database backups are taken every 24-hours via the managed RDS service. These backups are stored in a different AZ than the database. Uploaded documents are stored on AWS S3, which by default has its own disk-distribution across the set region.

Only authorized Artishok SRE team members have access to any of the production backup storage locations.

Artishok stores database backups for 30 days via the RDS managed backup system. Backup files are tested to assure their integrity in Artishok's yearly Disaster Recovery Simulation Exercise.

Disaster Recovery and Business Continuity

Artishok has a documented Disaster Recovery (DR) plan. This plan is reviewed and updated on at least a yearly basis. Updates to infrastructure and procedures in many cases requires updates to occur more frequently. The DR plan is tested on a yearly basis through an unplanned test called by the CEO and CTO with an expected Recovery Time Objective (RTO) of 24 hours Results of tests and issuesand mitigation plans are recorded post-test.
Artishok has a failover instance located in a different AZ then the primary production instance. All instancesare located in the us-west-2 region (Oregon), though use different AZs within that region.

The failover instance is constantly in hot-stand-by and can be manually promoted or the managed services by AWS will auto promote/failover. In the event of a catastrophic failure of an entire region, the RDS backups and S3 archives are being peered to their pair region in eu-central-1 (Frankfurt).

System Account Management

Artishok has implemented role-based security to limit and control access within the Artishok instances or any system that houses customer or confidential data. Employees are granted logical and physical access to these systems based on documented approvals by appropriate management personnel. All employee access is documented and approvals from either the CTOor CISO are recorded for any additions or modifications to existing access rights. The user accessis reviewed annually both via the review of the access list and audits of existing system accesscontrol list (ACL).
Permission to create or modify user access is restricted to authorized development operations personnel and the CTO.

Email and Single-Sign-On (SSO) or a magic link are required to authenticate all users to Artishok instances.
Username and password is required to access infrastructure and business systems. For all applications where MFA can be enabled, MFA is in place requiring users to have two factors to authenticate access to the system, one being a password or encryption key. Passwords have complexity requirements and have expiration settings that fit the classification of data contained within the system.

When an employee is terminated, the operations team notifies the development operations team through initiation of the off-boarding process. Off-boarding steps include revocation of all system access within one business day.

Data Transmission

Customers access the Artishok Console through a web browser. TLS 1.2 or higher is required to access thesystem. Users authenticate access through their corporate single sign-on identity provider.

Remote Access

Artishok is a cloud-native remote company. Thus, Artishok does not have its own network or systems to VPNinto.

Access to the Artishok infrastructure is limited to a select few Artishok SRE team members and the CTO. Toaccess the infrastructure, one must assume a privileged role that requires MFA or SSH to the jump host,which then will allow for SSH tunneling to the database. All Artishok infrastructure access is logged, andcustomer data can only be accessed through the database layers of the infrastructure.

Physical Media and Data Destruction

Artishok uses limited formats of electronic media, mostly laptops with hard drives. When no longer usable,hard drives, or other similar items used to process, store and/or transmit sensitive data are properlydisposed of in accordance with measures established by Artishok.

Physical media (print-outs and other physical media) are disposed of by shredding using cross-cut shredders.

Electronic media (hard-drives, printers and copier hard-drives, etc.) are disposed of by one of the following methods:

- Wiping - Artishok uses a Mobile Device Management solution to wipe the device, which securely erases the hard drive.
- Destruction – a method of destroying magnetic media. Media is physically dismantled by methods of crushing, disassembling, etc., ensuring that the media has been physically destroyed so that no data can be pulled. Artishok will send any decommissioned device to a third party for destruction.

Third-Party Due Diligence

The entity's vendor and business partner oversight program requires that all contracts with vendors or business partners clearly address (a) the size, scope, and nature of services being provided; (b) the hardware, software, and information requirements related to the provision of such services; (c) the responsibilities of each party; (d) the requirements for information security to meet Artishok's standards; (e)the ability to perform independent audits of the effectiveness of internal control processes; and (f) therequirement to obtain and review a third-party attestation report.

Artishok relies on third parties to perform a range of services and provide products. As such, Artishok performs due diligence to ensure that third parties have appropriate internal controls inplace to protect Artishok's customer data. To ensure that appropriate controls are in place atthird parties, Artishok's management reviews the following as necessary:

- SOC 1 and/or SOC 2 reports
- Internal controls
- Privacy policies

Availability

Artishok's infrastructure at AWS is designed to be redundant and resilient, utilizing AWS's availability zones feature within the eu-west-1 region for all deployed services (RDS, ElastiCache, and Elastic Kubernetes Service (EKS)). With Multi AZ enabled, data is securely copied and ready to failover in case ofan emergency. The managed services at AWS handle the fail over based on availabilitymonitoring. RDS is configured to run daily backups of the database system and also supports continuous backup and point-in-time recovery (PITR). This feature allows Artishok to recover RDSbackup data from a specific time within 5 minutes. To manage capacity, Artishok follows a two-stepprocess. The first step is a quarterly planning session where the engineering leadership team reviewstraffic levels across the stack, including firewall/DNS level in CloudFlare, bandwidth usage in Netlify for web applications, and Application Load Balancers (ALB) in AWS for the API tier. Thesecond step involves reviewing and adjusting the existing load-balancing thresholds as needed based on the data collected in the first step. Artishok uses EKS for its API tier, and based on CPU Utilization, EKS will spin up new nodes to distribute the load of requests across the API. Server-level monitoring and alerting is configured in CloudWatch and set to notify Artishok's senior engineeringleadership via email.

Confidentiality

The data classification and retention policy and relevant security and confidentiality policies describe how information is designated as confidential and ceases to be confidential. The handling, destruction, maintenance, storage, backup, and distribution and transmission of confidential information are documented in the data classification and retention policy and Artishok’s general business terms.

Confidentiality policies and processes have been implemented to limit access to logical input routines and physical input media to authorized individuals. Each type of confidential information is classified, handled, secured, retained, and disposed of. All nonpublic customer information is confidential. Data that carries a confidential classification is subject to the Company’s information security policy, which defines protection requirements, access rights, and access restrictions, as well as retention and destruction requirements. Customer, vendor, and business partner information is presumed to be confidential (as a default).

As part of Artishok’s standard process for establishing service levels and operational protocols with vendorsor business partners, Artishok will evaluate data shared between the two organizations and agreeon whatis confidential.

Artishok also requests that business partners disclose their security, data classification, and retention policies to ensure that Artishok's data is afforded the proper retention and information protection. TheCEO and CTO are responsible for maintaining and updating confidentiality, system security, and related policies.

At the time of hire or affiliation, the code of conduct and confidentiality agreements that employees are required to sign prohibit any disclosures, beyond the extent authorized, of information and other data to which the employee has been granted access. Artishok's business partners are also subject to non disclosure agreements. Customer contracts, service-level agreements, and vendor contracts arenegotiated before performance or receipt of service and formally signed off on by management.

Customers, groups of individuals, or other entities are restricted from accessing confidential information, other than their own. This is deployed by a single-tenant database architecture. For each customer account, a separate database is deployed and configured for that customer, and only that customer. There is no chance that the customer's data will cross-mingle another customer's data.

Data Retention

Retention periods, and policies for ensuring retention during the specified period and proper disposal of data at the end of the retention period, are also outlined in the Data Disposal policy. The retention period assigned to data is based on the (1) classification of the data, (2) regulatory requirements and legal statutes, and (3) the general requirements of the business. During the designated retention period, Artishokensures that backup media (whether offline or online) are stored in a protected environment for the duration of the designated document retention period, including computer backup media. When the retention period has ended, Artishok destroys theinformation securely. Electronic information and other information are disposed of securely by proven means.

Processing Integrity

Alongside input validation, change management runs through a rigorous quality assurance lifecycle confirming the assertion data integrity across the wide breadth of integrations, and the depth of each one of them across all of the provided services within. Significant changes to Artishok platform's architecture would trigger full scale regression testing of all system components to ensure the test results reported by Artishok, historical representations of control test results and other data remained accurate.

Privacy

Artishok maintains a Privacy program which includes the management of external privacy requests to meet state and international compliance and regulatory requirements. Artishok's privacy policy provides information on the type of personal information collected and shared, how that information isused, therights of data subjects and how they may exercise their rights.

Risk Assessment Process

Artishok maintains a comprehensive inventory of all information systems, which are assigned to a designated department or team based on their business value and criticality to the organization. These assets are subject to data protection, data classification, and data retention policies that outline parameters for ownership, classification, security, storage, and retention of data. Additionally, software and hardware assets are governed by the information security policy and asset management policy, which detail parameters for acquisition, development, maintenance, security, and disposal of information system assets. Every year, the information security team conducts a risk assessment to identify internal and external threats and vulnerabilities to the organization. This assessment evaluates the associated risks and vulnerabilities of information system assets and assigns scores based on likelihood and potential impact. The assessment also considers inherent and residual risks that may be present with external parties and the controls in place to address these risks. Policies and procedures are in place to assess and manage the requisition and engagement of vendors or business partners, taking into account any threats and vulnerabilities that may arise from these relationships.

Results of the risk assessment are evaluated by the CTO against criteria for risk acceptance to identify new or existing protective measures and develop or enhance information security policies and procedures.

Information and Communications Systems

Artishok has an information security policy in place to help ensure that employees are aware of their roles and responsibilities regarding security and controls. This policy includes training programs, both formal and informal, and the use of email to communicate time-sensitive information and processes related to security and system availability. These measures are in place to ensure that key personnel are promptly notified of any issues or problems.

Monitoring

System Monitoring

The SRE team employs a range of security tools to identify and detect potential threats and incidents. These tools include firewall notifications, IDS or IPS alerts, vulnerability assessment reports, and operating system event logs. The security team reviews these alerts and notifications daily. In addition, the team reviews several reports, including failed object-level access, daily IDS or IPS attacks, critical IDS or IPS alerts, failed login details, and firewall configuration changes.

Security events requiring further investigation are tracked using a ticket and monitored until resolved.

Incident Response

The Incident Response and Recovery Plan (IRP) includes tactical procedures to help triage, contain, monitor, or eradicate a security incident, including procedures to do the following:

- Respond to, recover from, and restore normal business operations in a timely manner with minimal, or no, business interruption or loss of data
- Continuously improve the cyber security risk management program to limit the likelihood andimpact of future incidents based on lessons learned from the Company's own experiences andthose of others
- Communicate with employees, stakeholders, regulators, and other constituents in a structured manner about the nature of the security incident, impact to the organization and others (if applicable), and the corrective action taken to recover

Virus Detection and Prevention

All Artishok servers, desktops, laptops, and email infrastructure must have antivirus software installed and centrally managed to ensure prompt delivery of signature updates. The antivirus software is preset to automatically update and locked to prevent user tampering or disabling. In addition, email filtering software is used to block and reject emails containing certain malicious file types, such as executable files.

Vulnerability Assessment and Penetration Testing

Artishok employs a third-party organization to conduct periodic internal and external vulnerability assessments and penetration tests against production systems to determine if thesystem can be penetrated through known vulnerabilities. Management reviews the results of the vulnerability assessments and penetrations tests and develops action plans to remediate high riskfindings.

Use of Subservice Organization and Complementary Subservice Organization Controls

Artishok uses AWS to provide cloud computing services.

The following are applicable trust services criteria that are intended to be met by controls at AWS and the types of controls expected to be implemented at AWS that are necessary to meet the applicable trust services criteria, alone or in combination with controls at Artishok.

Security Category	
Criteria	*Controls expected to be in place*
CC6.1 - The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	AWS is responsible for implementing controls for the transmission, movement, and removal of the underlying storage devices for its cloud hosting services where Artishok'ssystem resides.
CC6.2 - Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	
CC6.3 - The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	
CC6.5 - The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	
CC6.6 - The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	
CC6.7 - The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	
CC6.4 - The entity restricts physical access to facilities and protected information assets (e.g., datacenter facilities, backup media storage and other sensitive locations) to authorized personnel to meet the entity's objectives.	AWS is responsible for restricting physical access to data center facilities, backup media, and other system components including firewalls, routers, and servers where Artishok's system resides.

Availability Category	
Criteria	*Controls expected to be in place*
A1.2 - The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.	AWS is responsible for managing environmental protections within the datacenters that house network, virtualization management, and storage devices for its cloud hosting services where Artishok's system resides.

Artishok monitors the effectiveness of controls at AWS by performing the following monitoring controls:

- reviewing and reconciling output reports;
- reviewing the most recently available SOC report (type 2) on AWS' system;
- Obtaining bridge letters from AWS to obtain assurance that controls at AWS are operating as intended and no significant changes were made since AWS' most recently issued report.
- Monitoring external communications (such as customer complaints) relevant to the services provided by AWS.

Complementary user entity controls (CUECs) are identified in AWS' SOC report. Artishok reviews allapplicable CUECs and ensures that controls have been implemented to satisfy the applicable CUECs, asnecessary.

TRUST SERVICES CRITERIA NOT APPLICABLE TO Artishok

Artishok's operations, as described above, address all applicable Trust Services Criteria related to the security& availability category with the exception of the following criteria that are not applicable to Artishok'sservices:

- CC6.4 – The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives. AWS is responsible for the physical security of infrastructure housing Artishok customer data.
- A1.2 - The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives. AWS is responsible for the environmental protections of infrastructure housing Artishok customer data.

TRUST SERVICES CRITERIA AND RELATED CONTROL ACTIVITIES

The applicable trust services criteria and related control activities are included in Section IV of this report to eliminate the redundancy that would result from listing the items in this section and repeating them in Section IV. Although the applicable trust services criteria and related controls are included in Section IV, they are, nevertheless, an integral part of Artishok's description of its system.

COMPLEMENTARY USER-ENTITY CONTROLS

Artishok's services were designed with the assumption that certain controls would be implemented by user entities. These controls should be in operation at user entities to complement Artishok's controls.

The user entity controls subsequently presented should not be regarded as a comprehensive list of allcontrols that should be employed by user entities. User entities of Artishok's system shouldmaintain controls to provide reasonable assurance for:

- Notifying Artishok management immediately regarding any employee termination that would require a revocation of logical access to Artishok.
- Designating individuals for authorizing access to Artishok.
- Periodically reviewing their customer access lists to Artishok and informing Artishok of any access change requests.
- Implementing systems to protect against security and availability threats from sources outside the boundaries of the system.
- Applying logical access security controls, data encryption controls and related procedures to their network connected equipment.
- Protecting their equipment against infection by computer viruses, malicious codes and unauthorized software.
- Complying with their contractual obligations.
- Ensuring the supervision, management, and control of the use of Artishok's services by their personnel.
- Ensuring that procedures are in place for developing, maintaining, and testing their own business continuity plans.
- Ensuring data files transmitted to Artishok are protected by appropriate encryption protocols.
- Notifying Artishok to change passwords for its accounts in the event the accounts have been compromised.
- Changing passwords to its accounts on a periodic basis.
- Committing to monitoring and alerting Artishok to potential incidents.
- Ensuring all production instances of cloud infrastructure, version control, identity provider, and development tools are connected to Artishok's platform.
- Monitoring the Artishok platform for control failures and resolving identified control failures.
- Monitoring the Artishok platform for integration issues and notifying Artishok of such issues in a timely manner.

- Ensuring the completeness and accuracy of manually entered data.
- Verifying that all applicable employees and contractors have been onboarded to the Artishokplatform monitoring and identifying the appropriate rights and roles for Artishok to monitor.
- Users are responsible for determining what level of reliance to place on data generated from Artishok platform in determining the design and operating effectiveness of controls.
- Users are responsible for determining if the controls within the Artishok platform are appropriatefor meeting the applicable Trust Services Criteria and Categories.
- Users are responsible for determining if the data within the Artishok platform is adequate to supportthe design and operating effectiveness of controls.
- Users are responsible for determining how failed tests identified by the Artishok platform impact anorganization's ability to meet the applicable Trust Services Criteria.

IV. Description of Criteria, Controls, Tests and Results of Tests

Description of Criteria, Controls, Tests and Results of Tests

Relevant trust services criteria and Artishok related controls are an integral part of management's system description and are included in this section. Sensiba San Filippo LLP performed testing to determine if Artishok's controls were suitably designed and operating effectively to achieve the specified criteria for the Security, Availability, Confidentiality, Processing Integrity, andPrivacy set forth in TSP Section 100, *2017 Trust Services Criteria for Security,Availability,Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria)*, throughout the period December 1, 2021 to November 30, 2022.

Tests of the controls included inquiry of appropriate management, supervisory and staff personnel, observation of Artishok activities and operations and inspection of Artishok documents and records. The results of those tests were considered in the planning, the nature, timing, and extent of Sensiba San Filippo LLP's testing of the controls designed to achieve the relevant trust services criteria. As inquiries were performed for substantially all Artishok controls, this test was not listed individually for every control in the tables below.

Description of Artishok's Controls	Control Number	SSF Test of Controls	Test Results
CC1.0 - Control Environment			
CC1.1 - COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.			
Artishok has a formal Code of Conduct approved by management and accessible to all employees. Allemployees must accept the Codeof Conduct upon hire.	CC1.1.1	Inspected the entity's Code of Conduct to determine that the entity had a formal Code of Conduct approved by management and accessible to all employees. All employees must accept the Code of Conduct upon hire. Inspected the policy acknowledgements for a sample of new hires to determine that the entity had a formal Code of Conduct approved by management and accessible to all employees. All employees must accept the Code of Conduct upon hire.	No exceptions noted

Description of Artishok's Controls	Control Number	SSF Test of Controls	Test Results
CC1.1 - COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.			
Artishok's new hires are required topass a background check as acondition of their employment.	CC1.1.2	Inspected the completed background checks for a sample of new hires to determine that the entity required new hires to pass a background check as a condition of their employment. Inspected the Acceptable Use Policy to determine that the entity required new hires to pass a background check as a condition of their employment.	No exceptions noted
Artishok has policies and proceduresin place to establish acceptable useof information assets approved bymanagement, posted on thecompany wiki, and accessible to allemployees. All employees mustaccept the Acceptable Use Policyupon hire.	CC1.1.3	Inspected the entity's Acceptable Use Policy to determine that the entity had policies and procedures in place to establish acceptable use of information assets approved by management, posted on the company wiki, and accessible to all employees. All employees must accept the Acceptable Use Policy upon hire. Inspected the policy acknowledgements for a sample of new hires to determine that the entity had policies and procedures in place to establish acceptable use of information assets approved by management, posted on the company wiki, and accessible to all employees. All employees must accept the Acceptable Use Policy upon hire.	No exceptions noted
Artishok requires its contractors toread and accept the Code of Conduct, read and accept the Acceptable Use Policy, and pass a background check.	CC1.1.4	Inspected the employee activity records for a sample of current contractors to determine that the entity required its contractors to read and accept the Code of Conduct, read and accept the Acceptable Use Policy, and pass a background check.	No exceptions noted

Description of Artishok's Controls	Control Number	SSF Test of Controls	Test Results
CC1.2 - COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.			
A majority of the members of the Board of Directors are independent of management.	CC1.2.1	Inspected the board of directors listing and cross-refenced with executive management team to determine that a majority of the board of directors is independent of management.	No exceptions noted
The company's board of directors meets at least annually and maintains formal meeting minutes. The board includes directors that are independent of the company.	CC1.2.2	Inspected the most recent board meeting minutes to determine that the board meets at least annually and maintains for meeting minutes. Inspected the attendance record for the board of directors, to determine that the directors are independent of the company.	No exceptions noted
Management has established defined roles and responsibilities to oversee implementation of the information security policy across the organization.	CC1.2.3	Inspected the organizational chart as well as roles to determine that management has established defined roles and responsibilities to oversee implementation of the information security policy across the organization.	No exceptions noted
CC1.3 - COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.			
Artishok reviews its organizational structure, reporting lines, authorities, and responsibilities in terms of information security on an annual basis.	CC1.3.1	Inspected the organizational chart to determine that the defines roles, authority, responsibilities and is reviewed on an annual basis.	No exceptions noted

Description of Artishok's Controls	Control Number	SSF Test of Controls	Test Results
CC1.3 - COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.			
Artishok has an assigned security team that is responsible for the design, implementation, management, and review of the organization's security policies, standards, baselines, procedures, and guidelines.	CC1.3.2	Inspected the security committee roster to determine that the company has assigned a security team that is responsible for the overall information security program. Inspected the information security policy to determine that the company has documented procedures for the security committee to be responsible for the design, implementation, management, and review of the organization's security policies, standards, baselines, procedures, and guidelines.	No exceptions noted
CC1.4 - COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.			
Artishok's new hires are required topass a background check as acondition of their employment.	CC1.4.1	Inspected the completed background checks for a sample of new hires to determine that the entity required new hires to pass a background check as a condition of their employment. Inspected the Acceptable Use Policy to determine that the entity required new hires to pass a background check as a condition of their employment.	No exceptions noted
All Artishok positions have a detailed job description that lists qualifications, such as requisite skills and experience, which candidates must meet in order to be hired by Artishok.	CC1.4.2	Inspected a sample of job descriptions to determine that positions have detailed job descriptions that list qualifications and requirements for candidates to possess on order to be hired by the company.	No exceptions noted

Description of Artishok's Controls	Control Number	SSF Test of Controls	Test Results
CC1.5 - COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.			
Artishok has established training programs for privacy and information security to help employees understand their obligations and responsibilities to comply with Artishok's security policies and procedures, including the identification and reporting of incidents. All full-time employees are required to complete the training upon hire and annually thereafter.	CC1.5.1	Inspected the completed security training reports for a sample of current employees to determine that the entity had established training programs for privacy and information security to help employees understand their obligations and responsibilities to comply with the entity's security policies and procedures, including the identification and reporting of incidents. All full-time employees are required to complete the training upon hire and annually thereafter.	No exceptions noted
Artishok has policies and proceduresin place to establish acceptable useof information assets approved bymanagement, posted on thecompany wiki, and accessible to allemployees. All employees mustaccept the Acceptable Use Policyupon hire.	CC1.5.2	Inspected the entity's Acceptable Use Policy to determine that the entity had policies and procedures in place to establish acceptable use of information assets approved by management, posted on the company wiki, and accessible to all employees. All employees must accept the Acceptable Use Policy upon hire. Inspected the policy acknowledgements for a sample of new hires to determine that the entity had policies and procedures in place to establish acceptable use of information assets approved by management, posted on the company wiki, and accessible to all employees. All employees must accept the Acceptable Use Policy upon hire.	No exceptions noted

Description of Artishok's Controls	Control Number	SSF Test of Controls	Test Results
CC2.0 - Communication and Information			
CC2.1 - COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.			
Artishok maintains an accurate architecture diagram to document system boundaries to support the functioning of internal control.	CC2.1.1	Inspected the documented architecture diagram to determine that the company maintains an accurate architecture diagram to document system boundaries to support the functioning of internal control.	No exceptions noted
Artishok conducts continuous monitoring of security controls using Artishok and addresses issues ina timely manner.	CC2.1.2	Inspected the continuous monitoring of security controls to determine that the company uses the platform to monitor internal controls and remediate issues timely.	No exceptions noted
Artishok identifies, inventories and classifies virtualized assets.	CC2.1.3	Inspected the documented asset inventory to determine that the company identifies, inventories, and classifies virtual assets.	No exceptions noted
Artishok has a defined Information Security Policy that covers policies and procedures to support the functioning of internalcontrol.	CC2.1.4	Inspected the information security policy to determine that the company has defined and documented procedures that cover the evaluation and functioning of internal controls.	No exceptions noted
Artishok performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings.	CC2.1.5	Inspected the annual internal control review to determine that the company performs control self-assessment at least annually to gain assurance that controls are in place and operating effectively as well as remediating any finding.	No exceptions noted

Description of Artishok's Controls	Control Number	SSF Test of Controls	Test Results
CC2.2 - COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.			
Artishok provides a process to employees for reporting security, confidentiality, integrity, and availability features, incidents, and concerns, and other complaints to company management.	CC2.2.1	Inspected the implemented communication process to determine that employees have a way to report security, confidentiality, integrity, and availability features, incidents, and concerns, and other complaints to company management.	No exceptions noted
The security team communicates important information security events to company management in a timely manner.	CC2.2.2	Inspected a sample of communications to determine that the security team communicates important information security events to management in timely manner.	No exceptions noted
Artishok Management has approved security policies, and all employees accept these procedures when hired. Management also ensures that security policies are accessible to all employees and contractors.	CC2.2.3		No exceptions noted

Description of Artishok's Controls	Control Number	SSF Test of Controls	Test Results
CC2.2 - COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.			
Artishok has established a Data Protection Policy and requires all employees to accept it upon hire. Management monitors employees' acceptance of the policy.	CC2.2.4	Inspected the entity's Data Protection Policy to determine that the entity established a Data Protection Policy and requires all employees to accept it upon hire. Management monitors employees' acceptance of the policy. Inspected the policy acknowledgements for a sample of new hires to determine that the entity established a Data Protection Policy and requires all employees to accept it upon hire. Management monitors employees' acceptance of the policy.	No exceptions noted
CC2.3 - COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.			
Artishok's security commitments are communicated to external users, as appropriate.	CC2.3.1	Inspected the public facing website to determine that the company clearly communicates security commitments to external users.	No exceptions noted
Artishok communicates system changes to customers that may affect security, availability, processing integrity, or confidentiality.	CC2.3.2	Inspected a sample of communications to customers to determine that the company communicates system changes to customers that may affect security, availability, processing integrity, or confidentiality.	No exceptions noted
Artishok maintains a Terms of Service that is available to all external users and internal employees, and the terms detail the company's security and availability commitments regarding the systems. Client Agreements or Master Service Agreements are in place for whenthe Terms of Service may notapply.	CC2.3.3	Inspected the public facing website to determine the company had made available the terms of service which details the company's security and availability commitments regarding the systems. Inspected the master service agreement (MSA) template to determine that the company has in place an MSA in the event the terms of service does not apply.	No exceptions noted

Description of Artishok's Controls	Control Number	SSF Test of Controls	Test Results
CC2.3 - COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.			
Artishok maintains a Privacy Policy that is available to all external users and internal employees, and it details the company's confidentiality andprivacy commitments.	CC2.3.4	Inspected the public facing privacy policy to determine that it is made available to external users as well as details the company's confidentiality and privacy commitments.	No exceptions noted
Artishok has implemented a bug bounty program for external users to report security issues to appropriate personnel.	CC2.3.5	Inspected the implemented bug bounty program to determine that the company has implemented a bug bounty program for external users to report security issues to appropriate personnel. Inspected response time settings to determine that the company responds to reported bugs in a timely manner.	No exceptions noted
Artishok provides a process to external users for reporting security, confidentiality, integrity, and availability failures, incidents, concerns, and other complaints.	CC2.3.6	Inspected the public facing website to determine that the company has provided a process to external users for reporting security, confidentiality, integrity, and availability failures, incidents, concerns, and other complaints.	No exceptions noted
CC3.0 - Risk Assessment			
CC3.1 - COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.			
Artishok conducts a Risk Assessmentat least annually.	CC3.1.1	Inspected the annual risk assessment to determine that the company performed the assessment to identify relevant risk to the organization.	No exceptions noted

Description of Artishok's Controls	Control Number	SSF Test of Controls	Test Results
CC3.1 - COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.			
Artishok has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	CC3.1.2	Inspected the risk management policy to determine that the company has procedures documented that outline a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances. Inspected the annual risk assessment to determine that the company performed the assessment to identify relevant risk to the organization.	No exceptions noted
CC3.2 - COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.			
Artishok conducts a Risk Assessmentat least annually.	CC3.2.1	Inspected the annual risk assessment to determine that the company performed the assessment to identify relevant risk to the organization.	No exceptions noted
Artishok's Management prepares aremediation plan to formally manage the resolution of findings identified in risk assessment activities.	CC3.2.2	Inspected the annual risk assessment and remediation plan to determine the company prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	No exceptions noted
Artishok maintains a directory of itskey vendors, including its agreements that specify terms, conditions and responsibilities.	CC3.2.3	Inspected the full listing of vendors to determine that the company maintains a directory of its key vendors, including its agreements that specify terms, conditions and responsibilities.	No exceptions noted

Description of Artishok's Controls	Control Number	SSF Test of Controls	Test Results
CC3.2 - COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.			
Artishok has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	CC3.2.4	Inspected the risk management policy to determine that the company has procedures documented that outline a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances. Inspected the annual risk assessment to determine that the company performed the assessment to identify relevant risk to the organization.	No exceptions noted
CC3.3 - COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.			
Artishok conducts a Risk Assessmentat least annually.	CC3.3.1	Inspected the annual risk assessment to determine that the company performed the assessment to identify relevant risk to the organization.	No exceptions noted
Artishok's Management prepares aremediation plan to formally manage the resolution of findings identified in risk assessment activities.	CC3.3.2	Inspected the annual risk assessment and remediation plan to determine the company prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	No exceptions noted
CC3.4 - COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.			
Artishok conducts a Risk Assessmentat least annually.	CC3.4.1	Inspected the annual risk assessment to determine that the company performed the assessment to identify relevant risk to the organization.	No exceptions noted

Description of Artishok's Controls	Control Number	SSF Test of Controls	Test Results
CC3.4 - COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.			
Artishok engages with third-party to conduct vulnerability scans of the production environment at least monthly. Results are reviewed by management and high priority findings are tracked to resolution.	CC3.4.2	For a sample of months inspected the vulnerability scan reports to determine that the company has a third party perform vulnerability scans monthly to identify and remediate security issues.	No exceptions noted
Artishok engages with third-party to conduct penetration tests of the production environment at least annually. Results are reviewed by management and high priority findings are tracked to resolution.	CC3.4.3	Inspected the annual penetration test to determine that the company engages a third party to identify security issues and exploits of the production environment.	No exceptions noted
Artishok maintains a directory of itskey vendors, including its agreements that specify terms, conditions and responsibilities.	CC3.4.4	Inspected the full listing of vendors to determine that the company maintains a directory of its key vendors, including its agreements that specify terms, conditions and responsibilities.	No exceptions noted
CC4.0 - Monitoring Activities			
CC4.1 - COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.			
Artishok performs quarterly access control reviews.	CC4.1.1	For a sample of quarters inspected the documented access reviews to determine that the company performs user reviews quarterly.	No exceptions noted
Artishok engages with third-party toconduct penetration tests of the production environment at least annually. Results are reviewed by management and high priority findings are tracked to resolution.	CC4.1.2	Inspected the annual penetration test to determine that the company engages a third party to identify security issues and exploits of the production environment.	No exceptions noted

Description of Artishok's Controls	Control Number	SSF Test of Controls	Test Results
CC4.1 - COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.			
Artishok engages with third-party to conduct vulnerability scans of the production environment at least monthly. Results are reviewed by management and high priority findings are tracked to resolution.	CC4.1.3	For a sample of months inspected the vulnerability scan reports to determine that the company has a third party perform vulnerability scans monthly to identify and remediate security issues.	No exceptions noted
CC4.2 - COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.			
Artishok has identified an incident response team that quantifies and monitors incidents involving security, availability, processing integrity, and confidentiality at the company.	CC4.2.1	Inspected the incident response policy to determine that the company has identified an incident response team that quantifies and monitors incidents involving security, availability, processing integrity, and confidentiality at the company.	No exceptions noted
Artishok has an established Incident Response Policy that outlines management responsibilities and procedures toensure a quick,effective, and orderly response to information security incidents and annual testing.	CC4.2.2	Inspected the incident response policy to determine that the company has documented procedures that outline management responsibilities to properly manage, track, and remediate security incidents.	No exceptions noted
Artishok engages with third-party to conduct penetration tests of the production environment at least annually. Results are reviewed by management and high priority findings are tracked to resolution.	CC4.2.3	Inspected the annual penetration test to determine that the company engages a third party to identify security issues and exploits of the production environment.	No exceptions noted

Description of Artishok's Controls	Control Number	SSF Test of Controls	Test Results
CC4.2 - COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.			
Artishok engages with third-party to conduct vulnerability scans of the production environment at least monthly. Results are reviewed by management and high priority findings are tracked to resolution.	CC4.2.4	For a sample of months inspected the vulnerability scan reports to determine that the company has a third party perform vulnerability scans monthly to identify and remediate security issues.	No exceptions noted
Artishok has an assigned security team that is responsible for the design, implementation, management, and review of the organization's security policies, standards, baselines, procedures, and guidelines.	CC4.2.5	Inspected the security committee roster to determine that the company has assigned a security team that is responsible for the overall information security program. Inspected the information security policy to determine that the company has documented procedures for the security committee to be responsible for the design, implementation, management, and review of the organization's security policies, standards, baselines, procedures, and guidelines.	No exceptions noted
CC5.0 - Control Activities			
CC5.1 - COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.			
Artishok conducts a Risk Assessment at least annually.	CC5.1.1	Inspected the annual risk assessment to determine that the company performed the assessment to identify relevant risk to the organization.	No exceptions noted
Artishok's Management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	CC5.1.2	Inspected the annual risk assessment and remediation plan to determine the company prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	No exceptions noted

Description of Artishok's Controls	Control Number	SSF Test of Controls	Test Results
CC5.1 - COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.			
Artishok has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	CC5.1.3	Inspected the risk management policy to determine that the company has procedures documented that outline a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances. Inspected the annual risk assessment to determine that the company performed the assessment to identify relevant risk to the organization.	No exceptions noted
Artishok engages with third-party to conduct penetration tests of the production environment at least annually. Results are reviewed by management and high priority findings are tracked to resolution.	CC5.1.4	Inspected the annual penetration test to determine that the company engages a third party to identify security issues and exploits of the production environment.	No exceptions noted
Artishok engages with third-party to conduct vulnerability scans of the production environment at least monthly. Results are reviewed by management and high priority findings are tracked to resolution.	CC5.1.5	For a sample of months inspected the vulnerability scan reports to determine that the company has a third party perform vulnerability scans monthly to identify and remediate security issues.	No exceptions noted
CC5.2 - COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.			
Artishok has an established policy andprocedures that governs the use ofcryptographic controls.	CC5.2.1	Inspected the encryption & information security policies to determine that the company has formally documented procedures which outline the implementation and use of cryptographic controls.	No exceptions noted

Description of Artishok's Controls	Control Number	SSF Test of Controls	Test Results
CC5.2 - COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.			
Artishok authorizes access to information resources, including data and the systems that store or process customer data, based on the principle of least privilege.	CC5.2.2	Inspected user groups and federated roles to determine that company authorizes access to information resources, including data and the systems that store or process customer data, based on the principle of least privilege.	No exceptions noted
Artishok engages with third-party to conduct penetration tests of the production environment at least annually. Results are reviewed by management and high priority findings are tracked to resolution.	CC5.2.3	Inspected the annual penetration test to determine that the company engages a third party to identify security issues and exploits of the production environment.	No exceptions noted
Artishok engages with third-party to conduct vulnerability scans of the production environment at least monthly. Results are reviewed by management and high priority findings are tracked to resolution.	CC5.2.4	For a sample of months inspected the vulnerability scan reports to determine that the company has a third party perform vulnerability scans monthly to identify and remediate security issues.	No exceptions noted
CC5.3 - COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.			
Management reviews security policies on an annual basis.	CC5.3.1	Inspected the security policies and evidence of management review to determine that management formally reviews policies and procedures annually.	No exceptions noted
Artishok has a defined Information Security Policy that covers policies and procedures to support the functioning of internal control.	CC5.3.2	Inspected the information security policy to determine that the company has defined and documented procedures that cover the evaluation and functioning of internal controls.	No exceptions noted

Description of Artishok's Controls	Control Number	SSF Test of Controls	Test Results
CC5.3 - COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.			
Artishok has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	CC5.3.3	Inspected the risk management policy to determine that the company has procedures documented that outline a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances. Inspected the annual risk assessment to determine that the company performed the assessment to identify relevant risk to the organization.	No exceptions noted
CC6.0 - Logical and Physical Access Controls			
CC6.1 - The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.			
Artishok requires two factor authentication to access sensitive systems and applications in the form of user ID, password, OTP and/or certificate.	CC6.1.1	Inspected multi factor authentication (MFA) configurations to determine that the company requires elevated access in order to access the sensitive systems and the production environment.	No exceptions noted
Artishok ensures that a password manager is installedon all company-issued laptops.	CC6.1.2	In lieu of a sample inspected the full population and export of user's laptops to determine that all company issued laptops are required to have a password manager installed.	No exceptions noted
Artishok has an established key management process in place to support the organization's use of cryptographic techniques.	CC6.1.3	Inspected the implemented KMS policy to determine that the company has restricted access to appropriate personnel based on role. Inspected the rotating keys configuration to determine that the company properly manages encryption keys and rotates at defined intervals.	No exceptions noted

Description of Artishok's Controls	Control Number	SSF Test of Controls	Test Results
CC6.1 - The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.			
Access to corporate network, production machines, network devices, and support tools requires a unique ID.	CC6.1.4	Inspected user accounts to determine that access to systems and resources, require a unique user ID.	No exceptions noted
Role-based security is in place for internal and external users, including super admin users.	CC6.1.5	Inspected user groups and federated roles to determine that role-based security is implemented for accessing systems and resources.	No exceptions noted
Users can only access the production system remotely through the use of encrypted communication systems.	CC6.1.6	Inspected virtual private network (VPN) configurations to determine encrypted connections are implemented for users to access the production systems. Inspected roles and groups configured for the virtual private network (VPN) to determine that only authorized users have access to the use the VPN tunnel.	No exceptions noted
CC6.2 - Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.			
New hires are granted access to systems and resources after a formal approval by appropriate personnel.	CC6.2.1	Inspected the access authorization tickets for a sample of new hires to determine the entity granted access to systems and resources after a formal approval by appropriate personnel.	No exceptions noted
Terminated users have their access to systems and resources terminated after a formal approval by appropriate personnel.	CC6.2.2	Inspected the access revocation tickets for a sample of terminated employees to determine that terminated users had their access to systems and resources terminated after a formal approval by appropriate personnel.	No exceptions noted

Description of Artishok's Controls	Control Number	SSF Test of Controls	Test Results
CC6.2 - Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.			
External users must accept the Terms of Service prior to their account being created.	CC6.2.3	Inspected the user acceptance from the application to determine that the external users must accept the Terms of Service prior to their account being created.	No exceptions noted
CC6.3 - The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.			
Artishok performs quarterly access control reviews.	CC6.3.1	For a sample of quarters inspected the documented access reviews to determine that the company performs user reviews quarterly.	No exceptions noted
Role-based security is in place for internal and external users, including super admin users.	CC6.3.2	Inspected user groups and federated roles to determine that role-based security is implemented for accessing systems and resources.	No exceptions noted
New hires are granted access to systems and resources after a formal approval by appropriate personnel.	CC6.3.3	Inspected the access authorization tickets for a sample of new hires to determine the entity granted access to systems and resources after a formal approval by appropriate personnel.	No exceptions noted
Terminated users have their access to systems and resources terminated after a formal approval by appropriate personnel.	CC6.3.4	Inspected the access revocation tickets for a sample of terminated employees to determine that terminated users had their access to systems and resources terminated after a formal approval by appropriate personnel.	No exceptions noted

Description of Artishok's Controls	Control Number	SSF Test of Controls	Test Results
CC6.4 - The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.			
Artishok has security policies that have been approved by management and detail how physical security for the company's headquarters is maintained. These policies are accessible to all employees and contractors.	CC6.4.1	Inspected the physical security policy to determine that the company has formally documented procedures which outline physical security control for the company's headquarters. Inspected the shared location for security policies to determine that policies are readily accessible to personnel.	No exceptions noted
The company relies on Cloud Service Provider physical and environmental controls, as defined and tested within the Cloud Service Provider SOC 2 reports.	CC6.4.2	Inspected the cloud service providers SOC 2 report and evidence of management review to determine that management reviews subservice organizations SOC 2 reports to ensure internal controls are operating effectively.	The control is carved out and the responsibility of the subservice organization.
CC6.5 - The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.			
Artishok has formal policies and procedures in place to guide personnel in the disposal of hardware containing sensitive data.	CC6.5.1	Inspected the data deletion policy to determine that the company has formally documented procedures that outline for the organization to securely dispose of hardware containing sensitive data.	No exceptions noted
CC6.6 - The entity implements logical access security measures to protect against threats from sources outside its system boundaries.			
An intrusion detection system (IDS) is in place to detect potential intrusions, alert personnel when a potential intrusion is detected	CC6.6.1	Inspected the intrusion detection system (IDS) configurations and a sample of alerts to determine that the company has implemented an IDS and alerts personnel to follow-up on suspicious activity.	No exceptions noted

Description of Artishok's Controls	Control Number	SSF Test of Controls	Test Results
CC6.6 - The entity implements logical access security measures to protect against threats from sources outside its system boundaries.			
Artishok ensures that all connections to its web application from its users are encrypted.	CC6.6.2	Inspected the TLS settings on the application to determine that appropriate encryption standards are used for data-in-transit.	No exceptions noted
Users can only access the production system remotely through the use of encrypted communication systems.	CC6.6.3	Inspected virtual private network (VPN) configurations to determine encrypted connections are implemented for users to access the production systems. Inspected roles and groups configured for the virtual private network (VPN) to determine that only authorized users have access to the use the VPN tunnel.	No exceptions noted
WAF in place to protect Artishok'sapplication from outside threats.	CC6.6.4	Inspected the web application firewall (WAF) configurations to determine that a WAF has been implemented to protect the application from threats at the application layer.	No exceptions noted
Artishok uses configurations that ensure only approved networking ports and protocols are implemented, including firewalls.	CC6.6.5	Inspected firewall rules to determine that only appropriate ports and protocols are used to regulate ingress traffic.	No exceptions noted
Read/Write access to cloud data storage is configured to restrict public access.	CC6.6.6	Inspected cloud data storage configurations to determine that read/write access to cloud data storage is configured to restrict public access.	No exceptions noted
Artishok ensures that all company -issued computers use a screensaver lock with a timeout of no more than 15 minutes.	CC6.6.7	In lieu of a sample inspected the full population and export of user's laptops to determine that all company issued laptops are required to have screensaver lockout of no more than 15 minutes.	No exceptions noted

Description of Artishok's Controls	Control Number	SSF Test of Controls	Test Results
CC6.7 - The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.			
Artishok stores customer data in databases that is encrypted at rest.	CC6.7.1	Inspected encryption configurations for databases and storage buckets to determine that sensitive data is encrypted at rest.	No exceptions noted
Artishok ensures that company-issued laptops have encrypted hard-disks.	CC6.7.2	In lieu of a sample inspected the full population and export of user's laptops to determine that all company issued laptops are required to have local drive encryption.	No exceptions noted
Artishok ensures that all connections to its web application from its users are encrypted.	CC6.7.3	Inspected the TLS settings on the application to determine that appropriate encryption standards are used for data-in-transit.	No exceptions noted
Artishok uses encryption to protect user authentication and admin sessions of the internal admin tool transmitted over the Internet.	CC6.7.4	Inspected encryption configurations for the infrastructure to determine that appropriate encryption standards are used to protect user authentication and admin sessions of the internal admin tool transmitted over the internet.	No exceptions noted
Artishok uses DLP (Data Loss Prevention) software to prevent unencrypted sensitive information from being transmitted over email	CC6.7.5	Inspected the data loss prevention (DLP) settings to determine that the company has implemented software to monitor and prevent unencrypted information from being transmitted over email.	No exceptions noted
CC6.8 - The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.			
Artishok requires antivirus software to be installed on workstations to protect the network against malware.	CC6.8.1	In lieu of a sample inspected the full population and export of user's laptops to determine that all company issued laptops are required to have antivirus software installed and running.	No exceptions noted

Description of Artishok's Controls	Control Number	SSF Test of Controls	Test Results
CC6.8 - The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.			
Artishok has infrastructurelogging configured to monitor webtraffic and suspicious activity. When anomalous traffic activity is identified, alerts are automatically created, sent to appropriate personnel and resolved, as necessary.	CC6.8.2	Inspected the entity's infrastructure logging configurations to determine that the entity had infrastructure logging configured to monitor web traffic and suspicious activity. When anomalous traffic activity is identified, alerts are automatically created, sent to appropriate personnel and resolved, as necessary.	No exceptions noted
Artishok ensures that virtual machine OS patches are applied monthly.	CC6.8.3	For a sample of months inspected the resolved JIRA tickets to determine that the entity ensured that virtual machine OS patched were applied monthly.	No exceptions noted
Artishok 's workstations operating system (OS) securitypatches are applied automatically.	CC6.8.4	In lieu of a sample inspected the full population of employee computers to determine that all workstations operating system (OS) security patches were applied automatically.	No exceptions noted
An intrusion detection system (IDS) is in place to detect potential intrusions, alert personnel when a potential intrusion is detected	CC6.8.5	Inspected the intrusion detection system (IDS) configurations and a sample of alerts to determine that the company has implemented an IDS and alerts personnel to follow-up on suspicious activity.	No exceptions noted
Artishok ensures that file integrity monitoring (FIM) software is in place to detect whether operating system and application software files have been tampered with.	CC6.8.6	Inspected configurations for file integrity monitoring (FIM) to determine the companies has software in place that detects suspicious system and application changes.	No exceptions noted

Description of Artishok's Controls	Control Number	SSF Test of Controls	Test Results
CC7.0 - System Operations			
CC7.1 - To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.			
Artishok engages with third-party to conduct penetration tests of the production environment at least annually. Results are reviewed by management and high priority findings are tracked to resolution.	CC7.1.1	Inspected the annual penetration test to determine that the company engages a third party to identify security issues and exploits of the production environment.	No exceptions noted
Artishok engages with third-party to conduct vulnerability scans of the production environment at least monthly. Results are reviewed by management and high priority findings are tracked to resolution.	CC7.1.2	For a sample of months inspected the vulnerability scan reports to determine that the company has a third party perform vulnerability scans monthly to identify and remediate security issues.	No exceptions noted
An intrusion detection system (IDS) is in place to detect potential intrusions, alert personnel when a potential intrusion is detected	CC7.1.3	Inspected the intrusion detection system (IDS) configurations and a sample of alerts to determine that the company has implemented an IDS and alerts personnel to follow-up on suspicious activity.	No exceptions noted
When Artishok's application code changes, code reviews and tests are performed by someone other than the person who made the code change.	CC7.1.4	Inspected the change tickets for a sample of application code changes to determine that when the entity's application code changes, code reviews and tests were performed by someone other than the person who made the code change. Inspected the branch protection rule to determine that the version control tool is configured to restrict commits to the master branch unless reviewed and approved by someone else.	No exceptions noted

Description of Artishok's Controls	Control Number	SSF Test of Controls	Test Results
CC7.2 - The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.			
Artishok uses logging software that sends alerts to appropriate personnel. Corrective actions are performed, as necessary, in a timely manner.	CC7.2.1	Inspected configurations for logging and IDS to determine the company has enabled logging that sends alerts to appropriate personnel, as well as to remediate issues.	No exceptions noted
An intrusion detection system (IDS) is in place to detect potential intrusions, alert personnel when a potential intrusion is detected	CC7.2.2	Inspected the intrusion detection system (IDS) configurations and a sample of alerts to determine that the company has implemented an IDS and alerts personnel to follow-up on suspicious activity.	No exceptions noted
Artishok engages with third-party to conduct penetration tests of the production environment at least annually. Results are reviewed by management and high priority findings are tracked to resolution.	CC7.2.3	Inspected the annual penetration test to determine that the company engages a third party to identify security issues and exploits of the production environment.	No exceptions noted
Artishok engages with third-party to conduct vulnerability scans of the production environment at least monthly. Results are reviewed by management and high priority findings are tracked to resolution.	CC7.2.4	For a sample of months inspected the vulnerability scan reports to determine that the company has a third party perform vulnerability scans monthly to identify and remediate security issues.	No exceptions noted
Artishok uses a system thatcollects and stores server logs in a central location. The system can be queried in an ad hoc fashion by authorized users.	CC7.2.5	Inspected the entity's log management dashboard to determine that the entity used a system that collects and stores server logs in a central location. The system can be queried in an ad hoc fashion by authorized users.	No exceptions noted

Description of Artishok's Controls	Control Number	SSF Test of Controls	Test Results
CC7.3 - The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.			
Artishok has identified an incident response team that quantifies and monitors incidents involving security, availability, processing integrity, and confidentiality at the company.	CC7.3.1	Inspected the incident response policy to determine that the company has identified an incident response team that quantifies and monitors incidents involving security, availability, processing integrity, and confidentiality at the company.	No exceptions noted
Artishok tracks and prioritizes security deficiencies through internal tools according to their severity by an independent technical resource.	CC7.3.2	For a sample of security incidents inspected documented ticket to determine that the company tracks and prioritizes security deficiencies through internal tools according to their severity by an independent technical resource.	No exceptions noted
Artishok has implemented an Incident Response Policy that includes creating, prioritizing, assigning, and tracking follow-upsto completion.	CC7.3.3	Inspected the incident response policy to determine that the company has documented procedures which outline for personnel to properly manage, track, and remediate security issues.	No exceptions noted
The security team communicates important information security events to company management in a timely manner.	CC7.3.4	Inspected a sample of communications to determine that the security team communicates important information security events to management in timely manner.	No exceptions noted
CC7.4 - The entity responds to identified security incidents by executing a defined incident-response program to understand, contain, remediate, and communicate security incidents, as appropriate.			
Artishok has identified an incident response team that quantifies and monitors incidents involving security, availability, processing integrity, and confidentiality at the company.	CC7.4.1	Inspected the incident response policy to determine that the company has identified an incident response team that quantifies and monitors incidents involving security, availability, processing integrity, and confidentiality at the company.	No exceptions noted

Description of Artishok's Controls	Control Number	SSF Test of Controls	Test Results
CC7.4 - The entity responds to identified security incidents by executing a defined incident-response program to understand, contain, remediate, and communicate security incidents, as appropriate.			
Artishok tracks and prioritizes securitydeficiencies through internal toolsaccording to their severity by anindependent technical resource.	CC7.4.2	For a sample of security incidents inspected documented ticket to determine that the company tracks and prioritizes security deficiencies through internal tools according to their severity by an independent technical resource.	No exceptions noted
Artishok has implemented an Incident Response Policy that includes creating, prioritizing, assigning, and tracking follow-upsto completion.	CC7.4.3	Inspected the incident response policy to determine that the company has documented procedures which outline for personnel to properly manage, track, and remediate security issues.	No exceptions noted
The security team communicates important information security events to company management in a timely manner.	CC7.4.4	Inspected a sample of communications to determine that the security team communicates important information security events to management in timely manner.	No exceptions noted
CC7.5 - The entity identifies, develops, and implements activities to recover from identified security incidents.			
Artishok has implemented an Incident Response Policy that includes creating, prioritizing, assigning, and tracking follow-upsto completion.	CC7.5.1	Inspected the incident response policy to determine that the company has documented procedures which outline for personnel to properly manage, track, and remediate security issues.	No exceptions noted
Artishok has identified an incident response team that quantifies and monitors incidents involving security, availability, processing integrity, and confidentiality at the company.	CC7.5.2	Inspected the incident response policy to determine that the company has identified an incident response team that quantifies and monitors incidents involving security, availability, processing integrity, and confidentiality at the company.	No exceptions noted
Artishok tracks and prioritizes security deficiencies through internal tools according to theirseverity by an independent technical resource.	CC7.5.3	For a sample of security incidents inspected documented ticket to determine that the company tracks and prioritizes security deficiencies through internal tools according to their severity by an independent technical resource.	No exceptions noted

Description of Artishok's Controls	Control Number	SSF Test of Controls	Test Results
CC7.5 - The entity identifies, develops, and implements activities to recover from identified security incidents.			
Artishok ensures that incident response plan testing is performed on an annual basis.	CC7.5.4	Inspected the annual incident response tabletop exercise to determine that the company formally test their incident response process to ensure procedures are up to date and accurate.	No exceptions noted
Artishok performs backups daily and retains them in accordance with a predefined schedule in the Backup Policy.	CC7.5.5	Inspected backup configurations to determine that daily backup are configured. Inspected the backup policy to determine that procedures are in place to perform daily backups and retain accordingly.	No exceptions noted
CC8.0 - Change Management			
CC8.1 - The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.			
Only authorized Artishok personnel can push or make changes to production code.	CC8.1.1	Inspected the list of authorized personnel with permissions to push or make changes to production code to determine that only authorized personnel can push or make changes to production code.	No exceptions noted
Artishok has developed policies and procedures governing the system development life cycle, including documented policies fortracking,testing, approving, and validating changes.	CC8.1.2	Inspected the system development life cycle (SDLC) policy to determine that the company has formally documented procedures which outline implementation of an effective change management process.	No exceptions noted
Artishok uses a version control system to manage source code, documentation, release labeling, and other change management tasks. Access to the system must be approved by a system admin.	CC8.1.3	Inspected the entity's version control tool to determine that the entity used a version control system to manage source code, documentation, release labeling, and other change management tasks. Access to the system must be approved by a system admin.	No exceptions noted

Description of Artishok's Controls	Control Number	SSF Test of Controls	Test Results
CC8.1 - The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.			
Separate environments are used for testing and production for Artishok 's application.	CC8.1.4	Inspected the list of AWS change control environments to determine that separate environments were used for testing and production for the entity's application.	No exceptions noted
Artishok ensures that releases are approved by appropriate personnel prior to production release.	CC8.1.5	Inspected the change tickets for a sample of application code changes to determine that the entity ensured that releases were approved by appropriate members of management prior to production release.	No exceptions noted
Artishok ensures that code changes are tested prior to implementation to ensure qualityand security.	CC8.1.6	Inspected the change tickets for a sample of application code changes to determine that the entity ensured that code changes were tested prior to implementation to ensure quality and security.	No exceptions noted
CC9.0 - Risk Mitigation			
CC9.1 - The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.			
Artishok performs backups daily and retains them in accordance with a predefined schedule in theBackup Policy.	CC9.1.1	Inspected backup configurations to determine that daily backup are configured. Inspected the backup policy to determine that procedures are in place to perform daily backups and retain accordingly.	No exceptions noted
Artishok has an established Disaster Recovery Plan that outlines roles and responsibilities and detailed procedures forrecovery of systems.	CC9.1.2	Inspected the disaster recovery policy to determine that the company has formally documented procedures that outline roles and responsibilities and detailed procedures for recovery of systems.	No exceptions noted

Description of Artishok's Controls	Control Number	SSF Test of Controls	Test Results
CC9.1 - The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.			
Artishok maintains cybersecurity insurance to mitigate the financial impact of business disruptions.	CC9.1.3	Inspected the active insurance policy to determine that the company has active insurance to mitigate the financial impact of business disruptions.	No exceptions noted
CC9.2 - The entity assesses and manages risks associated with vendors and business partners.			
Artishok maintains a directory ofits key vendors, including their compliance reports. Critical vendor compliance reports are reviewed annually.	CC9.2.1	Inspected list of critical vendors to determine that the company maintains a directory of key vendors including their compliance reports. Inspected the management review of vendors to determine compliance reports were reviewed annually.	No exceptions noted
Artishok has a defined vendor management policy that establishes requirements of ensuring third-party entities meet the organization's data preservation and protection requirements.	CC9.2.2	Inspected the vendor management policy to determine that company has a formally documented policy that outlines procedures that establishes requirements of ensuring third-party entities meet the organization's data preservation and protection requirements.	No exceptions noted
A1.0 - Additional Criteria for Availability			
A1.1 - The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.			
Artishok has implemented tools to monitor Artishok's servers andnotify appropriate personnel of any events or incidents based onpredetermined criteria. Incidentsare escalated per policy.	A1.1.1	Inspected configurations for infrastructure monitoring to determine that tools to monitor the environment are in place and notify appropriate personnel of any events.	No exceptions noted

Description of Artishok's Controls	Control Number	SSF Test of Controls	Test Results
A1.1 - The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.			
Artishok uses a load balancer to automatically distribute incoming application traffic across multiple instances and availability zones.	A1.1.2	Inspected the load balancer configurations to determine that in-scope environments can automatically distribute incoming application traffic across multiple instances and availability zones.	No exceptions noted
Artishok has implemented tools to monitor Artishok's databases and notify appropriate personnel of any events or incidents based on predetermined criteria. Incidents are escalated per policy.	A1.1.3	Inspected configurations for backend monitoring to determine that tools to monitor the environment are in place and notify appropriate personnel of any events.	No exceptions noted
Artishok automatically provisions new server instances when predefined capacity thresholds aremet.	A1.1.4	Inspected auto-scaling configurations and threshold policies to determine that the infrastructure automatically provisions new server instances when predefined capacity thresholds are met.	No exceptions noted
A1.2 - The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.			
Artishok utilizes multiple availability zones to replicate production data across different zones.	A1.2.1	Inspected availability zone configurations to determine that the company utilizes multiple availability zones to replicate production data across different zones.	No exceptions noted
Artishok performs backups daily and retains them in accordance with a predefined schedule in the BackupPolicy.	A1.2.2	Inspected backup configurations to determine that daily backup are configured. Inspected the backup policy to determine that procedures are in place to perform daily backups and retain accordingly.	No exceptions noted

Description of Artishok's Controls	Control Number	SSF Test of Controls	Test Results
A1.2 - The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.			
The company relies on Cloud Service Provider physical and environmental controls, as defined and tested within the Cloud Service Provider SOC 2 reports.	A1.2.3	Inspected the cloud service providers SOC 2 report and evidence of management review to determine that management reviews subservice organizations SOC 2 reports to ensure internal controls are operating effectively.	The control is carved out and the responsibility of the subservice organization.
A1.3 - The entity tests recovery plan procedures supporting system recovery to meet its objectives.			
Artishok conducts annual BCP/DR tests and documents according to the BCDR Plan.	A1.3.1	Inspected the annual BCP/DR test to determine that the company performed a test in accordance with the BCDR plan.	No exceptions noted
Artishok performs backups daily and retains them in accordance with a predefined schedule in the Backup Policy.	A1.3.2	Inspected backup configurations to determine that daily backup are configured. Inspected the backup policy to determine that procedures are in place to perform daily backups and retain accordingly.	No exceptions noted
Artishok has an established Disaster Recovery Plan that outlines roles and responsibilities and detailed procedures for recovery of systems.	A1.3.3	Inspected the disaster recovery policy to determine that the company has formally documented procedures that outline roles and responsibilities and detailed procedures for recovery of systems.	No exceptions noted

Description of Artishok's Controls	Control Number	SSF Test of Controls	Test Results
C1.0 - Additional Criteria for Confidentiality			
C1.1 - The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.			
Artishok's customer data is segregated from the data of other customers.	C1.1.1	Inspected the entity's database cluster configurations to determine that customer data was segregated from the data of other customers.	No exceptions noted
Artishok uses test data within test environments.	C1.1.2	Inspected configurations for the entity's testing/development database environments to determine that the entity only used test data within test environments.	No exceptions noted
Storage buckets that contain customer data are versioned.	C1.1.3	Inspected the entity's storage bucket configurations to determine that storage buckets that contain customer data were versioned.	No exceptions noted
Artishok ensures that all connections to its web application from its users are encrypted.	C1.1.4	Inspected the TLS settings on the application to determine that appropriate encryption standards are used for data-in-transit.	No exceptions noted
Users can only access the production system remotely through the use of encrypted communication systems.	C1.1.5	Inspected virtual private network (VPN) configurations to determine encrypted connections are implemented for users to access the production systems. Inspected roles and groups configured for the virtual private network (VPN) to determine that only authorized users have access to the use the VPN tunnel.	No exceptions noted
Role-based security is in place for internal and external users, including super admin users.	C1.1.6	Inspected user groups and federated roles to determine that role-based security is implemented for accessing systems and resources.	No exceptions noted

Description of Artishok' Controls	Control Number	SSF Test of Controls	Test Results
C1.1 - The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.			
Artishok has established a Data Protection Policy and requires all employees to accept it upon hire. Management monitors employees' acceptance of the policy.	C1.1.7	Inspected the entity's Data Protection Policy to determine that the entity established a Data Protection Policy and requires all employees to accept it upon hire. Management monitors employees' acceptance of the policy. Inspected the policy acknowledgements for a sample of new hires to determine that the entity established a Data Protection Policy and requires all employees to accept it upon hire. Management monitors employees' acceptance of the policy.	No exceptions noted
Artishok has a clean desk policy in place to ensure that documents containing sensitive data are not in public areas or laying on unattended employee work areas	C1.1.8	Inspected the Information Security Policy to determine that the entity had a clean desk policy in place to ensure that documents containing sensitive data are not in public areas or laying on unattended employee work areas.	No exceptions noted
Artishok allows for external users to implement multi-factor authentication on their accounts in order to require two forms of authentication prior to authentication.	C1.1.9	Observed a user initiate an app.Artishok.com MFA prompt to determine that the entity allowed for external users to implement multi-factor authentication on their accounts in order to require two forms of authentication prior to authentication. Inspected a sample app.Artishok.com MFA prompt todetermine that the entity allowed for external usersto implement multi-factor authentication on theiraccounts in order to require two forms of authentication prior to authentication.	No exceptions noted
C1.2 - The entity disposes of confidential information to meet the entity's objectives related to confidentiality.			
Artishok has formal policies and procedures in place to guide personnel in the disposal of hardware containing sensitive data.	C1.2.1	Inspected the Data Deletion Policy to determine that the entity had formal policies and procedures in place to guide personnel in the disposal of hardware containing sensitive data.	No exceptions noted

Description of Artishok's Controls	Control Number	SSF Test of Controls	Test Results
C1.2 - The entity disposes of confidential information to meet the entity's objectives related to confidentiality.			
Storage buckets that contain customer data are versioned.	C1.2.2	Inspected the entity's storage bucket configurations to determine that storage buckets that contain customer data were versioned.	No exceptions noted
Artishok deletes customer data within30 days of the customer terminating its contract.	C1.2.3	Inspected the resolved JIRA tickets for a sample of completed data destructions to determine that the entity deleted customer data within 30 days of the customer terminating its contract.	No exceptions noted
Artishok has formal policies and procedures in place to guide personnel in the disposal of paper documents containing sensitive data.	C1.2.5	Inspected the Data Deletion Policy to determine that the entity had formal policies and procedures in place to guide personnel in the disposal of paper documents containing sensitive data.	No exceptions noted
PI1.0 - Additional Criteria for Processing Integrity (over the provision of services or the production, manufacturing, or distribution of goods)			
PI1.1 - The entity obtains or generates, uses, and communicates relevant, quality information regarding the objectives related to processing, including definitions of data processed and product and service specifications, to support the use of products and services.			
Artishok's application edits limit inputto acceptable value ranges	PI1.1.1	Observed the application restricting inputs to acceptable value ranges to determine that Artishok's application edits limit input to acceptable value ranges.	No exceptions noted.
Artishok system edits require mandatory fields to be complete before record entry is accepted.	PI1.1.2	Observed the application requiring mandatory fields to be completed before record entry is accepted to determine that the application required mandatory fields to be completed before record entry was accepted.	No exceptions noted.

Description of Artishok'sControls	Control Number	SSF Test of Controls	Test Results
PI1.1 - The entity obtains or generates, uses, and communicates relevant, quality information regarding the objectives related to processing, including definitions of data processed and product and service specifications, to support the use of products and services.			
A new tenant environment is created to onboard new Artishok clients, and once that environment is created, users and map data are loaded into the database and created clients can set up their connected accounts.	PI1.1.3	Inspected the database configurations to determine that a new environment was created to onboard new Artishok clients, and once that environment was created,users and map data were loaded into the database. Inspected the Artishok application configurations to determine that created clients could set up their connected accounts.	No exceptions noted.
Customer contracts include the communication of the Company's objectives related to processing, including data processed and product specifications.	PI1.1.4	Inspected the customer contract template to determine that customer contracts included the communication of the Company's objectives related to processing, including data processed and product specifications.	No exceptions noted.
PI1.2 - The entity implements policies and procedures over system inputs, including controls over completeness and accuracy, to result in products, services, and reporting to meet the entity's objectives.			
Artishok's application edits limit input to acceptable value ranges	PI1.2.1	Observed the application restricting inputs to acceptable value ranges to determine that Artishok'sapplication edits limit input to acceptable valueranges.	No exceptions noted.
Artishok system edits require mandatory fields to be complete before record entry is accepted.	PI1.2.2	Observed the application requiring mandatory fields to be completed before record entry is accepted to determine that the application required mandatory fields to be completed before record entry was accepted.	No exceptions noted.

Description of Artishok's Controls	Control Number	SSF Test of Controls	Test Results
PI1.2 - The entity implements policies and procedures over system inputs, including controls over completeness and accuracy, to result in products, services, and reporting to meet the entity's objectives.			
Support tickets are filed when there is an issue with an integration in a customer's account. Once the support ticket is generated, Artishok personnel receive an alert via a shared slack channel. Issues are tracked to resolution within the support ticket.	PI1.2.3	Observed the support ticket process to determine that support tickets are filed when there is an issue with an integration in a customer's account and that once the support ticket is generated, Artishok personnel receive an alert via a shared slack channel and that issues are tracked to resolution within the support ticket.	No exceptions noted
PI1.3 - The entity implements policies and procedures over system processing to result in products, services, and reporting to meet the entity's objectives.			
Artishok does application regression testing to validate key processing for the application during the change management process.	PI1.3.1	Inspected the change tickets for a sample of software changes to determine that application regression testing is performed to validate key processing for the application during the change management process.	No exceptions noted
The Jenkins job is configured to run on a nightly basis to persist historical reservations	PI1.3.2	Inspected the Jenkins job schedule and job history todetermine that the Autopilot job was configured torun on a nightly basis to persist historical reservations	No exceptions noted
The Artishok application uses data provided by connected customer systems and reconciles	PI1.3.3	Observed the Artishok application to determine that the Artishok application uses data provided by connected customer and reconciles data to create an holistic view of resource utilization	No exceptions noted
Artishok generates graphical representations of resource planning and utilization	PI1.3.4	Observed the Artishok application to determine that Artishok generated graphical representations ofof resource planning and utilization	No exceptions noted

Description of Artishok's Controls	Control Number	SSF Test of Controls	Test Results
PI1.4 - The entity implements policies and procedures to make available or deliver output completely, accurately, and timely in accordance with specifications to meet the entity's objectives.			
Artishok does application regression testing to validate key processing for the application during the change management process.	PI1.4.1	Inspected the change tickets for a sample of software changes to determine that application regression testing is performed to validate key processing for the application during the change management process.	No exceptions noted
Role-based and Attribute based security is in place for internal and external users,including super admin users.	PI1.4.2	Inspected user groups, federated roles and attributes to determine that role-based and ABAC permission models are implemented for accessing systems and resources.	No exceptions noted
The Artishok audit Service displays and exports unedited existing company data from the tenant database.	PI1.4.3	Inspected the Artishok audit module evidence to determine that the Artishok audit service displays and exports unedited existing company data from the tenant database.	No exceptions noted
Artishok completely accurately reports the users in each system integrated with the application.	PI1.4.4	Inspected the user listings for a sample of integrated systems to determine that Artishok completely and accurately reports the users in each system integrated with the application.	No exceptions noted
PI1.5 - The entity implements policies and procedures to store inputs, items in processing, and outputs completely, accurately, and timely in accordance with system specifications to meet the entity's objectives.			
Artishok stores customer data in databases that is encrypted at rest.	PI1.5.1	Inspected encryption configurations for databases and storage buckets to determine that sensitive data is encrypted at rest.	No exceptions noted
Artishok utilizes multiple availability zones to replicate production data across different zones.	PI1.5.2	Inspected availability zone configurations to determine that the company utilizes multiple availability zones to replicate production data across different zones.	No exceptions noted

Description of Artishok's Controls	Control Number	SSF Test of Controls	Test Results
PI1.5 - The entity implements policies and procedures to store inputs, items in processing, and outputs completely, accurately, and timely in accordance with system specifications to meet the entity's objectives.			
New hires are granted access to systems and resources after a formal approval by appropriate personnel.	PI1.5.3	Inspected the access authorization tickets for a sample of new hires to determine the entity granted access to systems and resources after a formal approval by appropriate personnel.	No exceptions noted
P1.0 - Privacy Criteria Related to Notice and Communication of Objectives Related to Privacy			
P1.1 - Privacy Criteria Related to Notice and Communication of Objectives Related to Privacy			
Artishok maintains a Privacy Policy that is available to all external users and internal employees, and it details the company's confidentiality and privacy commitments.	P1.1.1	Inspected the public facing privacy policy to determine that it is made available to external users as well as details the company's confidentiality and privacy commitments.	No exceptions noted
P2.0 - Privacy Criteria Related to Choice and Consent			
P2.1 - The entity communicates choices available regarding the collection, use, retention, disclosure, and disposal of personal information to the data subjects and the consequences, if any, of each choice. Explicit consent for the collection, use, retention, disclosure, and disposal of personal information is obtained from data subjects or other authorized persons, if required. Such consent is obtained only for the intended purpose of the information to meet the entity's objectives related to privacy. The entity's basis for determining implicit consent for the collection, use, retention, disclosure, and disposal of personal information is documented.			
Artishok has a well-defined documented scope that reflects the boundaries and applicability of its Privacy Program	P2.1.1	Inspected the publicly available privacy policy and GDPR document to determine that Artishok has a well-defined documented scope that reflects the boundaries and applicability of its Privacy Program.	No exceptions noted

Description of Artishok's Controls	Control Number	SSF Test of Controls	Test Results
P3.0 - Privacy Criteria Related to Collection			
P3.1 - Personal information is collected consistent with the entity's objectives related to privacy.			
Artishok maintains a Privacy Policy that is available to all external users and internal employees, and it details the company's confidentiality and privacy commitments.	P3.1.1	Inspected the public facing privacy policy to determine that it is made available to external users as well as details the company's confidentiality and privacy commitments.	No exceptions noted
P3.2 - For information requiring explicit consent, the entity communicates the need for such consent as well as the consequences of a failure to provide consent for the request for personal information and obtains the consent prior to the collection of the information to meet the entity's objectives related to privacy.			
Artishok maintains a Privacy Policy that is available to all external users and internal employees, and it details the company's confidentiality and privacy commitments.	P3.2.1	Inspected the public facing privacy policy to determine that it is made available to external users as well as details the company's confidentiality and privacy commitments.	No exceptions noted
Artishok's users are required to explicitly accept the notice of privacy practices prior to entering information into the application	P3.2.2	Inspected the new user sign up configuration to determine that Artishok's users are required to explicitlyaccept the notice of privacy practices prior to enteringinformation into the application	No exceptions noted

Description of Artishok's Controls	Control Number	SSF Test of Controls	Test Results
P4.0 - Privacy Criteria Related to Use, Retention, and Disposal			
P4.1 - The entity limits the use of personal information to the purposes identified in the entity's objectives related to privacy.			
Artishok maintains a Privacy Policy that is available to all external users and internal employees, and it details the company's confidentiality and privacy commitments.	P4.1.1	Inspected the public facing privacy policy to determine that it is made available to external users as well as details the company's confidentiality and privacy commitments.	No exceptions noted
P4.2 - The entity retains personal information consistent with the entity's objectives related to privacy.			
Artishok performs backups daily and retains them in accordance with a predefined schedule in the Backup Policy.	P4.2.1	Inspected backup configurations to determine that daily backup are configured. Inspected the backup policy to determine that procedures are in place to perform daily backups and retain accordingly.	No exceptions noted
Artishok establishes written policies related to retentionperiods for the confidential information it maintains.	P4.2.2	Inspected the data deletion policy to determine that Artishok establishes written policies related to retentionperiods for the confidential information it maintains.	No exceptions noted
P4.3 - The entity securely disposes of personal information to meet the entity's objectives related to privacy.			
Artishok establishes written policies related to retentionperiods for the confidentialinformation it maintains.	P4.3.1	Inspected the data deletion policy to determine that Artishok establishes written policies related to retentionperiods for the confidential information it maintains.	No exceptions noted

Description of Artishok's Controls	Control Number	SSF Test of Controls	Test Results
P4.3 - The entity securely disposes of personal information to meet the entity's objectives related to privacy.			
Artishok will delete personal information upon receiving a valid request via the privacy request form.	P4.3.2	Inspected data deletion evidence for a sample of deletion requests to determine that Artishok will deletepersonal information upon receiving a valid requestvia the privacy request form.	No exceptions noted
P5.0 - Privacy Criteria Related to Access			
P5.1 - The entity grants identified and authenticated data subjects the ability to access their stored personal information for review and, upon request, provides physical or electronic copies of that information to data subjects to meet the entity's objectives related to privacy. If access is denied, data subjects are informed of the denial and reason for such denial, as required, to meet the entity's objectives related to privacy.			
Artishok has a well-defined documented scope that reflects the boundaries and applicability of its Privacy Program	P5.1.1	Inspected the publicly available privacy policy and GDPR document to determine that Artishok has a well-defined documented scope that reflects the boundaries and applicability of its Privacy Program.	No exceptions noted
Artishok will modify personal information upon receiving a valid request via the privacy request form.	P5.1.2	Inspected the data modification evidence for a sample of data modification requests to determine that Artishokwill modify personal information upon receiving avalid request via the privacy request form.	N/A - No data modification requests were received over the audit period, so auditor was unable to conclude on the operating effectiveness of the control. Auditor examined the privacy policy to determine that the control was appropriately designed.

Description of Artishok's Controls	Control Number	SSF Test of Controls	Test Results
P5.2 - The entity corrects, amends, or appends personal information based on information provided by data subjects and communicates such information to third parties, as committed or required, to meet the entity's objectives related to privacy. If a request for correction is denied, data subjects are informed of the denial and reason for such denial to meet the entity's objectives related to privacy.			
Artishok will modify personal information upon receiving a valid request via the privacy request form.	P5.2.1	Inspected the data modification evidence for a sample of data modification requests to determine that Artishokwill modify personal information upon receiving avalid request via the privacy request form.	N/A - No data modification requests were received over the audit period, so auditor was unable to conclude on the operating effectiveness of the control. Auditor examined the privacy policy to determine that the control was appropriately designed.
Artishok will delete personal information upon receiving a valid request via the privacy request form.	P5.2.2	Inspected data deletion evidence for a sample of deletion requests to determine that Artishok will deletepersonal information upon receiving a valid requestvia the privacy request form.	No exceptions noted
P6.0 - Privacy Criteria Related to Disclosure and Notification			
P6.1 - The entity discloses personal information to third parties with the explicit consent of data subjects and such consent is obtained prior to disclosure to meet the entity's objectives related to privacy.			
Artishok maintains a Privacy Policy that is available to all external users and internal employees, and it details the company's confidentiality and privacy commitments.	P6.1.1	Inspected the public facing privacy policy to determine that it is made available to external users as well as details the company's confidentiality and privacy commitments.	No exceptions noted

Description of Artishok's Controls	Control Number	SSF Test of Controls	Test Results
P6.1 - The entity discloses personal information to third parties with the explicit consent of data subjects and such consent is obtained prior to disclosure to meet the entity's objectives related to privacy.			
Artishok discloses personal information only to third parties who have agreements with Artishok to protect personal information in a manner consistent with the relevant aspects of Artishok's privacy notice or other specific instructions or requirements.	P6.1.2	Inspected the agreements for a sample of third parties to determine that Artishok discloses personal information only to third parties who have agreements with Artishok to protect personal information in a manner consistent with the relevant aspects of Artishok's privacy notice or other specific instructions or requirements.	No exceptions noted.
P6.2 - The entity creates and retains a complete, accurate, and timely record of authorized disclosures of personal information to meet the entity's objectives related to privacy.			
Artishok maintains a directory of itskey vendors, including their compliance reports. Critical vendor compliance reports are reviewed annually.	P6.2.1	Inspected list of critical vendors to determine that the company maintains a directory of key vendors including their compliance reports. Inspected the management review of vendors to determine compliance reports were reviewed annually.	No exceptions noted
Artishok maintains a directory of its key vendors, including its agreements that specify terms, conditions and responsibilities.	P6.2.2	Inspected the full listing of vendors to determine that the company maintains a directory of its key vendors, including its agreements that specify terms, conditions and responsibilities.	No exceptions noted
P6.3 - The entity creates and retains a complete, accurate, and timely record of detected or reported unauthorized disclosures (including breaches) of personal information to meet the entity's objectives related to privacy.			
Artishok has a defined breach notification policy that establishes the requirements and procedures for reporting a breach of sensitive information.	P6.3.1	Inspected the breach notification policy to determine that Artishok has a defined breach notification policy that establishes the requirements and procedures for reporting a breach of sensitive information.	No exceptions noted

Description of Artishok's Controls	Control Number	SSF Test of Controls	Test Results
P6.4 - The entity obtains privacy commitments from vendors and other third parties who have access to personal information to meet the entity's objectives related to privacy. The entity assesses those parties' compliance on a periodic and as-needed basis and takes corrective action, if necessary.			
Artishok maintains a directory of its key vendors, including their compliance reports. Critical vendor compliance reports are reviewed annually.	P6.4.1	Inspected list of critical vendors to determine that the company maintains a directory of key vendors including their compliance reports. Inspected the management review of vendors to determine compliance reports were reviewed annually.	No exceptions noted
Artishok maintains a directory of its key vendors, including its agreements that specify terms, conditions and responsibilities.	P6.4.2	Inspected the full listing of vendors to determine that the company maintains a directory of its key vendors, including its agreements that specify terms, conditions and responsibilities.	No exceptions noted
P6.5 - The entity obtains commitments from vendors and other third parties with access to personal information to notify the entity in the event of actual or suspected unauthorized disclosures of personal information. Such notifications are reported to appropriate personnel and acted on in accordance with established incident-response procedures to meet the entity's objectives related to privacy.			
Artishok has a defined vendor management policy that establishes requirements of ensuring third-party entities meet the organization's data preservation and protection requirements.	P6.5.1	Inspected the vendor management policy to determine that company has a formally documented policy that outlines procedures that establishes requirements of ensuring third-party entities meet the organization's data preservation and protection requirements.	No exceptions noted
Artishok maintains a directory of its key vendors, including its agreements that specify terms, conditions and responsibilities.	P6.5.2	Inspected the full listing of vendors to determine that the company maintains a directory of its key vendors, including its agreements that specify terms, conditions and responsibilities.	No exceptions noted

Description of Artishok's Controls	Control Number	SSF Test of Controls	Test Results
P6.6 - The entity provides notification of breaches and incidents to affected data subjects, regulators, and others to meet the entity's objectives related to privacy.			
Artishok has a defined breach notification policy that establishes the requirements and procedures for reporting a breach of sensitive information.	P6.6.1	Inspected the breach notification policy to determine that Artishok has a defined breach notification policy that establishes the requirements and procedures for reporting a breach of sensitive information.	No exceptions noted
P6.7 - The entity provides data subjects with an accounting of the personal information held and disclosure of the data subjects' personal information, upon the data subjects' request, to meet the entity's objectives related to privacy.			
Artishok tracks and manages requests from data subjects andprovides a response to valid requests within30 days.	P6.7.1	Inspected the responses to a sample of valid requests to determine that Artishok tracks and manages requestsfrom data subjects and provides a response to validrequests within 30 days.	No exceptions noted
Artishok will delete personal information upon receiving a valid request via the privacy request form.	P6.7.2	Inspected data deletion evidence for a sample of deletion requests to determine that Artishok will deletepersonal information upon receiving a valid requestvia the privacy request form.	No exceptions noted

Description of Artishok's Controls	Control Number	SSF Test of Controls	Test Results
P7.0 - Privacy Criteria Related to Quality			
P7.1 - The entity collects and maintains accurate, up-to-date, complete, and relevant personal information to meet the entity's objectives related to privacy.			
Artishok maintains a Terms of Service that is available to all external users and internal employees, and the terms detail the company's security and availability commitments regarding the systems. Client Agreements or Master Service Agreements are in place for whenthe Terms of Service may notapply.	P7.1.1	Inspected the public facing website to determine the company had made available the terms of service which details the company's security and availability commitments regarding the systems. Inspected the master service agreement (MSA) template to determine that the company has in place an MSA in the event the terms of service does not apply.	No exceptions noted
Artishok maintains a Privacy Policy that is available to all external users and internal employees, and it details the company's confidentiality and privacy commitments.	P7.1.2	Inspected the public facing privacy policy to determine that it is made available to external users as well as details the company's confidentiality and privacy commitments.	No exceptions noted

Description of Artishok'sControls	Control Number	SSF Test of Controls	Test Results
P8.0 - Privacy Criteria Related to Monitoring and Enforcement			
P8.1 - The entity implements a process for receiving, addressing, resolving, and communicating the resolution of inquiries, complaints, and disputes from data subjects and others and periodically monitors compliance to meet the entity's objectives related to privacy. Corrections and other necessary actions related to identified deficiencies are made or taken in a timely manner.			
Artishok will modify personal information upon receiving a valid request via the privacy request form.	P8.1.1	Inspected the data modification evidence for a sample of data modification requests to determine that Artishokwill modify personal information upon receiving avalid request via the privacy request form.	N/A - No data modification requests were received over the audit period, so auditor was unable to conclude on the operating effectiveness of the control. Auditor examined the privacy policy to determine that the control was appropriately designed.
Artishok will delete personal information upon receiving a valid request via the privacy request form.	P8.1.2	Inspected data deletion evidence for a sample of deletion requests to determine that Artishok will deletepersonal information upon receiving a valid requestvia the privacy request form.	No exceptions noted
Artishok tracks and manages requests from data subjects andprovides a response to validrequests within30 days.	P8.1.3	Inspected the responses to a sample of valid requests to determine that Artishok tracks and manages requestsfrom data subjects and provides a response to validrequests within 30 days.	No exceptions noted