ARCOS LLC.

Report on Controls at a Service Organization Relevant to Security, Confidentiality, and Availability

SOC 3®

For the Period July 1, 2023 to June 30, 2024

SOC 3 is a registered service mark of the American Institute of Certified Public Accountants (AICPA)

Independent Service Auditor’s Report

To the Management of ARCOS LLC. (ARCOS):

Scope

We have examined ARCOS’s accompanying assertion titled "Assertion of ARCOS Management" (assertion) that the controls within the ARCOS SaaS-based Resource Acquisition, Planning, and Management Solution System (the “system”) were effective throughout the period July 1, 2023 to June 30, 2024, to provide reasonable assurance that ARCOS's service commitments and system requirements were achieved based on the trust services criteria relevant to security, confidentiality, and availability (applicable trust services criteria) set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, Trust Services Criteria).

Service Organization’s Responsibilities

ARCOS 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 ARCOS's service commitments and system requirements were achieved. ARCOS has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, ARCOS is responsible for selecting, and identifying in its assertion, the applicable trust service criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor’s Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements;
- Assessing the risks that controls were not effective to achieve ARCOS's service commitments and system requirements based on the applicable trust services criteria; and,
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve ARCOS's service commitments and system requirements based on the applicable trust services criteria.

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

Relevant Ethical Requirements

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

Inherent Limitations

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

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

Opinion

In our opinion, management's assertion that the controls within ARCOS's ARCOS SaaS-based Resource Acquisition, Planning, and Management Solution System were effective throughout the period July 1, 2023 to June 30, 2024, to provide reasonable assurance that ARCOS's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

BARR Advisory, P.A.

Fairway, KS

August 12, 2024

Assertion of ARCOS Management

We are responsible for designing, implementing, operating, and maintaining effective controls within the ARCOS SaaS-based Resource Acquisition, Planning, and Management Solution System (the "system") throughout the period July 1, 2023 to June 30, 2024, to provide reasonable assurance that ARCOS's service commitments and system requirements relevant to security, confidentiality, and availability were achieved. Our attached system description of the ARCOS SaaS-based Resource Acquisition, Planning, and Management Solution System identified the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period July 1, 2023 to June 30, 2024, to provide reasonable assurance that ARCOS's service commitments and system requirements were achieved based on the trust services criteria relevant to security, confidentiality, and availability (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). ARCOS's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in the attached system description.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period July 1, 2023 to June 30, 2024, to provide reasonable assurance that ARCOS's service commitments and system requirements were achieved based on the applicable trust services criteria.

ARCOS LLC.

August 12, 2024

ARCOS’s Description of the Boundaries of Its ARCOS SaaS-based Resource Acquisition, Planning, and Management Solution System

Description of Services Provided

ARCOS LLC. (“ARCOS” or the “company”) was founded in 1993 as an interactive voice response (IVR) consulting and custom application development company. ARCOS addresses accountability, transparency, and results for crew callout in industries with staffing qualification requirements, diverse regulations, and urgent response times.

The ARCOS SaaS-based Resource Acquisition, Planning, and Management Solution (the “system”) finds, assembles, and tracks repair crews to improve service restoration and emergency response for electric utilities, gas utilities, power generation plants, and airlines.

ARCOS’s system helps automate complex scheduling and callout business rules. ARCOS also provides support for customer service callout, emergency preparedness notifications, real-time employee availability information, and improved business intelligence.

The ARCOS system helps support the following solutions:

- **ARCOS Automated Callout Solution:** A utility/power generation plant’s ability to respond, restore, and report in real-time when service restoration issues and emergencies arise.
- **ARCOS Crew Manager:** Helps utilities to identify which crews, vehicles, and equipment are available for work and improves the ability to assign, manage, and track these resources.
- **ARCOS Resource Assist:** A centralized platform that unites utilities and utility service providers to automate the acquisition and assignment of contracted resources.
- **ARCOS Incident Management Software:** An organized solution to assist when transitioning from regular operations to emergency response and recovery.
- **ARCOS Damage Assessment:** Helps utilities arrive at an estimated time of restoration (ETR), reduce costs and restoration time, and increase safety of field personnel and customers following natural disasters and other emergencies.
- **ARCOS Mobile Inspection:** Functionalities of the main applications but in a mobile format.
- **ARCOS Mobile Workbench:** A configurable work order management software solution that compresses the amount of time it takes to assign, distribute, and manage work conducted in the field.
- **ARCOS Resource Planner:** Software platform to plan for and view all the resources they have, organized by type and location.
- **ARCOS RosterApps:** Manages the day-to-day staffing of airline ground crews through employee self-serve shift bidding, vacation bidding, trade requests, and time-off requests.

Components of the System Used to Provide the Services

The purpose of the system description is to delineate the boundaries of the system, which includes the services and commitments outlined above and the five components described below: infrastructure, software, people, data, and processes and procedures

Infrastructure

The system is hosted in Amazon Web Services (AWS) in a virtual private cloud (VPC) environment which protects the network from unauthorized external access. The network topology includes segmented VPCs and access control lists (ACLs). ARCOS employs intrusion detection systems (IDS) at strategic points in its network that complement its security policy network settings. User requests to ARCOS's web-based systems are encrypted using Transport Layer Security (TLS) using certificates from an established third-party certificate authority. Remote system administration access to ARCOS web, application, and database servers is available through a virtual private network (VPN) connection. Production servers at AWS maintain failover capabilities in the event of physical hardware or logical software failures. This infrastructure is hosted in high availability data centers with multiple availability zones.

Software

ARCOS is responsible for managing the development and operation of the ARCOS SaaS-based Resource Acquisition, Planning, and Management Solution System including infrastructure components such as servers, databases, and storage systems.

ARCOS does not host any infrastructure or software on premise. As such, physical and environmental controls are the responsibilities of the cloud providers ARCOS leverages.

People

ARCOS has a staff organized in the following functional areas:

- **Board of Directors:** Responsible for overseeing significant risks to the organization, obtaining assurance that executive management has established responsibilities, processes, and technology for an effective information security program, and reviewing risk assessment results to assist in risk management decisions for securing ARCOS's information assets. The board of directors includes members independent from control operators.
- **Executive Management:** Responsible for establishing responsibilities, processes, Information Security Policy reviews, and technology for an effective information security program.
- **Engineering:** Responsible for the development, testing, deployment, and maintenance of the source code for the system. Also responsible for the product life cycle, including adding additional product functionality.
- **Cloud Operations (CloudOps):** Responsible for maintaining the availability of production infrastructure and managing access and security for production infrastructure. Only members of the operations team have access to the production environment. Members of the operations team may also be members of the engineering team.
- **Security:** Responsible for access controls and security of the production environment, quarterly access reviews, reviewing policies and procedures related to security and communication of those policies, annual risk assessment, and the communication of the assessment to executive management.
- **People Operations:** Responsible for recruiting and onboarding new personnel, defining roles and positions for new hires, performing background checks, and facilitating the employee termination process.
- **IT:** Responsible for managing laptops, software, and other technology involved in employee productivity and business operations.
- **Customer Success:** Responsible for sales, account management, customer success, and customer support activities.
- **Customer Support:** Responsible for handling customer incidents and support.

- **Legal:** Responsible for client contracts relating to security, privacy, and compliance.

Data

Data, as defined by ARCOS, constitutes the following:

- Customer input via web browsers-based interface and SFTP;
- Web services (both client and server side) to give synchronous, programmatic integration with customers' back-office systems;
- APIs allowing input and retrieval of overtime, employee information, schedule information, etc.;
- Email and SMS alerts to customers;
- Phone calls to customers' employees during the callout process;
- Phone call recordings; and,
- Logging of all activity both for internal infrastructure maintenance and customer logins, actions, etc.

Information assets are assigned a sensitivity level based on the audience for the information. If the information has been previously classified by regulatory, legal, contractual, or company directive, then that classification will take precedence. The sensitivity level then guides the selection of protective measures to secure the information. All data is to be assigned one of the following sensitivity levels:

Sensitivity Level	Description	Examples of Data
Confidential	Highly valuable and sensitive information where the level of protection is dictated externally by legal and/or contractual requirements. Access to restricted information is limited to authorized employees, contractors, and business partners with a specific need.	● Customer operating data ● Personally identifiable information (PII) ● Anything subject to a confidentiality agreement with a customer
Restricted	Proprietary information requiring thorough protection; access is restricted to employees with a "need-to-know" based on business requirements. This data can only be distributed outside the company with approval. This is default for all company information unless stated otherwise.	● Internal policies ● Legal documents ● Meeting minutes and internal presentations ● Contracts ● Internal reports ● Slack messages ● Email
Public	Documents intended for public consumption which can be freely distributed outside the company.	● Marketing materials ● Product descriptions ● Release notes ● External facing policies

Processes and Procedures

Management has developed and communicated policies and procedures to manage the information security of the system. Changes to these procedures are performed annually and authorized by senior management. These procedures cover the following key security life cycle areas:

- Access Control Policy
- Asset Management Policy
- Business Continuity and Disaster Recovery Plan
- Change Control Policy
- Code of Conduct
- Cryptography Policy
- Data Management Policy
- Disaster Recovery Policy
- Human Resource Security Policy
- Incident Response Plan
- Information Security Policy (AUP)
- Information Security Roles and Responsibilities
- Operations Security Policy
- Physical Security Policy
- Record and Document Retention Policy
- Risk Management Policy
- Secure Development Policy
- Software Development Lifecycle Policy
- Third-party Information Sharing Policy
- Third-party Management Policy
- Vulnerability Management Policy

Principal Service Commitments and System Requirements

ARCOS designs its processes and procedures related to the system to meet its objectives. Those objectives are based on the service commitments that ARCOS makes to its customers, business partners, vendors, and subservice organizations and the operational and compliance requirements that ARCOS has established for the services. Service commitments are declarations made by management to its customers regarding the performance of the ARCOS system. Service commitments are set forth in standardized contracts, service-level agreements (SLAs), and in the description of the service offering provided online.

Security commitments include, but are not limited to, the following:

- System features and configuration settings designed to authorize user access while restricting unauthorized users from accessing information not needed for their role;
- Use of intrusion detection systems to identify potential security attacks from users outside the boundaries of the system;
- Daily vulnerability scans over the network and annual penetration tests over the client environment; and,
- Operational procedures for managing security incidents and breaches, including notification procedures.

Confidentiality commitments include, but are not limited to, the following:

- The use of encryption technologies to protect system data both at rest and in transit;
- Confidentiality and non-disclosure agreements with employees, contractors, and third parties; and,
- Confidential information must be used only for the purposes explicitly stated in agreements between ARCOS and user entities.

Availability commitments include, but are not limited to, the following:

- System performance and availability monitoring mechanisms to help ensure the consistent delivery of the system and its components;
- Responding to customer requests in a reasonably timely manner;
- Business continuity and disaster recovery (BC/DR) plans that include detailed instructions, recovery point objectives (RPOs), recovery time objectives (RTOs), roles, and responsibilities; and,
- Operational procedures supporting the achievement of availability commitments to user entities.

ARCOS establishes system requirements that support the achievement of service commitments, relevant operational and compliance requirements, applicable laws and regulations, and other system requirements including the following:

- System functional requirements derived from service commitments, published documentation of system functionality, and other descriptions of the system;

- Monitoring of third-party providers to detect failures of those service providers to meet service agreements that could threaten the achievement of the service organization's service commitments and system requirements and respond to those failures; and,
- Business processing rules, standards and regulations, such as U.S data privacy laws.

ARCOS establishes operational requirements that support the achievement of service commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in ARCOS'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 are documented on how to carry out specific manual and automated processes required in the operation and development of the system. Information security policies, including sanctions for policy violations, are approved by management at least annually and published on internal collaboration tools (i.e., Vanta) accessible to all personnel with access to the company systems.