AiDASH Inc.

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

SOC 2 Type 2®

For the Period April 1, 2024 to March 31, 2025

SOC 2 is a registered service mark of the American Institute of Certified Public Accountants (AICPA)

Contents

This report is intended solely for use by the management of AiDASH Inc. and its user entities (i.e., customers) that use the services covered by this report during the period. Unauthorized use, reproduction, or distribution of this report, in whole or in part, is strictly prohibited.

Section I

Independent Service Auditor's Report Provided by BARR Advisory, P.A.

Independent Service Auditor's Report

To the Management of AiDASH Inc. ("AiDASH"):

Scope

We have examined AiDASH's accompanying description of its AiDASH System, titled "AiDASH's Description of Its AiDASH System," throughout the period April 1, 2024 to March 31, 2025 (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) (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period April 1, 2024 to March 31, 2025, to provide reasonable assurance that AiDASH's service commitments and system requirements were achieved based on the trust services criteria relevant to security, confidentiality, availability, and processing integrity (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).

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

AiDASH 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 AiDASH's service commitments and system requirements were achieved. AiDASH has provided the accompanying assertion titled "Assertion of AiDASH Management" (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. AiDASH is also responsible for 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; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of the 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 AICPA. 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.

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

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; and,
- 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 suitability of 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 our tests are listed in Section IV.

Controls that Did Not Operate During the Period

The description discusses its procedures for data deletion as a result of ad-hoc data deletion requests. However, during the period April 1, 2024 to March 31, 2025, there were no ad-hoc data deletion requests that would have warranted the operation of the data disposal process.

Because the control OM-04 described above did not operate during the audit period, we were unable to test, and did not test, the operating effectiveness of the control as evaluated using the following trust services criteria:

- C1.2 - The entity disposes of confidential information to meet the entity's objectives related to confidentiality.

Opinion

In our opinion, in all material respects,

a. The description presents the AiDASH System that was designed and implemented throughout the period April 1, 2024 to March 31, 2025, in accordance with the description criteria.

b. The controls stated in the description were suitably designed throughout the period April 1, 2024 to March 31, 2025, to provide reasonable assurance that AiDASH'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 organizations and user entities applied the complementary controls assumed in the design of AiDASH's controls throughout that period.

c. The controls stated in the description operated effectively throughout the period April 1, 2024 to March 31, 2025, to provide reasonable assurance that AiDASH'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 AiDASH's controls operated effectively throughout that period.

Restricted Use

This report, including the description of tests of controls and results thereof in Section IV, is intended solely for the information and use of AiDASH, user entities of the AiDASH System during some or all of the period April 1, 2024 to March 31, 2025, business partners of AiDASH subject to risks arising from interactions with the AiDASH System, practitioners providing services to such user entities and business partners, prospective user entities and business partners, regulators, all of whom 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 and how those controls interact with the controls at the service organization to achieve the service organization'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; and,
- 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 is not intended to be, and should not be used by anyone other than these specified parties.

Fairway, KS

May 15, 2025

Section II
Assertion of AiDASH Management

Assertion of AiDASH Management

We have prepared the accompanying description titled "AiDASH's Description of Its AiDASH System" throughout the period April 1, 2024 to March 31, 2025 (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) (description criteria). The description is intended to provide users with information about the AiDASH System that may be useful when assessing the risks arising from interactions with AiDASH's system, particularly information about system controls that AiDASH 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, confidentiality, availability, and processing integrity (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).

AiDASH uses subservice organizations to provide data center hosting and infrastructure services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at AiDASH, to achieve AiDASH's service commitments and system requirements based on the applicable trust services criteria. The description presents AiDASH's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of AiDASH'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 AiDASH, to achieve AiDASH's service commitments and system requirements based on the applicable trust services criteria. The description presents AiDASH's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of AiDASH's controls.

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

a. The description presents the AiDASH System that was designed and implemented throughout the period April 1, 2024 to March 31, 2025, in accordance with the description criteria.

b. The controls stated in the description were suitably designed throughout the period April 1, 2024 to March 31, 2025, to provide reasonable assurance that AiDASH'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 organizations and user entities applied the complementary controls assumed in the design of AiDASH's controls throughout that period.

c. The controls stated in the description operated effectively throughout the period April 1, 2024 to March 31, 2025, to provide reasonable assurance that AiDASH'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 AiDASH's controls operated effectively throughout that period.

Controls That Did Not Operate During the Period

Our description discusses AiDASH's controls and procedures for data deletion as a result of ad-hoc data deletion requests. However, during the period April 1, 2024 to March 31, 2025, AiDASH did not experience ad-hoc data deletion requests that would warrant the operation of the data disposal process (control OM-04).

AiDASH Inc.

May 15, 2025

Section III

AiDASH's Description of Its AiDASH System

Overview of Operations

Description of Services Provided

AiDASH (the "company") is making critical infrastructure industries climate-resilient and secure. Using its satellite-first platform for grid inspection and monitoring, itsAI applications enable electric and gas utilities and landowners to transform how they manage and maintain assets. Benefits include reduced costs, improved reliability and advancements in sustainability goals.

The AiDASH System (the "platform") encompasses the following applications:

- **Intelligent Vegetation Management System (IVMS):** Helps utilities identify and manage vegetation risks along rights-of-way.
- **Climate Risk Intelligence System (CRIS):** Predicts where storms will hit hardest—and where outages are most likely; also gives utilities a clear, data-driven view of wildfire risk.
- **Asset Inspection and Monitoring System (AIMS):** Helps utilities better manage their assets.
- **Biodiversity Net Gain Management System (BNGAI):** Helps organizations manage biodiversity programs.

Principal Service Commitments and System Requirements

AiDASH designs its processes and procedures related to the system to meet its objectives. Those objectives are based on the service commitments that AiDASH makes to its customers, business partners, vendors, and subservice organizations and the operational and compliance requirements that AiDASH has established for the services. Service commitments are declarations made by management to its customers regarding the performance of the AiDASH 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 intrusion detection systems to identify potential security attacks from users outside the system's boundaries;
- Continuous vulnerability scans over the system and network, and penetration tests over the application; 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 agreements with employees, contractors, and vendors with access to customer data; and,
- Confidential information must be used only for the purposes explicitly stated in agreements between AiDASH and its customers.

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 through AiDASH's standard customer support services;
- Business continuity and disaster recovery (BC/DR) plans that include detailed instructions, roles, and responsibilities; and,
- Operational procedures supporting the achievement of availability commitments to customers.

Processing integrity commitments are standardized and include, but are not limited to, the following:

- Procedures to ensure definition of data processed and product and services specifications are documented and communicated to users of the system;
- Policies and procedures are in place to store inputs, data in process, and outputs completely, accurately, and timely; and,
- System checks to ensure completeness and accuracy of data processed, stored, and transmitted through the system.

AiDASH 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; and,
- 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.

AiDASH establishes operational requirements that support the achievement of service commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in AiDASH'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., Confluence, Sprinto) accessible to all personnel with access to the company systems.

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). AiDASH employs intrusion detection systems (IDS) at strategic points in its network that complement its security policy network settings. User requests to AiDASH'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 AiDASH's web and application servers is available through a firewall controlled by security groups. The hardware components that make up the aforementioned system include servers hosted, managed, and protected by AWS. 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.

All infrastructure noted in the Primary Infrastructure and Software table is hosted by subservice organizations, specified in the Complementary Subservice Organization Controls table.

Software

AiDASH is responsible for managing the development and operation of the system platform including software infrastructure components such as operating systems, databases, and storage systems.

The in-scope AiDASH infrastructure and software components are listed in the table below:

Primary Infrastructure and Software			
System/ Application	**Business Function/Description**	**OS/DB**	**Physical Location**
AiDASH System	Provides access to AiDASH SaaS products through a web interface and user authentication. This provides access to all components identified within the Description of Services Provided section above.	Linux/PostgreSQL (RDS)	AWS US-West (Primary) AWS US-East (Disaster Recovery)
AWS Identity and Access Management (IAM)	Service that provides identity and access management to various applications and supporting tools within AWS.	AWS Proprietary	AWS US-West (Primary) AWS US-East (Disaster Recovery)
AWS Kubernetes cluster	Used to deploy, manage, and scale containerized applications.	AWS Proprietary	AWS US-West (Primary) AWS US-East (Disaster Recovery)
Amazon Simple Storage Services (S3)	Provides an interface used to store and retrieve business unit data. S3 application programming interfaces (APIs) provide bucket- and object-level access and version control. S3 is controlled through the AWS IAM interface.	AWS Proprietary	AWS US-West (Primary) AWS US-East (Disaster Recovery)
AWS Systems Manager	Used to automate operational tasks across your AWS resources and maintain security and compliance by establishing zero-Secure Shell (SSH) on to production systems.	AWS Proprietary	AWS US-West (Primary) AWS US-East (Disaster Recovery)
AWS Route 53	Service that provides a highly available and scalable cloud domain name system (DNS) web service.	AWS Proprietary	AWS US-West (Primary) AWS US-East (Disaster Recovery)
AWS Jumphost	Public facing production gateway utilized to access production systems in the event of an emergency lockout.	AWS Proprietary	AWS US-West (Primary) AWS US-East (Disaster Recovery)

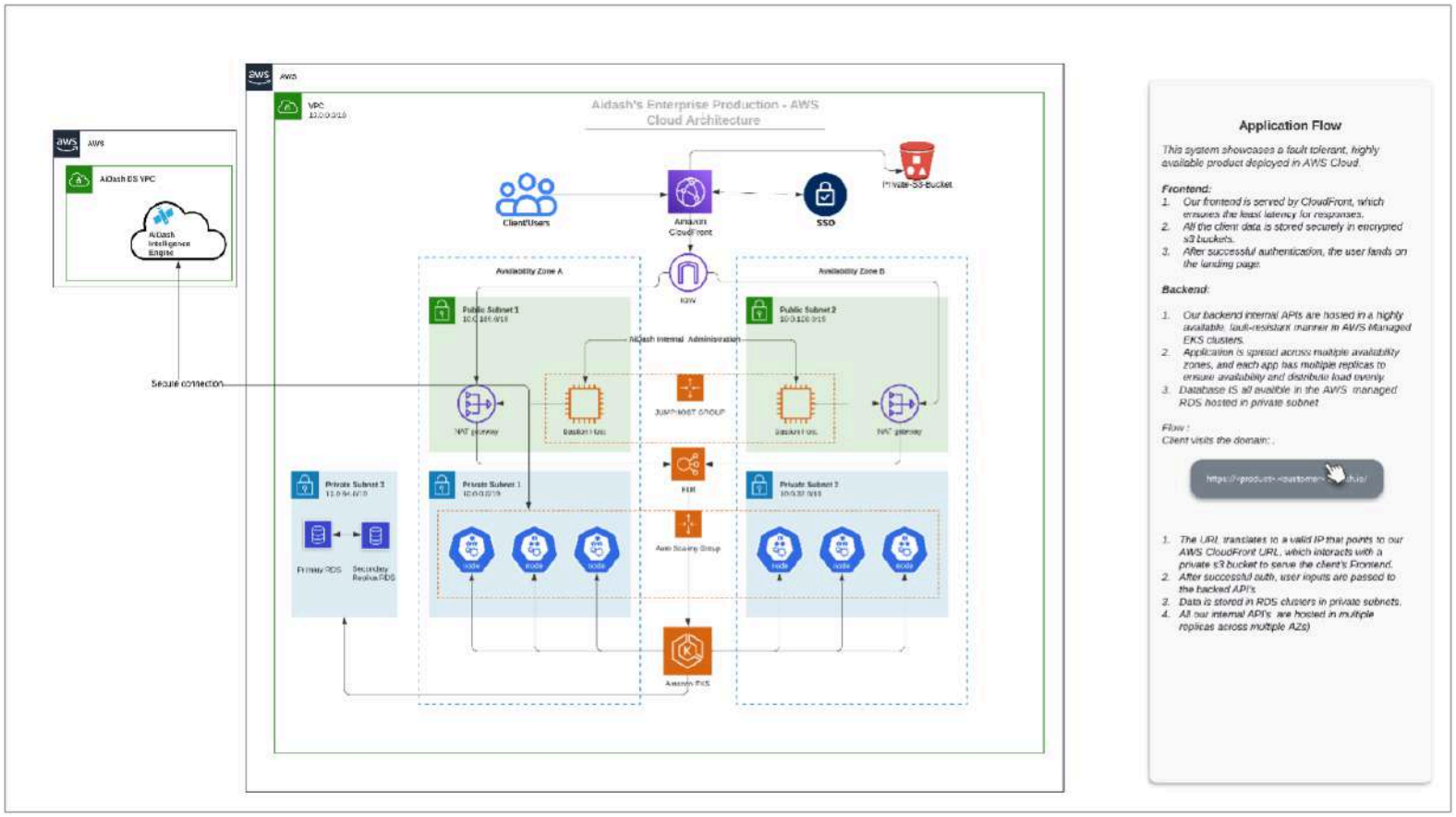
Primary Infrastructure and Software			
System/ Application	**Business Function/Description**	**OS/DB**	**Physical Location**
AWS Bastion Host	Used for securely accessing private instances in the VPC (Virtual Private Cloud).	AWS Proprietary	AWS US-West (Primary) AWS US-East (Disaster Recovery)
AWS CloudFront	Service that provides content distribution for web-facing assets of AiDASH offerings.	AWS Proprietary	AWS US-West (Primary) AWS US-East (Disaster Recovery)
AWS Firewalls	Front-end firewalls protect the network perimeter with rule-based ACLs and back-end firewalls segregate the database servers from internal traffic.	AWS Proprietary	AWS US-West (Primary) AWS US-East (Disaster Recovery)
Bitbucket	Source code repositories, version control systems, and build software.	Atlassian Proprietary	Atlassian Cloud
Microsoft Entra ID (Office 365 SSO)	Cloud-based IAM service utilized in conjunction with Office 365 SSO that provides single sign-on (SSO) and multi-factor authentication (MFA) for AiDASH personnel to authenticate to AWS and Bitbucket. Entra ID serves as the active directory for AWS, Bitbucket, and the AiDASH System.	Microsoft Proprietary	Microsoft Cloud
1Password	Individual password manager used as a shared vault for shared secrets to the AiDASH System and Microsoft.	1Password Proprietary	1Password Cloud

Supporting Tools	
System/Application	**Business Function/Description**
Allure	Used For API automation reporting and consolidation.
Auth0	Used for security and single sign-on purposes for various supporting tools.
AWS CloudTrail	Utilized to record logs of various account activities within the production and non-production infrastructure.
AWS CloudWatch	Application and infrastructure monitoring tool.
Burp Suite	Performs security testing over geographical web application components.
Checkr	Used for running background checks on candidates in the United States during the interview process.
Config Cat	It is a service that allows developers to manage feature flags and remote configurations for applications. It helps with feature rollout, A/B testing, and dynamic configuration without redeploying the app.
Confluence (Wiki)	A collaboratively edited wiki and document repository used for policies, procedures, and other documents.
Datadog	Used to collect and store log data.
Global Screening Solutions (GSS)	Used for running background checks on candidates in India during the interview process.
Grafana	Monitoring tool over server health, databases, tools, and services.
Groundcover	IDS utilized for application monitoring, alerting of performance, exceeding monitoring thresholds, and event management in real time.
Jenkins	Used to migrate changes to production, sandbox, and staging environments from other central repositories.
Jira	A customizable tool for agile software development; logs and tracks progress of bugs, tasks, features, incidents, and projects.
Lever	Tool used to track progress of candidates through the interview process.
Microsoft OneDrive	A central repository for all marketing materials, leads, API maps, and other centralized files accessible to all employees.
Microsoft Teams	Utilized for messaging and file retention for different teams within AiDASH.
Namely	Human resources software platform that integrates personnel info, payroll and benefits administration, and goal setting/performance.

Supporting Tools	
System/Application	**Business Function/Description**
Sprinto	A comprehensive compliance automation platform designed to streamline manual compliance tasks.
Sonar	Static analysis tool for code scanning.
TestRail QA	Web based quality assurance testing tool.
Webhook	Tool used for real-time notifications and communication between applications.
Zenduty	A tool used for incident management and response coordination.

Overall Technical Implementation Diagrams/Segregation

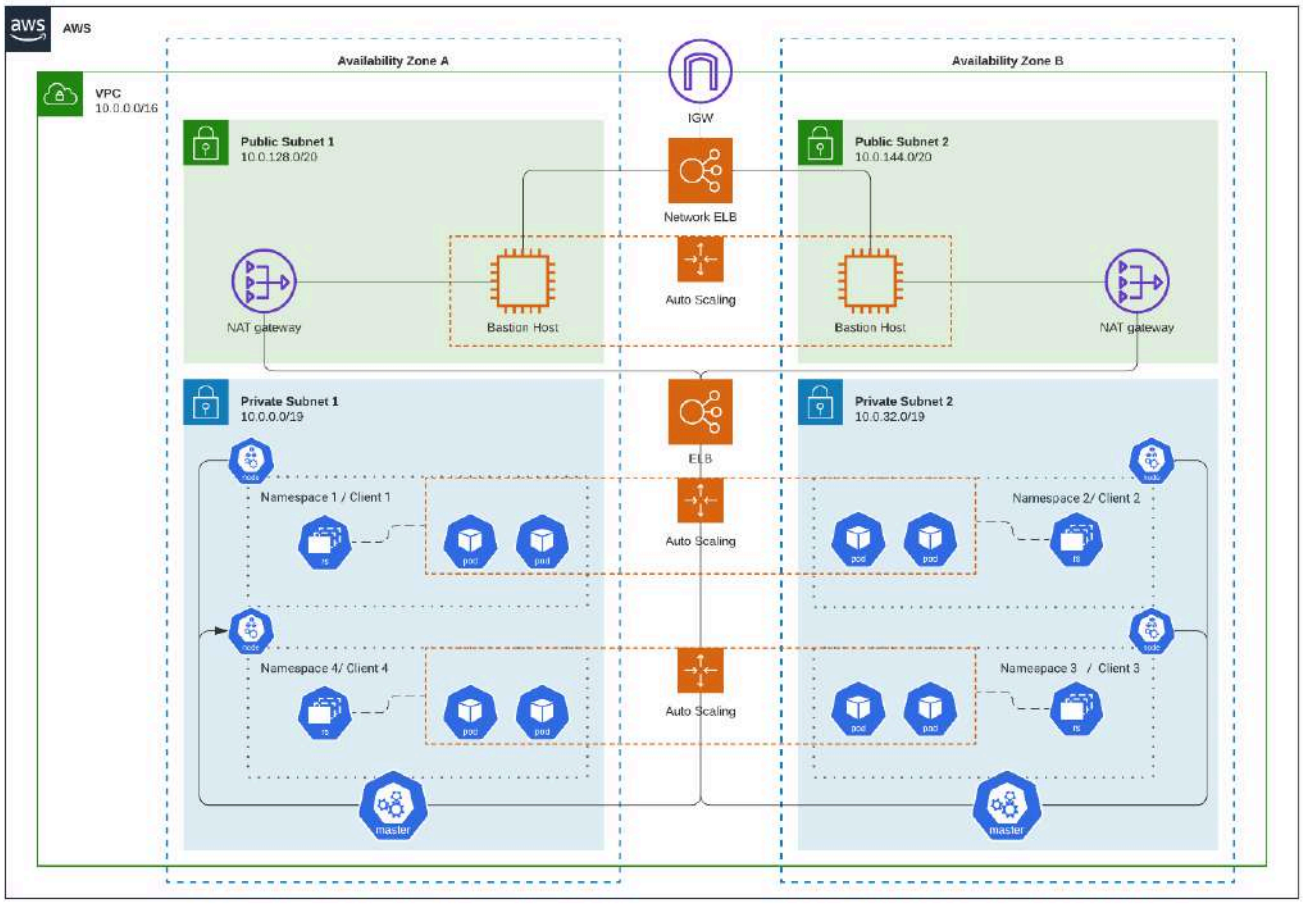
Diagram 1: End-to-end Deployment Architecture



AiDASH Intelligence: This is the core proprietary component where data science inferencing occurs. This system processes and analyzes the data specific to each client's needs.

Auto-scaled Deployment: Each client has a dedicated, auto-scaled deployment that dynamically adjusts resources based on demand. This ensures efficient resource utilization and optimal performance across different workloads.

Diagram 2: Logical Segregation Within Kubernetes Cluster



Kubernetes Namespaces: Each client is allocated a separate namespace within the Kubernetes cluster. This setup provides:

- **Isolation:** Ensures that the resources and processes of one client are completely isolated from those of another, enhancing security and reducing interference.
- **Resource Management:** Allows for tailored resource allocation and management, ensuring that each client can scale their operations independently within the cluster.
- **Custom Configuration:** Each namespace can be configured with specific permissions and settings that align with individual client requirements.

These diagrams illustrate a cloud architecture that leverages Kubernetes for scalability and isolation, integrated with AiDASH's proprietary intelligence for specialized data processing and inferencing.

People

AiDASH employees are organized in the following functional areas:

- **Board of Directors:** The board of directors is independent of management and provides oversight and management of the organization's information security program. The board ascertains that there is transparency about the significant risks to the organization and is responsible for the impartial oversight of internal controls.
- **Corporate:** Responsible for overseeing company wide activities, establishing, and accomplishing goals, and overseeing objectives.
- **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.
- **InfoSec:** Responsible for access controls and security and confidentiality of the production environment, the governance of the system, and risk management including vendor management. Also responsible for the annual review of policies and procedures and administering training to AiDASH employees. The information security team includes members of management independent from control operators and, with the assistance from key members of the engineering team, conducts formal risk assessments. Additionally, responsible for ongoing security operations program, system monitoring, vulnerability management, firewalls, and incident response.
- **IT and DevOps:** Responsible for maintaining the availability of production infrastructure and managing access and security for production infrastructure. Only members of the devops team have access to the production environment. Members of the devops team may also be members of the engineering team. Also responsible for managing laptops, software, and other technology involved in employee productivity and business operations, as well as for access controls, security of the production environment, vulnerability, incident management, and solving information security issues.
- **Human Resources:** Responsible for recruiting and onboarding new personnel, defining roles and positions for new hires, performing background checks, and facilitating the employee termination process.
- **Customer Success:** Responsible for sales, account management, customer success, and customer support activities.

Data

Data, as defined by AiDASH, constitutes the following:

Sensitivity Level	Description	Examples of Data
Confidential	Highly sensitive data requires the highest levels of protection; access is restricted to specific employees or departments, and these records can only be passed to others with approval from the data owner or a company executive.	• Customer data • Company financial and banking data • Salary, compensation, and payroll information • Strategic plans • Incident reports • Risk assessment reports • Technical vulnerability reports • Authentication credentials • Secrets and private keys • Source code • Litigation data
Restricted	AiDASH proprietary information requires 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 • Email
Public	Documents intended for public consumption which can be freely distributed outside AiDASH.	• Marketing materials • Product descriptions • Release notes • External facing policies • Company blog • Press releases

The AiDASH System processes the information types as described in the table above. To assist with the data handling procedures, AiDASH has a documented Data Management Policy that defines system and operational requirements for data classification, retention, encryption, storage, and secure disposal. The policy is reviewed and updated accordingly on at least an annual basis by management. Information assets are assigned a sensitivity level based on the audience for the information. Integrity checks are in place at the application level to help ensure data integrity. 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 types are to be assigned a sensitivity level as explained in the above table.

Processes and Procedures

AiDASH has developed and communicated policies and procedures to manage the information security of the system. Policies are reviewed on an annual basis and changes are made to the policies when necessary. Policies are approved by the infosec team on an annual basis. These policies and procedures cover the following key security life cycle areas:

- Access Control
- Asset Management
- Breach Notification
- Business Continuity and Disaster Recovery
- Code of Conduct
- Comprehensive Security
- Cryptography
- Data Management
- Human Resources Security
- Incident Response
- Info Transfer
- Information Security
- Information Security Roles and Responsibilities
- Operations Security
- Patch and Vulnerability Management
- Physical Security
- Risk Management
- Secure Development
- Third-party Management

Relevant Aspects of the Control Environment, Risk Assessment, Information and Communication, and Monitoring

The applicable trust services criteria and related controls are included in Section IV, they are an integral part of AiDASH's description of the system. This section provides information about the five interrelated components of internal control at AiDASH, including:

- Control environment
- Risk assessment
- Control activities
- Information and communication
- Monitoring controls

Control Environment

Integrity and Ethical Values

AiDASH has developed a Code of Conduct that addresses acceptable business practices, conflicts of interest, and expected standards of ethical and moral behavior. The company has also developed employee statement of confidentiality agreements that prohibit inappropriate use and disclosure of customer or company information. These documents are provided to all new employees and other personnel as needed. All personnel are required to sign an acknowledgement form that they received and agree to follow the Code of Conduct, information security policies, and statement of confidentiality agreement within 30 days of hire. The Code of Conduct, information security policies and statement of confidentiality must be re-signed in the event of changes to the documents.

Executive Management Oversight

AiDASH's control awareness is significantly influenced by its board of directors and executive leadership. Attributes that define “tone at the top” include executive leadership’s experience of its members, their involvement and scrutiny of operational activities, and their interaction with independent assessments of the company’s operations and information security posture.

Management’s Philosophy and Operating Style

AiDASH's control environment reflects the philosophy of management. AiDASH's infosec team meets frequently, including at least annually to review policies and procedures and set the information security program roadmap. These policies and procedures are published on internal collaboration tools which are accessible to all personnel. The infosec team, under the direction of corporate and board of directors, oversees the security activities and communication of its policies and procedures.

Authority and Responsibility

Management and employees are assigned levels of authority and responsibility to facilitate internal control. In addition to dedicated infosec, IT, and devops teams, each policy has an individual owner with accountability and authority over policy enforcement, supported by management. Roles and responsibilities for information security within the company are documented and reviewed annually.

Additionally, AiDASH has a documented organizational chart to communicate key areas of authority, responsibility, and lines of reporting to personnel that support the design, development, implementation, operation, maintenance, and monitoring of the system.

Human Resources

The company maintains formal hiring and termination policies and procedures. AiDASH has defined job descriptions for personnel responsible for designing, developing, implementing, operating, monitoring, and maintaining the system. To fill these job roles, candidates are evaluated against job requirements through a formal interview process. Interview notes and prospective personnel resumes are shared internally between interviewers. Additionally, competency evaluations may include reference checks, education and certification validations, and technical testing.

Background or verification checks are performed on personnel, as permitted by local laws, prior to gaining access to production. If an employee violates the Code of Conduct or the company's policies, or otherwise acts in a manner deemed contrary to the mission and objectives of the company, the employee is subject to sanctions up to and including termination of employment.

AiDASH maintains training programs to promote awareness of information security requirements. All employees are required to complete security awareness training within 30 days of hire and annually thereafter, as required by the Information Security Policy. The training courses cover basic information security practices and are designed to assist employees in identifying and responding to social engineering attacks and in avoiding inappropriate security practices.

Management evaluates employee performance on an annual basis against their job performance, job function, and company objectives.

Risk Assessment

AiDASH regularly reviews the risks that may threaten the achievement of its service commitments and system requirements related to the applicable trust services criteria set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, and Confidentiality* (AICPA, Trust Services Criteria).

The infosec team assesses risks on an ongoing basis and discusses these risks annually. These items may include evaluation of environments, regulatory, and technical changes that have occurred. This is done through regular management meetings with IT personnel, reviewing and acting upon security event logs, performing vulnerability assessments, and conducting a formal annual risk assessment in conjunction with company-wide risk assessments.

The annual risk assessment is performed by the infosec team and approved by corporate who are responsible for communicating detected risks and remediation steps needed to the appropriate staff for resolution.

Results and action items are communicated to the respective owners and tracked through internal risk management tools (i.e., Sprinto). As part of the assessment, risks affecting the organization and recommended courses of action are identified and discussed.

Where applicable, mitigating controls are recommended and implemented to address the risks.

Management realizes that the potential for fraud can occur when employees are motivated by certain pressures or incentivized to commit fraud. The absence of controls, or ineffective controls, provides an opportunity for fraud when combined with an incentive to commit fraud. Therefore, management considers fraud factors in each risk evaluated during the risk assessment process.

The infosec team, as part of its annual Information Security Policy review, considers developments in technology and the impact of applicable laws and regulations on AiDASH's security policies.

Risks related to external parties (such as contractors and vendors) are identified and addressed based on its procurement and third-party risk management program. Designated responsibilities are defined in reviewing risks associated with external parties and establishing relevant agreements.

Additionally, confidentiality agreements are in place for vendors with access to customer data.These agreements define service levels, processing specifications, rules of use, and additional terms for governing use of the system.

AiDASH has a process in place for evaluating vendor performance and compliance with contractual obligations. An annual third party risk assessment is performed including a review of attestation reports (i.e., SOC 2, ISO) for critical vendors where user data is shared. Results and action items are communicated to the respective owners and tracked through internal risk management tools.

Changes in security threats and risks are reviewed by the IT and devops teams, and updates to existing control activities and information security policies are performed as necessary.

Control Activities

AiDASH's control activities are defined through its established policies and procedures which address individual risks associated with the achievement of the company's objectives. Such statements may be documented, explicitly stated in communications, or implied through actions and decisions. Policies serve as the basis for procedures. Control activities are deployed through policies that establish what is expected and procedures that put policies into action.

Logical Access Control

Access provisioning

AiDASH has implemented role-based security to limit and control access within the system. Employees are granted logical access to in-scope systems based on documented approval by management personnel in accordance with need-to-know and least-privilege access principles. The ability to create or modify user access accounts and user access privileges is limited to the infosec and IT and devops teams.

Access Deprovisioning

There is a termination process to help ensure access is removed within 72 business hours of termination or when access is no longer required. The termination process begins with human resources notifying application owners to remove access to the corresponding application. Once completed, the application owner will notify human resources that access is severed. To ensure no inappropriate access is retained, an offboarding checklist is used to document the removal of access to systems.

Access Reviews

User access is reviewed quarterly by senior members of infosec, IT, and devops teams to determine if an individual's access is necessary for their job functions and to identify the existence of unnecessary, terminated, or over-privileged accounts. Access issues, if any, are remediated during the review and resolved.

Privileged Access

Administrative access to infrastructure systems is restricted to the IT and devops teams who have a business justification to possess elevated privileges. Unique user identification numbers, names, and passwords or tokens are required to authenticate users to the system. Powerful service/system accounts and keys are appropriate and are either restricted from direct user authentication or authorized to unique users through a password vault or equivalent security solution. User access key permission set templates, by default, are configured to allow a maximum of 12 hour sessions.

Additionally, access to the root account is configured to alert system administrators and record a log of all activity. The root account is enabled for the IT and devops team based on business needs. Business justifications are documented for each instance of root usage.

Authentication

Password parameters systematically enforce the company's Password Policy: eight characters, one uppercase, one number, one lowercase, and one special character. Additionally, access to cloud services or remote access systems requires MFA.

Physical Access and Environmental Controls

No servers or computer facilities supporting the AiDASH System are hosted on site at AiDASH facilities. All servers or computer facilities and physical access thereto are controlled at cloud infrastructure data centers. Therefore, controls related to physical security are the responsibility of the subservice organizations and are described in the complementary subservice organization controls presented in this system description.

Incident Management

AiDASH defines a security incident as a violation, or imminent threat of violation, of security policies, acceptable use policies, or standard security practices. An operational incident is an event that impacts the company's ability to meet availability SLAs or impairs processing capabilities. AiDASH leverages the NIST incident response lifecycle for preparing, detecting, analyzing, triaging, and performing postmortem reviews over incidents.

Preparation

AiDASH has an incident management framework that includes defined processes, roles, communications, responsibilities, and procedures for detection, escalation, and response to incidents internally and to customers. This framework is communicated to all personnel and maintained by incident response teams. Externally, descriptions of the system and its boundaries are available to external users via ongoing communications with customers, official blog posts, and through status portals. Customer incidents, if any, are reported and resolved through one-to-one communication via the customer ticketing system. Policy and procedure documentation for incident management, which includes the responsibility and escalation levels for reporting operational failures, security incidents, system problems, user complaints, and the process for doing so, is made available to internal and external users. Additionally, an information IT and devops narrative with roles and responsibilities is documented in the Information Security Policy and approved annually by management. The IT and devops team are responsible for the oversight of internal control and include members independent from control operators.

AiDASH prevents incidents via annual risk assessments, effective network security, anti-malware on devices, and security awareness training.

Detection and Analysis

Incident response procedures and centralized tracking tools consist of different channels for reporting production system incidents and weaknesses.

Automated mechanisms include system monitoring processes that alert the IT and devops team per configured events, thresholds, or metric triggers. Incidents may also be reported via email.

Monitoring and alarming are configured to identify and notify management of incidents when thresholds are crossed on key security and operational metrics. Issues are resolved in accordance with incident management processes.

Incidents are prioritized and ranked based on severity. Incident ratings and escalation procedures are as follows:

Incident Rating	Description	Escalation Procedures
Low and Medium	Issues meeting this severity are simply suspicions or odd behaviors. They are not verified and require further investigation. There is no clear indicator that systems have tangible risk and do not require emergency response. This includes lost/stolen laptops with disk encryption, suspicious emails, outages, strange activity on a laptop, etc.	A security Jira with P3/P4 label ticket must be created and assigned to the appropriate department for response.
High	High severity issues relate to problems where an adversary or active exploitation has not been proven yet, and may not have happened, but is likely to happen. This may include lost/stolen laptops without encryption, vulnerabilities with direct risk of exploitation, threats with risk or adversarial persistence on our systems (e.g., backdoors, malware), malicious access of business data (e.g., passwords, vulnerability data, payments information), or threats that put any individual at risk of physical harm.	A security Jira with P2 label ticket that should be created in case of a P2 event or incident. Tickets must be completed, and the appropriate manager must also be notified via chat and email with a reference to the ticket number.
Critical	Critical issues relate to actively exploited risks and involve a malicious actor. Identification of active exploitation is required to meet this severity category.	A security Jira with P1 label ticket that should be created in case of a P1 event or incident. Additionally, require immediate notification to IT and engineering management.

Where required, security incidents are escalated to infosec, IT and devops, or corporate team(s).

Containment, Eradication, and Recovery

Containment strategies should be identified and implemented before an incident overwhelms resources or increases damage. Information security key performance indicators (KPIs) are monitored continuously using automated tools that are configured to alert system administrators of activity that falls outside of predefined thresholds during the containment phase. Containment strategies vary based on the type of incident. Criteria for determining the appropriate containment strategy include:

- Potential damage to and theft of resources;
- Need for evidence preservation;
- Service availability (e.g., network connectivity, services provided to external parties);
- Time and resources needed to implement the strategy;
- Effectiveness of the strategy (e.g., partial containment, full containment); and,
- Duration of the solution (e.g., emergency workaround to be removed in four hours, temporary workaround to be removed in two weeks, permanent solution).

After an incident has been contained, eradication may be necessary to eliminate components of the incident, such as deleting malware and disabling breached user accounts, as well as identifying and mitigating all vulnerabilities that were exploited. During eradication, all affected hosts within the organization are identified and remediated.

In recovery, administrators restore systems to normal operation, confirm that the systems are functioning normally, and (if applicable) remediate vulnerabilities to prevent similar incidents. A documented business continuity and disaster recovery plan is in place and is tested and approved annually. Recovery may involve such actions as restoring systems from clean backups, rebuilding systems from scratch, replacing compromised files with clean versions, installing patches, changing passwords, and tightening network perimeter security. Backups of critical system components are performed at least daily and play a key role in system recovery.

Post-incident Activity

Post-mortem activities are conducted for incidents with critical and high severity ratings. Results of post-mortems may include updates to the security program or changes to systems required as a result of incidents. Additionally, log file validation is enabled to create a digitally signed digest file containing a hash of each log that writes to file shares which may also be reviewed during the post incident activity.

Network Operations Monitoring

Web applications are protected by deploying AWS security groups that inspect ingress traffic. The network is segmented based on the label or classification level of the information stored on the servers. This includes filtering between VPCs environments to help ensure only authorized systems can communicate with other systems necessary to fulfill their specific responsibilities. A variety of security utilities to identify and detect possible security threats and incidents. These utilities include, but are not limited to, firewall notifications, IDS, vulnerability assessment reports, and operating system event logs.

Security or operational events requiring further investigation are tracked using internal ticketing systems and monitored until resolved in accordance with defined SLAs.

AiDASH only uses network ports, protocols, and services listening on a system with validated business need to run on each system. Default-deny rules drop traffic except those services and ports that are explicitly allowed.

Cryptography

Strong cryptography standards for storage of data are enforced in accordance with the Cryptography Policy and customer commitments. User requests to AiDASH's systems are encrypted using TLS 1.2 using certificates from an established third-party certificate authority. Remote system administration access to AiDASH web and application servers is available through cryptographic network protocols (i.e., SSH). Data at rest is encrypted using at least Advanced Encryption Standard (AES) 256 bit.

Baseline Configuration Hardening

AiDASH maintains documented security configuration standards, including secure images or templates, for authorized operating systems and software in the enterprise. System deployments are imaged using one of these master images or templates. Master images are stored on securely configured servers and validated with integrity monitoring tools, to help ensure only authorized changes to the images are possible. To help detect and enforce system configuration standards, management tools automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals.

Before deploying any new asset, servers are hardened using configuration standards which are applied through automated deployment mechanisms to help ensure consistent application.

Change Management

AiDASH has a formalized security and systems development methodology that includes project planning, design, testing, implementation, maintenance, and disposal or decommissioning.

To initiate a change, the developer creates a feature branch on their local machine. Code changes are grouped into diffs, each of which represents a proposed change to the codebase. After a developer finishes a feature branch, they will make a pull request to merge those changes into the master branch. After this, the change will automatically be sent for a peer review.

Changes to infrastructure and software are developed and tested in a separate development or test instance before implementation. Customer content and personal information is not used in test and development instances.

Prior to migration to production, proposed changes are peer reviewed to determine if they present a security risk and what mitigating actions, including employee and customer notifications, must be performed. Access to migrate change to production is restricted to authorized personnel. Per the required branch protection settings, users may not bypass the standard change control configurations and must obtain at least one approval before the code is merged to production. For all code changes, the reviewer must be different from the developer. Changes are manually tested according to the nature of the change in an environment separate from production prior to deployment into a production release. Additionally, the change must pass static and dynamic code tested before it is merged. Change control, as defined by policy, requires approval and a peer review prior to implementation to help ensure change requirements are met, and security issues are resolved.

After all developing, testing, and reviewing criteria are met, the pull request is merged, and the change is implemented into production. The system is monitored continuously.

Should the site be negatively affected by a change, that code change is rolled back. Security analysis is performed to verify secure coding practices are followed during change control. Vulnerabilities identified, if any, are tracked to resolution.

AiDASH uses a standardized server build checklist to help secure its servers. Patches are applied regularly as part of change management release cycles and deployed through automatic patch update tools. Automated software update tools are used to help ensure the operating systems are running the most recent security updates approved by management.

Software Security Assurance

Secure coding practices are established based on the programming language and development environment used. In-house developed software includes explicit error checking and documented inputs, including size, data type, and acceptable ranges or formats. Static and dynamic analysis tools are used to verify that secure coding practices are adhered to for internally developed software. Issues identified follow a process to accept and address reports of software vulnerabilities.

Asset Management (Hardware and Software)

Assets used in the system are inventoried or tagged to include business descriptions, asset ownership, versions, and other configuration levels, as appropriate, to help ensure assets are classified appropriately, patched, and tracked as part of configuration management. AiDASH uses tagging tools (i.e., Sprinto, Jamf, Microsoft Intune) to automatically facilitate the company's hardware and software asset inventory. This helps to ensure a complete and accurate inventory of technology assets, with the potential to store or process information, is maintained.

Vulnerability Management and Penetration Testing

Vulnerability scanning tools are used to automatically scan systems on the network continuously to identify potential vulnerabilities. Issues, if any, are routed through change and risk management processes for resolution and resolved in accordance with the service-level agreements for high, medium, and low risk rankings. Vulnerabilities identified are risk-ranked to prioritize the remediation of discovered vulnerabilities.

External penetration testing is performed at least annually and includes a full scope of blended attacks, such as client-based and web application attacks. Issues, if any, are tracked through risk management processes and tools to resolution.

Endpoint Management

Endpoint management solutions are in place that include policy enforcement on company issued devices (i.e., mobile phones and laptops), as well as bring-your-own devices that could connect to or access data within the system boundaries. Policies enforced on endpoints include controls such as:

- Enforce encryption on devices for data at rest; and,
- Anti-malware software to continuously monitor and defend each of the organization's workstations and servers.

Availability

AiDASH has a documented business continuity and disaster recovery plan which is reviewed and tested annually through tabletop exercises, failover testing, test restores, etc.

At a minimum, daily backup schedules are maintained to protect sensitive data from loss in the event of a system failure. Backups are restored regularly as part of operational activities and included as part of the BC/DR test plan. Additionally, critical system components are replicated across multiple availability zones or regions to permit the resumption of critical operations in the event of loss of a critical facility.

Confidentiality

AiDASH has confidentiality commitments with their customers as described in terms and conditions set forth within master service agreements, which must be signed before services start. Additionally, confidentiality agreements are in place for vendors with access to customer data. These agreements define service levels, processing specifications, rules of use, and additional terms for governing use of the system.

AiDASH has documented policies and procedures to support customer confidentiality commitments which include a Cryptography Policy, Data Management Policy, and Information Security Policy. Collectively, these policies provide AiDASH employees with appropriate insight into the required procedures to help ensure customer data remains confidential. The Data Management Policy is in place that defines system and operational requirements for data classification, retention, encryption, storage, and secure disposal. These policies are reviewed and updated accordingly on at least an annual basis.

Customer data will be deleted in accordance with the Data Management Policy and within 60 days of service termination and receiving data deletion requests. For disposal requests, a confirmation is sent back to the customer to notify them that the disposal is complete.

Processing Integrity

AiDASH leverages Datadog to collect and store log data for 15 days. Additionally, CloudTrail is used to zip log files from the S3 buckets within the JSON format. The log file contains the object detail, hash value, and digital signature of the previous digest file. Integrity checks are in place at the application level and file system level to help ensure data integrity. If an integrity check fails, the issue is remediated per the normal change procedure and added to the FAQ and known issues listing pertaining to the integrity check or job for further future troubleshooting accessibility.

To help ensure the integrity of work quality, job schedules and run books are documented and jobs are scheduled to help ensure data is processed for completeness, accuracy, and timeliness. Additionally, AiDASH performs checks to ensure at least 85% precision and accuracy of outputs in accordance with system guides. Issues, if any, are resolved before delivery of the model to production.

Information and Communication

AiDASH has an Information Security Policy to help ensure employees understand their individual roles and responsibilities concerning processing and controls to ensure significant events are communicated in a timely manner. These include formal and informal training programs and the use of email to communicate time-sensitive information and processes for security and system availability purposes that notify key personnel in the event of problems. Internally, the company maintains internal informational websites describing the system environment, its boundaries, user responsibilities, and services. System documentation includes security and hardening guides to help ensure effective configuration, installation, and operation of the information system.

Externally, descriptions of the system and its boundaries are available to external users via ongoing communications with customers, official blog posts, and customer agreements. Customer incidents, if any, are reported and resolved through one-to-one communication via the customer ticketing system.

Monitoring Controls

In addition to daily oversight and ongoing vulnerability scans, information security KPIs are monitored continuously using automated tools (i.e., Sprinto) that are configured to alert the infosec and IT and devops teams of activity that falls outside of predefined thresholds.

Changes to the System During the Period

There were no changes that are likely to affect report users' understanding of how the system is used to provide the service during the period from April 1, 2024 to March 31, 2025.

Disclosure of Incidents

There were no system incidents during the period from April 1, 2024 to March 31, 2025, requiring disclosure that either:

- Were the result of controls failing; or,
- Resulted in a significant impairment to the achievement of systems requirements or service commitments to customers.

Complementary User Entity Controls and Responsibilities

Complementary User Entity Controls

There are no controls at the user entity that are necessary, in combination with AiDASH's controls, to provide reasonable assurance that AiDASH's service commitments and system requirements were achieved based on the applicable trust services criteria.

User Entity Responsibilities

There are, however, certain responsibilities that users of the system must fulfill for the user entity to derive the intended benefits of the services of the AiDASH System. The user entity responsibilities presented below should not be regarded as a comprehensive list of all controls that should be employed by user entities. User entities are responsible for their own control environments and their operational effectiveness.

User Entity Responsibilities	Criteria
User entity is responsible for protecting established user IDs and passwords within their organizations.	CC6.1, CC6.2
User entity is responsible for sending data to AiDASH via a secure connection and/or the data should be encrypted.	CC6.7
User entity is responsible for reviewing customer access to AiDASH's system periodically to validate appropriateness of access levels.	CC6.1, CC6.2
User entity is responsible for approving and creating new user access to AiDASH's system.	CC6.1, CC6.2
User entity is responsible for removing terminated employee access to AiDASH's system.	CC6.3
User entity is responsible for implementing policies and procedures over the types of data that are allowed to be entered into AiDASH's system.	C1.1, CC5.3
User entity is responsible for notifying AiDASH if they detect or suspect a security incident related to AiDASH's system.	CC7.4
User entity is responsible for reviewing email and other forms of communications from AiDASH, related to changes that may affect AiDASH customers and users, and their security or availability obligations.	CC2.3, CC7.1, CC7.2, CC7.3, CC7.4, CC7.5
User entity is responsible for endpoint protection of workstations used to access the system.	CC6.5, CC6.6, CC6.7, CC6.8, CC7.2
User entity is responsible for developing and testing their own business continuity and disaster recovery plan.	A1.1, A1.2, A1.3, CC7.4, CC7.5, CC9.1
User entity is responsible for inputting accurate data to the AiDASH System.	PI1.1, PI1.2

Complementary Subservice Organization Controls

AiDASH uses subservice organizations in support of its system. AiDASH's controls related to the system cover only a portion of overall internal control for customers. It is not feasible for the trust services criteria over the AiDASH System to be achieved solely by AiDASH. Therefore, customer controls must be evaluated in conjunction with AiDASH's controls described in Section IV of this report, taking into account the related complementary subservice organization controls expected to be implemented at the subservice organizations as described below.

AiDASH periodically reviews the quality of the outsourced operations by various methods including:

- Review of subservice organizations' attestation or certification reports
- Regular meetings to discuss performance
- Non-disclosure agreements

Control Activity Expected to be Implemented by Subservice Organizations	Subservice Organizations	Applicable Criteria
Logical access to the underlying network and virtualization management software for the cloud architecture is appropriate.	AWS, Microsoft	CC6.1, CC6.2, CC6.3, CC6.5, CC7.2
Physical access to the data center facility is restricted to authorized personnel.	AWS, Microsoft, Bitbucket, 1Password	CC6.4, CC6.5
Environmental protections, including monitoring and alarming mechanisms, are implemented to address physical security and environmental control requirements.	AWS, Microsoft, Bitbucket, 1Password	CC6.4, A1.2
Business continuity and disaster recovery procedures are developed, reviewed, and tested periodically.	AWS, Microsoft, Bitbucket, 1Password	A1.3
A defined Data Management Policy specifies classification levels and control requirements in order to meet the company's commitments related to confidentiality.	AWS	C1.1
A defined process is in place to sanitize and destroy hard drives and backup media containing customer data prior to leaving company facilities.	AWS	C1.2

Section IV

Description of Criteria, AiDASH's Related Controls, and BARR Advisory, P.A.'s Tests of Controls and Results

Procedures for Assessing Completeness and Accuracy of Information Provided by the Entity (IPE)

For tests of controls requiring the use of IPE (e.g., controls requiring system-generated populations for sample-based testing), BARR Advisory, P.A. performed a combination of the following procedures, where possible, based on the nature of the IPE to address the completeness, accuracy, and data integrity of the data or reports used:

1. Inspect the source of the IPE;
2. Inspect the query, script, or parameters used to generate the IPE;
3. Tie data between the IPE and the source; and/or,
4. Inspect the IPE for anomalous gaps in sequence or timing to determine the data is complete, accurate, and maintains its integrity.

In addition to the above procedures, for tests of controls requiring management's use of IPE in the execution of controls (e.g., periodic reviews of user access lists), BARR Advisory, P.A. inspected management's procedures to assess the validity of the IPE source and the completeness, accuracy, and integrity of the data or reports.

AiDASH Controls Mapped to the Security, Confidentiality, Availability, and Processing Integrity Criteria

Criteria	Supporting Control	Criteria Description
1.0 – Common Criteria Related to Control Environment		
CC1.1	HR-01, HR-02, IS-02, IS-03	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.
CC1.2	IS-01, RC-01	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.
CC1.3	HR-03, IS-01, IS-02, IS-03, IS-04, IS-05	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.
CC1.4	HR-01, HR-02, IS-01, IS-02, IS-03, IS-04, IS-05	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.
CC1.5	HR-02, HR-03, IS-01, IS-02, IS-03, IS-04, IS-05, RC-03	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.
2.0 – Common Criteria Related to Information and Communication		
CC2.1	AM-01, RC-01, RC-03, TV-01, TV-02	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.
CC2.2	IS-01, IS-02, IS-03, IS-04, IS-05, IS-06, OM-01, RC-03	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.
CC2.3	IS-07, OM-02, OM-03, RC-04	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.
3.0 – Common Criteria Related to Risk Assessment		
CC3.1	IS-01, RC-01, RC-03	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.

Criteria	Supporting Control	Criteria Description
CC3.2	AM-01, RC-01, RC-02, RC-03, TV-01, TV-02	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.
CC3.3	IS-03, RC-01, RC-02	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.
CC3.4	IS-03, RC-01, RC-02, RC-03	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.
4.0 – Common Criteria Related to Monitoring Activities		
CC4.1	OM-01, RC-01, RC-02, RC-03, TV-01	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.
CC4.2	RC-01, RC-02, RC-03, TV-01	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.
5.0 – Common Criteria Related to Control Activities		
CC5.1	IS-01, IS-03, RC-01, RC-03	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.
CC5.2	IS-01, IS-03, RC-01	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.
CC5.3	HR-02, IS-01, IS-03, RC-03	COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.
6.0 – Common Criteria Related to Logical and Physical Access		
CC6.1	AC-01, AC-02, AC-03, AC-04, AC-05, AC-06, AC-07, AC-08, AC-09, AM-01, CR-02, IS-08, SC-01	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.
CC6.2	AC-01, AC-04, AC-05, AC-06, AC-07	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.

Criteria	Supporting Control	Criteria Description
CC6.3	AC-03, AC-04, AC-06, AC-07, AC-09, AC-10, IS-08	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.
CC6.4	N/A - See complementary subservice controls	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.
CC6.5	AC-06, AM-01, TV-03	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	AC-03, AC-04, AC-05, AC-08, CR-01, CR-02, OM-01, SC-01, TV-01, TV-03	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.
CC6.7	AC-05, AC-08, AM-01, CR-01, CR-02, OM-01, SC-01, TV-03	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.
CC6.8	AC-08, AM-01, CM-04, CR-01, OM-01, TV-01, TV-03	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.
7.0 – Common Criteria Related to System Operations		
CC7.1	AC-08, AM-01, CM-04, OM-01, OM-02, TV-01, TV-02	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.
CC7.2	AC-02, AM-01, OM-01, OM-02, RC-03, TV-01, TV-02, TV-03	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.
CC7.3	OM-01, OM-02, RC-03, TV-01, TV-02	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.

Criteria	Supporting Control	Criteria Description
CC7.4	BC-01, OM-01, OM-02, TV-01, TV-02	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.
CC7.5	BC-01, IS-01, OM-01, OM-02, TV-01	The entity identifies, develops, and implements activities to recover from identified security incidents.
8.0 – Common Criteria Related to Change Management		
CC8.1	AC-09, CM-01, CM-02, CM-03, CM-04, CM-05	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.
9.0 – Common Criteria Related to Risk Mitigation		
CC9.1	BC-01, BC-02, OM-01, RC-01, RC-05	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.
CC9.2	IS-01, RC-01, RC-02, RC-04	The entity assesses and manages risks associated with vendors and business partners.
Additional Criteria for Confidentiality		
C1.1	CM-03, CR-01, CR-02, IS-03, IS-08, OM-04	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.
C1.2	IS-03, IS-08, OM-04	The entity disposes of confidential information to meet the entity's objectives related to confidentiality.
Additional Criteria for Availability		
A1.1	BC-01, BC-02, BC-03, OM-01	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.
A1.2	BC-01, BC-03, RC-01	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.
A1.3	BC-01	The entity tests recovery plan procedures supporting system recovery to meet its objectives.

Criteria	Supporting Control	Criteria Description
Additional Criteria for Processing Integrity		
PI1.1	IS-08, OM-03, OM-05	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.
PI1.2	OM-05, OM-08	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.
PI1.3	OM-03, OM-06, OM-07	The entity implements policies and procedures over system processing to result in products, services, and reporting to meet the entity's objectives.
PI1.4	OM-05, OM-06, OM-07, OM-08	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.
PI1.5	OM-05, OM-06, OM-08	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.

Security, Confidentiality, Availability, and Processing Integrity Criteria Mapped to AiDASH Controls, BARR Advisory, P.A.'s Tests, and Test Results

No.	Description of Controls	Criteria	Tests of Controls and Test Results
AC-01	Powerful service/system accounts and keys are appropriate and are either restricted from direct user authentication or authorized to unique users through a password vault or equivalent security solution.	CC6.1 CC6.2	Inquired of management and inspected the Access Control Policy, system-generated lists of powerful service/system accounts and access keys, and password vault evidence to determine if powerful service/system accounts and keys were appropriate and were either restricted from direct user authentication or authorized to unique users through a password vault or equivalent security solution in accordance with company requirements. **No exceptions noted.**
AC-02	Root level account usage is appropriate and logged with alerting configured. Business justifications are documented for each instance of root usage.	CC6.1 CC7.2	Inquired of management and inspected the Access Control Policy, log configuration settings, and root log to determine if root usage was logged and information security teams were alerted when accessed in accordance with company requirements. Inquired of management and inspected documentation for a selection of alerts, if any, to determine if root access was limited to appropriate instances with a reasonable business justification in accordance with company requirements. **No exceptions noted.**

No.	Description of Controls	Criteria	Tests of Controls and Test Results
AC-03	Administrator access is restricted to authorized system and security administrators.	CC6.1 CC6.3 CC6.6	Inquired of management and inspected the Access Control Policy, system-generated lists, and administrator access privileges for systems in the Primary Infrastructure and Software table to determine if administrator access was restricted to authorized system and security administrators in accordance with company requirements. **No exceptions noted.**
AC-04	User access is approved by management in accordance with the Access Control Policy based on least privilege access principles.	CC6.1 CC6.2 CC6.3 CC6.6	Inquired of management and inspected the Access Control Policy and onboarding forms for a selection of new users to determine if access was provisioned as approved by management based on least privilege access principles in accordance with company requirements. **No exceptions noted.**
AC-05	Password configuration settings are documented and systematically enforced in compliance with the Access Control Policy. Access to cloud services or remote access systems requires multi-factor authentication.	CC6.1 CC6.2 CC6.6 CC6.7	Inquired of management and inspected the Access Control Policy and password configurations for systems in the Primary Infrastructure and Software table to determine if password configuration settings were documented and systematically enforced and MFA was required to access cloud services or remote access systems in accordance with company requirements. **No exceptions noted.**
AC-06	Terminated user access is removed within 72 business hours in accordance with the Access Control Policy.	CC6.1 CC6.2 CC6.3 CC6.5	Inquired of management, inspected the Access Control Policy, system-generated user lists from systems within the Primary Infrastructure and Software table, and offboarding checklists for a sample of terminated users to determine if access was removed within 72 business hours in accordance with company requirements. **No exceptions noted.**

No.	Description of Controls	Criteria	Tests of Controls and Test Results
AC-07	User profile and access reviews are performed each quarter and include active user accounts for employees and contractors. Access issues, if any, are resolved.	CC6.1 CC6.2 CC6.3	Inquired of management and inspected the Access Control Policy, access review documentation for a selection of quarters, and system-generated user lists to determine if access reviews were completed for systems in the Primary Infrastructure and Software table and access issues were resolved in accordance with company requirements. **No exceptions noted.**
AC-08	Upon deployment, servers are hardened using configuration standards which are applied through automated deployment mechanisms to help ensure consistent application.	CC6.1 CC6.6 CC6.7 CC6.8 CC7.1	Inquired of management, inspected the Operations Security Policy, security configuration standards, and server deployment process to determine if servers were hardened via automated deployment mechanisms to help ensure consistent application in accordance with company requirements. **No exceptions noted.**
AC-09	Access to migrate change to production is restricted to authorized personnel.	CC6.1 CC6.3 CC8.1	Inquired of management and inspected the Operations Security Policy, a system-generated list of users with access to migrate change to production, and branch protection settings to determine if access was restricted to authorized personnel and if branch protection settings were enforced that restricted users from bypassing standard change control in accordance with company requirements. **No exceptions noted.**

No.	Description of Controls	Criteria	Tests of Controls and Test Results
AC-10	User access key permission set templates, by default, are configured to allow a maximum of 12 hour sessions.	CC6.3	Inquired of management and inspected the Cryptography Policy and configuration settings on the infrastructure environment to determine if user access key permission set templates, by default, were configured to allow a maximum of 12 hour sessions in accordance with company requirements. **No exceptions noted.**
AM-01	Assets used in the system are inventoried or tagged to include business descriptions, asset ownership, versions, and other configuration levels to help ensure assets are classified appropriately and tracked as part of configuration management.	CC2.1 CC3.2 CC6.1 CC6.5 CC6.7 CC6.8 CC7.1 CC7.2	Inquired of management and inspected the Asset Management Policy and current asset inventory to determine if assets used in the system were inventoried or tagged to include business descriptions, asset ownership, versions, and other configuration levels, as appropriate, to help ensure assets were classified appropriately and tracked as part of configuration management in accordance with company requirements. **No exceptions noted.**
BC-01	A documented business continuity and disaster recovery plan is in place, tested, and approved on an annual basis.	A1.1 A1.2 A1.3 CC7.4 CC7.5 CC9.1	Inquired of management and inspected the business continuity and disaster recovery plan to determine if it was in place and approved on an annual basis in accordance with company requirements. Inspected the most recent business continuity and disaster recovery test to determine if the plan was tested within the last year in accordance with company requirements. **No exceptions noted.**

No.	Description of Controls	Criteria	Tests of Controls and Test Results
BC-02	Critical system components are replicated across multiple availability zones or regions to permit the resumption of critical operations in the event of loss of a critical facility.	A1.1 CC9.1	Inquired of management and inspected backup configuration settings to determine if critical system components were replicated across multiple availability zones or regions to permit the resumption of critical operations in the event of loss of a critical facility in accordance with company requirements. **No exceptions noted.**
BC-03	Backups of critical system components are performed at least daily.	A1.1 A1.2	Inquired of management and inspected the Operations Security Policy, backup configurations, and backup logs of critical system components to ensure they were performed at least daily in accordance with company requirements. **No exceptions noted.**
CM-01	Change control, as defined by policy, requires approval and a peer review prior to implementation to help ensure change requirements are met and security issues are resolved.	CC8.1	Inquired of management and inspected the Secure Development Policy and documentation for a selection of changes to determine if changes were approved, a peer review performed, and security issues were resolved prior to implementation and in accordance with company requirements. **No exceptions noted.**
CM-02	Changes are tested according to the nature of the change in an environment separate from production prior to deployment into a production release.	CC8.1	Inquired of management and inspected the Operations Security Policy and change tickets for a selection of changes to determine if changes were tested according to the nature of the change in an environment separate from production prior to deployment into a production release in accordance with company requirements. **No exceptions noted.**

No.	Description of Controls	Criteria	Tests of Controls and Test Results
CM-03	AiDASH uses mock data in non-production environments to prevent personal data, including customer content and personal information, from being used outside of production.	C1.1 CC8.1	Inquired of management, inspected the Operations Security Policy, and observed non-production environments to determine if mock data was used in non production environments to prevent customer content and personal information from being used outside of production in accordance with company requirements. **No exceptions noted.**
CM-04	Automated software update tools are used to help ensure the operating systems are running the most recent security updates approved by management.	CC6.8 CC7.1 CC8.1	Inquired of management and inspected the Operations Security Policy and patch management configuration settings to determine if automated software update tools were used to help ensure the operating systems were running the most recent security updates approved by management in accordance with company requirements. **No exceptions noted.**
CM-05	A security analysis is performed to verify secure coding practices are followed during change control. Vulnerabilities identified, if any, are tracked to resolution.	CC8.1	Inquired of management and inspected the Secure Development Policy and documentation for a selection of code changes to determine if static and dynamic analysis tools were used to verify secure coding practices were followed and vulnerabilities were tracked to resolution in accordance with company requirements. **No exceptions noted.**
CR-01	Remote connections and data in transit over public networks are encrypted using strong encryption protocols such as SSH or TLS 1.2.	C1.1 CC6.6 CC6.7 CC6.8	Inquired of management and inspected the Cryptography Policy and cryptography and security protocols to determine if remote connections and data in transit over public networks were encrypted using strong encryption protocols such as SSH or TLS 1.2 in accordance with company requirements. **No exceptions noted.**

No.	Description of Controls	Criteria	Tests of Controls and Test Results
CR-02	Strong cryptography standards for storage of data are enforced in accordance with the Data Management Policy and customer commitments.	C1.1 CC6.1 CC6.6 CC6.7	Inquired of management and inspected the Data Management Policy, customer commitments, and encryption protocols in place for resources with stored data to determine if strong cryptography standards were enforced in accordance with the Data Management Policy, customer commitments, and company requirements. **No exceptions noted.**
HR-01	Background or verification checks are performed on personnel prior to gaining access to production, as permitted by local laws.	CC1.1 CC1.4	Inquired of management and inspected the Human Resource Security Policy and onboarding records for a selection of new personnel to determine if background or verification checks were performed on personnel prior to gaining access to production, as permitted by local laws, in accordance with company requirements. **No exceptions noted.**
HR-02	Personnel are required to read and accept the Code of Conduct, information security policies, and statement of confidentiality within 30 days of hire. The Code of Conduct, information security policies, and statement of confidentiality must be resigned in the event of changes to the policy.	CC1.1 CC1.4 CC1.5 CC5.3	Inquired of management, inspected the Human Resource Security Policy and acceptance records for a selection of new personnel to determine if new personnel accepted the Code of Conduct, information security policies, and statement of confidentiality within 30 days of hire in accordance with company requirements. **No exceptions noted.** Inquired of management and inspected document revision history and determined there were no significant changes to the content within the last year requiring re-acknowledgment. **Therefore, this portion of the control did not operate during the report period and no conclusion was reached regarding its operating effectiveness.**

No.	Description of Controls	Criteria	Tests of Controls and Test Results
HR-03	AiDASH has a documented organizational chart to communicate key areas of authority, responsibility, and lines of reporting to personnel that support the design, development, implementation, operation, maintenance, and monitoring of the system.	CC1.3 CC1.5	Inquired of management and inspected the AiDASH organizational chart to determine if the company had defined an organizational chart to communicate key areas of authority, responsibility, and lines of reporting to personnel that supports the design, development, implementation, operation, maintenance, and monitoring of the system in accordance with company requirements. **No exceptions noted.**
IS-01	An information security function with roles and responsibilities is documented in the Information Security Policy and approved annually by management. This information security function, which includes the board of directors, is responsible for the oversight of internal control and includes members independent from control operators.	CC1.2 CC1.3 CC1.4 CC1.5 CC2.2 CC3.1 CC5.1 CC5.2 CC5.3 CC7.5 CC9.2	Inquired of management and inspected the Information Security Policy to determine if: • An information security function with roles and responsibilities was documented and approved by management within the last year; and, • The information security function, including the board of directors, was responsible for the oversight of internal control and included members independent from control operators in accordance with company requirements. **No exceptions noted.**
IS-02	AiDASH provides security awareness training to employees within 30 days of hire and annually thereafter, as required by the Information Security Policy.	CC1.1 CC1.3 CC1.4 CC1.5 CC2.2	Inquired of management and inspected the Information Security Policy, Comprehensive Security Policy, and training records for a selection of new and current employees to determine if employees completed security awareness training within 30 days of hire and annually thereafter in accordance with company requirements. **No exceptions noted.**

No.	Description of Controls	Criteria	Tests of Controls and Test Results
IS-03	Information security policies, including sanctions for policy violations, are approved by management at least annually and published on internal collaboration tools accessible to all personnel with access to the company systems.	C1.1 C1.2 CC1.1 CC1.3 CC1.4 CC1.5 CC2.2 CC3.3 CC3.4 CC5.1 CC5.2 CC5.3	Inquired of management and inspected information security policies, policy approval documentation, and sharing permissions to determine if the policies included sanctions for policy violations, were approved by management within the past year, and were published on internal collaboration tools accessible to company personnel with access to the company systems in accordance with company requirements. **No exceptions noted.**
IS-04	AiDASH has defined job descriptions for personnel responsible for designing, developing, implementing, operating, monitoring, and maintaining the system. To fill these job roles, candidates are evaluated against job requirements through a formal interview process.	CC1.3 CC1.4 CC1.5 CC2.2	Inquired of management and inspected the Human Resource Security Policy, documentation of formal job descriptions, and interview notes for a selection of new personnel to determine if AiDASH had defined job descriptions and candidates were evaluated through a formal interview process in accordance with company requirements. **No exceptions noted.**
IS-05	Management conducts annual employee performance evaluations against company objectives.	CC1.3 CC1.4 CC1.5 CC2.2	Inquired of management and inspected the Human Resources Security Policy and performance review documentation for a selection of current employees to determine if management conducted employee performance evaluations against company objectives within the last year in accordance with company requirements. **No exceptions noted.**

No.	Description of Controls	Criteria	Tests of Controls and Test Results
IS-06	The company maintains internal informational websites describing the system environment, its boundaries, user responsibilities, and services. System documentation includes security and hardening guides to help ensure effective configuration, installation, and operation of the information system.	CC2.2	Inquired of management and inspected the Information Security Policy, internal system documents posted on internal collaboration tools, and sharing permissions for internal collaboration tools to determine if the system environment, its boundaries, user responsibilities, services, and security hardening guides were maintained and available to internal users in accordance with company requirements. **No exceptions noted.**
IS-07	Descriptions of the system and its boundaries are available to external users via ongoing communications with customers and official blog posts. Customer incidents, if any, are reported and resolved through one-to-one communication via the customer ticketing system.	CC2.3	Inquired of management and inspected system descriptions and communications to determine if descriptions of the system and its boundaries were available to external users via ongoing communications, blog posts, and status portals in accordance with company requirements. Inspected documentation for a selection of customer-reported incidents to determine if customer incidents were reported and resolved through one-to-one communication via the customer ticketing system in accordance with company requirements. **No exceptions noted.**
IS-08	A Data Management Policy is in place that defines system and operational requirements for data classification, retention, encryption, storage, and secure disposal. The policy is reviewed and updated accordingly on at least an annual basis.	C1.1 C1.2 CC6.1 CC6.3 PI1.1	Inquired of management and inspected the Data Management Policy to determine if it defined system and operational requirements for data classification, retention, encryption, storage, and secure disposal and that the policy was reviewed and updated accordingly on at least an annual basis in accordance with company requirements. **No exceptions noted.**

No.	Description of Controls	Criteria	Tests of Controls and Test Results
OM-01	Monitoring and alarming are configured to identify and notify management of incidents when thresholds are crossed on key security and operational metrics. Issues are resolved in accordance with incident management processes.	A1.1 CC2.2 CC4.1 CC6.6 CC6.7 CC6.8 CC7.1 CC7.2 CC7.3 CC7.4 CC7.5 CC9.1	Inquired of management and inspected the incident response plan and monitoring and alarming tool configurations to determine if security and operational metrics were monitored with predefined thresholds and if tools were configured to notify management automatically when thresholds were crossed in accordance with company requirements. Inspected documentation for a selection of alerts generated by monitoring and alarming tools to determine if each issue was resolved in accordance with incident management processes and company requirements. **No exceptions noted.**
OM-02	Policy and procedure documentation for incident management, which includes the responsibility and escalation levels for reporting operational failures, security incidents, system problems, user complaints, and the process for doing so, is made available to internal and external users.	CC2.3 CC7.1 CC7.2 CC7.3 CC7.4 CC7.5	Inquired of management and inspected incident response policies and procedures to determine if they included responsibilities and escalation levels for reporting operational failures, security incidents, system problems, and user complaints. Inspected evidence of communication of the incident response policies and procedures to determine if the documents were available to internal and external users in accordance with company requirements. **No exceptions noted.**
OM-03	Standard customer service agreements are executed between the company and each customer that define service levels, processing specifications, rules of use, and additional terms for governing use of the system.	CC2.3 PI1.1 PI1.3	Inquired of management and inspected executed agreements for a selection of customers to determine if standard service agreements were in place with defined service levels, rules of use, and additional terms for governing use of the system in accordance with company requirements. **No exceptions noted.**

No.	Description of Controls	Criteria	Tests of Controls and Test Results
OM-04	Customer data will be deleted in accordance with the Data Management Policy and within 60 days of customer termination and receiving data deletion requests. For disposal requests, a confirmation is sent back to the customer to notify them that the disposal is complete.	C1.1 C1.2	Inquired of management and inspected the Data Management Policy and documentation for a selection of service terminations to determine if customer data was deleted in accordance with the Data Management Policy and within 60 days of service termination in accordance with company requirements. **No exceptions noted.** Inspected results of the customer data deletion requests query and determined there were no ad-hoc customer data deletion requests during the audit period. **Therefore, this control did not operate during the report period and no conclusion was reached regarding its operating effectiveness.**
OM-05	Log file validation (i.e., CloudTrail) is enabled to create a digitally signed digest file containing a hash of each log that writes to file shares.	PI1.1 PI1.2 PI1.4 PI1.5	Inquired of management and inspected the Operations Security Policy and file validation logs to determine if logging was enabled to create a digitally signed digest containing a hash of each log that writes to file shares in accordance with company requirements. **No exceptions noted.**
OM-06	Job schedules and run books are documented and jobs are scheduled to help ensure data is processed for completeness, accuracy, and timeliness.	PI1.3 PI1.4 PI1.5	Inquired of management and inspected documented job schedules, runbooks, and configurations to determine if jobs were scheduled to help ensure data was processed completely, accurately, and in a timely manner in accordance with company requirements. **No exceptions noted.**

No.	Description of Controls	Criteria	Tests of Controls and Test Results
OM-07	Integrity checks are in place at the application level to help ensure data integrity.	PI1.3 PI1.4	Inquired of management and inspected configurations to determine if integrity checks were in place at the application and file system level to help ensure data integrity in accordance with company requirements. **No exceptions noted.**
OM-08	AiDASH validates reliability and accuracy of models to ensure at least 85% precision and accuracy in accordance with internal guides. Issues, if any, are resolved before model delivery.	PI1.2 PI1.4 PI1.5	Inquired of management and inspected model quality testing procedures and test results from a sample of models to determine if AiDASH validated accuracy of models to ensure at least 85% accuracy in accordance with internal guides, and that issues, if any, were resolved before delivery in accordance with company requirements. **No exceptions noted.**
RC-01	AiDASH performs a formal risk assessment annually where relevant risks to the organization, including fraud, are identified and evaluated. Identified risks, risk treatment options, and action items are assigned to risk owners and tracked within a centralized risk register.	A1.2 CC1.2 CC2.1 CC3.1 CC3.2 CC3.3 CC3.4 CC4.1 CC4.2 CC5.1 CC5.2 CC9.1 CC9.2	Inquired of management, inspected the Risk Management Policy and most recent risk assessment to determine if a risk assessment was performed within the last year, relevant risks, including fraud, were identified and evaluated, mitigation strategies were documented, and risk owners were identified within a centralized risk register in accordance with company requirements. **No exceptions noted.**

No.	Description of Controls	Criteria	Tests of Controls and Test Results
RC-02	An annual third-party risk assessment is performed including a review of attestation reports (i.e., SOC 2, ISO) when available. Results and action items are communicated to the respective owners and tracked through internal risk management tools.	CC3.2 CC3.3 CC3.4 CC4.1 CC4.2 CC9.2	Inquired of management and inspected the Third-party Management Policy and results of the most recent third party risk assessment to determine if it was completed within the last year, included all critical third parties and a review of attestation reports (i.e., SOC 2, ISO), and results and action items were communicated to the respective owners and tracked through internal risk management tools in accordance with company requirements. **No exceptions noted.**
RC-03	Information security KPIs are monitored continuously using automated tools that are configured to alert system administrators of activity that falls outside of predefined thresholds.	CC1.5 CC2.1 CC2.2 CC3.1 CC3.2 CC3.4 CC4.1 CC4.2 CC5.1 CC5.3 CC7.2 CC7.3	Inspected monitoring tools, alerting configurations, and an example notification to determine if KPIs were monitored continuously using automated tools that were configured to alert system administrators of activity that fell outside of predefined thresholds in accordance with company requirements. **No exceptions noted.**
RC-04	Confidentiality agreements are in place for vendors with access to customer data.	CC2.3 CC9.2	Inquired of management and inspected the Third-party Management Policy and agreements for a selection of vendors with access to customer data to determine if confidentiality agreements were in place in accordance with company requirements. **No exceptions noted.**
RC-05	AiDASH maintains a Cyber Liability Insurance Policy to provide additional protection in the event of a breach related to cybersecurity.	CC9.1	Inquired of management and inspected AiDASH's Cyber Liability Insurance Policy to determine if insurance protection was in place to provide additional protection in the event of a breach related to cybersecurity in accordance with company requirements. **No exceptions noted.**

No.	Description of Controls	Criteria	Tests of Controls and Test Results
SC-01	Security groups are configured to enforce perimeter security including configurations that deny all traffic by default, restrict ingress traffic from sensitive protocols, and restrict authentication to infrastructure systems to trusted IP addresses.	CC6.1 CC6.6 CC6.7	Inquired of management and inspected the Comprehensive Security Policy and production security group configurations to determine if security groups were configured to enforce perimeter security including configurations that deny all traffic by default, restrict ingress traffic from sensitive protocols, and restrict authentication to infrastructure systems to trusted IP addresses in accordance with company requirements. **No exceptions noted.**
TV-01	Vulnerability scans are performed continuously and issues, if any, are routed through incident and risk management processes for resolution and resolved in accordance with the service-level agreements for high, medium, and low risk rankings.	CC2.1 CC3.2 CC4.1 CC4.2 CC6.6 CC6.8 CC7.1 CC7.2 CC7.3 CC7.4 CC7.5	Inquired of management and inspected the Operations Security Policy, vulnerability scan configurations, and a selection of vulnerabilities to determine if vulnerability scans were performed continuously and the resolution of identified vulnerabilities was monitored against configured service-level agreements for high, medium, and low risk rankings in accordance with company requirements. **No exceptions noted.**
TV-02	External penetration testing is performed at least annually. Issues, if any, are routed through vulnerability and risk management processes for resolution.	CC2.1 CC3.2 CC7.1 CC7.2 CC7.3 CC7.4	Inquired of management and inspected the Operations Security Policy, results of the most recent penetration test, and evidence of management review, including risk and incident tracking, to determine if external penetration testing was performed at least annually and if issues were routed through vulnerability and risk management processes for resolution in accordance with company requirements. **No exceptions noted.**

No.	Description of Controls	Criteria	Tests of Controls and Test Results
TV-03	Encryption and antivirus software is installed on mobile devices (e.g., workstations and laptops).	CC6.5 CC6.6 CC6.7 CC6.8 CC7.2	Inquired of management and inspected the Information Security Policy mobile device management configurations to determine if encryption and antivirus software was installed on mobile devices with access to production systems in accordance with company requirements. **No exceptions noted.**