AiDASH Inc.

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

SOC 3®

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

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

BARR ADVISORY

Independent Service Auditor's Report

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

Scope

We have examined AiDASH's accompanying assertion titled "Assertion of AiDASH Management" (assertion) that the controls within the AiDASH System (the "system") were effective 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).

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 also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, AiDASH is responsible for selecting, and identifying in its assertion, the applicable trust service criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

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

Our examination included:

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

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

Relevant Ethical Requirements

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

Inherent Limitations

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

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

Opinion

In our opinion, management's assertion that the controls within the AiDASH System were effective 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 is fairly stated, in all material respects.

BARR Advisory, P.A.

Fairway, KS

May 15, 2025

Assertion of AiDASH Management

We are responsible for designing, implementing, operating, and maintaining effective controls within the AiDASH System (the ”system”) throughout the period April 1, 2024 to March 31, 2025, to provide reasonable assurance that AiDASH's service commitments and system requirements relevant to security, confidentiality, availability, and processing integrity were achieved. Our attached system description of the AiDASH System identified the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period 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's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in the attached system description.

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

We assert that the controls within the system were effective throughout the period 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.

AiDASH Inc.

May 15, 2025

AiDASH's Description of the Boundaries of Its AiDASH System

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.

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.

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.

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

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 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.

