ISPARTNERS

AlignOps

ToolWatch
BY ALIGNOPS

SafetyReports
BY ALIGNOPS

Report on ToolWatch, LLC's DBA AlignOps Management Assertion For the ToolWatch and SafetyReports System

July 1, 2024 through June 30, 2025

Relevant to Security, Availability, and Confidentiality

SOC 3®

I. INDEPENDENT SERVICE AUDITOR'S REPORT

ISPARTNERS

To the Management of ToolWatch LLC DBA AlignOps:

Scope

We have examined ToolWatch LLC's DBA AlignOps ("AlignOps" or the "Company") accompanying assertion titled "Management Assertion of ToolWatch LLC's DBA AlignOps" ("assertion") that the controls within AlignOps' ToolWatch and SafetyReports System ("system") were effective throughout the period July 1, 2024 through June 30, 2025, to provide reasonable assurance that AlignOps' service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, and Confidentiality ("applicable trust services criteria") set forth in TSP 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (with Revised Points of Focus–2022)* (AICPA, *Trust Services Criteria*).

Service Organization's responsibilities

AlignOps 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 AlignOps' service commitments and system requirements were achieved. AlignOps has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, AlignOps 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 the description is not presented in accordance with the description criteria and that controls were not suitably designed

IS Partners, LLC
1668 Susquehanna Road
Dresher, PA 19025

215.675.1400 main office
215.259.7928 fax
ispartnersllc.com

- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria

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

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the examination 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 AlignOps' ToolWatch & SafetyReports System were effective throughout the period July 1, 2024 through June 30, 2025, to provide reasonable assurance that AlignOps service commitments and system requirements were achieved based on the applicable trust services criteria, is fairly stated, in all material respects.

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

IS Partners, LLC

IS Partners, LLC
Dresher, Pennsylvania
December 8, 2025

II. MANAGEMENT ASSERTION OF TOOLWATCH LLC'S DBA ALIGNOPS

We are responsible for designing, implementing, operating, and maintaining effective controls within ToolWatch LLC's DBA AlignOps ToolWatch & SafetyReports System ("system") throughout the period July 1, 2024 through June 30, 2025, to provide reasonable assurance that AlignOps' service commitments and system requirements relevant to security were achieved. Our description of the boundaries of the system is presented in this report and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period July 1, 2024 through June 30, 2025, to provide reasonable assurance that AlignOps' service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, and Confidentiality ("applicable trust services criteria") set forth in TSP 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (with Revised Points of Focus–2022)* (AICPA, *Trust Services Criteria*). AlignOps' 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 this report.

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

We assert that the controls within the system were effective throughout the period July 1, 2024 through June 30, 2025, to provide reasonable assurance that AlignOps' service commitments and system requirements were achieved based on the applicable trust services criteria.

ToolWatch LLC's DBA AlignOps
December 8, 2025

III. DESCRIPTION OF THE BOUNDARIES OF TOOLWATCH LLC'S DBA ALIGNOPS TOOLWATCH & SAFETYREPORTS SYSTEM

Company Background

ToolWatch LLC DBA AlignOps ("AlignOps" or the "Company", headquartered in Denver, Colorado, provides a comprehensive suite of tools to help contractors, builders, and project managers push projects forward in a more safe, productive, and profitable way. ToolWatch and SafetyReports are two of those tools.

Overview of the Services Provided

Company and Product Lines

AlignOps is a Software as a Service (**"**SaaS**"**) provider, with software in its portfolio that serves construction and construction-adjacent organizations. The portfolio includes the ToolWatch operations product line and the SafetyReports Safety Reporting product line (including AlignOps EHS branding for administrative access). These offerings are designed to streamline field, warehouse, and back-office work and improve job site productivity.

ToolWatch (Operations Product Line)

ToolWatch provides capabilities that help organizations manage assets and operational workflows across the project lifecycle. Core usage scenarios include tracking tools and materials, scheduling equipment maintenance, and reporting on inventory levels. Each scenario aims to unify field, warehouse, and office teams in daily operations.

Customers access the ToolWatch service through:

- A desktop/web experience for office-based asset and operations management, or
- A mobile experience for field users who need quick access to asset and operational tasks on the go.

SafetyReports (Safety Reporting Product Line)

SafetyReports helps customers manage components of an environmental health and safety (EHS) program. Organizations can select from the suite's applications à la carte to support their specific jobsite safety processes.

Customers access the SafetyReports service through:

- A mobile application used by field personnel to execute safety workflows, or
- A browser experience for administrative configuration and review within the SafetyReports products (with AlignOps EHS providing a branded administrative layer for accounts using that option).

Customers deploy one or more of the following applications within SafetyReports, depending on programming needs:

- Inspection – allows the end-user to perform an inspection based on ad-hoc or checklist-based means, including file attachments, and creates a report which is submitted via email. Application has limited 'offline' capabilities, utilizing temporary local storage.
- Training – allows the end user to perform small group training events using pre-loaded material, track attendance and creates a report submitted via email. Application has limited 'offline' capabilities, utilizing temporary local storage.
- Job Safety Analysis ("JSA") – allows the end user to perform task-based job hazard analysis with the industry standard "Task, Hazard, Control" format created as a report submitted via email; this application also has an audience component. Application has limited 'offline' capabilities, utilizing temporary local storage.
- Observation ("Obs") – allows the end user to quickly report negative, positive, or agnostic observations and creates an email, if applicable, based on administrative settings. Application has no 'offline' capabilities.
- Incident – allows the end user to create and send a formalized incident report on one of six incident types via email, including diagrams and file attachments. Application has no 'offline' capabilities.
- Scan – allows the end user to both manage asset attributes through an edit function, and perform an inspection based on 'scanning' of a QR code; this creates an email, if applicable, based on administrative settings. Application has no 'offline' capabilities.
- Forms – allows the end user to fill out a form using content set up by the administrator. Application has no 'offline' capabilities.
- SafetyReports All in One - a single app that brings together all of the SafetyReports products so customers can download one app instead of multiple, separate apps.

Principal Service Commitments and System Requirements

AlignOps designs its processes and procedures related to ToolWatch and SafetyReports to meet its objectives for customer satisfaction with the solution including commercially reasonable security measures for the type of information being stored and processed.

Security measures are standardized and include, but are not limited to, the following:

- Role-based security that includes granularity sufficient to permit users in to access the data that is relevant to their job responsibilities and functions but no more than is required according to the principle of least access.
- The use of industry-accepted and encryption for both data at rest and data in transit.
- IT controls and technologies for the explicit purpose of preventing and minimizing the impact of malicious threats to AlignOps networks, computers, and production environments including but not limited to network

segmentation, endpoint detection and response products, access control lists, and firewalls.
- Management review, assessment, and oversight of the security practices by the personnel and teams responsible for the AlignOps infrastructure.

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

Components of the System

The system is comprised of the following five components:

- Infrastructure
- Software
- People
- Procedures
- Data

The following sections of this description define each of these five components comprising AlignOps' ToolWatch and SafetyReports system and other relevant aspects of AlignOps' control environment, risk assessment process, information and communication systems, and monitoring controls.

Infrastructure

The systems hosting AlignOps' product, ToolWatch and SafetyReports, are located in data centers within the United States. All systems operate on industry-standard server platforms managed within the hosting environment. All network infrastructure is provided by the data centers and managed by AlignOps personnel to the extent allowed within the data center's management portal.

Primary Infrastructure	
Hardware	**Purpose**
Load Balancers	Load balancer internal and external traffic

Primary Infrastructure	
Hardware	**Purpose**
Network Segmentation Framework	Protects the network perimeter and restricts inbound and outbound access
Object Storage Service	Storage, upload and download
Relational Database Service	Fully scalable relational database
Compute Hosting Environment	Hosts virtual servers that operate the business logic and web services for ToolWatch and SafetyReports
Application Server Platform	Primary OS used by application virtual machines

Software

AlignOps makes use of third-party software platforms delivered as a service to perform on-going application development for its ToolWatch and SafetyReports platforms:

- Project management and internal ticketing system
- Source control

AlignOps' software developers make use of a wide variety of coding tools which change depending on customer requirements. These tools can be installed on developer workstations or on virtual servers. Typical tools include:

- IDEs
- Database systems
- Database development tools
- Mobile application development environments
- Containerization platform

AlignOps' delivery team makes use of a wide variety of tools which change depending on technical requirements. These tools can be installed on developer workstations or on virtual servers. Tooling that AlignOps uses is provided by the customer by virtue of their third-party license entitlements.

People

The Company has a staff of approximately 240 employees organized in the following functional areas:

- Corporate and corporate-operations – Executives, senior operations staff, and Company administrative support staff, such as legal, compliance, training, contracting, accounting, finance, and human resources.

- Customer Success and Product Operations – Customer facing representatives interact directly with the Company's customers, typically on conference calls, phone calls and emails,
- Field Ops/Logistics – Team responsible for preparing telematics hardware for shipment to customers for installation and for handling returns and warranty issues on that hardware. They also assist customers' technicians with the installation and troubleshooting of the telematics devices.
- Sales – Customer/prospect facing representatives interacting directly with the Company's prospects and customers, typically on conference calls, phone calls and emails.
- Marketing – Supports the sales team, coordinates trade shows and publications, and generates inbound leads.
- Development – Software development, escalated application support, and software quality assurance.
- DevOps - IT infrastructure, IT networking, IT system administration, IT Support, Public Cloud Operations of AlignOps products, and technology support for staff.

Processes and Procedures

Management has developed and communicated to employees and contractors a set of policies, processes, and procedures in several operational areas which support the security and confidentiality objectives of the ToolWatch and SafetyReports system. As part of the wider Information Security Management Program, AlignOps has developed and organized the following policies and procedure documents that are used to support the ToolWatch and SafetyReports system.

The following policies and procedures are available to employees and contractors:

- Acceptable Use
- Access Control
- Business Continuity and Disaster Recovery
- Change Management
- Corporate Ethics
- Customer Support and SLA
- Data Retention and Disposal
- Incident Management
- Information Security
- IT Asset Management
- Key Management and Cryptography
- Network Security
- Personnel Security
- Risk Assessment
- Server Security
- Software Development

- Vendor Management
- Vulnerability Management
- Workstation Security

Control activities have been placed into operation to help ensure that actions are carried out properly and efficiently to achieve policies and procedures compliance. AlignOps has applied a risk management approach to the organization in order to select and develop control activities. After relevant risks have been identified and evaluated, controls are established, implemented, monitored, reviewed, and improved when necessary to meet the applicable trust services criteria and the overall objective of the organization.

Data

Data managed in the AlignOps products is mostly entered by either AlignOps staff or the end-user as part of client onboarding, with assets provided with attributes that allow different parts of their management within the system. Data can be edited by the end-users depending on the role they operate out of. Some data in the system comes from third-party integration with outside systems, if so set up by the client account.

Data managed in the SafetyReports product allows data entry through either a mobile or browser-based application. The system has two user roles, application, and administrative user. Data is either entered through use of template uploads by staff, or by the end-user role through use of any of the applications. Data management within the system is managed by the administrator user role. As of the time of this report's writing, no external system data is imported through integration into the back end managing the SafetyReports products.