# System and Organization Controls (SOC) 3 Report

## Management's Report of Its Assertions on Indio Technologies, Inc. & Tarmika's Indio & Tarmika Systems Based on the Trust Services Criteria for security, availability, and confidentiality

**For the Period April 1, 2024 to September 30, 2024**

# TABLE OF CONTENTS

## SECTION ONE: REPORT OF INDEPENDENT ACCOUNTANTS

To: Management of Indio Technologies, Inc. & Tarmika

**Scope**

We have examined Indio Technologies, Inc. & Tarmika (“Indio & Tarmika”) accompanying assertion titled "Assertion of Indio Technologies, Inc. & Tarmika Management" (assertion) that the controls within Indio & Tarmika's Indio & Tarmika Systems (system) were effective throughout the period April 1, 2024 to September 30, 2024, to provide reasonable assurance that Indio & Tarmika's 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 section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, *(With Revised Points of Focus—2022)* in AICPA *Trust Services Criteria.*

Indio & Tarmika uses a subservice organization for could hosting services. The description of the boundaries of the system presented in Attachment A indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Indio & Tarmika, to achieve Indio & Tarmika’s service commitments and system requirements based on the applicable trust services criteria. The description presents the types of complementary subservice organization controls assumed in the design of Indio & Tarmika’s controls. The description of the boundaries of the system does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description of the boundaries of the system presented in Attachment A indicates that certain complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Indio & Tarmika, to achieve Indio & Tarmika’s service commitments and system requirements based on the applicable trust services criteria. The description presents the complementary user entity controls assumed in the design of Indio & Tarmika’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*

Indio & Tarmika 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 Indio & Tarmika's service commitments and system requirements were achieved. Indio & Tarmika has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Indio & Tarmika is responsible for selecting, and identifying in its assertion, the applicable trust services 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 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 AICPA. 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.

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

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 Indio & Tarmika's service commitments and system requirements based on the applicable trust services criteria
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Indio & Tarmika'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.

*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 Indio & Tarmika's Indio & Tarmika Systems were effective throughout the period April 1, 2024 to September 30, 2024, to provide reasonable assurance that Indio & Tarmika's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

CyberGuard Compliance, LLP
October 29, 2024
Las Vegas, Nevada

## SECTION TWO: MANAGEMENT’S REPORT OF ITS ASSERTIONS ON THE EFFECTIVENESS OF ITS CONTROLS OVER INDIO TECHNOLOGIES, INC. & TARMIKA’S INDIO & TARMIKA SYSTEMS BASED ON THE TRUST SERVICES CRITERIA FOR SECURITY, AVAILABILITY, AND CONFIDENTIALITY

October 29, 2024

### Scope

We are responsible for designing, implementing, operating, and maintaining effective controls within “Indio Technologies, Inc. & Tarmika’s” (Indio & Tarmika's) Indio & Tarmika Systems (system)” throughout the period April 1, 2024 to September 30, 2024, to provide reasonable assurance that Indio & Tarmika's 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 section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, *(With Revised Points of Focus—2022)* in AICPA *Trust Services Criteria.* Our description of the boundaries of the system is presented in Attachment A (description) 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 April 1, 2024 to September 30, 2024, to provide reasonable assurance that Indio & Tarmika's service commitments and system requirements were achieved based on the applicable trust services criteria. Indio & Tarmika'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 Attachment B.

Indio & Tarmika uses a subservice organization for cloud hosting services. The description of the boundaries of the system indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Indio & Tarmika, to achieve Indio & Tarmika‘s service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system does not disclose the actual controls at the subservice organization.

The description of the boundaries of the system also indicates complementary user entity controls that are suitably designed and operating effectively are necessary along with Indio & Tarmika’s controls to achieve the service commitments and system requirements. The description presents the complementary user entity controls assumed in the design of Indio & Tarmika's controls.

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 September 30, 2024, to provide reasonable assurance that Indio & Tarmika's service commitments and system requirements were achieved based on the applicable trust services criteria.

*Indio Technologies, Inc. & Tarmika*

## ATTACHMENT A: INDIO TECHNOLOGIES, INC. & TARMIKA'S DESCRIPTION OF THE BOUNDARIES OF ITS INDIO & TARMIKA SYSTEMS

### *Company Background*

Indio Technologies, Inc. ("Indio") was founded in 2016 with the objective of providing a simplified application process for Insurance Brokers and their clients, as a need in the brokerage space for modernized technology was identified. Indio is a modern solution that enables agencies to automate internal application and renewal processes, eliminating redundancies in data gathering to minimize E&O and provide insureds a simpler, more collaborative customer experience. The organization is based in Austin, TX. Indio Technologies, Inc.'s web-based services and their related controls, including system redundancy, are key differentiators in providing and maintaining high availability, 24/7 access for customers.

Tarmika is a single-entry, multi-carrier platform designed to streamline the insurance quoting process. The Company was founded in 2019 and is designed to help independent insurance agencies by providing a more efficient way to quote with multiple carriers. The Company's mission is to empower independent insurance agents through technology. It is this technology that enables insurers and agents to expand distribution channels, gain new business and provide enhanced customer experience.

Both companies are owned by Applied Systems, Inc. ("Applied").

### *System Overview*

The System is comprised of the following components:

- ***Infrastructure -*** The physical and hardware components of a system (facilities, equipment, and networks)
- ***Software -*** The programs and operating software of a system (systems, applications, and utilities)
- ***Data -*** The information used and supported by a system (transaction streams, files, databases, and tables)
- ***People -*** The personnel involved in the operation and use of a system (developers, operators, users, and managers)
- ***Procedures -*** The automated and manual procedures involved in the operation of a system

**Infrastructure**

Indio & Tarmika use the parent company, Applied Systems, Inc.'s, internal IT expertise, internal business and policies and procedures to support its daily administration and service operation.

The Indio & Tarmika System is hosted in Amazon Web Services (AWS) across multiple Availability Zones for redundancy and disaster recovery purposes. Indio & Tarmika do not own or maintain any hardware in the AWS data centers. Services operate within a shared security responsibility model, where AWS is responsible for the security of the underlying cloud infrastructure, and each company is responsible for securing the System deployed in AWS (e.g., S3 bucket policies, Operating System and application security, Active Directory configuration, network traffic monitoring).

Three Virtual Private Clouds (VPC) separate the containerized production, staging, and development environments. Access to AWS production instances is allowed only through an encrypted VPN from Applied's corporate network to ensure the privacy and integrity of data transmitted over the public network. VPN connections are secured using AES-128 bit or greater encryption. Access is restricted to authorized administrators.

Production instances at AWS are logically and physically separate from the internal corporate network. All container hosts and database servers run on EC2 instances within Auto Scaling groups. AWS CloudFormation provides auto-scaling management of the production systems based on a defined template, which allows Integrate to deploy and configure consistently hardened instances.

All container hosts and database servers run on EC2 instances that are secured via Security Groups. Security Groups monitor incoming network traffic by analyzing data packets and filtering traffic based on an Integrate-defined ruleset. Access to manage the Security Groups is restricted to authorized DevOps personnel, and changes to these rulesets are governed by a Change Management Policy, which includes documenting, testing, and approving the change.

*Indio Technologies, Inc.'s Indio System Portal*

The user-facing Indio System portal is a front-end application for customers to access their services.

**Software**

The Systems run in a containerized environment with Amazon Linux 2 as the base image based on a generic Amazon Machine Images (AMI). Periodically, the continuous integration platform runs an automated process to update the image. A configuration management tool is used to configure software applications on individual instances using approved scripts.

Each System uses multiple software and utilities to configure, develop, and support the in-scope infrastructure and applications, including:

- *AWS* – Cloud Computing Platform
- *CrowdStrike* - platform purpose-built to stop breaches via a unified set of cloud-delivered technologies that prevent all types of attacks — including malware and much more
- *Snyk* – Industry leading security intelligence and DeepCode AI to find and automatically fix vulnerabilities in code, containers, and IaC
- *Orca* – Delivers industry-leading Cloud Security that identifies, prioritizes, and remediates security risks and compliance issues across Indio's & Tarmika's AWS infrastructure
- *Jira* – Issue collection and Agile Project Management
- *FullStory* – Digital Experience Intelligence Platform
- *Docker* – Container Engine
- *GitLab* – Online source code control repository and continuous integration platform
- *Keycloak Active Directory* – Identity and access management for VPN
- *Sentry* – Error reporting
- *Data Dog* – Monitoring and alerting
- *Figma* – Vector graphics editor and prototyping tool

**Data**

Inbound integrations to the Indio System are configured with third parties via Indio Technologies, Inc. & Tarmika's developed APIs.

Indio stores and processes contact data within the Indio System. All data is encrypted at rest and encrypts data in transit. Processed contact data is provided to customers in various ways:

- Customers can access the processed contact data via the Indio Technologies, Inc. Indio System portal.
- Reports of processed contact data can be configured to send to customers upon request.

Tarmika is a single-entry commercial lines comparative rating platform designed to help independent insurance agencies. The data it manages primarily revolves around insurance-related information. This includes data related to:

- Insurance Policies: Information about various insurance policies offered by different insurance providers. This includes details about policy terms, coverage, premiums, and more.
- Client Information: Personal and business information about clients seeking insurance. This can include names, contact information, business details, risk profiles, and more.
- Quotes: Information about insurance quotes provided to clients. This includes details about the insurance provider, policy, premium, coverage, and more.

- Insurance Providers:  Information about various insurance providers that the platform connects with. This includes details about their policies, terms, rates, and more.
- Transactions:  Information about transactions made through the platform. This includes details about policy purchases, renewals, cancellations, and more.

Under a managed services agreement, Indio & Tarmika manages the product on behalf of the customer.

**People**

The following functional roles/teams comprise the framework to support effective controls over governance, management, security, and operation:

- ***Executive Management*** establishes business and strategic objectives and provides oversight of financial and operational performance. Executive Management meets with the Leadership Team on a recurring basis. Executive Management oversees the Leadership team's system of internal control and is ultimately responsible for all aspects of service delivery and security commitments.
- ***Leadership Team*** oversees all aspects of service delivery and security commitments. Among other responsibilities, the Leadership Team ensures that controls are enforced, risk assessment/management activities are approved and prioritized, people are appropriately trained, and systems and processes are in place to meet security and service requirements.
- ***Human Resources*** is responsible for managing functions related to recruiting and hiring, employee relations, performance management, training, and resource management. Human Resources partners proactively with the Leadership Team and business units to ensure that all initiatives are appropriately aligned with Indio Technologies, Inc. & Tarmika's mission, vision, and values.
- ***Information Technology (IT)*** management has overall responsibility and accountability for the enterprise computing environment. Infrastructure Engineers administer systems and perform services supporting key business processes, including architecting, and maintaining secure and adequate infrastructure, monitoring network traffic, and deploying approved changes to production. The Engineering team is responsible for application development, initial testing of changes, and troubleshooting/resolving application issues.
- **Information Security** is responsible for performing assessing and managing risk, defining control objectives, monitoring performance of security controls, addressing and responding to security incidents, maintaining, and communicating updates to security policies, and conducting security awareness training of all users.
- **Implementation Managers (IM)** are responsible for initiating the creation of new customer instances on the Indio Technologies, Inc. Indio System & Tarmika platform, adding administrative users to new customer instances, providing user documentation to, and coordinating training for new customers,

- **Customer Support**, including Support Specialists, and Customer Success Managers (CSM) are responsible for fielding customer calls regarding the Indio Technologies, Inc. Indio System & Tarmika services, initiating and responding to help desk tickets based on customer requests, communicating with customers regarding any issues or outages, and overall management of the account to ensure continued customer satisfaction.

Indio & Tarmika, in alignment with Applied policy, are committed to equal opportunity of employment, and all employment decisions are based on merit, qualifications, and abilities. Employment-related decisions are not influenced or affected by an employee's race, color, nationality, religion, sex, marital status, family status, sexual orientation, disability, or age. All companies endorses a work environment free from discrimination, harassment, and sexual harassment.

**Procedures**

Indio & Tarmika leverage the parent company - Applied Systems, Inc.'s expertise and personnel. This includes a Chief Information Security Officer (CISO) who is responsible for the design and oversight of security initiatives. The CISO reports directly to the CTO (Chief Technology Officer) and indirectly to the Chief Executive Officer (CEO). The Information Security Policy framework describes the procedures followed to ensure the performance of consistent processes over the security, availability, confidentiality, and operation of each company's System. All Information Security policies are reviewed on an annual basis, or more frequently as needed, by the CISO.

All employees are expected to adhere to the parent company - Applied Systems, Inc.'s Information Security Policy framework as outlined during new hire onboarding and during annual security awareness training. The Information Security Policy framework includes procedures that provide guidance on the consistent performance of controls and processes necessary to meet service commitments and system requirements.

## Complementary Subservice Organization Controls

Certain principal service commitments and system requirements can be met only if complementary subservice organization controls (CSOC) assumed in the design of Indio & Tarmika's controls are suitably designed and operating effectively at the subservice organizations, along with related controls at Indio & Tarmika.

### Amazon Web Services (AWS)

Indio & Tarmika use Amazon Web Services (AWS) as the cloud hosting provider for the Indio & Tarmika Systems. The following Complementary Subservice Organization Controls (CSOCs) are expected to be operating effectively at AWS, alone or in combination with controls at Indio Technologies, Inc., to provide assurance that the required trust services criteria in this report are met.

| Applicable Trust Services Criteria | Complementary Subservice Organization Control |
|---|---|
| 5.2 | AWS is responsible for documenting and maintaining configuration standards. |
| 6.4 | AWS is responsible for restricting physical access to facilities and protected information assets to authorized personnel. |
| 6.7 | AWS is responsible for implementing security measures to protect information against threats during transmission, movement, or removal. |
| 8.1 | AWS is responsible for implementing procedures to address changes to infrastructure, data, and software. |
| A 1.2 | AWS is responsible for maintaining and monitoring environmental protections and recovery infrastructure. |

## Complementary User Entity Controls and Responsibilities

### *Complementary User Entity Controls* and Responsibilities

The control activities performed were designed with the understanding that certain user organization controls would be implemented by each customer. Each customer's internal control structure must be evaluated in conjunction with Indio Technologies, Inc. & Tarmika's controls, policies and procedures described in this report. The Complementary User Entity Controls (CUECs) below are the minimum controls that customers must have in operation to complement the controls of the Indio & Tarmika system and should not be regarded as a comprehensive list of all controls that should be employed by customers.

| Complementary User Entity Controls | Related Applicable Criteria |
|---|---|
| Users are responsible for adhering to all regulatory compliance issues when they are associated with Indio Technologies, Inc. & Tarmika in a service agreement. | 2.3, C 1.1 |
| Users are responsible for reviewing and approving the terms and conditions stated in service agreements with Indio Technologies, Inc. & Tarmika. | 2.3 |
| External users are responsible for creating the initial password to access the Indio System & Tarmika. | 6.1 |

| Complementary User Entity Controls | Related Applicable Criteria |
|---|---|
| Users are responsible for selecting and using strong passwords in accordance with Indio & Tarmika’s password requirements enforced on the application. | 6.1, 6.2 |
| Users are responsible for ensuring user access to reports and other information generated from Indio Technologies, Inc. & Tarmika is restricted based on business need. | 6.1, 6.3, C 1.2 |
| Users are responsible for ensuring user-owned or managed applications, platforms, databases, and network devices that may process or store data derived from Indio Technologies, Inc. & Tarmika are logically and physically secured. | 6.1, 6.3 |
| Users of Indio Technologies, Inc. & Tarmika hosted applications are responsible for maintaining appropriate IT General Computer Controls and Application Controls. | 6.1, 6.3 |

**ATTACHMENT B: PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS**

## *Description of Services Provided*

Indio & Tarmika provides a fully digital client risk capture and application experience by automating the data population across individual, unique insurer applications.

The Indio System consists of the following components:

- *Application Library* – Provides access to digitized insurance applications, to create a single data capture process and data mapping to automate application completion
- *Smart Forms* – Automaps data across multiple applications, increasing efficiency. Includes smart change tracking, and renewal automation
- *Intelligent Activity Tracking* – Alerts users when clients fill out information, sign forms, and submit data
- *E-Signature* – Indio's e-signature capabilities are built within smart forms

Tarmika provides a comparative rating solution built for the independent agent.

It consists of the following features:

- *Single entry quoting* - designed to help expand distribution channels, gain new business and provide enhanced customer experience
- *Tarmika Insured* - Embedded insurance solutions with a fully customizable interface
  - Embedded in Partner Platform
  - Data Prefill/No Duplicate Entry
  - 12 or Less Underwriting Questions
  - Multiple Real Time Options

## *Principal Service Commitments and System Requirements*

Indio & Tarmika's security, availability, and confidentiality commitments to customers are documented and communicated to customers in the Master Services Agreement and the Terms of Service, Privacy Policy, and Security Overview published on customer-facing websites.

The principal security, availability, and confidentiality commitments include, but are not limited to:

- Periodically test its infrastructure and applications for vulnerabilities and take remedial action on those that could potentially impact the security, availability, and confidentiality of customer data. Each team engages in penetration testing and continually seeks to evaluate new tools in order to increase the coverage and depth of its assessments.

- Maintain appropriate administrative, physical, and technical safeguards to protect the security and integrity of the Systems and the customer data in accordance with Applied's security, availability, and confidentiality requirements.
- Perform annual third-party security, availability, confidentiality and compliance audits of the environment, including, but not limited to:
  - Reporting on Controls at a Service Organization Relevant to Security, availability, and confidentiality (SOC 2) examinations
- Reoccurring application penetration testing on an annual basis
- Utilize Applied's formal HR processes, including background checks, code of conduct and company policy acknowledgements, security awareness training, disciplinary processes, and annual performance reviews
- Follow Applied's formal access management procedures for the request, approval, provisioning, review, and revocation of personnel with access to any production systems
- Prevent malware from being introduced to production systems
- Continuously monitor the production environment for vulnerabilities and malicious traffic
- Use industry-standard secure encryption methods to protect customer data at rest and in transit
- Transmit customer data via encrypted connections
- Maintain an availability SLA for customers of 99.9% uptime for each calendar quarter
- Maintain a disaster recovery and business continuity plan to ensure availability of information following an interruption or failure of critical business processes
- Maintain and adhere to a formal incident management process, including security incident escalation procedures
- Maintain confidentiality of customer data and notify customers in the event of a data breach
- Identify, classify, and properly dispose of confidential data when retention period is reached and/or upon notification of customer account cancellation

Indio & Tarmika, in support of Applied, establish system and operational requirements that support the achievement of the principal service commitments, applicable laws and regulations, and other system requirements. These requirements are communicated in policies and procedures, system design documentation, Terms of Service, Privacy Policy, Security Overview, and/or in customer contracts. Information Security policies define how systems and data are protected. These policies are updated as appropriate based on evolving technologies, changes to the security threat landscape, and changes to industry standards, provided any updates do not materially reduce the service commitments or overall service provided to customers as described in the customer contracts.

Indio & Tarmika regularly reviews the security, availability, and confidentiality commitments and performance metrics to ensure these commitments are met.